Atlas of Information Risk Maps

-

A Practical Guide to Navigating
400+ Categories of
Networked Information System Risks
and
Cybersecurity/Privacy Threat Vectors and Vulnerabilities
at and beyond
Perimeter(s) 2.0

A Multi-Stakeholder Project
Hosted by
University of Washington – Applied Physics Laboratory
Information Risk Research Initiative (IRRI)

Version 2020 –6/26
Compiled by Scott L. David – IRRI Executive Director

ATLAS OVERVIEW

• Slide 1	Title
• Slide 2	Atlas Overview
• Slide 3 to 10	Introduction To Perimeter 2.0 Risks
• Slides 11 to 44	Table of Contents
• Slides 45 to 1047	Atlas of Risk Maps
• Slides 1048 to 1072	Theory of Change for Networked Information Risk In Distributed Systems

The Unintended Consequences of the Internet – Failed and Weaponized Institutions

- **The Internet was NOT designed for its current use as a general-purpose information network for the globe**
  - The Internet was first developed as an open information network among research institutions

- **The Internet was characterized by Paul Baran (1966 RAND paper) as a defensive weapons system**
  - Distributed information network architecture could absorb and recover from nuclear attack on one of its nodes

- **The Internet grew organically as different groups experimented with the unique capabilities of its distributed architecture**
  - Experiments by individuals, companies, governments, universities
  - Internet's open architecture and lack of "identity" layer was mismatch with existing institutional power and control relationships for economic, political and social interactions, but benefits of scale, interconnection, scope and cost savings nonetheless fueled Internet adoption

- **ALL human institutions apply hierarchical decision-making that depends on centralized information flows and controls**
  - Human institutions create, operate and enforce interaction rules of various sorts

- **All institutions discovered that the same distributed Internet architecture that could resist attack also resisted ANY centralized controls**
  - Loss of institutional "rules-based" control was first described as the intra-organizational BYOD (bring your own device) problem (e.g., employee use of "apps" and hardware beyond employer control, etc.).
  - Loss of rulemaking/agenda setting/meaning-making control is detrimental to power and relevance of ALL existing human institutions

- **By the time this was discovered, most humans and human institutions had developed irreversible dependency on the Internet**
  - The dramatically enhanced de-risking and leverage ("negentropy") of Internet architecture cannot be resisted or replaced
  - Compare it to the irresistible energy-density of fossil fuels. Compare also to sym-bio-genesis (perhaps "Sym-info-genesis?")

- **At present, ALL hierarchical/centralized institutions (business, governments, agencies, co-ops, etc.) are entirely BLINDED on the Internet**
  - Traditional institutional (and market) metrics for performance aren't "tuned" to measure new risks

- **At present, the functional interaction surface of institutions is equivalent to the attack/accident surface**
  - Institutional "business as usual" is perpetuating and aggravating new harms at old metrics Perimeter 1.0

Urgent Need For Situational Awareness in Socio-Technical Systems That Host Exponentially Expanding *Interaction* Landscape

- **We need to enhance reliability/integrity of human/institutional *interaction* environment to account for the Internet**
  - **All institutions are clusters of behavior and performance norms to de-risk and leverage a given set of *interactions* among 3 types of "entity"**
    - People (humans)
    - Organizations (companies, governments, agencies, NGOs, religions, etc.)
    - Things (Tools, vehicles, computers, IoT devices, mobile devices, non-human animals, intangible rights, real estate etc.)
  - **4th order effect of "Moore's Law" is exponential increase in *interaction* volumes**
    - 1st order - Exponential increase in transistor density on chip
    - 2nd order - Exponential decrease in hardware size and cost of collecting, processing and communicating data
    - 3rd order - Exponential increase in application and ubiquity of digital ICT capability to collect, process and transfer data
    - 4th order - Exponential increase in ability to engage in and digitally record data from *interactions* among entities
  - ***Interactions* breed risks**
    - Risk arises when *interaction* behavior/performance of an "entity" does not conform to expectations/specifications, etc. of another entity
    - **5th order effect of Moore's Law is an exponential increase in risk**
  - **Internet has become a general *interaction* infrastructure for humans and other entities**
    - Organizations (governments, businesses, universities, informal groups, markets, supply chains, etc.)
    - People (friends, hackers, stalkers, neighbors, strangers, work colleagues, etc.)
    - Things (IoT, thermostats, cars, doorbells, computers, houses, mobiles, etc.)
  - **Hybrid groups of entities (humans, entities and things) that are coupled together by information networks are appropriately labelled and analyzed comprehensively as "socio-technical systems"**
  - **We need new metrics for system organization and operation that is not just "technical" (i.e. data-focused), but is also "socio-technical" (i.e., information focused) to address the exponentially increasing threats and vulnerabilities taking place on the Internet's *interaction* landscapes**

An Atlas to Measure and Map Information Risk
Beyond Network Perimeter 1.0

- **Information network "*Perimeter 1.0*" was at the measurable edge of our systems of technology and institutions**
  - Risk increases as perception dims at the edge of our tech and institutional-enhanced sensory/measurement capabilities
    - In this Atlas of Risk Maps, that older data-focused, measurement-of-performance edge is called "Perimeter 1.0"
  - Now new threats and risks are presenting themselves from beyond that old Perimeter 1.0
    - Traditional cybersecurity, privacy, IM, defense, and legal-compliance-based efforts are blind to the new risk vectors
  - We are experiencing new dimensions of *information* risk of which we were unaware, and for which we are unprepared

- **If we cannot measure a phenomenon: then we cannot see it, anticipate it, or deal with it**
  - Effective "Situational Awareness" is grounded in observation/metrics from multiple perspectives
  - The many threats and vulnerabilities from beyond Perimeter 1.0 are perceived as risky because we cannot yet measure them

- **What gets measured gets done. . . and the opposite is also true**
  - Unknown risks from beyond Perimeter 1.0 are constraining what we can get done in distributed information networks
    - Risk restrains resource deployment and investment

- **For the next wave of innovation in society, culture, governance, security, and economics, and our own growth, we need to break through the "risk boundary" at the edge of Perimeter 1.0 and explore, measure and map the risk borderlands of Perimeter 2.0**

- **The "fuel" to power (and pay for) this innovation/exploration & mapping is "high octane" individual & institutional "self-interest"**
    - Deliver levels of risk reduction and leverage that cannot be achieved unilaterally by any stakeholder
    - Build risk mitigation structures to create new value at the edge of disorder (historical e.g., rule of law, insurance,. etc.)
    - Cultivate "non-zero sum" risk-co-management structures (e.g., rules, norms, markets, etc.)

- **Information network *Perimeter 2.0* is in the "narrative" in the hearts and minds of people, and in the programmed responses of technology (derived from specifications) and institutions (derived from laws, foundational documents and contracts)**
  - How can we measure threat correlations, vulnerabilities and causative factors of risks from these "softer" non-technical sources?
  - How can a broad "systems engineering" approach that embraces "applied social science" and a new enthusiasm for measurement in new domains inform our next-gen risk mitigation architectures, trust frameworks and markets?

Proposal to Map Threats, Vulnerabilities and Risks at Network Perimeter 2.0

- **Problem: Information Network Perimeter 2.0 is:**
  - **Unmeasured**
  - **Unmapped, and**
  - **Presents unknown risks**

- **ALL of our systems are vulnerable to threats at "Perimeter 2.0"**
  - Vulnerable to "AAAA Threats" –
    - Attacks, Accidents, Acts of Nature and AI/Autonomous Systems
  - We *cannot* measure/detect AAAA threats *beyond* security Perimeter 1.0
  - We are all blind to AAAA threats and failures at system Perimeter(s) 2.0
  - We cannot yet achieve "distributed security" (or even AAAA threat measurement) at Perimeter(s) 2.0
  - Perimeter(s) 2.0 threats are currently undermining political/social and economic institutions at global scales

AAAA Threats

- ALL known human and institutional harms can be assigned to a "AAAA Threat" category
- Atlas is tool for analyzing and mitigating "AAAA Threats" of all types to information systems
  - Attack
    - Definition: *Intentional acts* of individuals and institutions
    - Many of the Atlas risks are currently being weaponized
      - In commerce "weaponization" is information arbitrage, competitive advantage, surveillance capitalism
      - In government "weaponization" is attack on populations, institutions, critical infrastructure
      - In civil society "weaponization" is fraud, undue advantage, extortion, mis-information
  - Accident (and unintended consequences)
    - Definition: *Unintentional acts (and unintended consequences)* of individuals and institutions
    - Many Atlas risks are due to ignorance of the effect of a given Atlas risk factor on actor or others
    - Law calls unreasonable ignorance "negligence"
  - Act of Nature
    - Definition: Harms NOT included in other categories (i.e., Attack or Act of Nature or AI/Autonomous Systems)
    - Many Atlas risks do not result from human or institutional action or inaction
      - Disease, weather, solar activity, tectonic activity, floods, etc.
  - AI/Autonomous systems (AI/As)
    - Definition: Harms caused by AI/Autonomous systems
    - AI/As is currently an "in-between" threat category that is emerging as "inert" machines evolve into independent systems that will enjoy "narrative discretion" (developed from what is now the AI "black box")
    - AI is not yet capable of (or legally culpable for) intentional acts or negligence that cause harm.
    - Currently the responsibility/causation/liability is with owner or operator of AI/Autonomous system

Socio-Technical Solutions for Socio-Technical Problems

- **Proposed Solution: Measure and Map AAAA Threats, Vulnerabilities and Risks at Perimeter(s) 2.0**

  - **Recognize multiple new vectors for "AAAA Threats" in hybrid *socio*-technical information network systems**
    - System integrity and performance depends on reliability of BOTH technology AND people/institutions
    - Perimeter 1.0 was the "technical" perimeter at the edge of performance measurement of technology
    - Perimeter(s) 2.0 is the measurement edge of multiple "socio" elements in "Socio-Technical" systems

  - **Atlas program will Identify, collect and make available *non-technical* (aka "policy") threat, vulnerability and risk metrics from Perimeter(s) 2.0 to be part of systems-engineering "requirements" for design, development, deployment, operation, testing/auditing, improving network-vulnerable systems**

  - **Current draft "Atlas" includes hundreds of new information system threat/vulnerability/risk dimensions that are currently inadequately measured to be able to fully contribute to systemic risk mitigation**
    - To enable "Distributed Security for Distributed Systems," this crowd-sourced program creates an open "Risk Atlas" wiki structure for cyber-insecure stakeholder groups to help inform both their joint AND individual R&D and Operations

IRRI Perimeter(s) 2.0 Mapping Tool

- **400+ Map Portfolios in the Atlas group metrics based on types or qualities of network nodes or edges**
  - Metrics in each map portfolio will be derived from multiple disciplines
    - Atlas helps to bring together interdisciplinary research and development work
  - Map making/metrics visualization will commence as candidate measurements/metrics are derived for given portfolio

- **400+ Map Portfolios are presented in this draft Atlas in random order**
  - Later online wiki format versions of Atlas of Risk Maps will be sortable to match stakeholder relevance
  - Will enable custom presentation of map portfolios in stakeholder-responsive order

- **Entries are color coded in Atlas Table of Contents to indicate relative degree of current metrics development**
  - Blue are "Known Known" Risks
    - Known risks/Known metrics
      - Blue Risks are Known AND some Risk Metrics are available
    - Blue questions: What other and/or improved metrics are needed by stakeholders to navigate interactions at their relevant Perimeters(s) 2.0? How can existing metrics be re-deployed to mitigate new risks?
  - Green are "Known Unknown" Risks
    - Known risks/Unknown metrics
      - Green Risks are known, but currently available Metrics are indirect, insufficient or not relevant
    - Green question: What new metrics are needed to help inform risk-exposed stakeholders?
  - Red are "Unknown Unknown" Risks
    - Unknown risks/Unknown metrics
      - Red Risks are speculative AND no current relevant operating Metrics are available
    - Red question: What is the nature of the risk AND what are relevant metrics?

Notes for Atlas Users and "Risk Cartographers"

- **Atlas Focus:** Content of Atlas is currently directed at next-generation "cyber" security AND information network-related threats, vulnerabilities and risks
  - Particular attention to risks associated with information network integrity, identity management (IM), security and privacy technologies and policies
  - Challenges raised and strategies suggested in the Atlas can also help reduce risk associated with other information technologies, technology systems that have an information component, insight and knowledge systems (e.g., markets, supply chains and other information systems with feedback), and various socio-technical systems.

- **Map Portfolios:** Each numbered "risk map" is really an invitation to create workstreams for portfolios of maps/metrics.
  - Maps are currently in form of descriptions of challenges and potential solution/suggested action structures
  - Example: "Risk map 6 – Individual Bias" anticipates dozens of separate measurements and potential mappings of individual bias-based risks that can affect reliability and predictability of networked information systems
    - See https://en.wikipedia.org/wiki/Bias
  - So, these hundreds of "map portfolios" in reality reflect *thousands* of possible measurements of threat, vulnerability and risk that are of potential value to information network stakeholders.

- **Map Portfolio Types:** The initial several hundred map portfolios are grouped by wildly-varying conceptual categories
  - The initial groupings of metrics/maps within each of the map portfolios is intended to invite the consideration of commonalities of measurable qualities among these many different concepts, categories, and abstractions
    - Ontologies and framing tools are in the process of being developed at multiple scales and across multiple sectors

- **Format:** Each of the hundreds of numbered Map Portfolios is presented on just two slides
  - Slide 1 – "Challenges" initial sketch of the types of risks and concerns that are included in that particular map portfolio
  - Slide 2 – "Candidate Analytical Frameworks/Metrics/Actions" suggests some "trial balloons" of possible approaches to identifying and applying measurements that can help to inform the organization and operation of networked information systems.

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

Atlas of Risk Maps

(table of contents)

- Normative cross reference to Ruth Atherton's research checklist (Gates Foundation).

1. Time

- Challenges
  - Innovation: Dynamic change in interaction networks compresses obsolescence of security, IM and privacy-related data collection, processing, and transfer technologies and architectures.
  - Adoption: Institutional “adoption curves” lag due to budgetary and other resource issues.
  - Supply Chain Dependencies: Development and adoption timeframes can be affected by those of related technologies.
  - Costs/Benefits Mismatch: Front-loading of development and implementation costs relative to enjoyment of benefits delays adoption decisions.
  - [Other?]
- References:

1. Time

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider and address variable risks in time phases of design, development, deployment and operations.
  - Consider risks of dynamic elements of operating environment at different scales.
    - Time dynamics of risks and threats (data life cycle, information supply chain, etc.).
    - Time dynamics of information arbitrage markets.
    - Time dynamics of interactions and emergent phenomenon in networks.
  - Consider relative rates of obsolescence/legacy systems in related and integrated technologies.
  - Lifetime cost (front loaded costs?): Consider cost accounting and other elements of how benefits match (or don't match) with costs for given expense.
  - Interaction velocity element: Analyze the extent to which system and/or technology will facilitate data/information flow and reduce interaction friction (or the opposite).
  - Analyze the adaptive ability of system and/or technology - Stability versus flexibility through time (Ref: Art Brock work here).
  - Block chain-related and "distributed ledger" technologies enable the conversion of problems of "time" (promises made in the past that encourage reliance in the future) into problems of "space" (distributed ledger to deter unilateral, *post hoc* changes).
  - [Other?]
- References:

2. Scale

- Challenges
  - Design, development and deployment of technologies and systems is frequently based upon a constrained model of the deployment environment, and the inattention to effects of the operation of a system or technology at other scales can have unintended and potentially harmful consequences.
    - Need to apply "systems engineering" approach at multiple scales to enable better scalar integration
    - Need to specifically unpack and explore those "out-of-scope" elements of system design
    - Be aware of scalar NIMBY-ism (intentional ignorance of negative impacts at other scales)
      - E.g., Commercial sales of high calorie foods causing increase in preventable diseases, the costs of which are borne by systems operating at other scales
      - E.g., Failure to immunize individual children can undermine" herd immunity" at larger scales
      - E.g., Lax computer security can open up individual systems to bot net recruitment that harms others.
    - Note that different types of organizations may be powerful in different scales, crimping inter-scalar planning
  - Is the subject system's and/or technology's impact and adoption strategy sufficiently scale-independent?
    - If not, then at what scale will it have an impact?
    - What is the effect of that impact (either + or -) at other scales?
      - E.g., increased LOA for IM at institutional level might be intrusive at individual level (intrusion versus insight privacy issues – See Map 53 – Constitutional Implications – 4th Amendment)
  - If the system and/or technology is deployed at one scale of socio-technical network (e.g., individual), what is needed to have it be impactful (and not harmful) at another scale (e.g., market)?
  - NOTE: "Scale" here is evaluated from WITHIN the deployed system/network
    - Compare "scope" framework for evaluation between and among systems
  - [Other?]
- References:

2. Scale

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider various alternative "scales" for technology-in-network analyses such as:
    - Network configurations at intermediate scales (See Map 63 - "Network Graph Theory Wiring Patterns")
    - Second and Third Order Structures (Ref: NATURE article on 2nd-order influence nodes and Science article on "Graphlets")
    - Phase change models
    - Thermodynamics-based models (Lagrangian coherent structures of reduced Shannon Entropy in Data Field (aka market arbitrage))
    - Fractal dimensionality insights (Ref: Mandelbrot economics and scale relationships)
    - other system analyses to revisit relationships among system elements at multiple levels (such as individuals, groups, companies, nations, networks, sectors, etc.)
  - Alternative analyses may reveal elements that are scale independent and/or scale dependent among different levels, yielding additional adoption and deployment alternative strategies (e.g., scale independence suggests fractal structures of markets, etc.
  - Consider notions of scale relationships through lens of distributed systems, rather than centralized or decentralized systems (See Ref: 1966 Paul Baran paper for RAND)
  - [Other?]
- References:

3. Scope

- Challenges
  - Is effectiveness of subject system and/or technology dependent on scope of its application or adoption?
  - Is system and/or technology impact dependent on presence of existing contiguous technologies, particular laws, or other system "externalities" in ways that can affect its resilience, reliability of efficacy?
  - When the system and/or technology is fully implemented in a system, what are the new risks that may arise at the edges of the system (Godel-incompleteness)? (See Map 41 - Provisional/Edge Governance).
  - "Scope" is evaluated from OUTSIDE the system network.
    - Compare analytical framework of Map 2 – "Scale" which is evaluated from *within* system
  - [Other?]
- References

3. Scope

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider operation of system and/or technology in distributed environment and how it will function in distributed environment (i.e., in absence of Perimeter 1.0).
  - Evaluate system and/or technology as part of larger ecosystem to understand new risks and differentials created by system and/or technology among stakeholders and beyond implemented system (i.e., external relationships are where Perimeter 2.0 is established)
  - Identify, evaluate and address constraints on expansion of scope of adoption/application of system and/or technology
    - such as national jurisdictional laws, “walled garden” operating systems, and other deployment-limiting factors
  - [Other?]

- References:

4. Stakeholder Type

- Challenges
  - What is the anticipated group of stakeholders that will be affected directly by the system?
  - What is the anticipated group of stakeholders that will be affected indirectly (in second and higher order indirect interactions) by the system when implemented in the real world?
  - What is the mechanism for identifying stakeholders that might be affected by the system, and in taking measures to mitigate harms to stakeholders based on both appropriate and inappropriate uses of the system?
  - When assigning responsibility for implementation and operation of a new system and/or technology, what are useful and efficacious categories (and useful performance measurements) for each separate role in security, identity management and privacy ecosystems?
  - What are risks associated with incorrect categorization and subsequent administration of selected "kinds" of stakeholders?
    - E.g., what happens to individuals if they are treated as engaging in online B2B transactions rather than B2C where they enjoy consumer protection laws?
  - Will legacy stakeholder categories (such as data subject, relying party, identity or attribute provider in identity management contexts, etc.) benefit from further development to evaluate different or additional motivations and behaviors of participants in distributed socio-economic information systems?
    - Subcategories of stakeholders have different needs
  - [Other?]

- References:

4. Stakeholder Type

- Candidate Analytical Frameworks/Metrics/Actions
  - Compare roles of individuals and institutions as described in the system and/or technology specifications/policies with those set forth in emerging candidate security, IM and Privacy standards
    - Consider whether there are gaps in stakeholder assumptions or ambiguities in descriptions that can result in new or additional risks in system operation.
      - Consider direct risks (e.g., experience harm) and indirect risks (e.g., liability for harm)
  - Does the system and/or technology anticipate new roles (new stakeholder types) for which a behavioral/performance profile is not yet available?
    - If so, what are the attributes of that stakeholder type/role, and what are the implications of that role existing beyond the system and/or technology being analyzed?
    - Are there new conflicts of interest issues arising with the role?
    - Is the role subject to external regulation or contractual duties, etc. that will influence the operation of the system in ways not anticipated in the system requirements and/or technology specification?
    - Does a change in the specific party occupying a role alter the related risks of bias, conflict, etc.
      - Analog is having an individual versus institutional fiduciary act of your behalf
  - Is it possible to create "fail safe default states" to protect anticipated (and unanticipated) uses by various groups of stakeholders with unique vulnerabilities?
    - Compare to guards placed on industrial equipment to prevent against operator and bystander injuries
  - [Other]

- References

5. Community of Interest

- Challenges
  - Networked security, IM and privacy technologies and systems typically seek to improve the reliability and reduce the risk (of security or privacy breaches) among one or more communities of interest (COIs).
  - Different types of COIs have different rulemaking processes, forms of rules and and enforcement profiles.
    - and they generate and operate under different performance and risk metrics.
  - How will the analyzed system and/or technology affect and be integrated into the existing rules of target COIs and contiguous COIs?
  - What will be the effect of adoption by an organization or individual who is involved in more than one COI?
    - Will they experience risk-profile-fragmentation, like the identity fragmentation of pre-federated online identity systems?
  - Is federation of the security, IM or Privacy service/function possible to alleviate fragmentation of security, IM and possible privacy gaps that might otherwise arise?
    - What are the hurdles to federating network risks among COIs?
    - What are risk implications of federation of service elements?
  - [Other?]
- References

5. Community of Interest

- Candidate Analytical Frameworks/Metrics/Actions
  - For maximum speed of solution adoption, look for various analytical and procedural interfacing opportunities ("hooks") into rulemaking processes and outputs/deliverables/artifacts of existing COIs such as:
    - State, local and federal governments (output = laws and regulations, enforcement policies, etc.)
    - Regional Trade Agreements (output=treaties and directives)
    - Communities (output = norms and ethics)
    - Markets (output = trading metrics)
    - Technical SSOs (output = specifications and IP cross licenses)
    - Industry associations (output = certification marks and standards)
    - Companies (output = products and services, policies)
    - Networks (output = operating standards)
    - Supply chains (output = contract terms)
  - [Other?]

- References

6. Bias - Individual

- Challenges
  - Operation of socio-technical systems (such as online products and services, etc.) depend on reliable performance and behavior of technologies and people.
  - Does (and how does) the reviewed system and/or technology address variation in individual behavior (and consequent system un-reliability) due to individual bias?
    - Individuals in role of users
    - Individuals in roles as system operators
  - In what ways can bias be referenced and applied as a *positive* factor in the recruitment of populations needed for such network-dependent strategies as "neighborhood watch," "crowd-sourcing of security solutions," etc.?
  - [Other?]
- References
  - "Processing Inaccurate Information – Theoretical and Applied Perspectives From Cognitive Science and the Educational Sciences," Edited by Rapp and Braasch (MIT Press, 2014)
  - See Risk Maps for "Bias – Cognitive - ___"

6. Bias - Individual

- Candidate Analytical Frameworks/Metrics/Actions
  - Bias as a negative system and/or technology performance factor
    - There are myriad biases that can negatively affect individual behavior. These include recency bias, bandwagon effect and many others. Some of the significant individual biases are included as separate Risk Maps under the headings "Bias – Cognitive." See, https://en.wikipedia.org/wiki/List_of_cognitive_biases
    - What are metrics to capture presence and potential harms of various biases?
  - Awareness (and mapping) of individual heuristics and biases typical of the roles involved in a given system and/or technology operation can help to positively influence the design, development and deployment of a given system and/or technology
    - E.g., it is easier to deploy flashlights and batteries after a blackout due to "recency bias"
    - E.g., it is easier to sell security services to a family in a neighborhood that has experienced burglaries, etc.
    - Flocking behavior in markets
    - Viral memes movements
  - [Other?]
- References

7. Bias -Institutional

- Challenges
  - The predictable performance of socio –technical systems (such as security, IM and privacy systems) depends on the reliability of system and/or technology, people and institutions.
    - What are the bases of reliable *institutional* behavior and performance?
    - What are "programmed" responses of institutional stakeholders in the subject technology systems and how can that reliability (or its absence) enhance or degrade performance of a given technology and/or system?
  - How do the institution's foundational and/or formation documents affect institutional behavior and system and/or technology behaviors
    - Articles
    - Bylaws
  - How do regulations and laws affect, constrain and direct institutional stakeholder responses in system and/or technology systems?
    - Laws and regulations as "scaffolds" for system deployment
  - How do existing binding obligations of institutions affect system and/or technology behaviors?
    - Voluntary, self-binding obligations (e.g., contracts)
    - Compulsory obligations (e.g., market pressures, laws)
  - [Other?]

- References

7. Bias -Institutional

- Candidate Analytical Frameworks/Metrics/Actions
  - Different types of organization have different mission-oriented "programming" found in their "organizational documents" and the set of their contractual obligations and rights that makes their system behaviors more predictable
    - Corporations – articles and bylaws
    - Country/State – Constitution
    - NGO – formation documents
    - Partnership – partnership agreement
    - Cooperative – cooperative agreement
    - LLC – operating agreement
    - Organizations formed under non-U.S. law – corresponding documents
  - It is critical to review and incorporate an analysis of the institutional programming in a given deployment setting to understand whether the adoption, deployment and operation assumptions of a given system and/or technology are valid.
  - Consider variations in use of system and/or technology in different types of organizations
  - Consider tendency toward Organizational Myopia for system and/or technology user?
  - Other issues of Institutional Bias include: official policies, group emotions, integrity and character of management, market-reinforced reputation, whistleblower-related policies, etc.)
  - [Other?]
- References
  - "Organizational Myopia," Catino (Cambridge Press, 2013)

8. Bias - Sectorial

- Challenges
  - Commercial entities and other organizations (such as regulators, consumers, etc.) operating in a particular industry or commercial sector are characterized by particular sets of externalities, expectations and behaviors that can affect their system behavior and performance individually and as a group.
  - Is the reviewed system and/or technology designed to fit the expectations and behavioral profile of individuals and/or entities in just one sector (e.g., banking, healthcare, Telco, retail, insurance, shipping, transportation, etc.), or can it be applied with consistent performance results in multiple sectors?
  - What are the potential harms of deployment of the subject technology and/or system outside of the sector for which it was designed?
    - E.g., To what extent would a HIPAA-compliant healthcare technology or system be functional and/or appropriate for application to financial records (usually covered by GLB) or educational records (usually covered by FERPA), etc.?
  - [Other?]

- References

8. Bias - Sectorial

- Candidate Analytical Frameworks/Metrics/Actions
  - Individual and organizational behavior in a particular sector is shaped by a number of potential sources that can be mapped to create a cartography of behavior/performance reliability, and risk
    - Regulatory (e.g., HIPAA, GLB, FERPA, etc.) shape the data and "privacy" related behaviors of their respective sectors, independent of organization type (corporate, individual, LLC, etc.)
    - Trade association standard terms/contract forms
    - Trade association insurance and self-insurance structures
    - Supply chain risk elements (e.g., risk of airline operations vs. hospital workers vs. food packers vs. manufacturing, etc., etc.)
  - Consider "root" sources that cut across sectors as potential avenues for cross-sector information network rules
    - Existing shared structures to address known threats and vulnerabilities in sector
    - E.g., FIPPs-based rules – but beware perpetuating FIPPs 1970's era approaches
    - E.g., Commonwealth countries share legal and language traditions that apply across industrial sectors in their respective jurisdictions.
  - [Other?]
- References

9. Bias – National/Cultural

- Challenges
  - Organizations and individuals from different nations and cultures have different expectations about the nature of security and privacy and the notions of individual and group identity that will affect their performance and their expectations of the performance of others when using a security, IM or privacy system and/or technology.
  - How does the system and/or technology address varying national/cultural norms, expectations, biases, etc. of people and institutions?
  - What are the challenges associated with deployment of a technology/system within a given jurisdiction (national boundary) where different cultural elements are present?
    - Does localization of a technology to accommodate a given set of national laws ignore opportunities for further customization for multiple cultural groups within that jurisdiction?
  - For technologies that will be deployed domestically, how might *regional* differences (within a given country) affect security, IM or privacy performance of the analyzed system and/or technology?
  - [Other?]

- References

10. Bias – Analytical/Statistical

- Challenges
  - What gets measured gets done - How is the reviewed system and/or technology “blinded” by its own design/operation and performance measurement assumptions?
  - What is the resulting bias in product and service design, development and deployment
    - How can that bias be revealed?
      - Monte Carlo simulation, etc.
    - How can that bias affect the system’s security, IM and privacy risk profile?
  - [Other?]
- References

10. Bias – Analytical/Statistical

- Candidate Analytical Frameworks/Metrics/Actions
  - Apply different assumptions to the operations phase of the system/technology to “stress test” the analytical bias of the system
  - Look at the edge of the performance measurements proffered by the system and/or technology proponents based on their interpretation of the system requirements.
    - Consider the performance characteristics beyond the edge of the suggested metrics.
  - Consider the questions that are not being asked, and potentially-relevant metrics that are not being anticipated, in the design, development and deployment of the system and/or technology that might undermine its anticipation performance?
  - Construct frameworks in the “negative analytical space” beyond the suggested metrics
  - [Other?]

- References

11. Reliability/Predictability/Trust

- Challenges
  - Trusted systems can gain traction and retain reputation by demonstrating reliability and predictability in operation ("mechanistic trust").
  - How does the reviewed system and/or technology help to generate reliability/predictability/trust that can foster adoption and other prerequisites to successful, sustainable and resilient network deployment of security, IM and privacy technologies?
  - What other elements or characteristics of the subject system and/or technology can potentially provide a reference point for measuring consistency in performance as a prerequisite to trust, or its absence?
  - What are the other sources of "Trust" beyond experienced reliability?
    - Word of mouth/recommendations
    - Certification/attestation
    - Access to enforcement
    - Insurance/guarantee/warranty arrangements
  - [Other?]
- References

11. Reliability/Predictability/Trust

- Candidate Analytical Frameworks/Metrics/Actions
  - What are the elements of the system and/or technology that can demonstrate reliability and predictability?
    - How can the more reliable elements of the system and/or technology help to stabilize the less reliable elements in a trustworthy network deployment of the system and/or technology?
  - What are the elements of the system and/or technology and/or the related systems that depend upon the system and/or technology, the unreliability of which can undermine trust in operation and hamper adoption?
  - How can individual bias (See Map 6 – Individual Bias) be positively recruited to help stabilize the reliability of individual performance in system and/or technology deployment?
    - In what situations does designing w/r/t bias offer greater reliability that other design parameters?
  - [Other?]

- References

12. Individual Attributes/Training/Education/Experience

- Challenges
  - In socio-technical systems (such as those that depend upon and also that deliver security, IM and privacy technology systems), individual behaviors and performance can vary among different people based on varying capacities and differences in physical and mental ability, training, education and other unique attributes.
  - How does the reviewed system and/or technology anticipate, accommodate and/or address individual differences among users, data subjects, etc. who will interact with the system in both personal and institutional settings?
    - In personal-use settings
      - How do users learn proper use of system
    - In employment settings, how is training on system achieved and funded
      - Seller model
      - Employer model
      - Hybrid models
  - [Other?]

- References

12. Individual Attributes/Training/Education/Experience

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider degree of dependency of system and/or technology performance on a given level of individual (consumer, user, service provider, employee, etc.)
    - Physical and mental ability
    - Training on specific system/technology
    - Education and general capacity building
    - Social and cultural motivations and factors
    - Positive identity and self-image
    - Creativity and critical thinking skills
    - Degree of emotional Intelligence and social awareness
    - other unique attributes
  - Consider OSHA standards, ADA standards, and other regulatory standard references.
    - Does the system and/or technology anticipate accommodations to enable differently-abled persons to participate in the effectuation of security, IM and privacy system goals?
      - Consider "paradigm of citizen participation in "neighborhood watch" security for open systems
  - Consider coordination with workforce development initiatives in cybersecurity (such as DHS NICE program, etc.)
  - Ref: "Economic Theory of Greed, Love, Groups and Networks," Frijters and Foster (Cambridge Press, 2013)
  - [Other?]
- References

13. Economic Incentives

- Challenges
  - Are potential and actual economic incentives (and disincentives) associated with each of the various system stakeholder roles (both individual and institutional) taken into account in the design of the system and/or technology?
    - What incentives/disincentives are there for system participants to follow system organizational and operational rules?
  - What is the level of dependency of the normal operation of the technology and/or system on the provision of incentives and application of penalties to enhance user performance and interface with the system
    - E.g., For commercial applications - can it be reliably deployed outside of compulsions of the employee setting?
    - What will cause stakeholders to use it?
  - Where incentives are identified as needed to motivate various stakeholder behaviors, what is the source of funding for such incentives
    - Is the funding sustainable?
    - Is the timing of the availability of the funding matched to the need to provide incentives
      - What intermediation models can be conceived to bridge any timing and other gaps to funding incentives?
  - [Other?]

- References

13. Economic Incentives

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider monetary/economic incentives motivating various positive and negative system behaviors
    - Leverage of insight – who benefits from information arbitrage in system
    - Tort of Conversion (theft) – what responsibilities/incentives are associated with handling valuable information?
  - Consider non-monetary economic incentives
    - Reputation in community
    - Fame and publicity as incentive
    - Information arbitrage value (insider trading, SEC Rule 10b-5)
  - Consider indirect structures of incentives
    - Employee "Respondeat Superior" relationship as economic incentive for performance conformity
    - Market and supply chain relationships (output and demand relationships and negotiation power relationships as forms of soft economic incentives)
    - Other forms of "soft" economic compulsion
- Additional Ref: "Innovation and Incentives" Schotchmer, (MIT Press, 2004)

14. Economic Setting

- Challenges
  - Does the system and/or technology accurately and sufficiently-comprehensively address the adoption and operation implications of the larger economic setting in which it will be deployed?
  - Is the system and/or technology adaptable (and does it lend itself to metrics) that will permit it to be integrated in operations and strategic planning within existing economic expectations of stakeholders?
    - Companies seek to externalize and delay costs delaying replacement of legacy systems
      - Bolt-on or “wrap around” capacity can be more cost effective and easier to adopt
  - [Other?]
- References

14. Economic Setting

Candidate Analytical Frameworks/Metrics/Actions

- Consider alternatives of “buy or build or become” strategies
- Cost Accounting and security, IM and Privacy system and/or technology
- ROI (timing) and GAAP for security, IM and privacy
- Competitive environment
  - “First mover” dis-incentives
- Institutional economic biases
  - corporations maximize income for shareholders
  - governments spend to benefit citizens
  - NGOs, trusts serve beneficiaries (trustee is economic fiduciary)
  - Cooperatives and trade associations serve industry members
- Need to understand deployment context of system and/or technology and relevant stakeholders economic interests to fully evaluate organization and operation of system and/or technology in real world contexts
  - E.g., company might balk at front-loading costs of pollution control facility if not required by regulation and not being done by competition, but government or NGO might find those costs consistent with their mission.
- Tax considerations (amortization and deduction variation of security, IM and Privacy strategies (See TVR “Privacy Beyond Compliance” paper).
- [Other?]

- References

15. Central v Distributed Architecture

- Challenges
  - Centralized/hierarchical institutions and governance structures are rendered blind by distributed information systems.
  - Many current problems and threats are artifacts of centralized/hierarchical institutions operating in distributed information/risk landscape.
  - How does reviewed system and/or technology address this institutional/deployment challenge?
  - [Other?]
- References
  - See Diagram from paper by Paul Baran at RAND corporation on distributed systems https://docs.switzernet.com/people/emin-gabrielyan/060921-thesis-for-experts/ac43_files/image003.png

15. Central v Distributed Architecture

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks of distributed governance to match distributed information systems
    - neighborhood watch
    - Self-binding to policy standards
    - Private rights of action
    - Crowd-sourced insight
    - Information arbitrage co-ops
  - Consider strategies for security/privacy/IM integrity in "open" systems, such as scaffoldings of institutional duties to frame citizen rights. Compare other "rights" manifested in open/public settings such as:
    - Katz v. U.S line of authority (reasonable expectation of privacy) – 4th amendment context
    - First amendment rights of expression, association, access to information
  - [Other?]
- References:

16. Complexity

- Challenges
  - What are performance and measurement assumptions made in evaluation of subject system and/or technology that are deployed in "complex settings"?
    - Are they based on normal (Gaussian) distributions of risk?
    - Are they calculated on another basis (such as power law distributions) that reflect unpredictability of non-linear events in complex systems?
  - What is the basis of the assumptions made and are they justified given the level of organizational and operational complexity in deployment of the system and/or technology?
  - Are those assumptions appropriate given the mathematical complexity of the variables associated with the interactions with respect to which the security, IM or privacy system and/or technology will be deployed?
  - Insight and intrusion are two opposing views (observer and data subject respectively) on "lower entropy" credentials (demanded at higher Levels of Assurance).
    - How does the relationship of measurement granularity (complexity?) to both information value (Shannon arbitrage) and privacy intrusion (intrusive PII) suggest a problem that could help lead to a operational and measurement solutions?
  - [NOTES: Feynman: Rules are simple (1million square checkerboard), but multiplicity of actions and pieces makes it complex. Like thermodynamics. Language of complexity is gradients? Arbitrage and thermodynamic behavior as gradients?]
  - [Other?]
- References:

16. Complexity

- Candidate Analytical Frameworks/Metrics/Actions
  - How measure risk in complex systems?
    - Metrics/Actions of complex systems associated with
      - Emergence
      - Self-Organization
      - Feedback
  - For those risk variables that cannot be modeled based on normal distributions, what alternative potential risk models can be applied for complex systems?
  - Complex systems might invite measurements of fractal dimensionality of deployed technology system.
    - See English Coastline example https://en.wikipedia.org/wiki/Coastline_paradox
    - Change in granularity of measurement alters length (an identity attribute) of a coastline
    - Change in granularity of identity measurement for IM alters identity attribute of person
      - See OMB 0404, NIST 800-63 – Change "granularity" of identity measurement for different LOAs.
- Source and measure of criticality?
  - See: From Wikipedia: The **stability of Boolean networks** depends on the connections of their nodes
  - [Other?]
- References:

17. Group Recruitment/Collective Efficacy/Neighborhood Watch

- Challenges
  - In distributed socio-technical systems, such as the Internet, humans (and their institutions) are not just beneficiaries of the value of the system, but are also critical components of its operation.
  - How does the system and/or technology help to cohere the behavior of populations of humans (in their respective roles as consumers, viewers, citizens, etc.) to deliver benefits that individuals cannot achieve unilaterally?
  - If the system and/or technology value proposition to improve security, IM or privacy depends on broad adoption, in what ways does the system and/or technology motivate, induce or accommodate individual participation?
  - [Other?]
- References:

17. Group Recruitment/Collective Efficacy/Neighborhood Watch

- Candidate Analytical Frameworks/Metrics/Actions
  - Nectar-based networks
    - Provide benefit to attract participation with incidental benefits to participants and/or third parties
      - Network TV advertising model
      - Retail banking model
      - Internet advertising model
  - "Catch 22" of social network value propositions
    - Efficacy of solution depends on broad adoption AND
    - Broad adoption is dependent on efficacy of solution
      - E.g., Under what conditions would you migrate to a social network alternative with only 100 members?
  - <u>Standards for safety and risk reduction recruits populations</u>
    - E.g., Fast food chain restaurants (voluntary commercial standard franchise agreements (and purchasing and licensing relationships) yield reliability of performance of socio-technical systems (cook + food + preparation protocols) at fast food restaurants)
    - E.g., Red light means stop (compelled standard yields reliability of performance of socio-technical systems (driver + car + traffic light) for enhanced safety at highway crossings)
  - <u>Purpose recruits populations</u>
    - SETI, Fold-it (Protein folding library), Other.
    - Awareness of different communities of interest based on geographic and non=geographic groupings.
  - <u>Convenience/Cost savings recruits populations</u>
    - eBay and Uber and AirBNB and. . .
    - PCI-DSS for payment cards
    - Etc.
  - [Other?]
- References:

18. Dual Use Issues/Weaponization

- Challenges
  - Both “insight” and “intrusion” are simultaneous and opposing views on information arbitrage gleaned from data that is applied to provide insight in security, IM and privacy contexts.
    - Both are “accurate,” and the paradox of their opposition reveals the reality of information arbitrage that makes it valuable
    - Sustainable and reliable system and/or technology helps to measure and balance the opposing positions
      - it does not need to “eliminate” them in order to be effective
  - Are there potential “off-label” uses of the security, IM or privacy system and/or technology that can cause harm?
    - Intentional harm
    - Accidental harm
    - Unintended consequences of operation
  - Can the system and/or technology be “weaponized” (or “productized”) in ways that can harm individuals, institutions, etc.?
    - What measures can be take to prevent/mitigate the weaponization of the security, IM or privacy system and/or technology?
  - [Other?]
- References:

18. Dual Use Issues/Weaponization

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider analogy to other dual-use technology markets to discern potential frameworks for managed use
    - Explosives
      - Nitrogen fertilizer
    - Pharmaceuticals
    - Firearms
    - Insurance
      - Investment in insurance without "insurable interest" is basically gambling - there is public policy against taking out life insurance on life of unrelated person
    - Financial Derivatives (used for hedging ("good") and speculative (potentially "bad") purposes)
  - Consider framework of various mechanisms and constraints (e.g., economic, licensing, training, normative, regulatory, P2P, supply chain liability, etc.) to reduce or eliminate undesirable uses of the security, IM or Privacy system and/or technology
    - Hybridize with Economic Incentives, Neighborhood Watch, Distributed Systems frameworks/metrics
  - [Other?]
- References:

19. Socio-Technical Integration Issues

- Challenges
  - Current online security, IM and privacy challenges can be interpreted as the early evidence of the socio-technical hybridization (in intangible information embodiment) of people and technology.
    - A creeping “singularity?”
  - That hybridization provides capacities of system and/or technology to individuals and institutions that are less-familiarly bounded, with the result that their utilization can cause harms to the user of those technologies and others.
    - Person with IM tech is like a baby with a handgun
  - Can the system and/or technology adequately integrate human/institutional behavior with system and/or technology performance to protect the user and others?
    - Protection from intentional harms
    - Protection from accidental/unintended harms
  - How does the system and/or technology deal with the vagaries and variables associated with human and institutional error, exercise of discretion, etc.?
  - [Other?]
- References:

19. Socio-Technical Integration Issues

- Candidate Analytical Frameworks/Metrics/Actions
  - To stabilize the system and/or technology portion of the sociotechnical system, consider application of responsibility frameworks such as
    - Asimov's rules for robots (yes, seriously!) for autonomous elements of IM or privacy system.
    - Derrida's reversal of "winners" and "losers" in policy decisions
    - Goal scoring exercises
  - See "AI and autonomous systems" framework below.
    - Consider application of same "3 rules" constraints to institutions that use security, IM or privacy technologies
  - To help stabilize the human/institutional portion of the sociotechnical system consider application of other frameworks in various maps of Atlas
  - [Other?]
- References:

20. Exponential Data and Interaction Growth

- Challenges
  - Data and Interaction "Firehose" problem
    - Nature article: 28-32% compounded annual growth in global abilities to collect, process and transfer data
  - Data, interactions, and resulting information are growing exponentially (from mathematical point of view)
    - 5^{th} order effect/amplification of Moore's Law
    - Interactions breed risks
    - What are implications of exponential rates of growth in risks?
  - How can the subject system and/or technology deal with/measure/tame exponential rates of increase of data inputs and the increased risk in interaction settings in which it is depended upon?
  - [Other?]
- References:

20. Exponential Data and Interaction Growth

- Candidate Analytical Frameworks/Metrics/Actions
  - System should promote and support foundations of governance in new and growing interaction normative "blank space."
    - Exponential increase in interaction growth is perceived/measured as exponential increase in data, information, risk, complexity, etc.
    - Data, risk, complexity, etc. are artifacts of the fact of exponential increase in interactions
    - Govern interactions, not artifacts of interactions.
  - Plug in system inputs and outputs into the metrics flows that will support the following functions in interaction "blank space"
  - 4 step ladder of organic institution construction
    - Collect practices library from stakeholders involved (directly and indirectly) in interactions
    - Present practices library to stakeholders for consideration as best practices (this is rulemaking/legislative process)
    - Support stakeholder group efforts to formalize, signal and enforce their voluntarily selected "best practices" as enforceable standards (this is enforcement/judicial function)
    - Support stakeholder group efforts to outsource operation of enforceable standards to separate entities (this is operational/executive function)
  - For all of the risks associated with the proposed technical system, check if the input and output metrics support the building of governance.
  - This governance-related activity will be driven by stakeholder self-interest, and the interdependency of the systems (including the attainment of de-risking and leverage at scales that are not accessible unilaterally by stakeholders provides the engine for the construction of these governance systems).

- References:

21. New Metrics in Markets

- Challenges
  - Market “macro” analysis affects perceptions of risk and trading behaviors of individuals and institutions interacting in those markets
  - Information arbitrage markets (aka “Big Data”) is supplying metrics and insights even before the questions are being asked
    - See Science Magazine article on the inversion of the scientific method (data precedes theory)
    - Will it be impossible to avoid potential for re-identification of PII in future systems?
      - Compare to environmental bulk gene sequencing, other big data contexts
  - How does the subject system and/or technology deal with new and emerging metrics, unexplained correlations, and new interactions as inputs to its security, IM and privacy systems?
  - How does the system and/or technology deal with changes in metrics that input into its operation?
  - [Other?]
- References:

21. New Metrics in Markets

- Candidate Analytical Frameworks/Metrics/Actions
  - Markets operate external to individual deployed technologies, and influence their application in interactions.
  - Data and information rights markets that utilize security, IM and privacy system and/or technology will encounter and will need to deal with market pressures and influences (promoted by market metrics).
  - "What gets measured" in markets is "what gets done" in individual interactions.
    - This is the power of monetization, e.g., in market contexts.
  - How can the system and/or technology enable the production of additional or alternative measurements to offset and/or inform the external market measurements that can affect the achievement of stated security, IM and privacy goals?
  - Consider re-identification challenges (inevitabilities?) of "Big Data" promoted by market
  - [Other?]
- References:

22. New Metrics in System Performance Evaluation

- Challenges
  - Beyond Market Metrics (Map 21), there are also new and emerging metrics of system performance being developed by governments (aka NSTIC/IDESG/EU), trade associations, companies, and others to evaluate security, IM and privacy technology system performance.
  - Is the subject security, IM or privacy system and/or technology conformant with one or more of such new sets of system metrics?
  - Does the system and/or technology offer new or additional performance measurements that can establish and support enhanced security, IM or privacy performance?
  - [Other?]
- References:

22. New Metrics in System Performance Evaluation

- Candidate Analytical Frameworks/Metrics/Actions
  - What gets measured gets done. If the subject security, IM or privacy system and/or technology offers new or additional metrics that are viewed as correlated with improved security, IM and privacy performance, the system and/or technology can provide a basis for a new framework for evaluation of security, IM and privacy efficacy.
  - Consider normative cross-references to existing standards (and their corresponding metrics of performance against such standards) as stabilizing elements to facilitate the deployment and adoption of new candidate security, IM or privacy technologies.
    - Consider tangential standards that can stabilize fast evolving areas with normative scaffolding
  - [Other?]
- References:

23. Death of Secrecy Challenge

- Challenges
  - Secrecy died (or is at least in “intensive care”) because of:
    - massive data system technical interoperability, and
    - collective quest for individual insight, and
    - desire for information advantage to gain leverage and lower interaction risks
  - How can Identity Management, Privacy, Information System integrity be manifested and preserved in the absence of secrecy?
    - Massive technical interoperability increases interaction volume exponentially
    - Interactions breed risk of intentional or accidental release of information
  - How can reliable and trustworthy security, IM and Privacy be measurably delivered in distributed systems where the expense of keeping secrets is increasing faster than the achievement of that goal?
    - Hybridize with “Power law” Map
  - [Other?]
- References:

23. Death of Secrecy Challenge

- Candidate Analytical Frameworks/Metrics/Actions
  - Measurably-reliable Privacy and Identity Management goals can be met even given the "death" of secrecy.
    - Compare: Why don't people steal each other's patio furniture?
    - Compare: Why do people stop at red lights?
  - Shared narrative of "rule of law" and sovereign authority projected onto governmental organization (Rooted in Peace of Westphalia – 1648) enable self-binding by citizens and commercial entities (the latter of which are formed pursuant to state (and rarely federal) laws) to compulsory laws and regulations which function as standards of behavior that convert duties from words into behaviors and practices, breathing life into the rights established by those laws.
  - Consider the ways in which the security, IM and privacy metrics generated by use or operation of the subject system and/or technology can result in a form of "democratized information" to encourage populations of stakeholders to self-bind to a set of rules in furtherance of the collective benefits.
    - Vary "enforcement" strategies depending on nature of values/harms involved.
  - Consider "information arbitrage co-operative structure"
    - Consider links to emerging online "reputation" systems as rules enforcement mechanism
  - See "Neighborhood Watch" Map
  - [Other?]
- References:

24. Uncanny Valley

- Challenges
  - There is a human resistance to certain AI and autonomous systems that are “too human.”
    - First described in visual terms, and later also in other “Creepiness factor” interaction settings
  - For systems and/or technology to deliver effective security, IM and privacy products and services (that relate to intrinsically human needs) will require attention to the “uncanny valley” problem.
  - How does the subject system and/or technology address risks arising in digitization of value and virtualization of risk in ways that will be helpful and effective for human users?
  - Do models applied in the system and/or technology system adequately fit the purpose of their application?
  - [Other?]
- References:

24. Uncanny Valley

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks that make explicit the nature of socio-technical systems
    - Compare FTC regulation of “pirate advertising”
      - FTC imposes “Notice” regime to alert users
  - Develop frameworks to parse information decision making tree to establish how security, IM or privacy system and/or technology operates to enhance information channel integrity and derive performance metrics that can be shared with user
    - intent to bridge the uncanny valley
    - Ease “existential” queasiness.
  - [Other?]
- References:

25. Infinite Duplication

- Challenges
  - Data can be infinitely duplicated and is non-rivalrous
    - it can be used by multiple parties simultaneously or serially without diminution of value.
      - Except with respect to diminution by dilution of data's "information" content
  - Sometimes those uses by parties acting either intentionally with malice (such as a hacker) or negligently (such as a careless employee) are contrary to social, individual and system security, IM and Privacy goals
  - Does the system and/or technology appropriately address the challenges of producing and maintaining multiple instances of protected PII, IM or privacy-sensitive data and information?
  - [Other?]
- References:

25. Infinite Duplication

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks that evaluate the propensity of the system and/or technology to lend itself to operational-izing the distinction between “data” and “information” consistent with Shannon’s quantitative theory of information
    - Data is not information, but data+meaning=information.
  - When frameworks separate “data” from “information” it provides additional dimensionality into the technology system, permitting different governance regimes for “data” versus “information”
    - The former (“data”) potentially regarded as a “commons” (and subject to co-management like riparian rights, fishing rights, etc.)
    - the latter (“information”) based on a more familiar “property ownership” notion, consistent as manifested in IP laws, with its enablement of serial value additions through licensing.
    - Viewed as a “knowledge supply chain,” when a person is “informed” by bringing their “meaning” to data, they bring value to that data by their regarding it.
    - This simple distinction seems theoretical, but can help bring market mechanisms to service of security, IM and Privacy system stabilization.
  - Can enhanced incentives in “information” markets create “neighborhood watch” to help to resolve Privacy and IM issues in “big data” markets, where infinite duplication is a risk driver?
  - Consider approaches to “artificial rivalrousness” such as is applied in copyrights, patents, trademarks, certification marks and trade secrets. (although “trade secret” law typically requires secrecy, and so is actually rivalrous).
  - Compare
    - Other commodity markets versus refined products
    - Online advertising model of data “informing” multiple advertisers
    - Compare IP enforcement that depends on private rights of action
      - neighborhood watch of IP by “Property owners” of infinitely duplicate-able materials)
  - [Other?]
- References:

26. Re-identification Challenges

- Challenges
  - Systems and/or technologies that depend on data "de-identification" as a strategy for information security, privacy and integrity can be undone by subsequent re-identification of data.
    - This calls into question the effectiveness of laws and rules that depend on de-identification (such as HIPAA, state data breach notice statutes, etc.)
      - They may do more for liability control for institutions than for protection of data subjects
        - » They establish statutory "duty of care" that helps data handling institutions to structure operations without regard to later re-identification harms.
  - Does the system and/or technology seek to deal with re-identification issues, and if so, how?
  - [Other?]
- References:

26. Re-identification Challenges

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider whether notion of "re-identification" is a red herring.
  - Note potential difference of EU (Hegel) and US (Locke and Utilitarians) here.
    - See OECD paper entitled "Personhood."
    - In EU data about a person is viewed as more closely associated with the person, whereas in the US, conformity with statutory de-identification protocols (such as under HIPAA and GLB) effectively absolves transferors of de-identified data from liability for subsequent re-identification activities.
  - If distinction is made between "data" and "information" (consistent with Shannon) then concept of "re-identification" is recast as an independent conversion of such de-identified "data" into "information," subject to whatever self-regulatory regime is developed and followed by stakeholders for such "data" and separately for such "information."
  - The parsing of re-identification into a series of independent "identifications" enables allocation of responsibility and liability under comparative negligence and contributory negligence statutes, and civil intentional tort and criminal law regimes.
  - Into what data use settings can the subject system and/or technology be placed to provide the stakeholders with activity reports and other system meta data that can help distinguish among multiple data "identifications" by multiple parties, helping to parse responsibility for unauthorized data uses in re-identification settings.
  - Consider court cases of de-certification of class action for failure to establish link of specific instance of lost data and identity theft event), it is evidentiary prerequisite to link harmful use of information with specific unauthorized data access.
    - Are there frameworks in which the system and/or technology help to establish these links?
  - [Other?]
  - References:

27. Incidental Harms and Unintended Consequences

- Challenges
  - "Negative space" problem
    - Does system and/or technology create new risk space for some parties while addressing old risk for other parties?
  - NIMBY-ing the lack of system integrity.
    - Will enhanced security, IM or Privacy performance of a system using the system and/or technology serve to move the problems of system integrity to the interaction "risk space" of another stakeholder, and if so, with what consequences to the other stakeholder?
  - Example of NIMBY of system integrity is evidenced by fact that Insight and intrusion are inversely proportional in IM and privacy systems
    - since enhanced LOA requires more extensive identity checking and invokes more intrusive authentication protocols (See NIST 800-63, etc.) and is therefore potentially more intrusive on privacy rights (mostly pursuant to the common law privacy concept of "intrusion on private affairs.")
  - [Other?]
- References:

27. Incidental Harms and Unintended Consequences

- Candidate Analytical Frameworks/Metrics/Actions
  - When an information technology or system reduces disorder in one stakeholder's interaction "phase space" it typically increases disorder in another phase space.
    - Example is breaking the code of Nazis in WWII with Colossus computer
  - It is worth investigating whether this is an indication that Information "entropy" is preserved, potentially revealing additional sources of useful system metrics
    - Following VonNeumann and Shannon
      - See MIT slides on "Entropy Accounting" based on thermodynamics laws
      - consider if calculus of thermodynamics can help frame transfers of information harm among parties.
  - What are the new risks created by operation of the system and/or technology, and how can harm to burdened parties be mitigated?
    - Compare concept of dyads of "benefitted" and "burdened" by real estate easements.
    - Compare legal concept of "nuisance" that prevents the "quiet use and enjoyment" of property.
      - Can harms to PI (such as reputation harms – aka libel and slander) be evaluated under nuisance-type framework?
  - [Other?]
- References:

28. Supply Chain/Outsourcing Risk

- Challenges
  - Networks, and the commercial and critical infrastructure that depend upon them, represent increasingly extended data-to-information "supply chains."
  - Supply chains are characterized by opacity regarding second and higher order interactions above and below those engaged in by a given party
    - This is the source of the challenge of "Green washing" in certification mark programs
  - How dependent is the system and/or technology on inputs and outputs being reliable, available, trustworthy, and stable in supply chain contexts?
  - [Other?]
- References:

28. Supply Chain/Outsourcing Risk

- Candidate Analytical Frameworks/Metrics/Actions
  - Does the system and/or technology produce metrics or operate at a sufficient scope in a given "supply chain" so that it is in a position to supply data that can inform insight at multiple levels of supply chains into supply chain performance against parameters?
  - Consider frameworks that apply metrics that are referenced at multiple levels of the supply chain to assure "neighborhood watch" against measurement gaming.
    - Periodicity of measurement and stakeholder access in decision making:
      - Compare input strategies of "flow" versus "batch" processing concepts in chemical and pharmaceutical manufacturing for framings of potential security, IM and privacy controls for intangible data inputs in information systems
  - [Other?]
- References:

29. Psychology

- Challenges
  - System reliability.
    - Since human behavior (in their capacities as individuals and employees, etc.) in systems and with technologies is variable based on myriad psychological factors (which can influence and be influenced by online content in recursive feedback and feed-forward loops), how can reliable security, IM and Privacy technologies account for and mitigate risk based on these variables?
  - Potential Harms.
    - Security, IM and Privacy issues can affect psychological and existential triggers in people causing temporary psychological conditions that may be inconsistent with optimal socio-technical security, IM and privacy systems
      - in extreme cases can possible neuroses and pathologies that can create new risks and security concerns.
    - What are the psychological risks associated with this system and/or technology, and how can they be mitigated?
  - [Other?]
- References:

29. Psychology

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks of user behavior to account for potential cross section of behaviors that may affect system performance associated with psychological states of people for different roles in security, IM and privacy system and/or technology deployments.
    - In their individual capacity
    - While filling a role or position for a company or another organization
  - Consider frameworks to evaluate psychological state and/or profile of users of the subject system and/or technology in real time
  - Note: Human research standards and protocols
    - IRBs and other safety measures to protect subjects
  - [Other?]
- References:
  - Ref: DSM V

30. User Role Profiles

- Challenges
  - Individuals interact with systems in multiple capacities and roles (such as employees, consumers, data subjects, etc.).
  - How does the system and/or technology accommodate and facilitate parsing of the multiple roles engaged in by a single individual user of the system
  - How does the system and/or technology address potential security, IM and Privacy issues that arise from ambiguities in system use, permissioning, authorization, security and other domains as a result of the multiple user role profiles to which a given information technology and/or system is subjected?
  - [Other?]
- References:

30. User Role Profiles

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider framework of analysis for BYOD challenges here
    - employees bring personal devices to work
  - Consider whether alternative rights and responsibilities management frameworks based on BYON (Bring your own network) might provide mechanisms (in the form of network policies) to help establish and enforce security, IM and privacy reliability that is superior to that available through characterization of the problem as one of hardware (BYOD), rather than the continually renewed service available through "networks" (BYON)
  - Consider frameworks based generally on "agency" law (and with reference to the subcategory of "respondeat superior" applicable to employer/employee relationships) to help separate an individuals interactions with information systems.
    - This is current practice, where TOUs invisibly characterize every user action on a website – the terms control the character of the interaction for legal and economic rights-management purposes.
  - [Other?]
- References:

31. System and/or Technology Niche Fitness

- Challenges
  - Existing standards-laden environments
    - Even the most innovative and paradigm-shifting technologies are introduced into existing "real world" context and settings that are characterized by an existing standardization/interoperability environment of both system and/or technology infrastructure policy which dictates and forms user habits and expectations into which it must integrate if it is to be broadly adopted.
  - What are the strategies for introduction of the new security, IM or privacy system and/or technology that can maximize the benefit of the existing contiguous system and/or technology and policy organization architecture and operational landscape for maximum positive impact and mitigation of risks?
  - How can the new technology/system best "fit in?"
    - Are there existing external metrics associated with existing "Tools and Rules" that can be normatively cross referenced for initial risk metric stability for the new system and/or technology?
  - [Other?]
- References:

31. System and/or Technology Niche Fitness

- Candidate Analytical Frameworks/Metrics/Actions
  - Sources for normative cross reference of performance metrics can be other existing technologies and/or existing policies/laws.
  - Consider system and/or technology metrics that can be normatively cross referenced as evidence of satisfaction of policy purposes, and vice versa.
    - E.g., Reference law for tech - when the operation of a specific system and/or technology or tech architecture is recognized (by regulation, regulatory authority, case law, etc.) to satisfy the legal "standard of care" associated with a security, IM or privacy right such as standard of "de-identification" protocols under HIPAA.
    - E.g., Reference tech for law - under the Americans with Disabilities Act, provision of certain assistance and access technologies is recognized to satisfy legal requirements
      - See also OSHA.
  - [Other?]
- References:

32. Governance Assumptions

- Challenges
  - The design requirements and operating parameters of all security, IM and Privacy technologies anticipate a certain degree of organization and certain level of coordination that might be collectively called “data governance.”
  - Deployed, networked security, IM or Privacy technologies rely upon certain assumptions regarding “internal” system governance and “external” operating environment governance
    - E.g., Uber involves the coordination of various security, IM and privacy technologies internally (ride matching, PCI-DSS, etc.) and external (livery regulations, user taxi habits, etc.). See also eBay, Airbnb
  - Are the assumptions made in the system and/or technology deployment plan regarding internal and external data rights governance realistic and achievable?
    - What are the other frameworks that can help to discern whether the governance assumptions will hinder or promote adoption?
  - [Other?]
- References:

32. Governance Assumptions

- Candidate Analytical Frameworks/Metrics/Actions
  - For those security, IM and privacy technologies where the governance assumptions are not made explicit, they can be gleaned from the affirmative statements about individual and institutional behaviors presented in the specification or proposal.
    - Look for use of words in proposal such as “must,” “shall,” “should,” etc. regarding the expected behavior of stakeholder employees and representatives
    - Consider whether there is existing incentive or penalty infrastructure present so that the positive assertions about behaviors can be relied upon during operation of the security, IM or privacy system and/or technology.
  - For internal governance testing, reference can be made to existing governance structures of institutions into which the subject system and/or technology will be introduced.
    - E.g., Consider variations among internal data and information governance environments of such disparate entities as manufacturer, agribusiness, air force base, bank, software manufacturer, electrical utility, etc.
  - For external governance testing, check first for applicable regulation that may establish specific statutory duties of care regarding security, IM and privacy behaviors.
    - Also reference contractual obligations established by trade associations, supply chain dominant players, etc.
  - [Other?]
- References:

33. Interfaces/UI

- Challenges
  - Security, IM and privacy technologies must typically be able to operate in situations characterized by significant interaction complexity beyond the understanding of individual humans
    - Some of these humans are responsible for the operation of the system and/or technology (such as employees at an RP or IDP)
    - Some of these humans are affected by its operation (such as data subjects).
  - Security, IM and privacy systems utilize technologies the operation of which is "under the hood" or "in a black box" and not available for scrutiny or understandable to individuals.
  - What are the strategies and mechanisms applied in the organization and/or operation of the subject security, IM or privacy system and/or technology that enables humans (as users and/or data subjects) to effectively, fairly, and safely interact with the system and/or technology?
  - How can a system that is not understood by a human be safely used by a human?
    - What are the mechanisms to help assure that result?
      - Agency/fiduciary duties in design and operation?
      - Guarantees?
  - [Other?]
- References:

33. Interfaces/UI

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks for training, instruction, education, warning, "informed consent," etc. pursuant to which human users are apprised of implications of using system and/or technology prior to use.
    - Compare aircraft, refrigerators, microwave ovens, mobile devices and other system and/or technology that is safely used by humans without understanding the mechanisms of its operation
  - Consider "black box" approach to metrics based on historical performance where complexity is too great for full explanation (and where unexpected system behaviors vis a vis a particular user are non-linear), but performance experience is sufficiently reliable to support explanation.
    - Payment card system suffers an historical/structural 2-3% default rate and also constant fraud levels which do not force abandonment of that sociotechnical system
  - Where security, IM or privacy system and/or technology is applied in dynamic interaction setting, consider UI frameworks and metrics that can be included in interaction decision trees that accommodate issues such as:
    - Safety (mobile phone use in cars)
    - Convenience (one touch ordering)
    - Attention courtesy (solicitation of single consent for multiple future uses of data)
      - But note limitation on such "multi-use consent' for deployments in the EU where such broad prior consent maybe held to be a "derogation" of a fundamental human right.
  - [Other?]
- References:

34. Privacy Legal Causes of Action – Intrusion on Seclusion

- Challenges
  - How might the subject system and/or technology help or hinder the accomplishment of protecting individual "privacy" as defined under one or more of the four traditional torts of privacy under common law?
  - When a system and/or technology purports to address "privacy" issues, what particular definition of "privacy" is applied?
    - If no such distinction or assertion is made by proponents of the system and/or technology, what particular harms are intended to be mitigated?
  - Is the applied "privacy" concept derived from recognized legal definitions of privacy rights and harms, or is it proposed as a "new" privacy right that is not yet recognized under law?
    - If so, what is the basis of the newly asserted right, and is it covered (in whole or part) by one or more of the legally cognizable concepts of privacy?
    - Does the system and/or technology confuse secrecy with privacy?
  - Does the system and/or technology affect the presence or absence of the elements of a cause of action for a given privacy tort, thereby validly constituting a "privacy" system and/or technology from a legal perspective?
    - The answer to this question may be relevant in evaluating the system and/or technology under applicable tests for admissibility into evidence of data derived from the system and/or technology.
    - Compare, Polygraph ("lie detectors") continue to be inadmissible under the court rules of many jurisdictions for failure to demonstrate relevance regarding truthfulness of statements.
  - [Other?]
- References:

34. Privacy Legal Causes of Action – Intrusion on Seclusion

- Candidate Analytical Frameworks/Metrics/Actions
  - One of four traditional privacy rights is the “right of seclusion.”
    - aka “the right to be left alone”
    - Popularly referred to as “unauthorized surveillance,” “eavesdropping,” "Peeping Tom," “wiretapping,” etc.
  - Consider framework that structures evaluation of subject system and/or technology’s ability to measure, provide evidence of and/or improve one or more of the elements of a legal cause of action (derived from the Restatement (Second) of Torts, or other authoritative resource), for a breach of a duty to forbear from actions that don't respect others’ “right to be left alone” by other persons and groups.
  - Does the system and/or technology stabilize or measure one or more of the following:
    - Did the defendant, without authorization, intentionally invade the private affairs of the plaintiff?
    - Would the invasion be offensive to a reasonable person?
    - Were the matters that were intruded upon “private” matters? and
    - Did the intrusion cause mental anguish or suffering to the plaintiff?
  - [Other?]
- References:

35. Privacy Legal Causes of Action – Publication of Private Facts

- Challenges
  - How might the subject system and/or technology help or hinder the accomplishment of protecting individual “privacy” as defined under the traditional tort of privacy under common law called “Publication of Private Facts?”
  - [Other?]
- References:

35. Privacy Legal Causes of Action – Publication of Private Facts

- Candidate Analytical Frameworks/Metrics/Actions
  - Does the system and/or technology provide measurement and/or mitigate the presence of one or more of the elements of a cause of action for “Publicity Given to Private Life”
    - aka Publication of Private Facts
  - The elements of this COA are:
    - The revelation by one person of private facts about another person
    - that are not of general public concern and
  - the act of which releasing would be highly offensive to a reasonable person
  - [Other?]
- References:

36. Privacy Legal Causes of Action – Defamation (Libel and Slander)

- Challenges
  - How does the reviewed system and/or technology help or hinder accomplishment of legal privacy right to be free from libel and slander (defamation) committed by third parties?
  - Note (and consider framework for) related tort (civil cause of action based on individual harm) of “false light,” which covers:
    - Publication by the defendant about the plaintiff
    - made with actual malice
    - which places the plaintiff in a false light and
    - which would be highly offensive to reasonable persons.
    - Note that “truth” is not a defense to “false light” claim.
  - Note also related tort in certain jurisdictions of “intentional infliction of emotional distress”
    - Potential claim when the “truth” of statements is raised as a defense to libel and slander - since true statements may still be actionable if uttered in contexts sufficient to constitute intentional infliction of severe emotional distress (tort of "outrage") or invasion of right to privacy.
  - [Other?]
- References:

36. Privacy Legal Causes of Action – Defamation (Libel and Slander)

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider framework structure to test whether the subject system and/or technology helps to address, measure or normalize one or more of the following causes of action for the privacy tort of "defamation" which is established upon a showing of the following elements:
    - Written publication (libel) or spoken assertion (slander) by defendant to a third person of
    - Defendant's false and defamatory language of or concerning plaintiff
    - That damages reputation of the plaintiff
    - Due to fault on defendant's part
  - If and to the extent that the subject system and/or technology can provide reliable measurement of one of the elements of this privacy tort (and/or other legally cognizable and enforceable privacy actions), it can also provide a monitoring function for security, IM and privacy system elements that can be applied to generate trust in the system.
    - UI "dashboard" meter representing such absence of privacy violations can help generate "Trust" in system, enhancing adoption.
  - [Other?]
- References:

37. Privacy Legal Causes of Action – Misappropriation

- Challenges
  - How does the subject system and/or technology help or hinder accomplishment and/or realization of the legal privacy right to be free from the harm of "misappropriation" committed by third parties?
  - Note also related tort (civil cause of action based on individual harm) of "conversion" (aka "theft")
  - Note that duty frameworks for evaluation of the efficacy of the system and/or technology in preventing misappropriation privacy harms may also be based on elements of various criminal violations (as opposed to civil causes of action in tort) established under federal, state and local laws such as theft, trespass (which is also a tort), computer fraud and abuse, etc.
  - See "Privacy Legal causes of Action – Statutory Duties of Care" Map
  - Does the system and/or technology help to provide measurements relevant to determination of presence or absence of cause of action for misappropriation, or otherwise help to prevent its occurrence?
  - [Other?]
- References:

37. Privacy Legal Causes of Action – Misappropriation

- Candidate Analytical Frameworks/Metrics/Actions
  - Elements of cause of action for misappropriation can provide framework for evaluation of the ability of a system and/or technology to help prevent or mitigate privacy harm.
  - Cause of Action for Misappropriation asks whether there was:
    - use by defendant
    - of plaintiff's picture or name
    - for defendant's commercial advantage
    - without plaintiff's permission
  - Does the subject system and/or technology enable or provide measurements, meta-data, or other evidence of the presence or absence of one or more of the foregoing elements of a cause of action for misappropriation?
  - If subset of metrics can be provided on dashboard in real time, it can help to provide dynamic feedback on reliability and consequent trustworthiness of system, viewed through the lens of the tortious harm.
    - Periodicity of meta-data metrics updates is dependent on frequency of interactions hosted by system.
  - [Other?]
- References:

38. Privacy Legal Causes of Action – Statutory Duties of Care

- Challenges
  - There are myriad statutes (and related regulations) in the US (39+ laws), states (50+ laws) and internationally that purport to protect privacy.
    - Many do so through mechanisms of data protection, rather than being harms based (like the traditional torts).
    - Under this approach, all data is treated as equally potentially sensitive.
  - What are the implications for the "harms gap" between established statutory duties of care for data protection and emerging potential "harms" from information misuses?
  - Do statutory duties of care in the privacy area protect regulated industries more than they protect data subjects?
  - For example, HIPAA proscribes the release of ALL healthcare data (as defined), without regard to diagnosis, subject, etc.
    - Compare tort of defamation under common law which relieved plaintiff of showing of scienter (bad intention) by defendant only in cases of false assertions of infections by venereal disease, but not other health conditions.
  - [Other?]
- References:

38. Privacy Legal Causes of Action – Statutory Duties of Care

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks for evaluating privacy fitness of examined system and/or technology based on various relevant statutory authorities
    - Ref: Privacy Harms Correlator Tool prepared by Scott David in work with ABA and WEF.
  - Note that existing statutes typically lag behind technology and do not protect against new and emerging harms.
    - As a result, compliance with their terms may do more to limit the liability of data handlers and users (who can align their behaviors with the requirements of the anachronistic laws) than to limit the emerging harms to data subjects (who are left without a venue for the assertion of emerging privacy harms that are not yet legally cognizable.
  - Ref: Compare and apply multiple "negative spaces" of statutory protection described in "Non-Legality in International Law – Unruly Law" by Fleur Johns (Cambridge, 2013).
    - Considers distinctions between and among:
      - extra-legal
      - illegal
      - prelegal
      - post legal
      - otherwise non-legal
    - Issues and harms and relationship to "legal" definitions of harms.
  - [Other?]
- References:

39. Information Channel Integrity (Beyond Data Channel Integrity)

- Challenges
  - IM expectations are based on definition of "Identity."
  - One definition of personal identity (a "social theory" of identity) might characterize it as being entirely an emergent phenomenon of the lifetime accumulation of feedback loops (sculpted by the narratives of culture, education, context, experience, etc.) of individual expression (action) and perception (re-action).
    - This perspective would suggest that there is no such thing as feral identity – rather it is entirely a social phenomenon.
  - Consistent with this view, "Identity" has at least two aspects for each person – the data subject's view of their identity (self identity) AND a separate (but related) third party's view of the data subjects identity (social identity or reputation).
    - There are 4 identities in operation in any dyadic social interaction (2 internal and 2 external)
    - Degree of integration of individual external and internal "identities" of a party is relevant in structuring reward and penalty systems, self actualization recruitment strategies, consumer expectations and a host of other adoption-affecting phenomenon associated with security, IM and privacy systems.
    - Emerging "social theory of identity" brings forward work of Erving Goffman, Julian Jaynes, Douglas Hofstadter, Hegel and others and work in so-called "mirror neurons" in considering strategies for recruitment of internal sense of self in system and/or technology deployments
  - Integration of internal and external identity can be fostered if data subject is provided with ability to monitor and affect degree of channel integrity of input (perception) and output (communication) channels relevant to their communications.
  - All current common law and statutory and other FIPPs-based privacy approaches are based upon efforts to increase the reliable and predictable integrity of individual perceptual and expressive communication channels.
    - All 4 privacy torts and all statutory data protection approaches can be described as seeking to "harden" individual communication channels in different contexts.
  - How can the reviewed system and/or technology help or hinder accomplishment of Channel Integrity?

39. Information Channel Integrity (Beyond Data Channel Integrity)

- Candidate Analytical Frameworks/Metrics/Actions
  - If and to the extent that the social theory of identity is efficacious in a given context (which remains a conjecture), does the system and/or technology offer insight and/or measurement into the integrity of individual data subject expression (output) or perception (input) that can help to provide coherent "identity" signal for consumption by individuals and third parties that are useful to help solve the challenges of security, IM and privacy.
    - Note that LOA structure of OMB 04-04 and 800-63 can be seen as stabilizing the "expressive" channel associated with assertions of individual identity
  - Where "identity" is gainfully viewed as emergent (in whole or part) from input and output channel integrity, the hard problems of identity management become more manageable (and measurable) problems of monitoring and hardening communication channels of expression and perception.
    - Suggests that first amendment (freedom of expression (out) and access to information (in)) rather than 4th amendment (limitation on admissibility of evidence derived intrusively) may be appropriate constitutional provision for framework of individual information privacy
    - Ability of organization to promise and deliver consistent channel integrity will permit that organization to be trusted with identity, and will invite that institution to compose a narrative for existential protection of digital identity. Will that be a commercial narrative? A governmental narrative? A stakeholder-derived self-regulatory narrative? Will the default existential narrative be composed with intention or as an incident to system function? This latter question is a source of some of the neuroses associated with emerging autonomous and AI systems, which are related to security, IM and privacy issues.
    - Shannon entropy can be used to help measure channel integrity under his "quantitative theory of information" (which examined how much information can be pushed through a given channel)
  - It is easier and more effective to address emergent phenomenon by addressing the underlying drivers of the phenomenon.
    - Does the reviewed system and/or technology treat the disease (therapeutic), or merely the symptoms (palliative).

40. Risk Appetite/Entrepreneurial Risk

- Challenges
  - Assumption of Risk.
    - Different individuals and organizations have different appetites for risk in their interactions and express those in their actions.
      - Not everyone chooses to skydive.
  - Risky Behaviors.
    - Different individuals and organizations can be perceived by others as engaging in more risky behaviors.
    - Note biological causes can be tested for - Toxoplasmosis
  - Some organization business models are based on certain set of risk assumptions, upon which reliance has been placed and planning (insurance, swaps, safety etc.) and investments have been made.
  - How will the system and/or technology affect and/or help measure these individual and organizational risk appetites, expressions and perceptions when manifested in security, IM and privacy contexts?
  - [Other?]
- References:

40. Risk Appetite/Entrepreneurial Risk

- Candidate Analytical Frameworks/Metrics/Actions
  - Engagement by individuals and organizations with risk, and the perception of such entities risk appetite, is multifaceted, and varies from one type of risk to another.
    - Useful frameworks should specify type of risk involved, and clarify limits
  - risk-taking in one domain is frequently perceived to suggest risk-taking in other areas
  - Does the system and/or technology consume or account for risk metrics from external sources (such as when credit reports are used for hiring decisions, etc.)
  - In what aspect of risk engagement business strategy is the system and/or technology designed to be deployed, and what are the policy components necessary to succeed in that deployment. Examples of risk engagement strategies of organizations include:
    - Risk Mapping
      - Situational awareness (e.g., data visualization) needs incentive to drive data inputs from stakeholders
        - » E.g., Traffic reports capturing 50% of drivers are useless.
    - Risk Mitigation
      - ISP TOUs regarding intermediary liability
      - Standards (PCI-DSS for payment cards shirt risk to edge of system where greatest interaction density)
    - Risk Mining
      - Insurance (turns risk into entrepreneurial risk that can share benefits with stakeholders who invest in premiums for possible payout on loss event. Compare insurance and gambling ROI propositions).
      - Practice of law (profession would not exist if not for risk)
    - Risk Monetization
      - Arbitrage
      - Short selling markets
      - Credit default Swaps markets

41. Provisional/Edge Governance

- Challenges
  - All organizations have an operating "edge"
    - Not a physical edge, but an "umbra" and "penumbra" of control
    - E.g., General Motors has tens-of-thousands of subcontractors – Where is the "edge" of GM?
      - What are the relevant "gradients" of governance from the board room to the outer edge of a company?
      - What are the nature of the measurements of data/information/identity governance gradients that can help provide insight and "control" of security, IM and privacy-relevant governance decisions by an organization?
  - Inside system edge (e.g., a company with a single business location),
    - risk is lower and control/leverage is higher
  - Outside of system edge . . .
    - Measurements fail
    - Controls diminish
    - Leverage weakens
    - Governance fades
    - Dependency grows
    - Risk increases
  - How can the reviewed system and/or technology help to address the governance challenges at the "edges" of a system.
  - How should the "edge" of the system be defined in the context of security, IM and Privacy concerns:
    - Technical edge
    - Business edge
    - Legal/responsibility/liability edge
    - Physical edge (hardware "ownership?")
    - Other?
- What is impact of outsourcing/cloud sourcing on deriving and applying metrics of gradients?

41. Provisional/Edge Governance

/Metrics

- Candidate Analytical Frameworks/Metrics/Actions
  - Information supply chains in massively interoperable and distributed information networks are becoming exponentially more complex and extended – and opaque. We have moved well beyond the just-in-time inventory innovations of the last century to an expanding "too big to fail" organizational symbiosis of outsourcing and cloud sourcing, across multiple domains (that can sometimes be confused for parasitism!).
  - In the massively interoperable ICT space, that "strange attractor" of scaled systems(in biology called "Cope's Rule"- Organisms tend to get bigger), provides an irresistible pull on existing companies and governments to cede an increasing portion of their essential business functions to third party networks.
    - » Brexit is an example of a reluctant governance symbiont
  - Companies and governments outsource many essential functions to third party networks:
    - » Shipping, Advertising, Payroll, Accounting, Data Processing, Etc.
  - When these functions are "outsourced" they are no longer unique qualities of given organization. They are generic.
    - » What is left at the "core" of the business or governmental organization that cannot be outsourced or cloud sourced to generic third party networks?
  - Risk at edges of any organization forces process and product innovation
- At edge, normal operations migrate to "Provisional Governance" (see REF) such as:
  - Standards Development
    - » define actions and systems and seek normalization
  - Harms and Risk Management
    - » focus on harms and risk itself because they are "known" quantities even if causation not yet established at system edge
  - Performance Measurement
    - » Provides feedback for whether provisional governance is "fit for purpose" in addressing risk and as candidate for permanent governance through policy standards
  - Clarifying Interests
    - » define relative rights (through property constructs or co-regulation structures)
- How well suited is given system and/or technology to serve needs of governance in "provisional governance" setting?
  - REF: "Governing Failure," by Jacqueline Best (Cambridge, 2014)(Review of IMF and World Bank through "Provisional Governance" lens above.

42. Institutional Collision (Risk Commons/Zero-Sum Setting)

- Challenges
  - In addition to challenges of "provisional" governance at the edge of organizations (that are in the process of being absorbed (aka "dis-intermediated") by serial delegations of function to outside organizations), there are additional P2P collisions that take place among the group of unfortunate organizations (commercial, governmental, etc.) that are in the process of being dis-intermediated by massively interoperable information networks.
    - security, IM and privacy issues arise where institutional organization is changing
- What happens to security, IM and Privacy when organizations encounter new competitive surroundings without inter-governance
- Surroundings include:
  - New competitors (including new cybersecurity adversaries for governments, etc.)
  - New sectors (an exposed cybersecurity, privacy flank)
  - New jurisdictions (new types of interactions)
  - New market demand
- Surroundings introduce:
  - New risks
  - New costs
  - New resource demands
  - New strains on internal operations
- What are the ways in which the reviewed system and/or technology helps to address issues of institutional collision resulting from conflicts associated with shared use of information infrastructure?
- Does the system and/or technology provide performance metrics or other meta-data that can help to establish premium setting or claims policy for cybersecurity insurance among peer ICT participants?

42. Institutional Collision (Risk Commons/Zero-Sum Setting)

- Candidate Analytical Frameworks/Metrics/Actions
  - Outsourcing of functions to third party networks is done pursuant to standard contracts and policies
    - TOUs, TOSs, Master Service Agreements, Standard shipping agreements, etc.
  - Standard contract terms offer vehicle for normalizing duties among P2P relationships.
  - Shared challenges of disintermediation can lead to cooperation among competitors to address shared risks
    - Trade associations
    - Selling cooperatives
    - Buying cooperatives
  - In what ways does the candidate system and/or technology help to measure or address the shared security, IM and Privacy challenges of peer organizations that are in the process of being dis-intermediated and occupy a shared "risk commons."
  - Insurance is an example of mechanisms for pooling of risk
  - [Other?]
- References:

43. Power Law Policy

- Challenges
  - There are risks that result from applying Gaussian (normal) distribution analytics for complex systems that display non-linear behaviors
  - How does this system and/or technology help to or lend itself to integration into multi-institutional settings to enable power law policy approaches?
  - Related to “Scaling” Map
  - [Other?]
- References:

43. Power Law Policy

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider use of fractal/power law distributions of behaviors of complex sociotechnical security, IM and Privacy systems (rather than normal distributions) to help inform security, IM and privacy policy and system and/or technology deployment strategies
    - Financial markets "outlying events" could be normalized with change in model from Gaussian distributions of events to power law distributions
      - the problem is that they are not sufficiently predictive for current market configurations
    - see "insurance" reference below for alternative risk spreading strategy based on shared, rather than proprietary, risk arbitrage
      - What happens to the "prisoner's dilemma" in game theory when the prisoners know the same information as the guards?
  - Bigger tails in power law curves, but how fund mitigation of remote risks?
    - Do we need "GAVI Fund" for orphaned cyber security, IM and Privacy risks
    - Is insurance/pooled risk a better approach to deal with unknown unknowns?
  - "Risk Commons" approach - Drive toward cooperative structures to resource remote security, IM and Privacy structures.
    - Standards
    - Sectorial – insurance, neighborhood watch
    - CERT
  - If Power Law Policy approaches are found to be efficacious for security, IM and Privacy, in what ways does the system and/or technology support such policies?
    - E.g., block chain based ledgers can help preserve mutual promises on which insurance and self-insurance undertakings are based.

44. Philosophical Assumptions

- Challenges
  - The laws of a country/region reflect the values, beliefs, customs and norms of a population.
  - In all cases, those laws reflect and reinforce those populations' behaviors and beliefs, even if they were first made effective in different historical contexts and economic and political circumstances.
    - Laws are an historical/anthropological record of a country's norms and beliefs
  - The sources of such cultural norms, etc. are complex, but examination of the roots of those norms can be helpful in understanding and anticipating future policy decisions made by representatives of that population.
  - Where individuals or organizations come into contact with one another across national or regional boundaries, those political borders can act as surrogates for corresponding philosophical boundaries that, among other things, affect how a given population views the relationship of the individual and the group – existential issues bound up in IM and Privacy system and/or technology deployments
    - US/EU "Safe Harbor" and "Privacy Shield" are efforts to bridge philosophical divide on data that can be used to create PI.
    - GDPR represents a unilateral imposition of FIPPs rules on affected interactions (FIPPs rules are consistent with Hegelian and Kantian philosophy that informs EU continental law. Query whether GDPR is consistent with Locke and Utilitarian notions deployed in US?
  - How does system and/or technology address or anticipate regional differences in philosophy/law that affect security, IM and Privacy?
    - If it does not, how will that constrain its impact (See "Scope" and "Scale" Maps).
  - [Other?]
- References:

44. Philosophical Assumptions

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks that make explicit differences in fundamental notions of personhood to help inform information sharing architectures that can better anticipate the real-world operating landscape for ICT.
    - Ref: OECD Paper entitled "Personhood," 2009.
      - EU policy on personal data is informed by Hegel, while Locke informs US and Commonwealth policy.
    - Consider philosophical "arbitrage" opportunities associated with differentials
      - Like venue shopping in tax planning for IP
  - Consider inconsistent laws through lens of varying notions of relationship of individual and group (company, government, etc.), and ask whether given system and/or technology can help bridge the gap
  - [Other?]
- References:
  - Ref: "Custom as a Source of Law," by David Bederman (Cambridge, 2010).

45. Treaties and Trade Agreements

- Challenges
  - What assumptions are made about operation and use of the reviewed system and/or technology in international markets, and about regulatory considerations in cross border deployments of the system and/or technology?
  - Is the system and/or technology “fit for function” in multiple markets?
    - If not, are there treaties or trade agreements that can help to identify bridges across jurisdictions and markets across which the system and/or technology might be deployed?
  - [Other?]
- References:

45. Treaties and Trade Agreements

- Candidate Analytical Frameworks/Metrics/Actions
  - Treaties and trade agreements are a potential source of scaffolding for building security, IM and privacy frameworks across national borders.
    - They establish “interoperable” policies across jurisdictions that can support related international expansions.
  - In analyzing system and/or technology fitness for deployment and international scale function, consider both specific security, IM and privacy provisions of existing treaties and overall structure of treaties that depend on evaluation and sharing of data about people and/or related intangibles
    - Global health treaties
    - Tax treaties
      - Note that income tax treaties “source” income differently depending on how it is derived (e.g., dependent services, independent services, property, etc.).
      - Query whether tech system under review creates “nexus” and/or “permanent establishment” for tax treaty purposes?
    - IP treaties
  - [Other?]
- References:

46. Industry Standard Contracts

- Challenges
  - Does the subject system and/or technology depend upon the terms of existing industry standard contracts and duties (private regulatory construct).
    - HIPAA and GLB drive toward standardization in the terms of data handling in their respective industries
  - Are the terms of such standard agreements sufficiently similar across industries and sectors so that the subject system and/or technology will enjoy adoption across sectors?
  - Does (or can) the system and/or technology establish/enable system metrics that can support objective allocations of responsibility for system performance and liability constructions (such as safe harbors, hold-harmless, indemnities, insurance, etc.) based on performance against standardized duties established by one or more of:
    - Government legislation/regulation
    - Government regulatory standard that normatively cross references a self regulatory standard
    - Stakeholder self-regulatory standard
    - Multilateral contractual standard duty (such as mutual hold harmless term)
  - [Other?]
- References:

46. Industry Standard Contracts

- Candidate Analytical Frameworks/Metrics/Actions
  - Where a security, IM or Privacy system and/or technology is developed for deployment in a given sector (particularly a regulated sector such as healthcare, financial services, education, etc.) it may also be helpful in another sector if the industry standard contracts in that other sector are sufficiently similar to invite inter-sector function.
    - E.g., Consider health insurance at the intersection of GLB and HIPAA?
  - Where sectorial forms of agreement are silent on a particular issue, it provides the opportunity for the development of new forms of agreement that can be standard across industries
    - New cloud service contracts are uniform across sectors, etc.
  - Does the system and/or technology generate new metrics or insights that could form the basis for the establishment of standard legal terms (and/or legal duties) that could operate across the security, IM and privacy systems of organizations operating in multiple sectors?
  - [Other?]
- References:

47. Policy Interoperability

- Challenges
  - Is the policy (privacy policy, TOU, license to tech, etc.) associated with the subject system and/or technology of a form and type that can work well with other:
    - industry standard policies
    - regulations (which are de facto policies)
    - existing supply chain standard contracts
    - insurance requirements
    - securities law standards?
  - [Other?]
- References:

47. Policy Interoperability

- Candidate Analytical Frameworks/Metrics/Actions
  - Frameworks of policy interoperability can facilitate rapid adoption of technologies that might otherwise be delayed as local/sectoral laws are reviewed and evaluated for application to the new system and/or technology
    - E.g., Many communities do not permit Uber or Airbnb to operate (under local licensing laws, employment laws, etc.), even though the infrastructure of the business is just a contract and a user interface.
  - Frameworks of policy interoperability can help make risk analysis more granular by unpacking the specific legal risks of a system and/or technology, and separating the unique risks from time-tested risks
    - Boilerplate provisions, and their respective risks, can follow traditional patterns even when applied to new system and/or technology, reducing risk of liability, failed performance, etc.
      - E.g., use standard notice provisions, bankruptcy provisions, change of law provisions, etc.
  - [Other?]
- References:

48. Public Company Disclosure Requirements

- Challenges
  - For companies that are subject to mandatory reporting obligations, how can the subject security, IM or Privacy system and/or technology help or hinder the satisfactory accomplishment of those obligations?
    - SOX
    - SEC
    - OSHA
    - ADA
  - Distributed transparency. Will the operation of the security, IM or privacy system and/or technology produce and/or reveal information outside of the control of the reporting company that must then also be taken into account and/or disclosed in public filings of public companies.
    - Will distributed security, IM and privacy architectures undermine efforts and expectations of traditional businesses to be able to "control" information
  - How might the operation of the system and/or technology affect accounting conventions:
    - Setting levels of reserves against risks
    - GAAP for digital data assets
    - Valuation of "customer lists"
    - Amortization of security, IM costs
  - [Other?]
- References:

48. Public Company Disclosure Requirements

- Candidate Analytical Frameworks/Metrics/Actions
  - Frameworks based on certain mandated data flows associated with compelled disclosure can help to inform design, development and deployment of security, IM and Privacy technologies
  - Compare the standardization of state data breach notice letters that quickly occurred to reduce costs of data breach response across industries, and the relationship of those responses to other disclosures
  - Consider both governmentally compelled disclosure obligations (SOX, SEC, etc.) and privately adopted obligations (PCI-DSS, certification mark programs, etc.)
  - [Other?]
- References:

49. FOIA and Sunshine Laws

- Challenges
  - For governments agencies using the proposed system and/or technology for security, IM and privacy, how will it affect their operations and their disclosure obligations?
    - Will the system and/or technology produce meta-data and/or reports that will be subject to mandatory or requested disclosure?
    - What will be the effect on operations and government decision making given the presence of the new meta-data, etc.?
  - [Other?]
- References:

49. FOIA and Sunshine Laws

- Candidate Analytical Frameworks/Metrics/Actions
  - Existing FOIA and Sunshine laws can provide helpful frameworks for the analysis of the settings in which the operation of the subject security, IM or Privacy system and/or technology could result in new or different reporting obligations of governmental entities.
  - Massive distribution of information systems reduces control of information for every organization, including governments, making information available beyond control of organization.
    - Frameworks of system and/or technology analysis should include consideration of effect of FOIA and/or inadvertent disclosure of "honey pots" of security, IM and privacy related information created by operation of the system and/or technology
  - [Other?]
- References:

50. Evidentiary Rules

- Challenges
  - Does the subject security, IM or privacy system and/or technology produce new or additional metrics and/or metadata, and what are the implications from the perspective of formal evidence rules?
  - For block chain-based architectures, what are the elements of the system performance metrics that will be affected by enhanced block chain evidentiary reliability (when and as such qualities are established)?
  - What are security, IM and privacy system elements that are NOT enhanced by block chain, and how does that affect system performance?
    - Does the answer vary with different contexts (e.g., under different laws, etc.)
  - How does the output of the subject system and/or technology align with the Federal Rules of evidence?
    - What are its implications for discovery in civil and criminal cases?
  - What are fourth amendment implications of deployment of the tech?
    - Consider data equivalent of thermal scan as “plain view?” Administrative search? Other exceptions to warrant requirement.
  - [Other?]
- References:

50. Evidentiary Rules

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks that recognize and help unpack the relationship of meta-data, evidence rules, and legal liability.
  - Introduce frameworks that draw in inquiry toward consideration of issues of prohibition against self incrimination under the 5th Amendment.
    - Better to anticipate that issue than to react to it.
  - [Other?]
- References:

51. IP Review

- Challenges
  - Data and information (including that subset of data and information that is associated with the operation of security, IM and privacy-related system and/or technology) is NOT itself protected by copyright, patent, or trademark laws.
    - Trade secret protection, the fourth category of IP, has a closer relationship with data and information traditionally applied in security, IM or privacy settings, as a consequence of their co-dependence on secrecy.
      - See "Death of Secrecy" Map.
      - It is recognized that aspects of a subject system and/or technology may be dependent upon "secrecy" (such as public key encryption, etc.), and that a subset of that secret information may qualify for "trade secret" protection under relevant state law. In those cases, where "trade secret" protection is part of the value proposition of a system and/or technology business, relevant state laws should be consulted to confirm that such protection will be available in accordance with expectations.
        - » These issues may become more challenging as distributed information systems give rise to distributed governance which gives rise to such shared infrastructure as distributed ledgers (block chain), distributed warehouse functions for distributed inventory (e.g., eBay,™ Amazon™), distributed fleet management (Uber™), infrastructure management (Airbnb), and their corresponding IM and Privacy issues.
  - In the absence of IP protection, does the system and/or technology make correct assumptions about copyright, patent, TM and trade secret protection for its operation that are consistent with desired deployment?
    - Will the system and/or technology get shut down in the "patent thicket?"
  - Will the broad adoption of the system and/or technology lead to "natural monopoly" in the networks IP infrastructure that will affect security goals?
  - What are open source (copyright) or open standard elements that could aid in adoption?
  - Does operation of the system and/or technology undermine or "abuse" IP rights?

51. IP Review

- Candidate Analytical Frameworks/Metrics/Actions
  - To facilitate broad adoption consistent with IP rights, frameworks of IP issues should be applied to test the IP operating assumptions of the subject security, IM or privacy system and/or technology.
  - What are copyright assumptions and implications of the subject system and/or technology?
    - Is “open source” licensing of copyrightable elements of the system helpful to achieving broad adoption?
    - Will there be restrictions on copyright licensing that will undermine technical interoperability of the system, hampering security, IM and privacy goals.
      - Compare issue of “portability” of social graph across multiple social networks
  - What are patent assumptions and implications of deployment of the system and/or technology?
    - Will deployments of the security, IM or Privacy system and/or technology involve interaction with other patented technologies? If so, will there be the potential for infringement of patent rights?
    - Is the security, IM or Privacy system and/or technology a compelling candidate around which to gather a standard setting effort with the consequent production of standard specification and the cross licensing of “Necessary Claims” of Patent right.
  - What are trademark assumptions and implications of deployment of the system and/or technology?
    - Will deployments of the security, IM require TM license associated with inputs of products and services?
    - Will the security, IM or privacy system and/or technology benefit from a Certification Mark program for system users to be able to identify its conformity to third party standards of security, IM or Privacy.
  - What are trade secret assumptions and implications of deployment of the system and/or technology?
    - If trade secret protection is relied upon to protect the information entropy of security, IM or Private data, laws of relevant jurisdictions should be consulted to affirm needed protection.
  - [Other?]
- References:

52. Anti-Trust and Competition Laws

- Challenges
  - Successful security, IM and Privacy systems that are deployed on distributed networks, such as the Internet, require coordination at various levels among multiple parties to be successful.
    - Certain types of coordination among competitors is prohibited under relevant anti-trust (US) and competition law (EU) and other relevant laws.
  - Will the subject security, IM or Privacy system and/or technology require (or foster) the exchange of information among competitors in a manner that is inconsistent with anti-trust and competition laws?
  - [Other?]
- References:
  - "Standardization Under EU Competition Rules and US Antitrust Laws – The Rise and Limits of Self-Regulation, by Lundqvist, Elgar Publishing, 2014
  - See ref: Monopsony in Law and Economics

52. Anti-Trust and Competition Laws

- Candidate Analytical Frameworks/Metrics/Actions
  - Anti-trust laws establish criteria for a number of “safe harbors,” as well as a variety of “per-se” violations, that help to bound and clarify the types of behaviors in which competitors can engage together.
    - Frameworks for security, IM and Privacy network policy should include clarifying statement describing proscribed and expected behaviors of participants in the network
      - Samples of language can be gleaned from documents of technical standard setting organization (SSOs)
  - Consider how the system and/or technology (and its optimal network structures) will effect and affect market structures tending toward both Monopoly (single provider) and Monopsony (single consumer) situations.
  - Review and consider structures and competition law issues in other third-party service and intangibles networks
    - Shipping
    - Payroll services
    - Advertising
    - Cloud services
    - Federated identity
    - Consumer finance/payment cards
  - [Other?]
- References:

53. Constitutional Implications

- Challenges
  - The US Constitution establishes standards for various elements of interactions between the US Government, the States and their citizens
    - Other jurisdictions have similar foundational documents
    - Many of these interactions are related (directly or indirectly) to security, IM and privacy concerns.
  - Does the subject system and/or technology invoke potential constitutional concerns if deployed by (or on behalf of) a governmental entity?
    - What about when deployed by a commercial entity that maintains data later made available to a government entity?
  - [Other?]
- References:
  - See Atlas entries for various specific constitutional provisions

53. Constitutional Implications

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks for analysis under constitutional provisions potentially relevant to security, IM and Privacy technologies:
  - U.S. Examples include (but are not limited to)
    - First amendment
      - free association, access to information, freedom of expression, prior restraint?
    - Fourth amendment
      - Does application of 4th amendment jurisprudence provide a floor or a ceiling for security, IM and Privacy rights?
      - Can it really be considered as aspirational, given its intended role as a evidentiary rule?
    - Equal protection
    - Due Process (5th and 14th amendment)
    - Self incrimination
  - See constitutional documents in other countries
  - [Other?]
- References:
  - See specific Atlas entries for detailed treatment of US constitutional rights

54. Regulatory Capture 2.0

- Challenges
  - Was the subject security, IM or privacy system and/or technology generated to operate within a particular industry sector (e.g., banking, Telco, healthcare, military), where the assumptions are different than in other contexts?
    - Will that legacy cause scaling and/or operations problems on deployments in other sectors
  - Will the successful deployment of the system and/or technology result in a creation of *de facto* standards of behavior for stakeholders and participants, that will constitute a form of "self-regulatory capture" (aka "natural monopoly" – where single provider makes sense)
    - Compare a water utility or a subway system in a city and where regulation replaces competition as the anti-monopolistic strategy
      - Note challenges of cross-border sovereign "regulation"
    - What are the implications of such "self regulatory" capture where the consequent rules and policies guiding use of the security, IM and privacy system and/or technology have social, cultural and political implications?
      - What are the distributed governance mechanisms that can be brought into service of distributed value of networks?
        - » Consider various forms of reputation systems
          - See Credit Union and "Micro-lending" with P2P bankers
          - See other "neighborhood watch" type systems
          - Consider market-based structure (e.g., using spreads in credit-default markets as less conflict-prone replacement for "rating agencies?)
  - [Other?]
- References:

54. Regulatory Capture 2.0

- Candidate Analytical Frameworks/Metrics/Actions
  - Scale, scope and regulatory issues are in flux in security, IM and privacy analysis because increases in the global ability to collect, process and transfer data, and global information network interoperability outpaces regulatory efforts of government, and even self-regulation of trade associations.
  - Recognize regulatory gaps for new security, IM and Privacy technologies as opportunities to consider frameworks that map the regulatory landscape for a given security, IM or privacy system and/or technology to include several sources:
    - Government regulation
    - Existing industry self-regulation
    - Potential system and/or technology-based self regulation
      - Involvement of stakeholders in self regulation
      - Selling cooperative or buying cooperative models for information arbitrage
      - REF: "The Five Stages of Self Regulation" Ronit and Porter
    - Regulation, like nature, abhors a vacuum. Stakeholder self regulation can fill the gap.
    - Institution is artifact of process to formalize the relationships that take place in the gaps
      - See "General Theory of Institutional Change" by Shiping Tang (in bibliography).
  - [Other?]
- References:
  - See "General Theory of Institutional Change" by Shiping Tang (in bibliography).
  - REF: "The Five Stages of Self Regulation" Ronit and Porter

55. Compliance Gaps

- Challenges
  - Does the technology/system lend itself to compliance audit, and other mechanisms to test performance against specifications?
  - How is the subject security, IM or privacy system and/or technology designed to enhance conformity to performance parameters set for the system and/or technology by humans and institutions that depend upon it?
  - What risks are created through the use of the system and/or technology in ways that are not measured by the system and/or technology?
    - What gets measured gets done, but the mischief (of intentional, negligent, and unanticipated harms) occurs in the unmeasured dimensions of system performance.
      - » Example of lack of temperature sensors in battery compartments on aircraft
  - Does the system/technology provide opportunities for measurement of behavior and interactions of humans and institutions regarding their performance under trust framework rules and policies (as well as those of "background law")
  - [Other?]
- References

55. Compliance Gaps

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks that address potential compliance issues (of humans and institutions) at level of granularity appropriate to a given element of the security, IM or privacy system and/or technology.
  - Consider continuous process approach to stakeholder engagement to dynamically address gaps
    - Create guidance to fill rules gaps
      - Instructions, training, checklists
  - Craft frameworks of incentives (and penalties where appropriate) to support behaviors that can coax discretionary decisions to support the "spirit" of the regulation of other compliance source.
  - [Other?]
- References

56. Conflict Resolution

- Challenges
  - All interaction systems experience some degree of conflict at multiple and varying levels among participants in the course of their operation.
    - What is the nature of the conflicts that might arise from the use of the subject security, IM or privacy system and/or technology?
  - Is the system and/or technology designed in a way to facilitate the resolution of disputes
    - forensics,
    - evidentiary data,
    - transparency,
    - audit, etc.
  - [Other?]
- References
  - Ref. Dictionary of Conflict Resolution, edited by Douglas Yarn, Jossey-Bass Inc. Publishers, 1999)

56. Conflict Resolution

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks that define conflict to include “Pre-dispute” period as way of avoiding costs of later resolution of avoidable conflicts
    - See work at U. Mass Conflict Resolution Center
  - Consider trust framework elements that help reveal potential conflicts among users and other parties as a result of the operation of the system.
    - Predictive analytics applied on a group basis
  - Consider frameworks that can help to reveal shared interests and exposures among participants that can lead to cooperative approaches to risk reduction associated with conflict resolution
    - Beware implications of standard clauses
      - See e.g., “no class action” clauses in financial arbitration terms.
  - Consider frameworks of conflict resolution that can help cohere P2P stakeholder interests
    - Common pool for payment of liquidated damages for small claims.
      - Compare FDIC insurance premiums of banks, but here for non-catastrophic losses in system
      - Compare pooled “by-catch” strategies in fisheries management.
    - Consider how joint stakeholder rulemaking process can become driven by enforcement function
      - Create feedback loop in system to inform future stakeholder rulemaking
        - » Compare use of XBRL in US Congress legislative impact analysis and SEC reporting
  - [Other?]
- References

57. Attention Economy (Episodic Attention)

- Challenges
  - What level of attention is needed from data subjects, users and operators in order for the subject security, IM or Privacy system and/or technology to achieve its optimal performance?
    - Is this level of attention realistic?
  - Consider “attention” from perspectives of both within an individual engagement “session” and among multiple engagement “sessions”
    - Providing notice and seeking consent of every use of data about a person could be equivalent to a “denial of service” attack on the person’s attention
      - Note European Court holding that broad pre-consent can be voided as violation of fundamental human rights.
  - [Other?]
- References

57. Attention Economy (Episodic Attention)

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider alternative structures, benefits and down-sides of various filters, intermediations, agencies and other methods for "delegation of attention" by persons and institutions
  - Consider how policies and reliable systems of "Tools and Rules" can help mitigate "interruption" of users by "substituting trust for attention"
  - Consider structures of various sorts of agency relationships as guide to framing the delegations needed to navigate the attention economy.
    - Consider special duties of various forms of "fiduciary" agency and gradations of trust that might be fostered
    - Consider making explicit the "percentage of conflict of interest" in an agency relationship to help guide decisions of data subjects as principals.
      - Put the conflict percentage on a sliding scale
      - Compare non-fiduciary role of brokers under 1934 Securities and Exchange Act with fiduciary role of investment advisers under the 1940 Investment Advisers Act
        - » see Dodd Frank discussions of same).
  - [Other?]
- References

58. Market Behaviors

- Challenges
  - In the proposed configuration and operation of the subject security, IM or privacy system and/or technology, what assumptions are made about market behaviors associated with adoption and operation?
    - Consider effect on markets *as markets*, rather than "economic" considerations addressed in another map
  - For example:
    - Effect of data as value-transfer medium
    - Cultures of different markets
    - Efficiency considerations
    - Emergent network effects
    - Accounting differences among industries
    - Effect of legacy system uptake delays
    - Etc.
  - [Other?]
- References

58. Market Behaviors

- Candidate Analytical Frameworks/Metrics/Actions
  - Market research on market operations should continue to be developed to gauge the unique elements of market behaviors in the context of markets trading in rights associated with security, IM and Privacy issues and markets dependent on those rights
  - Consider, e.g.,
    - Variable deployment/adoption curves in hardware, software and effect of legacy solutions.
    - Piggybacking
    - Bundling
    - Freemium Models
    - Etc.
  - [Other?]
- References

59. Game Theory and Other Modeling Assumptions

- Challenges
  - What game theory and other models were applied in the design and development of the security, IM or Privacy system and/or technology?
    - How and to what extent were they applied to address the information arbitrage differentials that are intrinsic in security, IM and privacy rights management activities?
    - How do you manage abuse of perspective/conflict of interest in the system supported by the subject technology/system?
  - What are the additional value propositions that can be gleaned from extension and additional attention to the models applied?
    - What are the criticisms of those models that can inform performance testing?
  - [Other?]
- References

59. Game Theory and Other Modeling Assumptions

- Candidate Analytical Frameworks/Metrics/Actions
  - Promoters of security, IM and Privacy system and/or technology should be explicit about the models applied in designing and developing their systems
    - Reveals assumptions of systems
    - Invites scrutiny of theoretical bases of systems
  - [Other?]
- References
  - Ref: “Telecommunications Network Economics: From Theory to Applications,” Maille and Tuffin, (Cambridge Press, 2014)

60. AI and Autonomous Operation

- Challenges
  - Does the security, IM or privacy system and/or technology rely for its operation on feedback or feed-forward loops that inform further operations in a manner that is characteristic of autonomous and AI systems?
    - Are those systems and operations viewable and auditable, or are they "black boxes"
    - Can the feed back be dynamically tuned to accommodate different contexts of system operations?
      - Does vesting that dynamic tuning in the autonomous operation of the system convert a feedback system into a feed forward system with different harm potential?
  - Does the proposed system and/or technology provide output that is helpful in other machine learning, autonomous system, or AI contexts or otherwise facilitate their operation?
    - What are the implications of cascading cross references among AI and/or autonomous systems
    - Does the added complexity hinder efforts to analyze the potential likelihood and severity of harms associated with the system in real world settings?
  - Can the technology or system produce data that can be applied in AI systems in real time?
    - What is the "refresh rate" of the data provided?
    - How can accuracy and veracity be tested in real time?
    - Compare "flow" processing vs. "batch" processing in chemical manufacturing.
  - [Other?]
- References

60. AI and Autonomous Operation

- Candidate Analytical Frameworks/Metrics/Actions
    - What protections are built into the security, IM or privacy system and/or technology to prevent runaway feedback or feed-forward in operations?
        - Prevent security, IM cascading defaults
    - Are protections of the system and its users that are roughly equivalent to Asimov's "three rules" present in the system, and if so how are they manifested in the system?
        - Consider limitations of Asimov rules in institutional contexts
        - Consider limitations in socio-technical systems contexts
    - Consider frameworks to establish shared default settings on how will independent, auto-catalytic, machine learning algorithms applied to security, IM and Privacy issues work and adapt
    - Consider frameworks of types of controls on security, IM and Privacy system outputs to assure against autonomous mission creep
        - What is the nature of and confidence in the system "off switch"
  - [Other?]
- References

61. Business Information Ethical Considerations

- Challenges
  - Concept of business information ethics is raised in the normative gap between archaic laws and today's technology applications that host our interactions
    - Ethics, by definition, is informed by *human* norms
    - IM and privacy are intrinsically *human* considerations
      - IM in organizational context is a form of inventory management for labor
    - Institutions and system and/or technology systems do not have intrinsic "ethics" since they are both programmed to achieve certain limited human goals.
      - To the extent they such institutions have "ethics" it is part of their programming.
      - Where that programming involves the delivery of security, IM and privacy functions, those functions must be included in their programming to be manifested in their operations.
    - How does the subject system and/or technology help to bridge the gaps left by legal lag and by institutional ethical neutrality?
  - [Other?]
- References

61. Business Information Ethical Considerations

- Candidate Analytical Frameworks/Metrics/Actions
  - Multiple companies and industry associations have launched "data ethics" and related research initiatives.
    - IEEE – Ethics of Autonomous Systems and AI
    - Accenture "Data Ethics" report
    - Etc.
  - Ethical constructions provide an opportunity to create human-centric constructions of risk reduction and value generation at the edge of legal and settled normative guidance.
    - Compare Edge Governance Map concept of "Provisional Governance" for ethics
  - [Other?]
- References

62. Incidental Benefits
Beyond security, IM and Privacy

- Challenges
  - Organizations with budgets seek ROI narratives for expenses investments
    - Are there incidental benefits to organizations and individuals, beyond security, IM and privacy, associated with the deployment of the subject system and/or technology that can help to drive adoption and justify internalization and front-loading of cost of the subject system and/or technology?
    - How can the implementation of the system and/or technology be supported beyond its security, IM and Privacy benefits?
  - How can the improvement of security, IM and privacy be understood and presented to improve other strategies, services, products and sectors?
    - Each improvement is a potential value proposition that can contribute to the overall adoption of the system and/or technology/system.
    - How can those value propositions be identified and applied by organizations deploying and operating the system/technology?
  - [Other?]
- References

62. Incidental Benefits
Beyond security, IM and Privacy

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider potential benefits to other (non IM and non-Privacy) compliance obligations:
    - SOX compliance
    - SEC compliance
    - Other regulations that require IM accountability
  - Consider variety of ROI benefits of sunk, compulsory privacy compliance costs
    - Tax and accounting
    - Brand and marketing
    - Borrowing rates and insurance premium savings
  - Consider variety of ROI benefits of contexts in which additional privacy investment is warranted.
    - Examine implications of system for different operations and divisions of given organization and analyze costs and benefits independently.
      - Roll up overall costs and benefits in budget context for help in weighting investments and expectations
  - [Other?]
- References: Privacy "Beyond Compliance Paper" by TechVision Research (co-authored by Scott David) for 29 additional benefits for businesses of investments in privacy.

63. Network Graph Theory "Wiring Patterns"

- Challenges
  - Different technologies applied in different network contexts will create different network structures among equivalent sets of nodes.
    - These structures are finer grained than the overall structure of the network (See Paul Baran network diagrams in Refs), and are equivalent to interaction eddies and vortices that emerge in the overall flow of interactions on a network.
  - What are the implications of these different potential "wiring diagrams" on security, IM and Privacy and security of the subject system and/or technology system?
    - Was the system designed to assume only one set of possible "edges"/connections for a given set of "nodes" in the system?
      - What are implications of other connections?
      - Conflicts of interest
      - Back-doors to system undermining trust
  - [Other?]
- References

63. Network Graph Theory "Wiring Patterns"

- Candidate Analytical Frameworks/Metrics/Actions
  - Networks of Information Systems display emergent effects at multiple levels of analysis.
  - Second order influence nodes have been analyzed in terrorist network analysis.
    - Ref: NATURE magazine article.
  - Local structures of nodes within a network also affect the behavior of networks at multiple scales.
    - See Ref. Science Magazine "Network analytics in the age of big data" July 8, 2016 page 123-124.
  - [Other?]
- References

64. Dynamic Entropy Level

- Challenges
  - If Identity insight and Identity Intrusion are viewed as two ends of a sliding scale, how can the degree of identity insight/intrusion be dynamically balanced in the system/technology to enable stakeholders to apply the appropriate balance in a given context/subject setting?
    - Does system and/or technology facilitate the application and provision of information at various levels of "identity entropy" (aka "Levels of Assurance" or "LOA") to help data subjects preserve their interests and rights
    - How can that data (or meta-data about system operation) also be made available to operators and users to enable function of the system in balance with the preservation of privacy?
  - [Other?]
- References
  - NIST 800-63 is an example of how levels of entropy of identity correlates with identification and potential privacy intrusion.

64. Dynamic Entropy Level

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks of “step up authentication” and beyond
  - Consider frameworks that dynamically and contextually rebalance and reflect correlation of insight and intrusion in security, IM and privacy related systems.
    - Should match entropy with LOA, but more granular.
    - Does system and/or technology apply “flack” and de-identification processes to protect identity information to a level of entropy appropriate to the interaction?
  - Consider challenges of “re-identification” as separate identity entropy-lowering events
    - Measure breaks in chain of responsibility for identity intrusions caused by subsequent re-construction of identity from data “in the wild”
    - Informs analysis of causation in intentional tort and criminal contexts of intrusion involving unauthorized use of data to construct PI
  - [Other?]
- References

65. Risk/Cost Accounting Issues

- Challenges
  - Commercial and governmental organizations already run sophisticated systems to account for risks and costs of their respective organizations.
    - How does candidate security, IM or privacy system integrate with existing organizational risk and cost accounting systems?
    - How does it improve (or undermine) existing risk mitigation efforts of organizations (both real and aspirational efforts)?
      - What is the answer for the expected risk mitigation efforts?
      - Is there a different answer for the actual risk mitigation efforts?
  - Does the proposed system produce additional system performance data and other data that could help improve accounting and risk management in organizations?
    - Face saving benefits of technologies that can bring organizations up to a level that matches consumer and 3rd party expectations with reality.
  - [Other?]
- References

65. Risk/Cost Accounting Issues

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks of security, IM and Privacy system analysis based on existing standards for risk analysis and reporting.
  - Consider frameworks based on existing standards for accounting and tax reporting.
  - Consider existing GAAP and GAAS data flows and implications of the system and/or technology for accounting.
  - Consider initiatives to establish “GAIP” (Generally Accepted Information Practices) to standardize and normalize information practice in a manner similar to GAAP
    - Those standards in accounting help mediate the secondary liability battle of accounting, legal and other professionals
      - Consider how GAIP might establish a liability DMZ that can help to attract service providers into the IM and data markets
      - Standards enable contractual P2P liability “safe harbors.”
        - » Establish “duties of care” that are available for recognition by courts.
  - [Other?]
- References

66. Legal

- Challenges
  - Technology systems are built on the laws of physics, which are global, but they are operated in systems that are constrained by the laws of people (and their governments)
    - The gap of technical capacity and legal operation is the source of significant risk and mischief in multiple domains
  - There is significant confusion about the operation of legal constraints, and their enforcement, in sociotechnical systems that host or raise security, IM and Privacy issues.
    - How does the subject security, IM or Privacy system and/or technology help to clarify the way in which it supports, invites, clarifies or otherwise integrates with the legal considerations that undergird security, IM and Privacy systems?
  - Does the technology and system produce data, logs or other information that can serve an evidentiary or other audit/enforcement function in existing information systems?
  - What are the regulatory implications of full adoption/deployment of the system/technology?
    - Does interaction of large populations with the system drive behaviors toward standardization that can support “best practices” as candidate “duties of care” for application in “reasonable person”-type texts?
  - [Other?]
- References

66. Legal

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider introduction of framework based on a standard “legal liability algorithm” to clarify ways in which security, IM or Privacy technology system improves human and institutional performance.
    - Rights (invoke)
    - Duties (which when subject to)
    - Breach (can result in)
    - Causation (of)
    - Damages (with consequent)
    - Liability (for the breaching party, that may be shared with)
    - Insurance
  - Consider potential impact of system and/or technology at various stages of legal process
    - Negotiation
    - Performance
    - Enforcement
    - Assignment
    - Etc.
  - [Other?]
- References

67. Advanced Computing Architectures

- Challenges
  - What are the implications of advanced computing architectures on operation of the system/technology
    - E.g., ability to break cryptographic keys, etc.
  - What are the implications for concepts of Advanced Computing of defining "computing systems" as a form of "Sociotechnical systems" of people and institutions that don't just use and consume the output of ICT networks, they are also "components" of those systems, the reliable behavior of which is necessary for trusted system function.
    - Reliable employees help prevent data breaches
    - Reliable commercial and governmental institutions only intrude on information integrity (e.g., privacy) in predictable ways
      - E.g., Warrant requirements for government search
      - E.g., Data analysis by companies consistent with published TOU.
  - How can computing architecture and system design principles be applied to "organizational science" of human and machine hybrid systems.
    - What are the potential negative implications for humans and for computers of treating people and institutions as "components" in larger computing systems?
  - [Other?]
- References
  - Ref: Seth Lloyd – "Programming the Universe"

67. Advanced Computing Architectures

- Candidate Analytical Frameworks/Metrics/Actions
  - Advanced computing architectures (such as massive parallel processing), etc. can yield insight (aka "information arbitrage") with great value
    - Consider mechanisms for spreading the benefits of that value in ways that are sustainable and resilient
    - Is organization of a "data production co-op" among data subject populations a form of advanced computing architecture?
  - For next-generation advanced computing architectures built within and among sociotechnical domains, consider that trust frameworks establish integrated specifications for tech and rules for humans and institutions in system
    - Enable reliable Sociotechnical architectures that can be trusted at large scales
  - Systems approach to computing architectures beyond traditional programming
    - Consider recruitment of attention as form of "massive parallel processing" in individual and institutional contexts
      - Crowd sourcing
      - Fold-it, SETI and other recruitment of human perception and cognition in massive parallel configurations
  - [Other?]
- References

68. Information "Signal Transduction" Across Heterogeneous Media

- Challenges
  - Signal propagation for information (including "identity-related" information) through different media, different channels, etc. is inconsistent, leading to signal losses
    - Consider variations in media beyond physical variations:
      - Cultural differences in people along channel, motivation differences in multiple-institutional information channels, etc.
    - Compare to children's game of "telephone" when messages get garbled as serially retold.
    - Different taxonomies, definitions, information flows affect signal across legal and policy domains
    - E.g., cannot share law enforcement-related information across jurisdictions without protective arrangements
  - Interoperability challenged when signal/information moves across media
    - Different performance metrics
    - Different carrier "media"
  - How can the policy differentials be accounted for in the design, development and deployment of the technology/system
    - What are the corollaries of electrical circuit in analyzing information flow?
    - What measurements are needed to measure "signal loss" (information arbitrage dissipation) along channel.
    - Can future quantum communications help mitigate a subset of that dissipation (through eavesdropping detection, etc.)
  - Is electrical-circuit analog helpful in dealing with "entropy accounting?"
    - Are there generic measurements of signal loss that can apply across different identity signal transduction environments?
      - Federated identity systems deal with this challenge
    - How is "Shannon Information Entropy" (e.g., surprise value) distinguished from "market arbitrage?" How do Shannon entropy and market value interact (e.g., of message with cookie recipe vs. message with cure for cancer)
  - [Other?]
- References

68. Information "Signal Transduction" Across Heterogeneous Media

- Candidate Analytical Frameworks/Metrics/Actions
  - Need to identify metrics that can be "consumed" on both sides of a media divide to facilitate transfer across interoperability "synapses" of different kinds
    - Differences in technology and operating systems
    - Differences in policy and rules systems
  - Where multiple metrics are needed (for legacy, etc.) consider conversions of metrics and ability to make conversions in real time.
  - Consider other systems that integrate hybrid channels to facilitate cross channel interactions:
    - ATM networks that accept different cards
    - Currency conversions at airports
    - Translators at U.N.
  - Note example of federated identity which deploys identity signal across different domains
    - Pattern of adoption of approach of one domain
      - Banks or Telco's bid to be identity providers for other sectors
    - Pattern of creation of new approach for adoption by multiple domains
      - Social network new entrants identity system as identity utility.
        - » E.g., Open ID connect, Facebook connect, etc.
  - [Other?]
- References
  - See article from NATURE on testing circuits and biological signal transduction

69. Market Structures and Assumptions

- Challenges
  - Is the technology/system designed with accurate market assumptions?
    - Assumptions about actual and perceived risks to system and/or technology development and deployment that are inconsistent with market realities will retard adoption of desired technologies.
  - Market realities have multiple alternative vectors
    - Market structure
      - commons (stakeholder self-regulated)
      - Competitive markets
      - state controlled
      - SRO - “exchange”
      - Hybrid models
      - etc.
    - Market dynamics
      - Trading frequency
      - Reporting frequency
      - In person trading
      - Online exchanges
  - Market processes vary across market sectors, jurisdictions, cultures, etc.
    - Are these differences accounted for in the technology operations and deployment plan?
  - How will market evaluation of product or service value inform future development of system or technology?
  - [Other?]
- References

69. Market Structures and Assumptions

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider "Commons" structures for co-management of rights
    - Oceans/fish
    - Space
    - security references
    - risk commons – Insurance, IP and other distributed intangible rights settings
  - Market default behaviors
    - Consider "attractors" in market settings
    - E.g., Market as Boolean network (from Wikipedia:
      - Since a Boolean network has only 2^N possible states, a trajectory will sooner or later reach a previously visited state, and thus, since the dynamics are deterministic, the trajectory will fall into a cycle. In the literature in this field, each cycle is also called an attractor, etc.
  - Consider how attractors affect adoption curves in markets
  - Consider alternative "Empire of Value" model
    - i.e., where desire for exchange drives markets, not intrinsic value of asset (node).
    - Drive to connect and exchange, not just purchase
    - Not satisfied in things, but relationship to people and things
    - Consider Graph Theory version: Data and information are conversion from nodes to edges – quantification of the edges not the nodes – quantification of the empire of value model – edge value.
  - [Other?]
- References

70. Network Structures and Substructures

- Challenges
  - Higher dimensional structures of and within the network confound more traditional “node-based” analysis
    - Compare to “post-synaptic paradigm” in cognitive science
    - Does “thinking/consciousness” reside in linear (or massively parallel) synaptic activity, or in waves (solitons) in electrical activity across brain structure?
  - How can graph theory and other analytical approaches identify network patterns and structures that can reveal data/identity flows and sources of unreliability that undermine security, IM and privacy system function?
    - Are there network patterns and/or graphlets that correlate to:
      - Security
      - Malfeasance
      - Negligent behaviors?
  - [Other?]
- References

70. Network Structures and Substructures

- Candidate Analytical Frameworks/Metrics/Actions
  - Look at “second order” influence nodes research
  - Look at “graphlets” research – emergent “species of local interest sharing – types can be described
    - Example of franchise operations as supply chain instance.
      - 100 carbon copies of information networks can reveal aberrations in data flows that disclose positive and negative differences in local operations
      - Commercial and relationship regularity
  - The attention to market structures and flows permits analysis beyond the “property” concept (that tends to focus on the value and protection of “nodes”)
    - instead related to relationship (“edge”) structures that illuminate market and relationship structures
  - [Other?]
- References

71. “Desire for Exchange” Market Modeling

- Challenges
  - If and to the extent that market activities reflect a desire by participants to engage in interactions, rather than a mechanisms for access to utilitarian value for the goods and services exchanges, what are the implications for adoption of the proposed system and/or technology in such exchange contexts?
  - What are the metrics for measuring risk and performance of the system where exchange, rather than utility value, provides the basis for market behavior?
    - Does the system/technology produce performance data that fosters evaluation of exchange behaviors toward optimization?
  - Can the security, IM and privacy measurements enabled by the system and/or technology or system be brought into the service of indirectly measuring relationship reliability to support the “desire for exchange” model?
  - [Other?]
- References

71. “Desire for Exchange” Market Modeling

- Candidate Analytical Frameworks/Metrics/Actions
  - Metrics associated with “edges” of relationship rather than “nodes” of value may help identify variables in network supported by system and/or technology
  - [Other?]
- References
  - Ref: “The Empire of Value” (which advocates for a post-utility-value approach to analyzing market behaviors.

72. Information Entropy Arbitrage/ Balancing

- Challenges
  - Does operation of the technology/system (either alone or in conjunction with other systems) offer new or superior insight to one or more parties to valuable interactions?
    - Could that superior view fuel abuse, harm, conflicts of interest" or harmful information arbitrage?
  - What are mechanisms through which source of arbitrage/insight value and its use are or could be measured/regulated to prevent undue harm
    - How measure acceptable levels of harm in new interaction settings
  - Consider that difference of fraud and arbitrage is that
    - in fraud setting the value extractor creates the information differential
    - In the arbitrage setting, the value extractor "discovers" the information differential
  - How democratize information entropy arbitrage
    - Lack of mechanisms that are perceived as fair for distribution of benefits strains social fabric
    - The 99% of population who don't know the risk
    - Railroad right of way purchase from farmers is historical example of "sharp practices."
  - How can organizational stability and resilience (and information arbitrage) be correlated with negentropy (variance from Gaussian signal for output of organization)
  - [Other?]
- References

72. Information Entropy Arbitrage/ Balancing

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider approaches to "light-touch-regulation" that constrain exploitations of information arbitrage to defined "performance band"
    - Cage the wild animals as in regulation of intermediaries
      - E.g., Broker dealer regulation
  - How measure "amount" of arbitrage?
    - Use market measure of advantage gleaned?
      - Like "Philadelphia Bridge Amusement Company" tax case
        - » Value of thing received defines value of thing transferred.
    - Does the amount of "value" generated in markets provide a reliable measure of the amount of potential "harm" experienced?
  - See Wikipedia entropy on "Negentropy"
    - Consider information theory negentropy as basis for arbitrage calculations and institutional value-add
      - divergence from "normal" or "Gaussian" decisions)
  - What are other mechanisms for "disorder accounting?
    - Compare assignment of "damages" to myriad civil wrongs as example of "money" as entropy exchange metric
      - What are limits of single metric for varieties of disorder/entropy/harm?
  - [Other?]
- References

73. ROI and Investment Considerations For Tech

- Challenges
  - Gauntlet of Design, Development and Deployment presents several separate and independent financing challenges
    - ROI for system and/or technology developers
      - Owner of IP
      - Compensation for developers
        - » Employees
        - » Contractors (work for hire")
    - ROI for investors and financers
    - ROI for users/consumers of system and/or technology
  - How do the financial requirements for the particular system and/or technology at each stage impact strategies for its design, development and deployment?
  - (See "Economic Setting" for more)
  - [Other?]
- References

73. ROI and Investment Considerations For Tech

- Candidate Analytical Frameworks/Metrics/Actions
  - Challenges of evaluating return potential for system and/or technology
    - Monetary measures
    - Metrics for other value propositions
  - Challenge of applying traditional valuation methods
    - Cost approach (will typically understate value of intangibles)
    - Income approach (new system and/or technology doesn't have track record of earnings for calculation – Compare Associated Patentee's case valuation method for tax purposes)
    - Comparables (breakthrough technology makes comparison difficult)
  - What are financial dependencies of the system and/or technology beyond those owed to the direct investors?
    - Is the system and/or technology associated with other system and/or technology
      - Might it be eligible for bundling to speed adoption?
    - Are there social and political dependencies that affect the system and/or technology's implementation profile?
  - [Other?]
- References

74. Accident-Proofing Organizations

- Challenges
  - How can the system and/or technology and the networks in which it is deployed in enterprises or communities be “hardened” against:
    - Accidents
    - Negligence
    - Unintended consequences
    - Errors
  - How do the system challenges presented by accidents vary from those of attack and acts of nature?
    - Is the system or technology configured or designed to deal with accidental harms that arise from its operation?
  - AAAA risk –
    - Note that accident is just one source of risk
      - Others are “Attack” and “Acts of Nature” and “AI/Autonomous Systems”
        - » See those separate risk maps
      - Prevention of “accidental risk” is costly, and requires different strategies
  - [Other?]
- References

74. Accident-Proofing Organizations

- Candidate Analytical Frameworks/Metrics/Actions
  - Alternative strategies for accidental-risk mitigation
    - Telephone game
      - "Hamming Distance" measurement as likelihood of confusion?
    - Consider role of negligence/accident both as independent causative factor of system failure AND as aggravating factor in other risk settings
      - In attack or act of nature
        - » E.g., Accident/negligence can undermine response to disaster/attack
    - Consider training and practice/habit as an accident-proofing strategy
    - Consider non-linear analyses of accidental risk
      - Implications for preparation/investment
    - Consider strategies of "HROs" (high reliability organizations) where accidents are presumed as part of operations
  - [Other?]
- References

75. Policy as Quantum Probability (wave?)

- Challenges
  - If all action is probabilistic, how can policy help?
  - Standard, deployed policies can create teleology (retroactive causality) that can help “predict” future (by constraining it), or at least can shape ALL observers vision of the future (like Kuhn’s paradigms in operation), so that it has a predictive role in SOCIO-technical systems
    - where recruitment of observers to conform to paradigm is much easier than recruitment of external phenomenon (AAAA risk, e.g.)
  - Since uncontrolled (AAAA) risks are a shared problem for all people and institutions, then shared approaches relieve the community of observers (victims of the vagaries of a probabilistic world), of individual responsibility
    - This is why imperial powers sent children of occupied territory to language schools.
    - Vestiges of “ the Commonwealth” and traces of German law in Asian countries are examples of lasting power (and cognitive/policy interoperability) of recruitment of communities of “observers” of “like mind.”
  - [Other?]
- References

75. Policy as Quantum Probability (wave?)

- Candidate Analytical Frameworks/Metrics/Actions
  - What tools could be made available to policy makers to help enhance the efficacy of policy processes and outputs?
  - How can “probability” be mapped for stakeholders as policy makers?
    - Probability is the square of the amplitude (amplitude is the radius and probability is the area of a circle)
    - What are rules for drawing amplitudes (using Feynman diagrams) for different frameworks.
  - What system metrics (or combinations of metrics) can help supply amplitudes for probabilistic models?
  - [Other?]
- References

76. Educational and Training Considerations

- Challenges
  - How can the system/technology help to improve the state of cybersecurity and privacy education today?
    - What is level for cyber-professionals?
    - What is level for non-cyber-professionals?
  - What is the "negative space" that surrounds current "cyber-security" teaching and training and how does the technology/system help to define that space?
    - What is being left out of training along the spectrum from professionals to ordinary citizens that use and rely on cyber systems?
  - What is the balance of practice and theory that is appropriate at different levels of stakeholder engagement?
    - Training for trade, professional education, etc.
  - What are the implications of evolution of cybersecurity from a technical/computing/IEEE platform?
    - How does history affect questions asked today about cybersecurity?
    - How can non-technical (Policy) work be introduced into workforce
    - What is role of training?
      - words on paper aren't enough
    - How can "critical thinking" and other valuable perspectives be taught?
  - How can the Atlas of Risk Maps and other risk visualization and planning tools be coordinated with educational initiatives to improve cybersecurity workforce to "harden" open/distributed systems?
    - For cybersecurity professional training, consider amenability of the system and/or technology to correlation with NICE KSAs and other structures of cybersecurity teaching
  - [Other?]
- References

76. Educational and Training Considerations

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider education and training at all levels
    - K-12
    - Higher Ed
    - Professional education
  - Consider use (and updating) of NICE KSA framework framework for preparing units for use in cybersecurity professional education
  - For neighborhood watch, need training of citizens
    - Consider modular curriculum and online approaches to delivering context appropriate security, IM and privacy learning opportunities at multiple levels:
      - K-12
      - Undergrad
      - Graduate (other than cybersecurity professionals)
      - On the job training, professional development
  - [Other?]
- References

77. Insurance Requirements /Actuarial Analysis

- Challenges
  - Coverage of existing insurance policies may not address emerging risks in cybersecurity, privacy, identity-rights and other domains
  - Implementation of the new system may create or exacerbate risks and harms that are inconsistent with existing insurance policies and structures.
  - Metrics used to set current premiums and claims payouts may not take account of new sources of risk and loss
  - Loss event measurement may be based on measurement of deviation from expected performance that is unrelated to actual source of new emerging harms
    - Legacy approach to performance measurement may be outdated
    - Costs such as from negative brand impact, and other market factors may be difficult to define.
  - [Other?]
- References

77. Insurance Requirements/Actuarial Analysis

- Candidate Analytical Frameworks/Metrics/Actions
  - Ability to define metrics from other policy frameworks will help to define performance criteria for technology and systems that will foster insurance availability.
    - Metrics from each of the Risk Maps in this Atlas are candidates for inclusion in actuarial and similar analyses
  - Consider insurance products in other markets for intangibles, rights management, and structures of insurance for risks in those markets for potential models
  - Consider natural progression of predictive markets into insurance markets and the challenges of that evolution
    - See Economist article on failures of ARC system (crop insurance based on weather), since actuarial parameters were insufficiently comprehensive to measure actual harms experienced by stakeholders.
  - Non-linear system failures in complex systems might not be modeled by normal (Gaussian) distributions, challenging actuarial analysis
    - but may still invite cost-spreading and cost-sharing approaches of insurance to enable mitigation of risk
  - [Other?]
- References

78. Banking/Financing Regulatory and Market Requirements

- Challenges
  - Consider “Data” as commodity/quasi-currency:
    - Will data rights co-management standards cause the commodification of data to the degree that it can enjoy the same market and exchange patterns and operational efficiencies as other commodity markets?
      - How will those patterns be governed and managed in the case of data?
    - If so, what are the implications for other information management issues (such as privacy, security, identity management, etc.) of that commodification?
  - Financing for new technologies may delay R&D and deployment
  - Bank and Financial Regulations may struggle with intersection of set of all data with the subset of data that is within the regulatory penumbra of the SEC, CFTC, Fed, banking agencies, etc.
  - Money is (mostly) moved in the form of data (other than currency and coinage).
    - How will future data regulations (including security, IM and privacy) intersect with existing monetary and banking regulation?
  - What are implications of the technology/system for future crypto-currency and related domains?
  - [Other?]
- References

78. Banking/Financing Regulatory and Market Requirements

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider how the candidate security, IM or privacy system and/or technology supports (or undermines) existing banking/financial regulatory structures
    - Computational sovereigns
      - Blockchain and distributed ledger
      - Intangible value portability
      - Cryptographic secrecy
    - Beyond distributed ledgers
      - Consider potential for distributed architectures of other apparatus of finance and implications for financial and other regulation
        - » Move to “neighborhood watch” and “reputation-based enforcement” systems
  - Consider how existing banking and financial regulation can be applied (by either direct application or analogy) to emerging data markets.
  - [Other?]
- References

79. Consumer Protection Law Constraints

- Challenges
  - Consumer protection laws establish particular legal “duties of care” and other obligations in case of relationships with consumers (non-B2B contexts).
    - security, IM system and/or technology data flows must be consistent with consumer protection laws
  - Is the optimal operation of the system and/or technology consistent with consumer protection laws?
    - Is that consistency maintained across laws of multiple jurisdictions/markets?
  - In what ways does the candidate system and/or technology foster or facilitate application of consumer protection laws
    - FTC privacy regulation
    - Consumer protection laws
  - Does the technology produce data and/or metrics that can help support protections of consumer laws in US or abroad?
  - Can the system/technology operation and/or output enhance consumer protection beyond that currently required by law and regulation?
    - What are the negative implications of that “innovation of protection?”
      - Does it involve Vigilantism?
      - Is “due process” lost in market-based systems?
  - [Other?]
- References

79. Consumer Protection Law Constraints

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider application of elements of statutory claims as guidance in product design/development
    - Can use elements of various consumer protection laws as framework for development of metrics and data collection structures for application of the system and/or technology.
      - Adopt subset of existing legal obligations as “requirements” for system build
      - Gain adoption benefits of law as “de facto” standardization
  - Consider adoption of “highest common denominator” (most consumer protective law) as guideline for technology/system design and development
    - Can then introduce technology/system in lesser-regulated setting as “race to the top” for consumer protection.
    - Example of using private law (contract and TOU, etc.) as mechanism to recruit populations and help bridge differences of public law among jurisdictions
  - [Other?]
- References

80. FTC Enforcement Policies FOR Privacy

- Challenges
  - FTC administrative rulings have established new requirements and duties for “privacy”
    - Rulings based generally in FTC Title V “unfair and deceptive acts and practices”
    - This foundation constrains FTC jurisdiction at some point
  - What areas of emerging harms are NOT being addressed as a result of FTC prominence in the realm of privacy, but subject to its limitations based on the source of its authority?
    - What additional mechanisms (beyond FTC substantive and procedural boundaries) are available to identify and realize emerging individual harms and rights associated with new information technologies including that subset that are associated with security, IM systems.
  - [Other?]
- References

80. FTC Enforcement Policies FOR Privacy

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider incorporation of FTC rulings as guidance
    - FTC administrative rulings add details to application of privacy rules in US.
    - Note that FTC approach is narrower than broader emerging privacy considerations
      - Based on FTC auspices over “consumers”
  - Consider opportunity to review other FIPPs-based systems for interoperable policy opportunities
    - See article by Bob Gellman in bibliography.
    - Consider that FIPPS is the *genus* of which there are various *species* of regulatory and self-regulatory laws and rules
      - Regulatory examples (GDPR, DHS Privacy Rule)
      - Self regulatory examples – GSMA
  - Consider limitations of FIPPS approaches (including as applied by the FTC), and potential mechanisms to extend the foundation of FIPPS beyond current protections (even as many of those original principles remain aspirational).
  - What other agencies of government might help to define privacy rights beyond consumer privacy?
    - Commerce/SBA? – frameworks for people as ”data producers”
    - OSHA – Employee data rights
    - IRS – Tax data
  - [Other?]
- References

81. FTC Enforcement Policies for OTHER THAN Privacy

- Challenges
  - FTC jurisdiction (and auspices) extend to the protection of individuals (and businesses) beyond just privacy considerations of individuals, in ways that affect security, IM and Privacy.
    - Antitrust
      - What is interaction of security, IM, Privacy and market structures?
    - Commercial practices
      - What is the relationship of IM, security and privacy to the presentation and consumption of services and data collection activities?
        - » Consider the "nectar" based model and consumer disclosures relating to receipt of free services.
    - Mechanisms for rights under 4 traditional torts?
      - Imagine what FTC or other government enforcement might be for traditional privacy torts
        - » Defamation (Libel and Slander) - Reputation harms
        - » Invasion of private space
        - » Publication of private facts (false light)
        - » Mis-appropriation – commercial harms from data?
  - [Other?]
- References

81. FTC Enforcement Policies for OTHER THAN Privacy

- Candidate Analytical Frameworks/Metrics/Actions
  - Are there aspects of FTC enforcement and administrative policy and processes that relate to policy areas contiguous to privacy (such as data security, consumer credit, etc.) that have not yet been recruited into the service of making reliable those consumer-facing services upon which privacy is dependent?
    - Consider the "information channel integrity" model of privacy
      - i.e., if can enhance the integrity of the "expressive" and "perceptual" channels (as measured through multiple vectors) available to people, that will help address privacy, security, etc.
      - Erving Goffman 2.0?
  - [Other?]
- References

82. “Quantum” State Collapse

- Challenges
  - The origins of information network risks are complex, and AAAA risk elements may not lend themselves to prediction relying on data regarding prior system performance.
    - Past performance is not a predictor of future performance in complex systems
      - such as markets
      - seismic activity
  - How can system risk be quantified in the absence of effective predictive analytics?
  - Are there correlations that can help guide behavior of organizations and people where the potential timing, severity and likelihood of system failures are unknown?
  - Are there statistical or other models of security, IM architectures and technology systems that can be helpfully constructed to capture and/or apply extant sensory data to capture identity entropy?
  - What are the “Lagrangian Coherent Structures” of identity and how can they be applied in security, IM settings?
    - Compare to Lenticular cloud on mountaintop – Wind moves, while cloud appears stationary
    - In online identity – data flows with interactions, and identity appears stationary
  - Statistical approaches to IM authentication?
  - Statistical approaches to authorization?
    - Explore how to turn vast complexity of context and subjective variables into statistically cognizable and parse-able value variables
  - [Other?]
- References

82. “Quantum” State Collapse

- Candidate Analytical Frameworks/Metrics/Actions
  - Among models for complex systems
    - Consider “Wave Function Collapse” as a “black box” for thermodynamically irreversible interaction with the classical environment.
    - A system that is statistically unpredictable and immeasurable can become measurable and predictable when phase space narrows with irreversible interactions
    - How can mechanisms of interactions be recruited for causing discretion-collapse to constrain behaviors and reduce risk
      - Consider distributed ledger as mechanism of statistical irreversibility of interactions
  - Consider other forms of “controls” external to system that is behaving unpredictably
    - Insurance
      - Don’t reduce risk of AAAA event, but mitigate harm to single individual or organization
    - Standards
      - Convert “unknown unknowns” of risk into “known unknowns”
        - » E.g., Stoplights don’t guarantee driver compliance with laws.
  - [Other?]
- References

83. Phase Change Potential (Technology as “Seed Crystal”)

- Challenges
  - When all individual elements of a material are in a uniform state, a small disturbance can cause a dramatic change across the mass of the material
    - Consider water at 32 degrees turning to ice
    - Risk phase change? - Consider risks of one type of insect pest to single species forest
    - Consider memetic narrative structures across a population
  - In hybrid socio-technical systems, people and organizations are not just “users” of the risk reducing system, they are also “elements” of the system, and their reliable performance of system duties and responsibilities is critical to system optimal performance
    - Where “Tools and Rules” are needed to render system and/or technology and people reliable In hybrid sociotechnical systems, the behavior of one can enhance (or degrade) the performance of the other
  - Are there aspects of the system and/or technology that can help to cultivate dramatic changes in the level of risk mitigation in the system, not just by operation of the system and/or technology alone, but also by enabling or recruiting people and organizations in the system to dramatically alter their behavior in fundamental ways?
    - Pay-forward-type activities
    - Socialization in work environments and other semi-compulsory settings.
  - [Other?]
- References

83. Phase Change Potential (Technology as "Seed Crystal")

- Candidate Analytical Frameworks/Metrics/Actions
  - Candidates for "seed crystals" to change "policy phase" can be technical in nature or policy in nature
  - Policies can involve new incentives and penalties that can alter behavior across current set of behaviors
  - Technologies can affect risky behavior directly and indirectly
    - Example of direct mitigation is installing breathalyzer on a car's ignition switch to prevent car (technology) from being driven by a drunk driver (person).
      - When "rules" (aka laws against drunk driving) don't work, "tools" (aka technologies) can decrease threat from sociotechnical systems
    - Example of more indirect mitigation is traffic stoplights that elicit a standard behavior across populations to reduce statistical risks.
      - Traffic light creates orderly system of standard rule application so that populations, none of which want to be in an accident (shared behavioral "phase", can ALL engage in self-interested behavior (i.e., avoiding an accident) that manifests self-less behavior (i.e., not causing an accident).
      - Regulated markets create systems where IT system and/or technology provides standard information to recruit trader self-interested behavior (of reducing trading risks) into self-less behavior (abiding by trading rules)
  - How can the identity or data system and/or technology help promote the normative phase change of populations to mitigate risks
    - Consider technologies that democratize arbitrage by standardizing information flows
  - See David Thouless vortex unbinding mechanism
    - Patterns of topological configurations can give rise to non-trivial features
      - See Nature magazine article, May 9, 2019 (p. 193)
- References
  - Ref: "The Structure of Scientific Revolutions" by Kuhn in bibliography

84. Fourier policy, contract term parallax, regulatory compliance interferometry

- Challenges
  - Risks of various kinds arise from settings where individual and organizational expectations of IM and data system and/or technology performance are different than the reality experienced by the system in operation
    - What are the mechanisms through which the differentials between system expectations and performance can be dynamically measured and presented to stakeholders to mitigate risks?
  - Are there patterns in human and institutional economic, political and social phenomenon that display a periodicity at various time scales that makes them amenable to analysis using wave forms or other mathematical structures that can help to guide conceptualization and analysis of their behaviors?
  - What are the risks of applying these methods to discerning and predicting behaviors of animate objects (such as humans and institutions)
    - Reductionism of analysis?
    - Undermining institutions that are based on notion of “free will?’
  - [Other?]
- References

84. Fourier policy, contract term parallax, regulatory compliance interferometry

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the various conceptual, analytical and technological mechanisms through which dynamic differences between system parameters and performance can be measured and fed back into a system
    - What is the capacity of the system and/or technology to present dynamic performance in real time to stakeholders?
    - How can the related performance be correlated across domains?
      - E.g., When an auto manufacturer issues a recall due to brake failure (a technological failure), its stock price goes down (a market effect that hurts shareholders).
      - Current generalizations about the "cost to companies of data breaches" are examples of this kind of cross-domain comparison. Even without demonstrated connection to data subject harm, still results to organizational costs of:
        - » Cost to brand/reputation
        - » Direct costs of notification and data monitoring, etc.
        - » Statutory penalties
  - If and to the extent that various phenomenon described in this atlas display periodicity, feedback and feed forward characteristics, harmonic qualities, etc. consider the various elements of analysis applicable to wave forms, interference, turbulence etc. that might provide insight into their behaviors
    - Consider nature of "Coupled Harmonic Motion" among network "graphlets" – measure meta-edges among groups of nodes as independent organizational variable
  - [Other?]
- References
  - See book "Order from Disorder – The study of turbulence" in bibliography

85. Tax Considerations

- Challenges
  - What are the tax-related implementation challenges of the design, development, deployment, etc. of the system and/or technology?
    - Is there unfavorable tax treatment that increases costs of acquisition and operation, of training and education, or operation and updating?
  - Are tax laws optimized to foster investment in the critical security infrastructure needed by societies?
  - How can tax policy be used to support and promote secure and privacy-enhancing IM and information network technology and systems?
  - How might design, development and deployment hurdles be mitigated through tax strategies?
  - [Other?]
- References

85. Tax Considerations

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider revenue recognition and related variables associated with innovative technologies
    - Do they foster innovation?
  - Consider tax treaty considerations of income sourcing, etc. on international operations of ITC companies
    - What is the relationship to international data policies?
- Consider tax policies in multiple taxes and jurisdictions and their effect on intangible value propositions associated with information networks
  - Services characterization of income?
  - Consider state and federal rules
  - Consider different taxes (property, sales, income, VAT, etc.) and different bases and their effect on the development and deployment of IM and privacy-friendly technologies
  - Consider cost mitigations of deductions and credits
    - Changes in tax law can encourage broad adoption of new technologies
      - Contribute to achievement of "network effect" of implementation of desirable technologies.
    - Consider different taxes at different levels (income taxes, sales taxes, property taxes, excise taxes, etc.)
    - Consider different jurisdictions and levels (state, local, federal)
    - Consider income tax treaty context (issues of jurisdiction and sourcing of income associated with information systems and services, etc.)
    - Consider different tax incentives, mitigations
      - Deductions (e.g., MACRS), credits (e.g., ITC), rate changes, exemptions, etc.
  - [Other?]
- References

86. Network Architectural Nuisance Potential (Data NIMBY-ism)

- Challenges
  - One party's insight is another party's intrusion.
    - Will the deployed system produce forms of harm/disorder ("entropy exhaust") that will undermine operations of contiguous or related/dependent systems?
  - Consider analogy to other law where legal concept of "quiet enjoyment" is breached
    - nuisance law
    - environmental law
      - Consider role for CERCLA-type liability structure.
  - [Other?]
- References

86. Network Architectural Nuisance Potential (Data NIMBY-ism)

- Candidate Analytical Frameworks/Metrics/Actions
  - Insight/Intrusion Paradox
    - Map the relationships of duties/rights and insight/intrusion among parties with access to given datum and measure information arbitrage advantage made available to each
      - Market of information arbitrage (Shannon entropy) provides monetary measure
      - Other metrics can be imagined.
    - Consider "thermal map" of relative insight/intrusion
    - What might be said about flows among insight/intrusion parties (information insight losers and winners)
      - Note that Carnot's equation of the 2nd law can be applied to determine both physics "work" and market "arbitrage"
      - Note that isothermy of 2 systems under 1st and 2nd law of thermodynamics is akin to market with no exchange energy
        - » What if the game theory prisoners knew the same information as the guards?
        - » See the "Empire of Exchange" for suggestion that market dynamic is desire for exchange
          - Is that exchange information transfer.
    - Put each Insight and intrusion on a "sliding scale" to analyze their relative balance in various contexts
    - Dynamic balance of scale over time
      - Example of the insight/intrusion balance in a policy context is provided by cases under the 4th amendment "exigent circumstances" or "border search" exemptions which are example of settings where the balance is recognized by courts to tip toward "insight" (aka the admission of evidence in court) with understanding of the implications of the consequent intrusion that results.
        - » The Insight/intrusion "balancing" is not just theory, but the object of the 4th and 1st amendment, suggesting that well conceived and executed digital identity and privacy architectures may help facilitate US Government operations consistent with constitutional rights.
  - [Other?]
- References

87. Bankruptcy Risk

- Challenges
  - To what extent is the system and/or technology dependent on systems and organizations in the supply chain or ecosystem that might cease or constrain their activities in the event of bankruptcy?
  - How can bankruptcies of critical stakeholders in supply chains be protected against in critical infrastructure and non-critical, but still heavily-depended-upon domains
    - such as social networks used in business communication, etc.?
  - How can bankruptcy laws be reformed to help foster more innovative development in IM, security and privacy domains, particularly in those jurisdictions that have harsh penalties for debt-related offenses
  - [Other?]
- References

87. Bankruptcy Risk

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider UCC concept of “cover” and solutions where supplier is forced to deliver substitute goods in supply chain context.
    - Is there a “cover” concept in mass-data settings?
  - Consider how identification of “gradients of interoperability” can help to identify potential alternative sources of supply in information supply chains when one stakeholder is bankrupt or otherwise reduces supply.
  - Consider differences of Chapter 7 and Chapter 11 status of bankruptcy on the ability of the supply chain to have access to assets or services needed to continue to perform functions for end users and critical infrastructure.
  - [Other?]
- References

88. Critical Infrastructure Issues

- Challenges
  - Does the system/technology play a role in the provision of services that are identified by one or more parties as critical infrastructure?
  - As a greater number of industries are dependent upon information infrastructure, should that expand the definition of “critical infrastructure”
    - what are the implications of that expanded definition?
  - To what degree does the subject technology or system protect or put at risk various critical infrastructures and in what ways)
  - PPP Problems: Given the high percentage of critical infrastructure that is owned/operated/controlled by non-governmental entities, how does the architecture and/or trust framework associated with the system/technology enable stakeholder participation in decision making that is critical to both producers and consumers of that critical infrastructure?
  - [Other?]
- References

88. Critical Infrastructure Issues

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider economics of commercial ownership and implications for operations in cybersecurity planning
    - ROI
    - Tax considerations (ITC and MACRS for security investments?)
    - Study CERT experience
  - Reprogram commercial engagement with cybersecurity
    - Government "power of the purse" may not be enough to move large 3rd party information network providers revenue needles. May need to consider strategies that recruit markets. Government as promoter of buying and selling coops model?
  - Neighborhood watch in markets – Consider UBER, Airbnb and eBay models that recruit resources to shared set of duties (with contract and UI). What are the shared assets and behaviors that need for cybersecurity. Organize COIs around shared interest in mitigating risk that they cannot address unilaterally.
  - [Other?]
- References

89. Incidental Risks

- Challenges
  - What incidental harms or consequential risks are caused by the achievement of the goals of the system/technology?
    - E.g., does a technology/system that enhances “security” result in privacy harms, and vice versa?
  - In what ways does does proprietary and/or privacy-enhancing system and/or technology constrain insights needed for system security and vice versa?
  - Are there balances in benefits and risks that can be balanced to achieve stakeholder goals in a given context?
  - Consider implications of deployment and operation at multiple levels (second-order, third-order, etc. risks).
  - [Other?]
- References

89. Incidental Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - How can insight/intrusion be balanced in real time and in context to avoid "overshooting" either goal?
    - Consider the "slider" model of insight vs. intrusion
    - Unpack "exigent circumstances" models from 4th amendment cases
  - What can history of insurance teach about incidental risks?
  - What models and maths can be applied to help anticipate and understand second order risks and other higher order implications of actions?
    - Consider "insurance" models (and related investment, cost-sharing and spreading and "hedging models") to address non-linear risks where potential harms are unknown in terms of severity, frequency, likelihood or incidence. Insurance for "unknown unknowns?
  - How measure the ways in which order is "shadowed" by disorder?
    - Can Shannon entropy model help identify situations where large information differentials (such as in consumer interactions, social institutional settings, commercial arbitrage settings or in strategic, geo-political intelligence settings) can reflect concentrations of order (negentropy) that the second law of thermodynamics (as described by Carnot, Clausius, etc.) suggests must yield increased disorder (entropy) elsewhere.
  - [Other?]
- References

90. Digital Estate Planning

- Challenges
  - In socio-technical information network systems, how do interruptions and constraints on interactions and information flow associated with the death or disability of a human in the system affect overall system reliability and security?
    - Institutional setting – What is succession planning for role covered by human?
    - Individual setting – What are dependencies of third parties on information flow from person
      - Account settings
      - Beneficiary designations to enable interaction continuity (consistent with estate plan)
  - Does lack of IM planning by individuals enable account hijacking of decedent's accounts?
  - When security is deployed in citizen-based systems (where various forms of market-based "neighborhood watch" are elements of the security play), how does the death or disability (through loss of legal capacity, competence to contract, etc.) affect security in the network associated with that "node."
  - Does the security, IM or privacy system/technology anticipate or accommodate disposition and management of data and other rights post-death of a data subject?
  - How is account (and its associated data, links, content, etc.) managed in event of death of registered user?
  - Do generic TOU/TOS terms serve the needs of individuals that use those systems?
    - Is account recoverable by designated user?
    - What about when user dies without relations?
      - Should data "escheat" to state
      - Should all data necessarily be deleted and destroyed in absence of data estate plan?
  - [Other?]
- References

90. Digital Estate Planning

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider preparation of model estate planning language that can be offered for inclusion in estate planning documentation to help address cybersecurity-related digital transfer issues.
  - Consider disposition of digital assets and other intangible assets under various state estate laws and U.S. federal tax rules
  - Consider treatment of online accounts under various Terms of Service and Terms of Use
    - Is data about a person transferable?
    - Is the decedent's social graph portable?
    - What are the practical and legal implications of actions taken after the death of a user of the system and/or technology?
    - Are there assets and/or data that might "escheat" to the state?
  - [Other?]
- References

91. Authentication-Related Risks

- Challenges
  - Does the system/technology help or hinder operation and improvement of existing and future identity authentication approaches?
  - For those technologies/systems that support anonymity and pseud-animity (and other similar modes of interaction) in identification and credentialing, etc., what are the implications of those modes of interaction for other systems that consume those credentials/attributes/ID signals?
    - How can attributes be matched with relying parties needs?
    - What
  - How do challenges of context in “Authorization” and “Access” interactions affect the analysis of authentication risks?
  - [Other?]
- References
  - Consider U.S. OMB 04-04 and NIST 800-63

91. Authentication-Related Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider how “Levels of Assurance” (LOA) might be updated for current and anticipated higher levels of interaction velocity and density?
  - Consider application of statistical methods based on interactions for authentication
    - Behavioral analytics as the “new authentication?”
    - Consider models of identity as “Lagrangian Coherent Structures” of Shannon entropy in data interaction flows.
  - [Other?]
- References

92. Authorization-Related Risks

- Challenges
  - Given the myriad contexts in which identity management and interaction risk systems/technologies are depended upon, how can technology and policy standards of performance for authorization-related risks system technologies and policies be established that are not too "ham handed" to enjoy adoption?
  - Does the system/technology help or hinder operation and improvement of existing and future authorization approaches (standard authorization for Relying Parties (RPs)?
  - [Other?]
- References

92. Authorization-Related Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - Given the myriad contexts in which authorization is engaged in, are "standards" possible for authorization?
    - If so, then what elements of authorization interactions lend themselves to standardization?
    - Consider both technology and separate policy standardization opportunities.
  - How can we enable a form of "mass customization" for authorization standards?
    - Create standards for generic elements of system/technology, and set of constrained elements to address different contexts.
  - What are the risks associated with standardization of authorization?
    - Consider risks for relying parties, data subjects, identity and attribute providers and others.
  - [Other?]
- References

93. Backward-Compatibility Issues

- Challenges
  - What are the risks and challenges of integration of the subject IM, Security or privacy technology into both technical and institutional/policy legacy systems?
  - What are the hurdles of the proposed technology or system being amenable to integration with or addition to ("blend in or bolt on") existing technologies and systems?
    - What other strategies can be considered to enable the acceleration of adoption curves of a given IM, security or privacy technology and/or system?
      - Consider strategies of recruitment of humans (as private citizens/consumers or employees) to enable existing organizations to "become" more effective socio-technical systems.
  - [Other?]
- References

93. Backward-Compatibility Issues

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider measurements of potential interoperability at multiple “Tools and Rules” levels.
    - Standard setting as pathway to system integration?
  - Consider education and training to enhance adoption and integration into existing systems.
    - [Other?]
- References

94. Ethical Considerations

- Challenges
  - What are the existing ethical constructions and systems that can help to inform new issues of IM, security and privacy?
    - UN Declaration of Human Rights
    - Other sets of individual identity and privacy principles
  - What are the processes that can help populations to self-derive ethical rules to help address new types of harms and interactions?
    - How can those emerging systems of ethics be most effectively integrated with other similar systems
    - Encourage normative "interoperability"
  - Ethics and normative guidance is under-developed in areas of rapidly evolving technology leading to a "normative gap" that is most rapidly (but not most sustainably) filled by market-based considerations.
    - Ethics in design
      - which stakeholders receive direct and incidental benefits?
      - Which stakeholders are burdened?
    - Ethics in deployment (e.g., broadband access issues)
    - Ethics in use of technology (e.g., can it be used In ways that are legal but still produce new harms)
  - To what extent can "ethical/normative" considerations be built or programmed into the system and/or technology?
    - If "ethics" involve norms that originate in "human" systems, what are implications of "programming" ethics into non-human systems?
  - [Other?]
- References

94. Ethical Considerations

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider application of multiple “maps” from this Atlas to help scaffold the analysis of ethical considerations
    - Compare “apples” and “oranges” that affect decision making in ethically-oriented contexts.
    - Use new metrics to create bridges among previously-distinct ethical contexts
  - Apply “ethics in context” analysis to identify sources of ethical compromise
    - Beware relativistic approaches to ethics that undermine consistent application of ethical constructions
    - See Nature Magazine article “When should your car kill you?” and consider market-implications of analysis beyond self-driving cars to other autonomous and semi-autonomous systems upon which security depends.
  - See “Business Ethical Considerations” map for separate discussion of that subset of considerations.
  - [Other?]
- References

95. AI and SI ("Synthetic Intelligence")

- Challenges
  - How does system/technology address AI and autonomous system issues regarding security, IM and privacy technologies?
  - How can human (and human institutional) governance be applied to the "black box" of AI/algorithmic decision making?
  - How does system/technology foster forms of "SI" (synthetic intelligence), which in most rudimentary form is situational awareness (precursor to a "neighborhood watch" among stakeholder groups?
    - SI systems may offer different self-regulatory opportunities from AI systems.
  - What is the relationship of the weighted inputs and outputs of AI (so called "sigmoid neurons") with market structures and other organizational structures (such as corporations, etc.) that cultivate weighted inputs and outputs?
    - Can those existing social and economic structures be helpfully analyzed as "distributed AI" systems?
    - Can emerging AI systems be helpfully evaluated in light of tools and analysis formerly applied to markets and organizations?
  - [Other?]
- References

95. AI and SI ("Synthetic Intelligence")

- Candidate Analytical Frameworks/Metrics/Actions
  - Can market structures offer mechanisms for governance of AI and SI systems?
    - What are the limitations of those forms of governance?
    - See NATURE Article on markets and AI entitled "When should your car decide to kill you?"
    - AI and SI-based systems generate insights (information arbitrage) that can have value (and the potential for harm if misused)
      - How can the value be maximized and the harm be minimized from such insight in ways that are consistent with human norms, and how can market mechanisms (and constraints) help to inform those structures
      - What are the opportunities for "self regulation" among distributed systems of stakeholders
        - » People-as-data-producers
  - If and to the extent that market and other organizational structures can offer insights into some of the benefits and challenges of emerging AI systems, what are the limits of that analysis?
    - See NATURE magazine article suggesting market failure of self-driving cars entitled "When should your car decide to kill you? [ref here]
  - Speculation of risk territory *Beyond* Perimeter 2.0?
    - Our AI anxieties are associated with the nervous anticipation of Perimeter 3.0 – i.e., the responses from the un-programmed "minds" of technology (See Map 7 – Bias Institutional)
  - [Other?]
- References

96. Expressive Leverage and Innovative Societies

- Challenges
  - In what ways can security, IM or Privacy technology and systems foster and support innovation, expression and social advancement?
    - Shift focus from prevention of harm to aspirational goals made possible by security, IM and privacy enhancement
    - How can security, IM and privacy be moved from defensive postures (and perception as "costs" without ROI) to being positive drivers of innovation, social and economic advancement, and cultural expression?
  - Can stabilization of interactions involving IM and privacy help to create a "safer space" for investment of time and resources for innovators to cultivate the rigor and investment needed to advance new ideas in the economy and society?
  - [Other?]
- References

96. Expressive Leverage and Innovative Societies

- Candidate Analytical Frameworks/Metrics/Actions
  - Protections for individual expression are among the rights preserved by multiple constructions in law, society and economics.
    - These protections enable individuals and institutions to "make the investment" of time and money, with the knowledge that they can enjoy the benefits from some consequent stabilization of their interactions involving their creative and expressive output.
    - Consider what elements of expressive output are stabilized as a consequence of enhanced IM, security, and privacy reliability
    - Consider first amendment (freedom of expression)
  - Compare history of IP as innovation "safe space"
    - IP paradigm includes the assertion that the protection (and constraint on copying, infringement, etc.) cultivates innovation.
  - How does reliability, predictability and normalization of interactions of IM, security and privacy help to create a "safe space" similar to the exclusivity (government recognized monopoly) of IP rights
  - Compare identity elements of scientific and academic publishing, where "currency" is reputation generated by publications quantity and impact.
    - See "ORCID" for initiative for IM in scientific publishing
  - [Other?]
- References

97. Change Management – Is Tech Amenable to Standardization?

- Challenges
  - How and to what extent is the technology and/or system standardized, built on existing and accessible (perhaps open) standards, or amenable to standardization?
  - To what extent is the optimization of the system and/or technology dependent on interoperability, and how can that be fostered through standardization?
  - What new interactions capacities (and corresponding risks) are created by deployment and use of the system and/or technology and are they of the type that can be subjected to measurement and controls under existing systems and standards?
  - What is the nature of the "patent thicket" associated with the system and/or technology
    - e.g., a mobile phone relies on implementations of hundreds/thousands of patents
    - how might that set of legal rights entanglements hamper design, development and/or deployment of the technology/system?
    - What is the form of SSO (standard setting organization) that might help to resolve the patent setting for the new system?
    - What are the hurdles to pursuing an SSO for the system?
  - [Other?]
- References

97. Change Management – Is Tech/System Amenable to Standardization?

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider existing SSO (standard setting organization) structures for IPR considerations and other similar structures applied to foster interoperability
  - Consider balance of dynamic change with stability of product offerings in markets
    - What elements of the system can be componentized to facilitate standards where helpful, but to enable other portions of the system to continue to evolve in response to market conditions.
    - What are the challenges of "bundling" where one company controls the multiple elements of a system, and desires to maximize distribution of existing product to enhance ROI?
  - [Other?]
- References

98. Change Management: Is Tech/System Amenable to Evolution?

- Challenges
  - Is the system and/or technology poised for further development and evolution to meet stakeholder needs in multiple markets and settings?
    - What needs to happen outside of the proposed system for that to occur?
  - Proprietary elements: Are core elements of the tech/system subject to IP or other proprietary control in ways that will constrain the creation of derivative works or contiguous technologies due to concerns about creating "infringing implementations?"
    - For Socio-technical systems, are there other constraints (such as privacy rules, community norms, etc. that impose similar constraints to proprietary constraints for businesses
      - Note "cross over" nature of individual economic harms
        - » Tort of Misappropriation
        - » Trade secret protection
  - What part of the system and/or technology is subject to "open source" treatment for IP or "open standards" structures of interoperability?
    - Are there security and privacy challenges associated with those "open" elements?
    - Can hybrid open/proprietary systems enable interoperability (and scaling) without compromising important security and privacy needs?
  - To what extent is it necessary for the system and/or technology to remain stable over time to optimize its advantages?
    - Can the elements that benefit from stabilization be isolated to enable variable rates of change in system elements?
  - [Other?]
- References

98. Change Management: Is Tech/System Amenable to Evolution

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider elements in "Time" Risk Map (#1) to stimulate consideration of rates and trajectories of system evolution and challenges of same for stable, reliable technology and systems.
  - Consider "process-oriented" systems that incorporate change as a favorable element.
    - Consider example that regular "change" in passwords enhances security
      - is it possible to conceive of other change oriented architectures that could positively impact security and privacy goals without imposing undue costs of change management
  - Consider biological models
    - Environmental processes of change management
    - Evolutionary processes of change management in niche change
    - Organismal processes of change management in growth
  - Consider non-linear displacements in complex systems (disasters, financial breaks, etc.) as forms of "abrupt change"
    - In what ways are preparations for and responses to change and non-linear displacement similar and different?
      - Consider ROI differences for preparation
      - Consider nature of probabilities affecting resource allocation decisions.
  - [Other?]
- References

99. Mass Media and Distributed Media Impact and Implications

- Challenges
  - How will technology/system be viewed in media?
    - Will perspective help or hinder adoption and improvement of system and/or technology?
  - How well suited is system and/or technology (and its effects) for contribution to media role in preserving social resilience and infrastructure resistance to cybersecurity-related failure and attack?
    - Does system and/or technology output data that can be easily consumed and interpreted by media
  - Can effect of system and/or technology be described in simple and accessible terms?
  - Does difficulty in understanding system function and operation hinder broad adoption of positive and effective “network hygiene” practices by general population?
  - [Other?]
- References
-

99. Mass Media and Distributed Media Impact and Implications

- Candidate Analytical Frameworks/Metrics/Actions
  - What are benefits, positive narratives and incentives that can be presented to support broad adoption of a technology/system to enhance “network effect” of positive reliability in information networks?
  - How do the shifts in the “attention economy” affect IM, security and privacy issues?
    - Can secure/reliable IM, privacy and security practices be iterated across new information channels and apps as they arise?
  - Like “product placement” in mass media by companies, can positive models of information network behavior be elaborated in other media outlets to enhance uptake?
  - [Other?]
- References

100. Institutional Decay

- Challenges
  - Existing institutions are all artifacts of history's earlier embodied solutions to earlier problems.
    - Some of those problems remain current, and enable those institutions to remain relevant.
    - Some new problems defy solution via existing institutions.
  - What is the general nature of such "institutional decay" and how might it be analyzed as a challenge of time?
  - Einstein's General Relativity described our environment as space/time
  - Human existential risk comes from its environment
  - Humans parsed space through the collective narrative of property
    - Property law is relationship among humans, not about relationship of humans to stuff (See bibliography author "Purdy" for ref.)
  - Humans parse time through the collective narrative of "institutions"
    - "Perpetual life" given to corporations by law from governments
  - But these institutions were granted auspices over time within a too limited space to "contain" global networked information space
    - Countries geographically limited – borders constraint
    - Corporations purpose is too limited – mission constraint
  - What are the institutional constructions through which humans can tame time in a trans-jurisdictional way?
  - [Other?]
- References

100. Institutional Decay

- Candidate Analytical Frameworks/Metrics/Actions
  - Human history presents examples of the use of institutions as vehicles to extend power through time
    - Monuments, pyramids, statues, flags and other physical artifacts reflect persistent reminders of institutional authority in physical world.
  - Distributed systems (distributed ledger is an example) are ways that humans "turn problems of time into problems of space" in the information world.
  - "Computational sovereigns" as offer pathway for humans to tame "wild time" (quoting ___), just as previously tamed "wild space"
    - Cryptography is form of computational sovereignty
    - Bitcoin was early effort at sovereignty of currency issuance
      - It was undermined because of inadequate development of its surrounding "rules" (policies, etc.) – See current parlance of "permissioned block chain" as solution
      - Other "Blockchain" (serial-hash) solutions
  - Apply relative inviolability-through-time of mathematics to help tame time for humans
  - Project mathematical certainty through time as form of sovereignty through managing risks of time
    - "Right to be remembered"
    - Forgetting is "anonymity in an expanded time coordinate"
  - [Other?]
- References

101. Interoperability as De-Abstraction of Duties

- Challenges
  - Data, information and identity are “intangibles” that occupy “abstract space”
    - The physical recording of information is not the “information” itself
      - information is intangible
      - Information is non-rivalrous
      - Information Can be infinitely duplicated without loss of fidelity
  - Physical symbols are used to “transfer” intangibles, including various “rights”
    - Cash or payment card systems transfer “money”
    - Licenses transfer copyrights rights
    - First discs, and then SaaS, transferred copyrighted works
    - Etc.
  - How can abstract concepts associated with Identity, security and privacy be made actionable through testable duties and standards of performance?
      - Time, physical space, interaction space, identity space
      - Compare other interoperable abstractions
        - » Kairos to Chronos for time – time standards
        - » Commons to property for space – occupy and possession standards for physical space
        - » Babel to language – interaction/communication standards
      - What is nature of similar duty de-abstraction for data space, identity space, security space
  - [Other?]
- References

101. Interoperability as De-Abstraction of Duties

- Candidate Analytical Frameworks/Metrics/Actions
  - Interoperable "Networks of Thought" (aka "memes" and "narratives") to create broadly "interoperable" human and institutional duties
  - Networks of memes rely on reinforcing symbols to invoke behaviors that are consistent with shared narrative of duties
    - "Stop at the red light" as distributed meme
    - Green paper with symbols is "good for all debts public and private"
  - Look at other broadly interoperable sets of duties created relative to other intangibles for duty clue strategies
    - IP licensing and infringement
    - Securities trading
    - Monetary policy
    - Property law enforcement
      - Ref: Jedediah Purdy "Property and the Legal Imagination"
  - [Other?]
- References

102. Interdisciplinary taxonomy and measurement gaps

- Challenges
  - Disciplines and sectors develop familiar metrics, analytical paradigms, language, taxonomies and other communication conventions known to members of the community
    - Normative aspects of such conventions range from informal “folkways” to formally statutorily-cross-referenced “industry practices”
  - Disconnect of communication elements “between” disciplines may hinder interdisciplinary communication and obscure hybrid solutions
    - Consider loss of Mars Orbiter due to failure to convert metric and imperial units of measurement
  - What strategies can be applied for gaps to be bridged most effectively in a given system/technology/architecture?
  - How can systems be designed to self detect and self heal gaps?
  - [Other?]
- References

102. Interdisciplinary taxonomy and measurement gaps

- Candidate Analytical Frameworks/Metrics/Actions
  - Create incentives for cooperation across disciplines
    - Consider outside funding to draw research together
    - Outside recognition of success
    - Narrative of common goals
  - Identify goals common to different disciplines
  - Consider machine learning/AI solutions to “self healing” systems
    - Could automatically fill gaps arising in systems as they arise
      - Compare to “immune system” function
    - Beware “positive feedback” in AI systems!
      - Self-healing information networks could potentially confuse “self” and “other” resisting human and institutional controls
  - [Other?]
- References
  - Ref: “The Immune Self – Theory of Metaphor” by Tabor for relationship of “self” and immunity.

103. Traditional Data Collection Structure and Focus Differences

- Challenges
  - Unstructured data is often an artifact of decisions made by initial data collector
  - Formatting and holding of data is not standardized
  - Needs of the initial data collector/data-base creator (that incurs the costs of data collection) are typically paramount in formatting and data structure decisions
  - Potentially useful data from other collectors and disciplines is rendered less accessible by heterogeneous formatting and structure.
    - This set of problems may be disappearing (or at least changing) with advances in various "big data" analysis approaches
  - "Notice and Consent" issues are implicated when data was collected for a stated purpose, and is later proposed to be used for a purpose with a different focus
    - It is particularly ironic when the later use wasn't even possible at the time of initial collection
      - See human tissue sample issues in large bio-banks
  - [Other?]
- References

103. Traditional Data Collection Structure and Focus Differences

- Candidate Analytical Frameworks/Metrics/Actions
  - Update research on challenges of analyzing unstructured data
    - Identify best practices for dealing with unstructured data
    - Consider pathways to semi-structured data
  - Consider separate risk map for analysis of “notice and consent” issues associated with later use of earlier-collected data.
    - Compare FIPPS (Fair Information Practice Principles) associated with “use specification” applied in various jurisdictions since early 1970s as one type of later use limitation.
  - [Other?]
- References
-

104. Export and Import Restrictions

- Challenges
  - Export and import regulations in various jurisdictions restrict or limit the transfers of certain technologies and systems into and/or out of the country
  - How might existing regulations affect deployment of security, IM and privacy technology in systems that are used in multiple jurisdictions?
    - Are applicable regulations helpful or harmful to achieving certain security, IM and/or privacy goals on global information networks?
    - How might those regulations be updated to better address current security, privacy and IM goals
    - Is the technology and/or system one that includes multiple components that are naturally divisible in a way that eases navigation of export and import restrictions?
      - Are there constraints on transfers of data during operations or other operating limitations that continue to apply even if a portion of the system components can be exported
  - With respect to limitations on data transfers, compare prior "EU Safe Harbor"/"EU Privacy Shield" and current GDPR as forms of data export regulation
    - Are these Non-Tariff Barriers to trade?
  - Consider various forms of cryptography that are subject to export restriction, and their use in or similarity to the cryptographic and other similar approaches applied in security systems.
  - When IoT devices are exported that contain cryptographic and other DRM-type limitations for data, how does that affect transfers?
    - Do exported or imported IoT devices automatically transfer data across borders?
  - What updates to export and import legislation and regulation are needed to accommodate new systems and architectures?
  - [Other?]
- References

104. Export and Import Restrictions

- Candidate Analytical Frameworks/Metrics/Actions
  - Do import and export regulations impede the transfer and distribution of certain technologies that are potentially applicable to security, IM and privacy systems and technologies?
    - What is the nature of those limitations and can they be accommodated while still promoting advancement of network standards for security, IM and privacy?
    - Is it the hardware, software, data or another components that invokes the limitation?
    - Can that limitation be addressed by "unbundling" the product, while still protecting national interests intended to be furthered by the regulation?
  - Are there treaties and bilateral agreements that can help to foster international transfers of relevant security, IM and privacy technologies and systems?
    - What are the risks of fostering import and export of the relevant technology/system?
      - National Security Risks?
      - Economic Risks?
      - Social Risks?
  - [Other?]
- References

105. Attack-Proofing Organizations

- Challenges
  - Of the several “AAAA risks” (Attacks, Accidents, Acts of Nature and AI/Autonomous Systems), Attacks include risks for various types of intentional behaviors by individuals and organizations.
    - Cyber attacks from various sources
    - State sponsored attacks/spying and industrial espionage
    - Commercially motivated intentional actions
    - Other intentional intrusions, denials of service, ransom ware incidents, etc.
  - Note unique elements of “Attack” versus other AAAA Risks
    - Persistence of attack
    - Intention drives intensity of threat
    - Different elements of predictability
  - [Other?]
- References

105. Attack-Proofing Organizations

- Candidate Analytical Frameworks/Metrics/Actions
  - The profile of “Attack” risks is different than other AAAA risks
    - Unlike Accident and Act of nature, “Attack” is more likely to have quality of multiple vectors, persistence
  - Note that AAAA risks are “sovereign risks”
    - The vectors of attack don’t “Play by the rules,” and are not “preventable” in the traditional sense
    - If “first order” risk of attack cannot be prevented, can still consider “second order” approaches to risk mitigation
      - “No-fault” Insurance,
      - Pooled funding
  - [Other?]
- References

106. “Act of Nature”-Proofing Organizations

- Challenges
  - Of the several “AAAA risks” (Attacks, Accidents, Acts of Nature and AI/Autonomous Systems), “Acts of Nature” include risks of various types of threat from natural occurrences
    - Consider threats of the type listed in the “Act of God” section of contracts
      - Strikes, hurricanes, earthquakes, floods, utility outages, wars, civil unrest, etc.
  - Note unique elements of “Act of Nature”
    - May occur in combination with other challenges that hamper recovery
      - Disasters, earthquakes, hurricanes, etc. may affect other systems that interfere with efforts at system recovery
        - » Lack of communication systems
        - » Lack of transportation systems for repair element
        - » Lack of electrical systems to power other systems
  - Some “Acts of Nature” are periodic, while others are non-linear.
    - Difficult to encourage parties to incur costs of preparation for infrequent occurrences.
  - [Other?]
- References
  -

106. “Act of Nature”-Proofing Organizations

- Candidate Analytical Frameworks/Metrics/Actions
  - The profile of “Act of Nature” risks is different than other AAAA risks
    - Unlike “Attack” and “Accident,’ it is more likely to have quality of multiple vectors or simultaneous interference with systems and multi-stakeholder harms.
  - Consider frameworks developed by national and NGO entities with operational experience in disaster settings
    - CERT
    - FEMA
    - NetHope
    - Red Cross
  - Consider community resilience models for information sharing based on other analogous structures
    - Community escrow?
    - Credit Union (based on common bond)
  - Note that AAAA risks are “sovereign risks” – may not be “preventable”
    - Consider second order approaches to risk mitigation
      - Insurance
  - [Other?]
- References

107. Accident-Proofing Organizations

- Challenges
  - Accidents, unintended consequences and risks associated with negligent behavior are by their very nature unpredictable
    - This can frustrate efforts by stakeholders to prevent and/or prepare for them
  - The profile of "Accident" risks is different than other AAAA risks, requiring alternative strategies to address these risks and additional costs and resources
    - Unlike "Attacks" and "Act of nature," Accidents may yield to actuarial and experiential analysis quality of multiple vectors
    - AI/Autonomous Systems at present levels of development are not recognized as being themselves culpable for either negligence/accident or intentional attack. The responsibility is still more likely assigned to the owner/operator of the AI/Autonomous system. Query whether the AI/Autonomous threats may eventually be more appropriately covered by attack and accident analysis in the AAAA framework?
    - Does the technology/system enable adaptations to improve its performance in light of operating experience among its user populations?
  - [Other?]
- References

107. Accident-Proofing Organizations

- Candidate Analytical Frameworks/Metrics/Actions
  - Note that AAAA risks are “sovereign risks” and are typically not “preventable”
    - Consider second order approaches to risk mitigation
      - Insurance is one form of risk sharing
  - The risk of accidents may be mitigated with training and education programs
    - Refine security and privacy technology/system curriculum to “unpack” AAAA risks, and focus on variations on strategies of prevention and mitigation
  - Because “accidental” risk may not be preventable by any stakeholders, it offers an opportunity to pool multiple-stakeholder resources into efforts to curb their occurrence (e.g., through joint training) and impact/severity (e.g., through insurance)
    - Consider opportunity for multi-stakeholder “risk commons” structures as framework to co-manage risks
  - [Other?]
- References

108. Risks From Interoperability

- Challenges
  - Interoperability provides benefits that can also "come with baggage" of third party elements and/or subsystems that may not perform as expected
    - Third party elements and services may enable pathway to viruses, attacks, etc.
    - Potential problems when third party system elements are interoperable, but have problems associated with performance of additional elements beyond those that are interoperable
  - Interoperability is a system characteristic that is typically associated with multiple systems and/or stakeholder use of standard technical specifications and uniform laws/rules
    - but specifications and laws that are insufficiently comprehensive (but are nonetheless sufficiently comprehensive to enable some interoperability) can yield "gaps" in expected system interoperability and performance that can result in new and additional risks and harms
  - Interoperability by its nature introduces multiple "doorways" into a system (both from a policy and technical perspective), and each such entry point is also a source of potential breach and intrusion
  - [Other?]
- References

108. Risks From Interoperability

- Candidate Analytical Frameworks/Metrics/Actions
  - Interoperability is a reinforcing quality of distributed systems, and it introduces new information architectures and flows into organizations that may result in security, IM and privacy risks
  - For issues associated with risks from dependencies on third parties (that are reinforced by interoperability), consider approaches taken in various "outsourcing" settings (including but not limited to various levels of "cloud" contracts) to assuring that third party elements are reliable, and that responsibility and liability for harms from risks are traceable to the responsible party
    - Compare "checklists" applied to cloud services negotiations for lists of possible "policy" harms encountered from reliance on 3rd party systems in ICT, data processing, etc.
  - Consider "stress testing" protocols and pre-deployment requirements that are designed to identify performance gaps
    - This is particularly important where a technology and/or system is deployed in contexts and settings that may not have been anticipated in the original design specification
      - Compare "off label" use of pharmaceuticals
      - Compare "dual use" maps
      - Consider NICE KU relating to "supply chains"
  - [Other?]
- References

109. Risks From Misuse of Statistics and/or Algorithms

- Challenges
  - The data outputs relating to performance of technologies and systems can sometimes be misinterpreted as indicating reliable performance of elements beyond those originally intended
  - Algorithms might not be designed for application in contexts and situations in which they are applied and relied upon.
  - Algorithms operating in machine-intelligence and other closed "feedback loop" settings such as in autonomous or semi-autonomous systems can be isolated from human, institutional, or other system intervention, preventing oversight
    - Compare harms from "positive feedback loops" in algorithm operations
  - Undue reliance on algorithmic certainty can distract attention of operators, users and relying parties from non-algorithmic elements of system which can result in harm
    - Compare legal concept of "detrimental reliance"
    - Compare nature of challenges of Bitcoin, Dau, and other early, deployments of block chain that failed adequately define system scope to account for necessary stabilizing components for system
      - Consider current discussions of distinction of "permissioned" and "Permissionless" block chain
  - [Other?]
- References

109. Risks From Misuse of Statistics and/or Algorithms

- Candidate Analytical Frameworks/Metrics/Actions
  - Stakeholders and users of systems should be educated and trained to assure that they don't "over-use" or "over-apply" technology/system data beyond intended scope
    - Compare "black box" map issues regarding undue or overbroad reliance on algorithms
  - Compare NICE KSA on "probability"
  - Consider risks to multiple stakeholders in the technology/system supply chain.
    - What are ways in which the "output" of a given technology/system can be "tagged" to alert subsequent users of that output against the hazards of "off label use" of the data, etc.?
    - Compare the risks to data subjects of use of certain regulated data beyond the original purposes for which it was collected
      - Secondary uses protections for data subjects
      - Enablement of research balanced with protection of data subject interests.
  - [Other?]
- References

110. Risk of Technology Mis-Application (Accidental)

- Challenges
  - Positive impact of technology or system in one setting may promote use in settings that are broader than the purposes for which technology/system was designed
    - Use beyond tested parameters may cause non-optimal performance
  - See “framework” of “Dual Use Technology” for intentional (as opposed to accidental) mis-application of technology.
  - Consider separate challenges of mis-application of of system and/or technology in wrong setting, by wrong parties, at wrong time, etc.
    - Multiple possible misapplications can lead to accidental harms
  - Consider offensive and defensive uses
    - What are potential contexts of accidental use or use in inappropriate contexts given the nature of the specific technology/system involved?
  - [Other?]
- References

110. Risk of Technology Mis-Application (Accidental)

- Candidate Analytical Frameworks/Metrics/Actions
  - Training and education can help users to understand limitations and appropriate/safe uses of systems and/or technologies
  - Internal alert systems, “deadman switches,” safety guards, and the digital equivalents of other design components can help to alert stakeholders and prevent users from engaging in potential misapplications to mitigate potential harms.
  - Deployment of successful technology/system in other contexts (“off-label use”) can lead to innovation in application
  - [Other?]
- References

111. IoT and Embedded Systems

- Challenges
  - With IoT, the functional interface of system and/or technology increasingly becomes the threat surface
    - Creating a situation where users may perpetuate harms without having an ability to mitigate those harms
  - IoT and embedded systems have unique characteristics that can create unique risks for which users and other stakeholders may not be prepared
    - Broad distribution makes security difficult
  - IoT processing power may be "hijacked" by third parties
    - Consider Botnet potential of IoT
  - Black boxes at Home
    - Lack of obvious data collection component makes consumer choices illusory
    - Lack of standards for notification and for user controls of IoT and embedded system functionality can interfere with efforts to curb harms
  - Lack of alternatives sources of equipment functionality can undermine positive user experience
    - Where IoT is linked to "feedback loop" will data collection failures undermine device functionality
      - E.g., will refrigerator shut down based on false signal from remote thermostat
  - [Other?]
- References

111. IoT and Embedded Systems

- Candidate Analytical Frameworks/Metrics/Actions
  - The source of the problems is the source of the solutions
    - Consider approaches to distributed security/privacy for distributed systems
      - P2P reputation systems AMONG IoT devices
        - » Linked devices can offer mechanism for "neighborhood watch" AMONG devices to help detect anomalous behaviors associated with AAAA risks
  - Consider hybrid "trust frameworks" of technical and policy standards to enhance deployment of IoT in various contexts
  - Consider "liability" standards that encourage adoption of "best practices" for system reliability and security associated with IoT and related harms
    - Consider "no-fault insurance" structures funded by device manufacturers to compensate victims?
  - [Other?]
- References

112. SCADA and Industrial Control Systems

- Challenges
  - SCADA system security and defense that focuses merely on protection of the system and/or technology from "attack" might ignore other additional potential harms and solutions for "hardening" SCADA and similar critical infrastructure programs
    - Consider also "Accidents" and "Acts of Nature"
    - Consider "secondary risks" to other systems that depend SCADA and could suffer from loss of system functionality
  - Balancing: How address dependencies in civil society and industrial contexts consistent with other rights and interests?
  - Given that much critical infrastructure is privately owned, what strategies can encourage investment in system and/or technology and training needed to protect systems
    - How overcome resistance to investment in updates when there is lack of demonstrable ROI to encourage internalizing costs
  - [Other?]
- References

112. SCADA and Industrial Control Systems

- Candidate Analytical Frameworks/Metrics/Actions
  - Look at SCADA from socio-technical system, not just as system and/or technology
    - How mitigate risks in system and/or technology
    - Help to justify investment by public (not just private owners)
      - Public investment can take form of tax breaks for SCADA improvements
    - How mitigate risks in human and institutional factors
      - E.g., how promote investment in security by private organizations that own and operate system and/or technology?
        - » How create ROI or spread costs to encourage investment
          - Insurance as shared risks
  - With respect to secondary harms (and second order strategies for mitigation of harm)
    - Analyze different systems by nature of system and/or technology in system
    - Analyze different systems by nature of risks associated with loss of functionality of system for relevant stakeholders
  - Consider systems to encourage investment in desirable systems/technologies by private companies that own critical infrastructure
    - Tax breaks for desirable investment
      - Compare investments for renewable energy
    - Safe harbors or limitations on liability for private entities that make needed investments
      - "Duty of care standard"
    - Better insurance rates for businesses that protect critical infrastructure.
    - More favorable borrowing rates for companies that cyber-protect their assets that secure borrowing
  - [Other?]
- References

113. Mobile Devices

- Challenges
  - Mobile devices and the systems that support them have unique characteristics that can create unique risks for which users and other stakeholders may not be prepared
    - Broad distribution makes security difficult
      - Compare IoT and Embedded system map
    - Broad deployment among untrained populations challenges behavioral standards
    - Conflicting technical standards in different jurisdictions and different systems makes interoperability and inter-system enforcement of system rules difficult.
  - Design, development and deployment of mobile devices anticipates a certain legal/regulatory operating environment that may be different than that in which a mobile device or system of devices, or subcomponents of those technologies and systems, is operated and used, causing performance gaps and regulatory concerns
  - Mobility of devices may hamper some enforcement efforts
    - Movement of the device beyond jurisdiction of authority
  - Intimacy of devices (in terms of physical contact with users and constancy of presence with users, etc.), creates unique opportunities for data "telemetry" to be collected
    - If insight and intrusion are inversely proportional, intimacy of mobile devices raises concerns about potential for intrusion, etc.
  - [Other?]
- References

113. Mobile Devices

- Candidate Analytical Frameworks/Metrics/Actions
  - To the extent that mobility is viewed through the lens of an isolated issue that introduces just the additional element of the physical location of the device, strategies for risk identification, measurement and mitigation can still gain benefit from other strategies that are not diminished by mobility
    - Isolate those risks that are associated with mobility per se from other sources of risk and threat to system
    - Consider risk elements that are exacerbated by mobility separately from those that are caused by mobility.
  - To the extent view other issues with "mobility," consider strategies associated with relevant Maps for application to mobile versions of technology
    - Intimacy of devices to humans
    - Conversion of BYOD issues into "Bring Your Own Network" challenges
  - [Other?]
- References

114. Cryptographic Elements

- Challenges
  - Cryptographic elements in systems and technologies introduce asymmetries of access and insight ("information arbitrage") into system outputs and operations that can hamper more traditional strategies of harm measurement and mitigation and system rules enforcement
  - Cryptographic elements introduce forms of "computational sovereignty" into systems that can render them independent of control through application of familiar controls and enforcement mechanisms
  - Systems and technologies that employ cryptographic elements to protect one group of stakeholders can introduce unique and new risks and harms to other groups of stakeholders that may require special and additional strategies and approaches to mitigation, auditing and enforcement
    - It is intrinsic in the use of technology that one party is intending to protect information from being available to another party, to the disadvantage of that second party – the remaining question is the nature of the protection and the normative alignment (or deviation) in a given context
    - Consider cryptography in data storage and communication
    - Consider block chain and other "hashing" approaches
  - [Other?]
- References

114. Cryptographic Elements

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider frameworks applied in efforts to regulate application of cryptographic "power" in other domains
    - Export regulation contexts
    - Preservation of "backdoors" by authorities
      - Are non-governmental authorities qualified and capable of providing trusted service of maintaining backdoors for exceptional circumstances
        - » Loss of key
        - » Law enforcement access
  - Consider whether information asymmetries associated with cryptography are amenable to adjustment and regulation through mechanisms applied to other information arbitrage settings
  - Consider whether power asymmetries reflected in narrative of risks associated with specific cryptographic deployments are (or are not) amenable to correction by cryptographic means alone
    - Stated otherwise: Does cryptography provide power that is contrary to sovereign power – the power of superior perspective/omniscience?
    - What does the ubiquity of cryptographic access suggest about the distribution of sovereign power
      - Consider Blockchain based currency as an example of sovereign power changes.
  - Separate out situations in which symmetric (e.g., Kerberos) and asymmetric (e.g., public key encryption) appropriate solutions?
  - [Other?]
- References

115. Quantum Computing Challenges in Socio-Technical Systems

- Challenges
  - Knowledge is power: Quantum computing and quantum communication technologies promise to offer users with exceptional new abilities in processing and transferring information that can create asymmetries in insight and secrecy, respectively, that can manifest in power asymmetries.
    - Where power asymmetries are not aligned with responsibility, risk can arise to parties that depend on the more traditional structures of responsibility
      - Governments
      - Other forms of centralized information gatekeepers
  - [Other?]
- References

115. Quantum Computing Challenges in Socio-Technical Systems

- Candidate Analytical Frameworks/Metrics/Actions
  - To the extent that quantum computing and/or quantum communication make available new powers of insight and secrecy that foster new forms of "Computational sovereignty," consider harm measurement and mitigation approaches associated with cryptography as potentially applicable to quantum computing and quantum communication approaches.
  - Assuming that additional power and authority is gleaned from the advances in quantum computing and quantum communication (via application/exploitation of the resulting information arbitrage), what are the mechanisms to help assure that the power will be applied and distributed consistent with context-appropriate norms and individual and institutional expectations?
  - [Other?]
- References

116. Data Administration and Big Data Operation

- Challenges
  - Collection and Processing Operations:
    - Parties involved in the administration and operation of big data systems potentially have access to unique insights (and higher-system dimensional perspectives) that can result in temptations (both individual and institutional) to exploit that information in ways that can harm data subjects and others, creating conflicts of interest in various forms
  - Collection, Processing and Transfer:
    - Standardized processes and/or concentrations of data associated with standard administration and operation systems of data collection, processing and/or transfer may create settings in which AAAA risks are exacerbated
    - Data "honeypots" may encourage Attacks
    - Data "arterials" and localized collection can increase the severity of harm and loss in the case of Accidents and Acts of Nature
  - System vulnerability
    - Paul Baran's distributed architecture developed for RAND was intended to make information networks less vulnerable, it did so successfully, and the same distributed architecture made them less subject to centralized control
      - How does the operational and administrative "concentration" in these distributed systems serve to undermine the security of the technology and system deployment?
        - » Concentration geographically – service farms, processing centers
        - » Concentration technologically –reliance on one or few operating systems, network platforms, etc.
  - [Other?]
- References

116. Data Administration and Big Data Operation

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider other frameworks that are designed to control potential conflicts of interest where intermediaries with access to superior insight are provided with access to information about third parties
    - Consider various sorts of fiduciary settings
      - Banking, law, medicine, etc.
      - Consider EU “operator” rules
  - Source of problems (distributed systems) is also the source of the solutions
    - consider systems of distributed “storage” and “processing” of data
      - Consider eBay, UBER, Airbnb model for data that “moves duties to the data instead of moving data to the duties.”
    - Compare proposal to use electric car batteries as storage for electric grid
  - [Other?]
- References

117. Technology Life Cycle

- Challenges
  - Lags and legacy systems:
    - Broad adoption of successful systems and technologies leads to dependencies that can impede timely updates and transitions to new desirable systems and technologies
      - Cost impediments
      - Training challenges
      - Change management challenges
  - User Adoption challenges:
    - Frequent updates to systems and technologies can exhaust user and operator patience and attention to updates, delaying or preventing broad transitions
      - Creates heterogeneous system profiles at large scales that can be exploited by Attacks, and subject to higher incidence of Accidents
  - Complex information system relationships:
    - Information network "supply chains" create a "risk thicket" that is not subject to centralized or coordinated management
      - Characterized by multiple bilateral agreements
      - Opacity of relationships beyond first order relationships heightens risks
  - [Other?]
- References

117. Technology Life Cycle

- Candidate Analytical Frameworks/Metrics/Actions
  - Lags – Consider policy regimes that reward behaviors that reflect current "best practices" and standard "duties of care"
    - Incentives for good behavior
      - Lower insurance premiums for good drivers/frequent password changers?
      - Contractual safe harbors – contractual and/or regulatory Limitations of liability for positive behaviors
        - » Form of "payment" for desirable actions
      - Tax credits/deductions for costs incurred to keep local instance of system up to date
  - Update Exhaustion
    - Help with profile of anticipated effort. Consider institutional constructions that can assemble and present predictions about future system and/or technology updates to help stakeholders to predict/presage future updates
      - Allows more accurate budgeting
  - Heterogeneity
    - Consider mechanisms that share and spread costs of updates among stakeholders to mitigate differentials among network update profiles
  - [Other?]
- References

118. Risk Analysis and Mitigation

- Challenges
  - Networked information systems and technologies are “dual use” technologies that can be used for BOTH harmful AND positive purposes
    - How can the positive purposes be maximized and the negative uses minimized consistent with optimization of the system?
      - Do we need a new definition of “optimization?”
    - From which stakeholders’ perspectives are the positives and negatives evaluated?
    - From which level of the system is that evaluation made?
      - Is evaluation of the “Greatest good for the greatest number” sufficient?
  - Recursive effects of system insight
    - How can the insights of the system be directed and applied to minimize risk
      - What is effect and risk of positive and negative feedback loops?
  - Insight and intrusion are inversely proportional in “dyadic” (2 party) interactions associated with networked information system function, and so will often have “winners and losers.”
    - One stakeholder’s insight is another stakeholder’s intrusion
    - How can benefits of insight be moderated to assure that they do not cause “undue” harm to the party that is the subject of that insight in a given context
  - How can interdependencies of risks of multiple stakeholders be managed?
  - [Other?]
- References

118. Risk Analysis and Mitigation

- Candidate Analytical Frameworks/Metrics/Actions
  - Dual Use Technology Risks
    - Consider ways in which data about data use can be included in system governance and feedback mechanisms to inform future use decisions
      - Aggregate data ABOUT data use can inform use profiles to help identify potential harmful settings
  - Recursive application of system data
    - Consider "Bayesian" learning as model for system development to gain security/reliability benefits from system data
      - Provide support to enable system stakeholders to "fail early and fail often" (Archetype of "Silicon Valley business model") to tighten and power "Bayesian feedback loops" for distributed systems
  - Insight/Intrusion "sliding scale"
    - Consider inclusion of "value" of insight as basis for calculation and consideration of negative value of harm
  - [Other?]
- References

119. Certification and Accreditation

- Challenges
  - How can users, data subjects and operators in broadly distributed and large scale systems assess the quality, reliability and other positive traits (and the absence of negative traits) of systems, technologies, products and services with which they interact in online settings?
  - How do the statutory requirements associated with certification marks in various jurisdictions affect the manner in which a certification program is deployed?
  - How can consistent standards of individual and institutional behavior be conveyed (and enforced) efficiently and effectively in broadly distributed systems and markets?
  - How does the technology/system fit in to existing certification regimes
    - Certification for regulated organizations
    - Certification for self-regulated organizations
  - Do the technology/system, and/or the metrics it generated lend themselves to certification structures?
    - Do they generate standard performance metrics?
    - Can the performance metrics be accurately reflected in certification marks? (simplicity question).
  - [Other?]
- References

119. Certification and Accreditation

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider positive and negative elements of self-certification programs and third-party certification regimes.
    - Different levels of verification at different levels of system dependency
    - Hybrid systems of self and third party certification
      - E.g., PCI-DSS
    - Match certification regime to length and attenuation of the supply chain
    - Consider expansive set of subjects for self certification
    - Consider using crowd sourced systems as third party verification
      - Neighborhood watch
      - [Other?]
  - Note antitrust consideration of commercial entity cooperation
    - Consider need for objective criteria in testing and accreditation
  - "Certification Marks" as defined under US Trademark law (and similar laws in other jurisdictions) anticipate the presentation of marks to consumers of services and products to help inform their buying decisions
    - Certification marks IP rights are owned by a different party than the party that displays them to consumers
      - Idea is to demonstrate conformity to "objective" set of third party standards
    - [Note other requirements of "certification marks" here]
  - See also, "IP as Information Network "Scaffolding" – Trademark
    - "Certification Marks" are distinct from "Trademarks" but are recognized in US Trademark statutes
  - [Other?]
- References
-

120. ADA and User/Operator Accommodations

- Challenges
  - Does the technology and/or system user interface, architecture and/or other elements enable (or diminish) access?
  - What are the boundaries of implementation of the technology/system in terms of operator and user capacity and capability?
    - Consider multiple vectors of capacity differentials among users and operators
      - Perceptual (vision, hearing, touch, etc.)
      - Physical
      - Cognitive
      - social
  - In addition to the potential for risk and harm to individuals participating in the system and/or using the technology,
    - is overall risk to the system operation and other stakeholders increased as a result of the failure of the system to accommodate stakeholders with different capacities and/or capabilities?
  - [Other?]
- References

120. ADA and User/Operator Accommodations

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider various sorts of physical, psychological, cognitive, behavioral, perceptual and other measures of user and/or operator behavior when assessing reliability of system from both individual perspective and overall system perspective.
  - Review ADA and other relevant authorities to provisions to assess system and technologies and to assure that technology and system performance are optimized across the user base
  - Consider populations with heightened sensitivities in positive way (in addition to the potential negative elements).
  - Consider aspects of socio-technical systems that could enjoy optimized performance with participation of populations with enhanced capacities, or engaged in activities in which system operation is incidental to their task
    - Compare use of "Captcha" function to decipher ancient texts
    - Compare Nathan Eagle's programs that recruit attention
  - Consider "compensating controls" that can help
    - E.g., Mercaptan is added to "odorize" colorless, odorless natural gas to de-risk its distribution
  - [Other?]
- References
  - SCIENCE magazine 10 May 2019, p. 544. Article about recruiting Aboriginal populations for spotting Yellow Spotted Monitor Lizards – different data with different observer acuity.)
-

121. Technical Simplicity

- Challenges
  - What is the level of simplicity of the technology/system, the simplicity of the UI and the relationship between the two?
    - Is the UI too simplistic so that it obscures certain operating risks (aka a “black box”), potentially exposing individuals to harm?
    - What is the nature of the “coupling” of the system operation to the UI?
    - What aspects of system operation are obscured to simplify the interface?
  - Does implementation and operation of system require special knowledge, training or degree?
    - Computer programming expertise?
    - Other specialized knowledge and/or skills?
  - What are the system dependencies resulting from these specialized requirements?
  - How can the system be simplified to enhance usability and decrease error incidence without enabling potentially harmful uses?
  - [Other?]
- References

121. Technical Simplicity

- Candidate Analytical Frameworks/Metrics/Actions
  - Paraphrasing Einstein's comment about explanations/theories, "System architectures should be as simple as possible, but no simpler"
  - Consider trade off of simplicity in design, UIs, etc. with loss of functionality and loss of user engagement
    - Balance of user engagement appropriate for context and minimal intrusion from "attention economy" perspective
      - E.g., could have high LOA (levels of assurance) with 4 factor authentication processes, but the inconvenience to users would drive them to work around system.
  - Consult with design parameters from various sources regarding UIs for other similarly complex systems that are deployed in consumer and institutional contexts
    - Consider BYOD (Bring your own device) issues and BYON (Bring your own network) issues associated with individual use for personal and organizational contexts
      - Individuals tend to favor using same devices at work and home, which can affect usefulness of systems and technologies that are made for only one or the other domain.
  - [Other?]
- References

122. Amenability to Education and Training

- Challenges
  - Above and beyond the issues of education and training of users regarding the use of the system or technology, is the technology and/or system *itself* useful and helpful in one or more of the domains that help to enhance/improve human and institutional performance within such systems
    - Consider domains such as:
    - Professional and Career development
    - Mentoring
    - Socialization
    - Diversity
    - Communication
    - Negotiation
    - Critical Thinking Skills
  - [Other?]
- References

122. Amenability to Education and Training

- Candidate Analytical Frameworks/Metrics/Actions
  - Examples of systems and technologies that are amenable to education and training include:
    - Those that lend themselves to familiar approaches to training and pedagogy
    - Those that can be readily included in “table top” exercises
    - Those that can be introduced in a familiar context in which education and training opportunities already exist
      - Teaching “secure coding” as part of computer coding class
    - Those that can can be offered online or in other scalable approaches.
  - Systems and technologies that can be architected in a modular form that may facilitate separation into discreet lesson plans, levels of training, etc.
    - In Cybersecurity context, consider different levels of training that is provided to individuals with different levels of clearance and design of learning modules to accommodate continuity of education and training across levels.
      - K-12
      - Undergraduate
      - Graduate level
      - Security-clearance level training
      - Professional training
      - Training of professionals in other domains regarding cybersecurity
        - » CEO, CFO etc. training about cybersecurity
    - Consider development of modules that can create continuity of education about the technology across different stakeholder roles
      - User
      - Professionals engaged in system operation
      - Third parties relying on system operation
  - Consider parsing training to track the NICE KSAs and other broadly recognized educational standards and approaches.

123. Bias – Network/System

- Challenges
  - Among the network/system biases that can increase system risk are those intrinsic performance trends, approaches and tendencies in the system that that reflect its:
    - Architecture
    - Structure
    - Operating system
    - and other qualities of networked system organization and operation
  - Network biases can sometimes increase risk by perpetuating security and performance paradigms that were applied in the original design, development and deployment of the system.
    - The particular network bias may have been functional in the context of the original deployment, but may be less so in other settings
      - If users and relying parties are not aware of these network biases, the system outputs can convey a false impression of performance and appropriateness of application in a given context and subjective application
      - E.g., if a credit card system machine learning algorithm used to detect fraud is tuned too sensitively, it can result in false positive readings, leaders to customer dissatisfaction with card unavailability
  - Includes such things as Connection bias, reciprocity arrangements, organizational identity boundaries (“Cylinders of Excellence”), Provincialism of efficacy, systems integration habits
  - [Other?]
- References

123. Bias – Network/System

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider network/system bias from multiple structural and architectural sources
    - Technology operating systems
    - Terms of Use/Terms of Service of online platforms
    - Business forms of organization (Corporate, partnership, etc.)
    - Organizational formation documents and mission statements
  - Consider the metrics and measurements consumed by the organization as potential evidence of the bias of the systems deployed by the organization
    - Like "x-ray crystallography" for organizations – re-construct structure of bias based on external evidence of where organization directs its "perceptual apparatus."
    - Like reading the "Poker face" of the organization
  - Compare map of "Organizational Structural Risks"
  - [Other?]
- References

124. Organizational Structural Risks

- Challenges
  - Related to network/system bias is the concept of intrinsic organizational structural risks
    - Both reflect intrinsic biases associated with application in practice by an organization of what might be called "organizational programming"
      - the sources of that "programming" are multiple
        - » Legal/compliance
        - » Technical
        - » Commercial considerations
        - » Other?
  - Network/system bias is that which arises from technical systems applied by the organization
    - Organizational Structural Risks are those that arise from non-technical, organizational systems applied by the organization.
  - Settings in which organizational structural bias can create risks for the organization include such examples as:
    - Dependency on default rules, policies and protocols – even in inappropriate contexts
      - E.g., Undue constraint of information sharing rules by organizations in disaster response settings
    - Ability of organization to operate outside of normal operations in ordinary course of business – such as in crises and disaster recovery
    - Operational resilience in settings of adversity
  - [Other?]
- References

124. Organizational Structural Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - It is conceptually useful to separately analyze organizational risk from operational risk as separate types of "structural risks"
    - Consider "organizational" (intended/imagined) flows of information in organization as compared to "operational" (actual) flows
- Consider governance innovations such as blockchain, smart contracts and other hybrid technical/legal settings in which "organizational" elements simultaneously invoke both technology and policy measures
  - Consider "trust frameworks" to document such hybrid systems
- Compare map of "Bias – Network/System"
  - [Other?]
- References

125. Resiliency and Adaptivity

- Challenges
  - How quickly can the system/organization/technology return to original function in various terms of quality and quantity following a displacement
    - how quickly can the system/organization/technology adapt to such changes.
  - What are the best strategies for different types of systems/organizations to prepare for resiliency challenges?
    - What strategies are best for risks "typical" of the sector/industry in which the technology is anticipated to be used?
    - What strategies using the technology/system are best for risks that are not "typical" for the sector/industry in which the technology/system will be used
      - Is there an opportunity for pooled risks among stakeholders to enhance resiliency against intermittent, occasional and other non-linear risks
        - » E.g., trade association insurance against shared threats
  - In what ways does the system/technology enable and enhance resiliency (return to critical function post event) and "adaptively" adjustment of critical function post event)
  - [Other?]
- References

125. Resiliency and Adaptivity

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider design and implementation of context appropriate “stress testing” that can provide advanced indications of a system/technology/organization’s ability to be resilient and adaptive
  - Review research for evidence that habituation/practice by employees improves performance in change management, and hence increases resiliency and adaptively
  - [Other?]
- References

126. Sustainability/Operating Costs of Technology/System

- Challenges
  - All entities (commercial, governmental, social, biological) operate under resource constraints which force them to consider the cost/benefit analysis of any solution or strategy.
    - What is the cost profile of the current system/technology during initial deployment and during ongoing operations?
    - Are costs of implementation and operation allocated to the parties that benefit from the system/technology?
      - If not, how are they allocated and is that allocation sustainable?
    - If not, what can be done to better align costs and benefits toward a sustainable model?
  - Is cost a limiting factor to adoption?
  - Is the overhead of legacy systems adding to the burden of new system acquisition?
    - How might "transition" be encouraged through incentives/penalties?
      - How can those incentives be funded?
        - » E.g., tax incentives for new investment, insurance premium hikes for outdated system and/or technology, etc.
  - [Other?]
- References

126. Sustainability/Operating Costs of Technology/System

- Candidate Analytical Frameworks/Metrics/Actions
  - In highly networked systems and systems with strong interdependencies (such as commercial supply chains) costs may be born by parties in disproportion to the benefit received.
    - System sustainability is enhanced to the extent that the system is able to directly or indirectly re-allocate the costs and/or is able to allocate benefits in ways that compensate parties that endure disproportionate shares of costs.
    - Consider various accounting mechanisms to capture costs to multiple parties in shared systems
    - Consider various mechanisms applied to help reallocate costs among stakeholders
      - Cost accounting?
      - Tithe
      - Taxes, tariffs, usage fees, concessions, licenses, etc.
  - [Other?]
- References

127. Autocatalytic Incentives?

- Challenges
  - It is often difficult for a system to independently generate and distribute sufficient volumes and types of new value that can help to incentivize various stakeholder groups to participate in a new system or technology.
    - Does the technology generate new sorts of "in kind" benefits that can be made available to one or more stakeholders directly or indirectly to encourage and participation and adoption of the system and/or technology?
    - E.g., social networks thrive on "network effect" through which a critical mass of users is needed to generate benefit to joining the network
  - Does second law of thermodynamics suggest that "perpetual motion" of autocatalytic incentives is impossible?
    - Can a system "produce" more value than it consumes?
  - [Other?]
- References

127. Autocatalytic Incentives?

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider structure and sources of monetary benefits made available by system operation and strategies for reallocating same in context of deployment of new system and/or technology
    - maximum flexibility/leverage at early stages of deployment/adoption
    - Can monetization made available to system stakeholders available through benefits provided to third parties as a result of system activity?
      - Consider models where third party benefits drive system
        - » Network TV advertising (free TV benefits paid for by 3rd party advertisers)
        - » Internet services (free social networks, search function paid for by 3rd party advertisers)
        - » Retail banking (free banking services (depository) paid for by third party lending activity
  - Consider benefits beyond monetary benefits
    - Consider "safe harbor" and other risk mitigation benefits available based on quality of actions or maintaining a certain status in a system
      - "Hold harmless" provisions in agreements
      - "Covenant not to sue"-type approaches
    - Does mixture of types of benefits for different types of stakeholder allow "side-stepping" the second law of thermodynamics, and producing a net gain in "value" (Shannon negentropy), in effect a perpetual-motion machine of value creation?
      - If "Maxwell's Demon" (second law thought experiment) does apply, where does the "entropy exhaust" end up?
  - [Other?]
- References

128. Black Box Operations?

- Challenges
  - What is the degree of operator and/or user discretion and/or control of the technology/system that is made available in the course of its operation?
    - Note the Algorithm black box problem raised in Science magazine Article [citation here]
  - To what degree is the system/technology auditable, transparent?
    - What are the limits of auditability of system operations?
  - How are tasks organized to eliminate or limit problems associated with runaway positive feedback loops and/or context-inappropriate applications of a system/technology?
  - How can the risks of "black box" elements of the system be isolated or accounted for in larger systems that depend upon those operations?
  - [Other?]
- References

128. Black Box Operations?

- Candidate Analytical Frameworks/Metrics/Actions
  - As degree of autonomy increases, need for auditability and transparency increases
    - Consider selective policy/incentive/penalty "control rods" for governance of system operations at critical decision points
      - "kill switch" approach to prevent runaway positive feedback loops
  - Where machine learning or other systems don't generate an auditable record of internal decision-making processes, consider alternative metrics to capture and preserve to inform future system/technology design/development/deployment
    - Compare reverse engineering techniques "x-ray crystallography" and similar methods for reconstructing original patterns
  - Where complexity of operations precludes human or institutional oversight of "black box" operations, consider alternative approaches for "isolation" of risks through allocation of liability and responsibility for harms caused by systems
    - Consider "strict liability" standard for harms done by systems
      - Like liability of owners of wild animals, or sellers of explosives
    - Consider "no fault" insurance arrangements to spread costs of damages for harms to population that benefits from systems
  - [Other?]
- References

129. B2B v. B2C v. B2G

- Challenges
  - Information networks are ubiquitous, but their subsystems are sometimes designed for operation in a subpart of the larger network.
    - Is the intended/desired operation of the system or technology dependent on certain assumptions made with respect to the composition or context of markets and, if so, what are the implications for deployment in other markets?
      - E.g., BYOD was originally a problem of consumer devices being introduced into commercial (employee) contexts
      - E.g., the Internet was intended as a piece of defensive weaponry (See 1966 Paul Baran paper at RAND corporation), but found its way into civilian operation with unintended consequences
      - Certain levels of encryption and other defensive and offensive security measures are available only to subsets of the user population.
  - Are there potential secondary harms associated with the use and operation of the system technology in the context of interactions of a type for which it was not designed
    - In what ways is the system/technology dependent on market assumptions?
  - When
  - [Other?]
  - [References?]

129. B2B v. B2C v. B2G

- Candidate Analytical Frameworks/Metrics/Actions
  - Systems engineered and architected for security, IM and privacy goals in one class of interactions may yield unexpected results in other contexts.
    - BYOD problems relate to this challenge
    - Encryption standards parse different categories of users
    - Individual users don't have ITC support structures available to institutional users
  - Note that B2C transactions invoke consumer protection-type laws, while B2B/G do not
    - E.g., FTC privacy activity in consumer contexts
    - E.g., GLB, HIPAA and FERPA privacy provisions
    - E.g., state data breach notice statutes
    - E.g., Warranties (Magnuson-Moss in the US) imputed to advertising declarations of sellers
  - Note that there are certain types of transaction friction that apply to a subset of technology transfers that may be affected by the types of exchange being engaged in, for example:
    - Sales tax doesn't apply to wholesale sales (VAT is reimbursed in wholesale interactions)
    - Government procurement regulations may guide system/technology design and development in ways that don't need to constrain non-governmental applications of a given technology
  - [Other?]
  - [References?]

130. Nature of Technology/System Measurement

- Challenges
  - Risk is frequently associated with failures of measurement
    - Ignorance of need for measurement
      - Unmeasured system parameter is an unknown risk
      - E.g., No temperature sensor in battery compartment of Boeing 777
    - Reliance on wrong measurement
      - What gets measured gets done, but measurement of the wrong system quality can provide a false sense of security regarding unmeasured parameters
      - E.g., GNP (Gross National Product) as measure of national financial health has been criticized as narrowing the attention on other quality of life measurements
  - Context can drive efficacy of different types and standards of measurement
  - What do proposed system performance and impact measurements indicate?
    - Are system performance metrics capturing all relevant parameters of system operation and risks?
      - If not, what is missing, and what are the mechanisms to improve the metrics?
    - Need to distinguish among measurement systems in operation
    - Data measurement scales and variables include nominal, categorical, ordinal, interval and ratio
  - Question of relative value of measurements of parameters that are correlated with system function versus capture of causative factors.
  - [Other?]
- References

130. Nature of Technology/System Measurement

- Candidate Analytical Frameworks/Metrics/Actions
  - Evaluate totality of measurements used in decision making in given system/technology
    - Contemplate unmeasured qualities of system by residual identified unknowns in system
  - Consider categories of metrics based on correlation vs. causation and respective roles for each type of measurement in system
    - Don't dismiss correlative metrics, particularly in absence of knowledge of causative relationships
      - Particularly in "black box" settings where "causation" relationships are unavailable.
  - Consider different current system measurements and what they represent, and whether they are being applied too narrowly and/or too broadly in practice. Types of numbers – ordinal, nominal, etc. (see ref for 5 types and use blood pressure example to illustrate)
    - Characteristics – (blood quantity)
    - Performance – blood pressure
    - Relationship – optimal blood pressure
    - Capacity for change – band of
  - [Other?]
  - References: See E.g., Art Brock's work on parsing of systems of measurement

131. Degree of Disruption

- Challenges
  - Innovation is perceived as generally desirable, but is often the driver of disruptions that are costly for various elements/components of a system
    - How can an individual an/or institution best evaluate the relative burdens and benefits of disruption in contemplating a system change, upgrade, etc.
  - In increasingly interoperable architectures for ITC, the presence of frequently-less-secure and less-private "legacy" systems undermines broader system security and privacy
    - How can resistant legacy systems be encouraged to traverse the prohibited "threshold energy" of costly disruption to be brought into conformity with broader systems best practices?
  - There are few available measurements (other than direct and indirect costs (the latter of which is frequently a "ballpark" figure) of the various degrees of disruption to help guide decisions of individuals and institutions regarding investment in and adoption of new systems and technologies.
    - Existing metrics are primarily market/economic considerations, which mask many elements of social, political and cultural disruption that can ultimately be adverse to system goals.
  - What are the metrics that can inform stakeholder decision making regarding the degree of disruption in information networks?
    - What is relationship of stability and disruption for different stakeholders from same action
      - Consider notion of "entropy" in context of "zero sum" analysis of disorder and disruption
      - Consider metrics that can help parse mutual, simultaneous disorder NIMBYism
  - [Other?]
- References

131. Degree of Disruption

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider hybridization of multiple Atlas "risk maps" as one mechanism to evaluate relative degrees of disruption from multiple stakeholder perspectives.
  - Consider "goals weighting" exercise to enable stakeholder groups to improve strategies of engagement among stakeholder groups of relative levels of disruption in and among communities
  - Consider the extent to which elements of the system/technology operation are amenable to traditional industrial organizational principles, systems engineering principles and other frameworks for allocating disruption and disorder
  - Consider various "change management" frameworks as sources of assistance for managing ITC, security, IM, privacy and related system changes.
  - [Other?]
- References
  - See NATURE magazine article on SDG "Goals Scoring" strategy for potential process for multi-stakeholder evaluation of heterogeneous goals at: http://www.nature.com/news/policy-map-the-interactions-between-sustainable-development-goals-1.20075

132. Quality of Testing/Use-Cases Applied

- Challenges
  - Was adequate criteria applied for selection of testing protocols and use cases during design and development stages of system/technology?
    - Are the selected protocols and use cases representative of what a system and/or technology will encounter in the field?
      - Were they selected non-objectively for maximum "positive" results which fosters adoption but skews reliability and usefulness?
  - What are the standards, protocols for evaluating the quality of use cases and testing protocols for the subject technology/system?
  - How should the clarification of testing/use case protocols be linked to auditing and enforcement mechanisms meant to stabilize behaviors of stakeholders through time?
    - What gets measured gets done, so link of shared measurements through all phases of product/system design, development, deployment, testing, audit should be linked or at least correlated to assure that performance in operation helps inform technology and system improvement.
  - What subset of existing testing protocols and use cases are inappropriate for use in broader contexts because they reflect influences that are different than system reliability/security needs?
    - When, and in what ways, do non-objective criteria and slanted use cases negatively affect cybersecurity and privacy systems?
  - [Other?]
- References

132. Quality of Testing/Use-Cases Applied

- Candidate Analytical Frameworks/Metrics/Actions
  - Need to develop parameters for testing of testing protocols
    - Who will “watch the watchers?”
    - Who will “test the testers?”
  - Need to develop standards and criteria for development and testing of Use Cases
  - Need to encourage publication of null and negative results in cybersecurity and privacy testing
    - Consider contrary challenge of publication as revelation of system weakness
    - Compare NSF and NIH programs to require publication of negative results in sponsored scientific research.
  - [Other?]
- References

133. Threat Vector Sub-Analysis

- Challenges
  - AAAA Risks (Attacks, Accidents, Acts of Nature and AI/Autonomous Systems) reflect only the "first order" parsing of risks, and each category contains myriad sorts of threats that warrant further investigation and analysis if they are to be better understood and addressed
  - Ignorance of specific source of harm or threat undermines defensive and mitigation strategies for cybersecurity and information network integrity. Compare:
    - Ignorance of sources of disease prevention causes waste of resources directed against false harm vectors
    - Misunderstanding of complex market relationships feeds arbitrageurs, high-speed traders, etc.
  - Security "tunnel vision" leaves systems exposed to unanticipated risks
  - How can threat vectors that are sub-categories of all types of AAAA risks be evaluated to improve efficacy of risk mitigation?
    - What is nature of causative relationships where multiple factors feed into risk setting?
    - How can the interdisciplinary study and practice of risk mitigation be improved through normalization of risk analyses?
  - [Other?]
- References

133. Threat Vector Sub-Analysis

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider relationship to “Scale” maps in atlas
    - Address relationships within AND among levels of system
  - Triage attention toward refinement and subdivision of risk models to maximize efficiency of existing security resource deployment
    - Also attend to resulting “externalities”
    - Red Flag risks that arise whenever you hear phrase “that is out of scope.”
    - Establish the practice of “mining the externality” for new risk insights
  - Mature models of cybersecurity and network integrity will “unpack” sources of risks as they are encountered to better understand potential strategies and tactics to prevent and respond to risks
    - Compare model of human (and avian) learned immunity systems, as compared to innate immunity.
  - Start with known risk categories and consider differences within that category
    - E.g., for “Attack” is the nature of the attack for economic or political gain
      - What are the attack profiles and potential defenses and mitigations for the two different scenarios and how do they differ
    - E.g., for “Accident” is the nature of the cause due to lack of training, or intentionally ignoring risky situation, etc.
  - [Other?]
- References
  - Ref. Jennifer Best “Governing for Failure” in Bibliography

134. Degree of Habituation and Adherence

- Challenges
  - To the extent that the exercise by counterparties of discretion in interactions is viewed by stakeholders as risky, assurances of behavioral predictability can reassure parties and decrease transaction friction.
    - Contracts perform the function of aligning expectations of parties on various negotiated points.
    - What other avenues can be applied to encouraging behavioral predictability
      - Habituation of response
      - Adherence to norms and rules
      - Other
  - Various studies support the notion that reliable performance of humans (and socio-technical systems of which humans are a part) is strongly dependent upon training and habituation of behaviors that are consistent with system rules
    - What are the evaluative criteria to establish predictive metrics for this critical element
    - Is subset of research on “autonomous” systems applicable to “autonomous” reactions of humans acting in a representative capacity in institutional settings?
  - How can useful performance metrics be developed for security performance by socio-technical information systems, including the notion of “SAAR” (Security-as-a-Reflex)
    - How measure SAAR in citizen populations?
  - [Other?]
- References

134. Degree of Habituation and Adherence

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider game-ification of scenarios to engage various individual stakeholders
  - Consider training modules, checklists and other materials to make available to citizens to encourage predictable behaviors and responses
  - Consider analogy to practice “drills” and “exercises”
    - Earthquake “Drop and cover” drills
    - Change battery in smoke alarm when change clocks for daylight savings time
    - “Look both ways before you cross the street”
    - “Look before you leap” – “think before you click?”
  - Compare and contrast setting with other models of commercial distributed reliability
    - Bank notes and coins anti-counterfeit measures
    - Commercial “brand” awareness and loyalty building
    - Compare PCI-DSS model that pushes financial responsibility to “insecure edge” of half-open system of payment cards
  - [Other?]
- References

135. Portability of Situational Awareness

- Challenges
  - How do you cultivate awareness and response to system challenges in massively distributed systems?
  - Big data “insights” include those associated with security, IM and privacy awareness arising with respect to system operation
    - What are the mechanisms through which awareness of these and other system challenges can be spread through the system to enhance appropriate system response?
  - Interoperable information networks yield high degrees of interconnection that enable responses to breaches of system integrity to spread “like wildfire.”
    - What are mechanisms to enable security responses and defenses to system integrity to can enjoy rapid and broad adoption?
  - In complex systems, users and operators filter information to enable them to focus on the most relevant information
    - How can relevant security, IM and privacy related information be made available throughout a system most efficiently?
  - [Other?]
- References

135. Portability of Situational Awareness

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider incentives for "nodes" in system to pay attention to larger system operation
    - Incentives and penalties coax performance within parameter band established by various standards for behavior of technology (via specifications) and people/institutions (via laws and norms)
    - Uniformity of performance around standards makes it easier for stakeholders to detect aberrational behaviors in system
  - Consider also biological immunity models
    - Innate versus learned immunity (Metchnikoff)
  - "Zero-Day Exploit" models
    - Zero-day exploit "buying cooperative" among nation states as form of cyber-symbio-genesis and DMZ creation for shared commercial interests?
    - Is ZDE market amenable to shared risk model (at least in part) based on AAAA risks as uncontrolled externality common to nation states?
      - Contrary trend of unilateral weapon-ization of ZDE
  - [Other?]
- References

136. Transferability of Risk

- Challenges
  - When risk (such as AAAA risks) cannot be prevented, how can the harms and costs be shared/spread among stakeholders to enhance overall system resilience?
  - Is the given risk context one that lends itself to pre-planning for risk transfer/sharing, or can that only be achieved after the harm/damages are incurred?
    - Is an “ounce of prevention” perceived as being worth “a pound of cure?”
  - What are the available vectors of risk sharing?
    - Pricing, Monetary systems (e.g., insurance)
    - Social/regulatory systems – harm NIMBY-ism, zoning
  - [Other?]
- References

136. Transferability of Risk

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider alternative vectors of risk transfer
    - Reputation systems (for individuals, institutions)
  - Consider traditional and emerging insurance models
  - Consider Community support models
    - Credit Unions ("Common Bond") recognize social bonds as reducing risk in financial contexts
  - Consider timing issues of risk
    - What is narrative to support acceleration and internalization of costs prior to risk being realized?
  - Link governance with community interests
    - Build interest in efficacy of system
      - » Neighborhood Watch model
  - [Other?]
- References

137. Degree of System Failure Tolerance

- Challenges
  - To what extent will the failure of the system/technology be "tolerated" by relevant stakeholders?
    - What types and degrees of "tolerance" have what sorts of implications for system operation
      - E.g., Do users have option to migrate to another system?
      - E.g., Do employees' failures to periodically reset passwords affect organization cyber risks?
  - What are the implications of different types and degrees of "dependency" on the system/technology?
  - What are the "second order" implications of failure in a given system?
    - Are stakeholders that depend upon a system, but who are not involved in its operation harmed by "tolerance" or parties in a system.
      - This is a form of risk-cost-NIMBYism
    - Compare aphorism in public administration about imposing charges on stakeholders that "don't have a vote" in the system.
  - [Other?]
- References

137. Degree of System Failure Tolerance

- Candidate Analytical Frameworks/Metrics/Actions
  - Compare arrangements of governance frameworks for “High Reliability Organizations” (HROs)
    - Assumption of failure
    - Migration toward standards
    - Etc.
  - Consider “assumption of breach” models
    - Project narrative of risk setting to invite behavioral and expectation changes.
  - Construct models for security in open systems
    - Consider traffic laws as analogy, etc.
    - Unpack risk from different “AAAA sources”
      - Attacks
      - Accidents
      - Acts of Nature
      - AI/Autonomous Systems
  - [Other?]:
  - References:

138. Legal/Jurisdictional Constraints

- Challenges
  - To what extent is the design/architecture of the technology/system based upon its anticipated use/deployment in a particular legal/jurisdictional context?
    - What are the deployment limitations associated with those architectural constraints?
      - What are the potential harms to stakeholders if the technology/system is deployed in an unanticipated/inappropriate context?
      - E.g., are there some "background laws" that offer protection for system stakeholders in one jurisdiction that are not present in another jurisdiction, thereby undermining system performance?
    - Can those jurisdiction-based limitations be overcome with alterations to terms of service or other contractual changes to "localize" the technology/system by accommodating local laws and legal standards?
  - [Other?]:
  - References:

138. Legal/Jurisdictional Constraints

- Candidate Analytical Frameworks/Metrics/Actions
  - Identify whether areas of legal difference that are currently perceived as constraints offer opportunities for conceptual arbitrage
    - Compare forum shopping in tax planning, IP planning
    - Compare treaty processes to bridge populations under different rules
    - Consider market and other mechanisms for sharing/spreading risk across legal borders
  - Trace out philosophical roots of local laws to identify areas of difference and similarity.
    - "Gerrymander" areas with shared philosophy into communities of interest around shared norms documented in shared terms of information network engagement
      - Then explore links of similarity and difference among COIs.
    - Consider philosophical foundations of legal and jurisdictional rule constructions as "operating systems" of law
    - Identify shared philosophical constructions as basis for future mimetic alignment of rules
  - [Other?]:
  - References:
    - OECD Paper entitled "Personhood" (notes "Identity" roots of Hegel in EU, and Locke in U.S.)

139. IP as Information Network "Scaffolding" - Copyright

- Challenges
  - The term "copyright" describes a set of relatively-well-established specific rights associated with specific types of works
    - works of authorship, fixed in a tangible medium of expression, etc.)
  - Trust in information networks (and the many systems that depend upon them) is proportional to the stakeholder realization of various types of rights OTHER THAN copyright, many of which are not fully developed/matured in the online context:
    - E.g., privacy rights, publicity rights, proprietary rights, various security rights, "quiet enjoyment"-type rights (to be free from intrusion by nuisance, tortious behavior, criminal behavior, etc.), civil rights, etc.
  - How might established copyright law provide a scaffolding for supporting the development of other rights associated with reliability of socio-technical networked information systems?
    - What are the limits of what copyright can do to help?
    - What lessons can be learned from the history of copyright as a mechanism for the transfer and handling of intangible rights?
  - Is the concept of "property" intrinsic in copyright as "IP" fundamentally adverse to concepts of co-management that will be necessary to support scaled reliable information network systems?
  - How does the concept of "Moral Rights" (Droit Morale) in Europe relate to EU treatment of personal data
    - Is there a connection of expressive output/production with "self" manifest in both areas?
    - How does that conception help map the boundaries between EU and US concepts of production and commodification of labor in goods?
  - [Other?]

139. IP as Information Network "Scaffolding" - Copyright

- Candidate Analytical Frameworks/Metrics/Actions
  - Copyright as Scaffolding for Information Rights:
    - Compare copyright license terms for technical specifications produced by technical standard setting organizations (SSOs) as potential framework for multi-stakeholder policy standard-setting organizations
      - Parse rights in design, development and deployment phases
  - Copyright as Analogous Authority for Information Rights:
    - Copyright as "property interest"
      - Note Ref: Jedediah Purdy – (property as social construction and shared hallucination).
    - Copyright as vehicle for trading in intangible commodity
      - Note scaling challenges of bilateral contracting in property construction
        - » ASCAP/BMI history
    - Copyright as supply chain discipline tool
      - Consider history of EULAs (end user license agreements) as bridge of tangible and intangible rights management
      - Uniform Commercial Code treatment
  - Copyright as distributed process for distributed challenge
    - No general "copyright police" – rely on private rights of action
    - Compare "neighborhood watch" – vigilance of parties with interest
  - [Other?]
- References

140. IP as Information Network "Scaffolding" - Patent

- Challenges
  - The term "patent" describes a set of relatively-well-established specific rights associated with specific types of works
    - a government grant that confers a right for a set period to exclude others from making, using, importing or selling an invention without permission, etc.)
  - While the technical aspects of information networks involve the interoperation of a vast array of patented technologies, Information networks as socio-technical systems also rely on various types of rights OTHER THAN patent, many of which are not fully developed in the online context:
    - E.g., privacy rights, publicity rights, information rights, confidentiality rights, proprietary rights, various security rights, "quiet enjoyment"-type rights (to be free from intrusion by nuisance, tortious behavior, criminal behavior, etc.), civil rights, etc.
  - How might established patent law provide a scaffolding for supporting the development of other rights associated with networked information systems?
    - What are the limits of what patent law can do to help?
    - What lessons can be learned from the history of patent as a mechanism for the transfer and handling of intangible rights?
  - Patent as analogous authority?
    - Is the concept of "property" intrinsic in patent as "IP" fundamentally adverse to concepts of co-management that will be necessary to support scaled reliable information network systems?
  - [Other?]
- References

140. IP as Information Network "Scaffolding" - Patent

- Candidate Analytical Frameworks/Metrics/Actions
  - Patent as Scaffolding for Information Rights:
    - Compare patent ("necessary claims" etc.) license terms produced by technical standard setting organizations (SSOs) as potential framework for multi-stakeholder policy standard-setting organizations
      - Parse rights in design, development and deployment phases
      - Consider SSO patent Kabuki as akin to Collective Escrow of rights, with specification approval as rights release event.
  - Patent as Analogous Authority for Information Rights:
    - Patent as "property interest"
    - Patent as vehicle for trading in intangible commodity
      - Note scaling challenges of bilateral contracting in property construction
        - » SSOs as contractual solution to "Patent Thicket" problem
    - Patent as supply chain discipline tool
      - Market Management
      - Challenges encountered at border of human rights and patent rights
        - » Compare Pharmaceutical patents
        - » Consider indigenous knowledge issues at intersection of IP and "identity"
  - Patent as distributed process for distributed enforcement challenge
    - No general "patent police" – rely on private rights of action
    - Compare "neighborhood watch" – vigilance of parties with interest
  - [Other?]
- References

141. IP as Information Network "Scaffolding" - Trademark

- Challenges
  - The term "trademark" describes a set of relatively-well-established specific rights associated with specific types of IP works
    - word, phrase, design, legally registered or recognized from use as indicating provenance or product or service, etc.)
  - Information networks rely on various types of rights OTHER THAN trademark, many of which are not fully developed in the online context:
    - E.g., privacy rights, publicity rights, proprietary rights, various security rights, "quiet enjoyment"-type rights (to be free from intrusion by nuisance, tortious behavior, criminal behavior, etc.), civil rights, etc.
  - How might established trademark law provide a scaffolding for supporting the development of other rights associated with networked information systems?
    - What are the limits of what trademark law can do to help?
    - What lessons can be learned from the history of trademark as a mechanism for the transfer and handling of intangible rights?
  - Is the concept of "property" intrinsic in trademark as IP fundamentally adverse to concepts of co-management that will be necessary to support scaled reliable information network systems?
  - What role can certification marks play in establishing trust in emerging rights networks?
    - What are the "green washing" challenges associated with data/identity certification?
  - [Other?]
- References

141. IP as Information Network “Scaffolding” - Trademark

- Candidate Analytical Frameworks/Metrics/Actions
  - Trademarks as scaffolding:
    - “Brand” notion is a subset of “Trust” concept, and is symbolically carried by TM
    - How can trusted “brands” help to enhance trust
  - Trademarks by analogy:
    - Note relationship of trademarks and trust
      - How can “trust” be supported with trademark presentations by reliable stakeholders in system
  - Consider “Certification Marks” application in networked information “supply chains”
    - See 15. U.S.C. Sec. 1127
    - Cert. marks are “three party” marks – include third party that produces standards to which product or service provider asserts adherence.
      - Certification marks
  - [Other?]
- References

142. Fake News - Propagation of Misinformation

- Challenges
  - Distributed information systems employ many-to-many architecture with both positive and negative consequences
    - Positive – enhanced opportunities for the expression and perception of marginal views
    - Negative – decreased opportunities for curation by narrative "gatekeepers" who can help to create meaning around "big information" fire hose
  - Societal habits of relying on one-to-many information systems atrophied population-wide critical thinking skills yielding compliant populations
    - See Ref: "The True Believer" by Eric Hoffer
  - [Other?]
- References

142. Fake News - Propagation of Misinformation

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider training and programs to enhance critical thinking skills
  - Consider certification program to enable individuals to identify provenance of information
    - Beware crimping of first amendment rights in U.S.
  - Consider regulation/self-regulation of intermediaries to match responsibility with potential for disorder (entropy accounting)
  - Consider perspectives and strategies for other contexts in which inaccurate information is proffered to populations
    - See Ref: "Processing Inaccurate Information - Theoretical and Applied Perspectives from Cognitive Science and Educational Sciences" by Rapp and Braasch.
- Analytical Signal versus Noise - Consider opportunity to apply Shannon distinction of data from information as part of educational component
  - Not everything you hear is information.
- Consider implications for identity in society
  - Social theory of identity (Goffman, Hofstadter, Hegel, etc.) attends to Bayesian accumulation of linked "expressive output" and "perceptual input" as foundations of sense of identity/self.
  - Note "fake news" as breach of integrity of perceptual channel integrity.
  - Note First Amendment of U.S. Constitution as protection of "Freedom of Expression" (output) and "Freedom of Access to information" (perception).
- [Other?]
- References:

143. Filter Bubbles – Problems of Partial Perception

- Challenges
  - Mass customization of information network channels enables people and institutions to "tune in" to content of greater interest, with the consequent reduction/exclusion of content that is not of interest
    - Positive: Enables individual choices about perception of information
    - Negative: Can shield individuals and organizations from information that may be of interest/use to that stakeholder, but might not come through expected channels.
  - Compare with concepts in other Maps in Atlas to identify potential frameworks for addressing related issues, e.g.:
    - Biases (individual and institutional)
    - Echo Chambers (Filter bubbles constrain input, while echo chambers re-ifies existing content)
  - [Other?]
- References

143. Filter Bubbles – Problems of Partial Perception

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider various educational approaches to enhancing individual and institutional "curiosity" to encourage attention and engagement beyond filter bubbles
  - Consider mechanisms for converting "self-interest" of narrowing focus into participation in broader exchange of ideas
    - Risk awareness
    - Efficacy of knowing views and arguments of opposing views
    - Application of "information arbitrage" gleaned from broader exposure in everyday settings
      - Value of "gossip fodder" in social settings
      - Critique of efficacy (and reality) of the "Efficient Market Hypothesis"
        - » Does the market really "know" everything already, or is it also the hyper-victim of self-constructed structural "filter bubbles"
  - [Other?]
- References:

144. Echo Chambers – Cognitive Reification

- Challenges
  - Distributed information network architectures invite participants (both individuals and organizations) to customize their interactions to suite their needs and interests
    - Predisposition to connect and interact with similarly situated stakeholders narrows scope of external input, potentially limiting stakeholder situational awareness of outside views, risks, opinions, threats, etc.
  - Exposure to self-consistent views builds coherence of organizational paradigm internally, but may limit exposure to external views, constraining awareness of reality from which risks emerge
  - How can the system/technology assist users and other stakeholders from falling victim to lack of awareness caused by "echo chamber" effect?
  - [Other?]
- References:

144. Echo Chambers – Cognitive Reification

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider models of information governance that enhance integration of externalities to benefit stakeholders within an echo chamber
    - Innovation models
    - Risk reduction models
      - E.g., Insurance and law are sectors that mine value at the edge of ordered systems
    - Governance at the edge (See Ref: Jennifer Best – "Governing Failure")
  - Consider mechanisms to capture arbitrage opportunity at edge of knowledge systems (aka "markets," "paradigms,")
  - Compare with concepts in other Maps in Atlas to identify potential frameworks for addressing related issues, e.g.:
    - Biases (individual and institutional)
    - Echo Chambers (Filter bubbles constrain input, while echo chambers re-ifies existing content)
  - Consider checklist approach to externalities to provide tool to stakeholders to break out of echo chambers
    - Atlas of Risk Maps is an example of a "checklist" tool.
  - [Other?]
- References:

145. Non-Zero Sum Games

- Challenges
  - The “zero sum” paradigm dampens enthusiasm for group engagement in multiple settings, but there are a host of settings in which group engagement yields risk reduction outputs that are greater than the costs.
    - How can stakeholders be encouraged to engage in these activities and incur these costs?
  - A subclass of non-zero sum games are non-competitive, but still do not manifest in real world systems due to various habits, norms, and many external structures of incentives, penalties, conditions and considerations for the stakeholders
  - Institutional structures that are based on competitive models of markets foster externalization of costs by each stakeholder, and incentivize “free rider” behaviors
    - How get over “threshold energy” of prompting investment in “meta-objects” structures of risk mitigation
    - What is equivalent of “trade association,” but convened around a shared set of risks, rather than an industry sector?
  - What do markets based on ubiquity look like?
    - Inquiry by C.B.
  - [Other?]
- References

145. Non-Zero Sum Games

- Candidate Analytical Frameworks/Metrics/Actions
  - Identify situations and harm avoidance strategies for security, IM and privacy, that can only be gleaned by stakeholders through mutual structured effort among stakeholders
    - If the same results can be achieved unilaterally, that stakeholder will not reliably cooperate
  - Existing models include
    - Insurance
    - Physical resource co-management arrangements (commons)
      - Riparian/water rights management
      - Fisheries co-management arrangements
    - Shared language
    - Shared norms, laws, rules
      - E.g., stopping at a red light reduces risk in ways humans cannot achieve unilaterally
  - [Other?]
- References

146. Eminent Domain/Takings

- Challenges
  - How does eminent domain/takings powers of governments intersect with IM, security and privacy issues
    - Under what conditions do government interests in security and privacy of citizens warrant "takings" of privately-owned critical infrastructure?
  - What intangible assets are amenable to "takings" powers?
    - Are data assets amenable to government takings?
    - Are Identity rights amenable to takings power?
      - What about in jurisdictions where governments supply identity?
      - What is the nature of government rights in government issued credentials?
        - » SSNs
        - » Passports
        - » Driver's licenses
    - Compare nation-state policies on revoking citizenship
      - Does that constitute a "taking" of identity
  - What if the nation state is the issuing authority/sovereign
  - [Other?]
- References

146. Eminent Domain/Takings

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider variables associated with private ownership of critical infrastructure
    - What are mechanisms in which state interest can warrant exercise of additional state power regarding the ownership and operation of critical infrastructure assets?
    - Does that state interest extend to the information network components of critical infrastructure or to information network assets AS critical infrastructure?
  - What are the IM, security and privacy implications of extending eminent domain authority to intangibles such as data, information etc., including data that could be used to identify individuals?
  - What are the “takings” implications of revocation of national citizenship?
    - What is identity implication of “paper-less” populations in nation state?
  - [Other?]
- References

147. “Second-Hand” Entropy

- Challenges
  - Any reduction in entropy of a system is accompanied by an increase in entropy outside of that system
    - This applies to thermodynamics and also to “information entropy”
  - Information entropy has been described as “surprise” (see ref)
  - Arbitrageur applies superior information to the “surprise” of other parties to an interaction.
  - How can the disadvantaged parties in an interaction be protected from excess or undue advantage of the other party
  - Entropy “exhaust” can be incidental and inadvertent
    - Like second-hand smoke, but for risk
    - How separate mere ignorance of secondary effects versus indifference to secondary effects?
  - [Other?]
- References
  - Claude Shannon – Quantitative theory of information

147. “Second-Hand” Entropy

- Candidate Analytical Frameworks/Metrics/Actions
  - Distinguish fraud from arbitrage:
    - In fraud – information differential is “created” and then exploited
    - In arbitrage – information differential is “discovered” and then exploited
    - “Insider-trading” (10b-5 violations in US securities law) operate at the margins of fraud and arbitrage
  - In information networks/markets, intermediaries have the capacity to glean superior insights and collect “metadata” that offers perspectives not available to the data subjects.
    - What are mechanisms for assuring that the benefits and burdens of information arbitrage are fairly and sustainably applied?
    - Note that the legal notion of “accounting” relates to both providing information and value to stakeholders
  - [Other?]
- References

148. The “Imp of the Perverse”

- Challenges
  - Humans frequently take actions that are contrary to their own self-interest in an effort to project and reaffirm their discretion and control
  - When parties act against their own interests, it is more difficult to recruit communities of interest from among populations to implement strategies that depend upon “neighborhood watch,” network effects, “golden rule,” etc.
  - [Other?]
- References
  - Edgar Allen Poe reference

148. The “Imp of the Perverse”

- Candidate Analytical Frameworks/Metrics/Actions
  - Identify settings in which “Imp of the Perverse” applies and seek to address underlying sources of behavior
    - What are direct and indirect causes of stakeholders acting against their own self interest?
  - Consult DSM V for “self harm” conditions?
    - Psychological variables may be in play in individuals and populations under various stresses
  - Explore sources of underlying social inefficacy that leads to behavior
  - Consider that the behavior is functional in the context and then reverse engineer why the behavior was perceived as functional initially.
  - Offer alternative pathways to provide individuals with “choice” in an effort to build efficacy and self-esteem that may help counter self-0destructive behaviors.
  - [Other?]
- References
  - https://en.wikipedia.org/wiki/The_Imp_of_the_Perverse

149. Peer and Community Pressure

- Challenges
  - Actions of individuals may be influenced by group dynamics that can cause them to act unpredictably in a given situation
    - May affect individual action in both personal and representative capacities (e.g., as employees)
    - Pressure types include temporal element
      - Short term examples are so called ”mob” behaviors
      - Medium term examples include deference to perceived authority (e.g., Milgram experiments)
      - Long term examples include community, religious, and social/ethical norms
  - [Other?]
- References

149. Peer and Community Pressure

- Candidate Analytical Frameworks/Metrics/Actions
  - Socialization techniques from organizational psychology can help dissipate performance impacts of contextually dis-functional peer and community pressures
  - Narrative differences between outside pressure and system performance requirements that affect behaviors can be unpacked, and synthesized into a hybrid narrative that can help reduce the pressure of different behavioral influences for stakeholders working with a given system.
    - Consider narrative synthesis of goals to mitigate differentials in performance and behaviors in conflicting paradigms.
  - [Other?]
- References

150. Ambiguity of Bias

- Challenges
  - Bias is multi-dimensional
    - Various inclinations and prejudices affect biased decisions and systems
    - Many different bias causes and effects
  - Different forms of bias invite application of alternative interventions to better mitigate their respective harmful effects on system operations and performance
  - Ambiguity of term “bias” obscures variety of effective strategies
  - [Other?]
- References
  - Wikipedia site

150. Ambiguity of Bias

- Candidate Analytical Frameworks/Metrics/Actions
  - Eliminate ambiguity of system “bias” to deal specifically with different types
    - Parse varieties of “bias” in individual Atlas slides to categorize interventions
    - In an effort to reduce the ambiguity, individual Atlas slides capture the challenges and possible approaches to various types of bias.
  - Slides dealing with Bias contain word “Bias” in the slide heading.
  - [Other?]
- References
  - See Atlas slides on different sorts of “Bias” for specific references

151. Undue Reliance on “Science”

- Challenges
  - Assertions of science and empirical analysis carry increasing strength and efficacy in policymaking, but might not be appropriately relied upon as so extended
    - Real, empirical science has appropriate authority to answer certain questions
    - Scientific explanations should not obscure more holistic inquiry and explanation, particularly to non-scientific questions
      - Economics, cultural and social factors, etc.
  - This set of challenges includes primarily “unintended” over-reliance, as opposed to intentional mis-assertions of scientific conclusions to sway policy
  - [Other?]
- References
  - Milgram “white coat” authority experiments

151. Undue Reliance on “Science”

- Candidate Analytical Frameworks/Metrics/Actions
  - Maintain awareness of “hype cycle” with new scientific and technical announcements and advances
    - Invite contrary views into analysis
    - Invite non-technical and non-scientific views into the analysis
      - Be careful to “weight” the inputs – no veto power for any one perspective
  - Encourage technical announcements to be specific about the scope and context of a given value proposition
    - Try to anticipate and address market and public “unjustified enthusiasms” in announcements and discussions of new technologies, etc.
  - Encourage scientists to work with editors/writers to help temper the enthusiasm for politicians and citizens to overstate technical and scientific advancements.
  - [Other?]
- References

152. Cross-Border Applications of Existing Solutions

- Challenges
  - Successful hybrid technical/policy system approaches might be applied in other jurisdictions, sectors and contexts, but might not anticipate or accommodate such other realities of new “local” operating contexts, with disappointing results
    - Solutions that are “plucked” from context can have unexpected and disappointing results
  - Technical systems (especially ITC systems) can have data and information handling attributes and capabilities that may be incompatible or illegal in other jurisdictions
    - Incompatible with local workforce skills
    - Incompatible with local user needs and expectations
    - Incompatible with local legal and regulatory requirements
  - [Other?]
- References
  - Compare to Map portfolio 153 “Misapplication of Historical Solutions” which is the “time” version of this “space” policy flaw

152. Cross-Border Applications of Existing Solutions

- Candidate Analytical Frameworks/Metrics/Actions
  - Separate out different sources of cross border challenges to identify and specify adaptations needed for desired function in new jurisdiction context
    - Different laws?
    - Different language?
    - Different technical infrastructure?
    - Different user or worker training and expectations?
  - Compare “adaptation studies” in writing and theatre
    - How convert “meaning” across cultural divisions
    - How convert “meaning” across jurisdictional boundaries?
    - Are cultural differences aligned with border differences.
      - How “localize” solutions for COIs (communities of interest) within national borders?
  - [Other?]
- References
  - Cambridge Handbook of Adaptation Studies

153. Misapplication of Historical Solutions

- Challenges
  - Successful policy approaches from the past might be applied at later times and in other temporal contexts (such as accelerated or attenuated pursuit of policy, etc.), but might not reflect temporally "local" realities, with disappointing results
    - How adapt yesterday's solutions to today's problems?
  - Institutional knowledge of systems operation that resides in trained knowledge and responses of long-term employees may be out of date and inapplicable to new systems
    - How do you teach and old dog new tricks?
  - [Other?]
- References
  - Book "The Past is a Foreign Country"

153. Misapplication of Historical Solutions

- Candidate Analytical Frameworks/Metrics/Actions
  - Include continuous training for workers and users in new systems and approaches
    - Internal training
    - Supplier training
    - Online training opportunities
    - 3rd party training
  - When buying or building new technology systems, be sure to confirm that maintenance, support and warranties are consistent with organization needs in the future.
    - Insulate system from vendor abandonment of support.
    - Also will technology provider help with bridging to new system at end of current agreement?
  - Work with legal function to identify the implications for "duty of care" associated with changes in technology.
    - Duty of care can affect responsibility and liability for harms caused by technology.
    - When determining whether a particular duty exists, courts generally consider several factors, including:
      - (1) the relationship between the parties;
      - (2) the social utility of the actor's conduct;
      - (3) the nature of the risk imposed and foreseeability of the harm incurred;
      - (4) the consequences of imposing a duty upon the actor; and
      - (5) the overall public interest in the proposed solution.
  - [Other?]
- References
  - T.J. Hooper case – Tugboat owner held liable for wrongful death to crew in storm because didn't have marine radio, even though marine radios were not yet industry standard.

154. Confusion of Status of Humans as "Biological" vs. "Information" Beings

- Challenges
  - De-risking strategies that are effective with respect to physical risks to humans (as biological beings) might not serve to address emerging risks to humans acting online in their "information" capacities
    - Police, defense, public safety officers not trained to offer protection against new information-related risks
    - Medical treatment equipment and implants might not be cyber-secure
    - Laws and regulations are designed to protect interactions among people in a mostly physically oriented world
      - What modifications of laws are needed to protect peoples "digital appendages?
    - Other examples
  - [Other?]
- References

154. Confusion of Status of Humans as "Biological" vs. "Information Beings

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider implications of MAAS ("Metabolism as a service")
  - Consider new individual harms that can be suffered by the digital instance/representation of the individual
    - What is corollary of standard privacy torts in the digital/online world?
      - Intrusion on private affairs
      - Publication of private facts
      - Defamation (Libel and Slander)
      - Misappropriation
  - Provide support/resources/education to first responders (police, fire, etc.) in emerging information related harms
    - Information-related aggravations to physical harms
      - Social network stalking associated with assault
      - Mis-information regarding vaccines lower individual and group immunity
    - Information harms as stand-alone harms.
      - Phishing attacks on elderly
      - Violations of COPPA – Children's Online Privacy Protection Act
  - Identify those new online/information harms that do not have a natural relationship to any physical harms and seek to assign responsibility for addressing these.
    - Don't allow such "orphaned information harms" to slip through the gaps in current agency/institutional coverage.
  - [Other?]
- References
  - Book "Turning Troubles into Problems" – Description of mechanism for institutionalizing generic narrative "troubles" through measurement to convert them into standard quantified issues that can be dealt with by institutions.

155. Computational Sovereigns

- Challenges
  - The concept of “sovereignty” is an axiom of human organizational narratives.
    - In this material, working definition of “Sovereign” is an entity that doesn’t have to ask for permission or forgiveness for its actions
    - Sovereigns are narratives (teleological projections) to which human populations can self bind.
      - Deities, Kings, Countries, Naval Commanders, Companies
    - Sovereigns/institutions (narratives all!) have shaped human behavior to conform to the performance metrics, behavioral norms (normal (Gaussian) distribution of behaviors) and beliefs consistent with their respective narratives
    - Sovereign authority is founded in the de-risking and leverage offered to populations that conform their behaviors to performance metrics consistent with their narratives
  - Information authority of prior sovereign narratives is being supplanted by information authority of “computational” forms of sovereignty and their respective emerging narratives
    - AI
    - Blockchain
    - Cryptography
  - Humans and institutions acting in conformance with prior sovereign narratives might be found to act contrary to the metrics applied by emerging computational sovereigns
  - [Other?]
- References

155. Computational Sovereigns

- Candidate Analytical Frameworks/Metrics/Actions
  - Capacities of different emerging "computational sovereign" narrative forms to de-risk and leverage human and institutional interactions should be carefully matched with actual capacity of those sovereign forms to do so
    - Dangerous to assume that new computational sovereigns can just "step into the shoes" of existing sovereign narratives as foundation of group behavioral norms
    - E.g., blockchain may help de-risk flawed individual and institutional memory (via distributed ledger and computational challenge, etc.), but will require supporting structure to address broader real-world concerns
    - E.g., AI may help to de-risk flawed individual and institutional decision making capacity, but will require ethical and normative "training data" to suggest and implement solutions that are consistent with human and institutional needs and expectations.
  - Review perceived scope of authoritative output of a given computational system to confirm that the current or planned dependency is consistent with the intended information arbitrage management potential of that system
  - [Other?]
- References

156. Mis-Application of Federated Identity

- Challenges
  - ”Federated Identity” involves the use/consumption/reliance by multiple relying parties on the identity credentials issued by a central authority
    - The use of federated identity in organizations raises the possibility that the efficacy and application of their authority might extend beyond their effective capacity
    - Opportunities for over-dependency on federated identity is heightened in newly emerging interaction spaces where risk and leverage metrics are underdeveloped, and institutional structures are absent
  - Where identity credentials and identity attributes are applied and consumed by “relying parties” in contexts beyond their original intended relevance there is risk that the processes of federated identity (including identification, credentialing, authentication, authorization, etc.) could be undermined by variables that were not anticipated in the organization and operation of the federated identity system.
  - Compare to “Stored value” systems that challenge the authority of the M-1?
    - E.g., purchase of stored value card (i.e., Starbucks™ card) effectively doubles currency in circulation (original currency is given to company that it can use, and card acts as currency in other interactions. For this reason, use of stored value cards is historically limited to one company where credits and debits can be matched.
  - [Other?]
- References

156. Mis-Application of Federated Identity

- Candidate Analytical Frameworks/Metrics/Actions
  - Compare original and proposed contexts for application of a given federated identity system to confirm whether systems of federated identity actions (identification, credentialing, authentication, authorization, etc.) are consistent with goals of new deployment.
    - E.g., Identity system may depend on authoritative documents that are issued in jurisdiction of original deployment, but not available in another context.
      - Birth certificates issued in another country and offered for evidence of identity in passport application
  - Unpack procedural elements (and related metrics) of federated identity system to identify those that are acceptable in new context.
    - Identify surrogate measurements and processes to create "compensating controls" for those identity integrity processes that don't translate easily to new context.
  - [Other?]
- References

157. Language/Translation Issues

- Challenges
  - Technologies where the design, development and deployment are optimized for one population may rely on language that is unfamiliar to another population
    - Different languages of human culture
    - Different languages of professional sectors
  - [Other?]
- References

157. Language/Translation Issues

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the ways/contexts in which technology performance is dependent on language
    - UIs
    - Instructions
    - Emergency notifications
    - Audit and Performance guidelines
    - Promotional and marketing materials
      - Potential liability for over-promising to consumers (Magnuson Moss Act in US)
    - Descriptions of data flows in system
      - Some laws in countries with different languages require disclosure of some data flows AND that the company act consistent with the data
      - US FTC enforcement rule of thumb: "Say what you will do with data and then do what you said you will do with data"
  - Assure that language barriers don't lead to performance issues
    - Does user consent constitute "informed consent" if disclosures are presented in unfamiliar language?
    - Consider uses of graphics and other neutral methods of communication to convey important system details across different languages.
  - Review literature on "localization" efforts for other goods (software, etc.) and services
    - What variables inform triage of translations?
    - Are contracts effective in limiting liability for system performance to the amount paid for the system to help drive translation resources to high deployment jurisdictions?
  - Review literature on "adaptation studies" in literature and the arts
    - Integration of cultural factors associated with understanding beyond language
  - [Other?]
- References
  - Oxford Encyclopedia of Adaptation Studies [citation here]

158. Inattention to the Distinction Between "Data" and "Information"

- Challenges
  - The access to "data" is necessary but insufficient to inform a party
    - If A hands a book to B that is written in Russian, but B doesn't know how to read Russian, then B has all of the "data" (the book), but cannot be "informed" because B doesn't know the "meaning" of Cyrillic characters and Russian language.
    - Data + Meaning = Information (Shannon)
  - Confusion regarding the distinction leads to all sorts of technology misapplication and policy ambiguity.
    - The shadow of ambiguity is where mischief (both intentional and inadvertent) resides.
  - Many laws, regulations, policies and rules use the terms "data" and "information" interchangeably within their text
    - They were written in a period where the distinction was less important because data was not as broadly shared beyond its original organization (w/ consistent meaning) in pre-networked worlds.
  - Many laws, regulations, etc. use the terms "data" and "information" in ways that are inconsistent with other laws and rules
    - People and institutions that need to comply with inconsistent laws are between a rock and a hard place.
    - US federal and state definitions of "Personal Information" differ from that in EU GDPR.
  - Confusion of the terms is responsible for retarding potential innovation in security, privacy, liability management, un-insurability, and other elements of online risk.
    - Potential for different strategies to deal with qualitatively different threats and vulnerabilities.
  - [Other?]
- References

158. Inattention to the Distinction Between "Data" and "Information"

- Candidate Analytical Frameworks/Metrics/Actions
  - Since data + meaning = information, that means that levels of "information integrity" depend both on levels of "data integrity" and "meaning integrity"
    - Working assumption that "privacy," "security," and "liability," are symptoms of the underlying illness of lack of system integrity.
  - FIPPs based rules are grounded in data security as a surrogate for information security/privacy
    - Born in 1970s in pre-networked world where data was generated by the same entity that applied the "meaning"
    - Now rampant secondary use of data (and practical death of secrecy) results in data being applied in various meaning-laden contexts
      - No longer appropriate to ignore distinction of data and information
  - Examine referenced materials for tunable vectors of meaning security
  - [Other?]
- References
  - UW IRRI Atlas of Information Risk Maps

159. Attention Economy (Technology Socialization Processes)

- Challenges
  - Notices and training regarding strategies and tactics to reduce threat and vulnerabilities associated with the organization and operation of new technology systems are diluted in the flood of information and input experienced by people (acting in personal and institutional contexts)
  - System security/privacy/integrity notification and training is difficult and costly
    - Distributed populations of human users make it difficult to intervene to enhance system integrity
  - No natural institutional leadership in online risks
    - Commercial entities won't internalize costs of notices/training
      - Want to educate users/consumers only to extent consistent with mission of revenue generation
      - No legal requirement of specific relationship of provider and user
        - » Exceptions are regulated industries (finance, healthcare) and paternalistic jurisdictions (EU, California)
  - [Other?]
- References
  - Compare map portfolio number 57 (attention economy - Periodic)

159. Attention Economy (Technology Socialization Processes)

- Candidate Analytical Frameworks/Metrics/Actions
  - Integrate technology socialization training modules in other subjects and at all levels of training and education
    - K-12
    - High School
    - Higher education
    - Professional Education
  - Explore avenues for compelling commercial interests to resource notification and training campaigns associated with the emerging risks associated with the technologies/services that they promote and sell.
    - GAAP – match costs and revenues in the system
  - [Other?]
- References

160. “Old Dog, New Tricks” Problems

- Challenges
  - The expression/idiom ”You cannot teach an old dog new tricks” is intended to convey that it is difficult to change the behaviors, attitudes, etc. of a person who has developed certain habits over long periods.
  - In multiple time scales, habituation of behaviors by individual humans and groups can retard advancement of change management goals.
    - Particularly challenging when old habits are inconsistent with large scale installations of new technology systems
  - [Other?]
- References

160. “Old Dog, New Tricks” Problems

- Candidate Analytical Frameworks/Metrics/Actions
  - Review change management literature regarding behavioral habituation in organizations at individual and group levels.
  - Practice, practice, practice new scenarios and use cases to create new habits and reflexive actions of individual and group behaviors in organization.
  - [Other?]
- References

161. Apparent Agency

- Challenges
  - Agents represent the interests of principals
  - Agents hold themselves out to third parties as having certain authority to act on behalf of principals
  - Agency relationships are established by law or private contract
  - Agents may be individual or institutional
    - Even institutional agency duties are often discharged by humans as employees of the institution
  - The scope, duration and degree of the agency relationship can be confusing to third parties
    - potentially leading to undue and detrimental reliance by third parties on commitments of agents.
  - Agents may sometimes (either intentionally or accidentally) exceed the scope of their agency
    - Raises the question of who is responsible for Agent's actions.
  - [Other?]
- References

161. Apparent Agency

- Candidate Analytical Frameworks/Metrics/Actions
  - Need greater clarity regarding data, identity and information agency relationships
    - Includes potentially important fiduciary agent relationships
    - Clarify criteria for acceptable behaviors and performance
    - Consider duties in various data-related activities
      - Collection
      - Transfer
      - Use
      - Processing
      - Disposal
      - Etc.
  - Identify and support initiatives to create standards and signals for information professionals and/or identity professionals
    - Include certification against standard metrics
    - Likely involve the promulgation of codes of ethics
      - Like those applied in other guilds and current professions
    - can help to provide guidance and signals for people and institutions consuming those services.
  - [Other?]
- References

162. Over-Dependency

- Challenges
  - Typical fight is over maintenance and support obligations over long term
  - Tightly integrated and coupled information institutions and supply chains create dependencies such that the withdrawal of those services and supports (even without malice) can create vulnerabilities
  - “The day Facebook went down.”
  - Compare “requirements contracts” and “output contracts” in physical asset supply chains
    - Contractual duties to supply (or take) in effort to de-risk inputs flow
  - Compare map portfolio number 108 (Interop Risk)
  - Compare Monopoly and Monopsony power based on market dominance and the dependencies it causes.
    - If powerful company dominates markets, dangerous dependency develops
  - Compare “platform” scaling issues
    - Mismatch of risk re-allocation to the “edge” but knowledge of risk is centralized.
    - Creation of information arbitrage differential leveraged by network effect.
    - Appropriation of de-risking in system?
  - Dependency on legacy systems can delay implementation of newer, fit for function systems
  - [Other?]
- References

162. Over Dependency

- Candidate Analytical Frameworks/Metrics/Actions
  - Spread risk of obsolescence among stakeholders
    - Craft contract language to include:
      - Maintenance
      - Service
      - Support
  - Address needs for assistance in transferring data and materials in program
    - Avoid walled garden systems for mission-critical needs
  - Cultivate “ecosystem” or alternative suppliers to assure future choice in acquisitions decisions
  - Incorporate flexibility into system design and architecture
    - Enables reliance on multiple alternative suppliers of technology
  - Avoid “lock in” of patented solutions if possible
    - Patent is form of government granted monopoly
  - [Other?]
- References

163. Secondary Information Risks

- Challenges
  - Consider risks to human and institutional parties that act as guarantors, vouchers, etc. for others in online interactions
    - What is responsibility for vetting, auditing by parties “vouching” in reputation network?
    - What is responsibility for schools and universities teaching security, privacy and identity to professionals and then “certifying” their completion of the program
    - What is responsibility of parties in technology system “certification” programs?
  - Consider effect of secondary risk in emerging reputation networks
    - Compare concepts of “negligent hiring”
    - Compare concepts of ”publisher’s liability” for defamatory and infringing material
  - Consider possible effect in “infinite factor authentication”
    - which entity is responsible/liable for which “detrimental reliance” in the delegation chains?
  - [Other?]
- References
  - Compare slide 164 (Risks to and from intermediaries, i.e., where there is no explicit vouching or guarantee).

163. Secondary Information Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - Implement specific duties by contract for parties in supply chain and clarify limits of their duties
  - Carefully examine “assignment” clauses in contract to assure that liability effects of any assignments of rights and delegations of duties are adequately clarified
  - Be explicit on which party to agreement has responsibility for performance failures of subcontractors
  - Craft appropriate disclaimers of liability for presentation to users that directly access intermediary services
    - Compare “hand off” language on websites
  - [Other?]
- References

164. Intermediary Risks

- Challenges
  - Online and networked technology systems involve the participation of multiple parties
    - When systems fail to perform, how is responsibility addressed and assigned among intermediary parties?
  - Parties might be “intermediaries” in the design, development, deployment and/or operation phases
  - Consider risks ***to*** intermediaries
    - Compare “common carriers” risk for content with “publishers’” risk for content in US law
  - Consider risks ***from*** intermediaries to others
  - Consider risks of human and institutional parties that act as guarantors, vouchers, etc. for others in interactions
    - Example: Are cloud services and/or data hosting services liable for content they hold, process and transfer?
    - Example: Are online social networks responsible for the materials that members post online?
    - Example: Are online search services responsible for harms caused by people following bad advice they discovered online?
  - [Other?]

- References

164. Intermediary Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - Apply standard “legal algorithm” to ascertain responsibility and assign liability
    - Duty – Does the party have a duty?
    - Breach – Was that duty breached?
    - Causation – Did that breach cause harm?
    - Damages – Was there damage from that harm?
    - Liability – Are there contract or statutory framings to assign liability?
    - Insurance – Even if there is liability, is it insured?
  - Consider mitigation of intermediary liability with notice process mechanism
    - Compare Digital Millennium Copyright Act (DMCA) has “take down” notice process to address intermediary liability concerns
  - [Other?]
- References

165. Identity Risks

- Challenges
  - All interactions with all systems, including online systems, among all entities begin with question “Who goes there?”
    - The identity of the counterparty sets risk expectations for the interaction
    - The accuracy and integrity of the identity system needs to be managed to sustainably balance the interests of the identified party and the relying party (and the credential issuing party if different from the relying party)
  - Identity systems employ many different approaches to establishing and maintaining identity “signals” for relying parties
  - Each data action of each identity approach should be designed and developed and deployed to be secure from accidental and intentional misuses.
  - Data actions include those associated with:
    - Identification
    - Credential Issuance
    - Authentication
    - Authorization
    - Credential Maintenance
    - Disposal of credentials
  - [Other?]
- References
  - See Challenges of “Federated Identity Systems” (slide number __) for related federated identity issues

165. Identity Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - Recall that “identity” strategies and tactics can be applied to address the identity of humans, organizations and things
  - When identity of humans and institutions is involved, consider the application of the “Insight/Intrusion slider” to balance stakeholder needs
    - The degree of “insight” as to the identity of a human or institution is
  - Shared tactical pathways
    - Look at other identity system sub-actions to discern potential strategies for new identity systems
      - Identity contexts may vary, but pathways for identity signal entropy reduction might be borrowed.
      - E.g., Multi-factor authentication can be helpful in multiple identity use cases and domains to reduce potential damage from lost or stolen credentials
  - [Other?]
- References

166. New Iterations of Traditional Frauds

- Challenges
  - Frauds include a large number of harms based on intentional deception of a party intended to secure unfair or unlawful gain or deprive the victim of a legal right.
  - Many historical sources and “types” of fraud appear in new guises in online and digital interactions, such that they could evade detection by traditional fraud detection mechanisms and measurements
  - How can current structures of fraud (or that support fraud) be identified and mitigated in distributed and networked information systems?
    - Do traditional “badges” of fraud offer guidance and “red flags” for modified current forms of fraud?
  - [Other?]
- References

166. New Iterations of Traditional Frauds

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider relationship-based analogs to historical frauds (see financial frauds for e.g.s)
    - Fictitious Payee, endorsements, and other check fraud
    - Ponzi/pyramid schemes
    - Lending and short-term credit fraud
    - Credit card-based frauds
    - Identity theft
    - Online sales fraud
    - Website re-directions
    - Charities-based schemes
    - Etc.
  - Examine various strategies and tactics that were applied to mitigate traditional frauds
    - Legal
    - Economic
    - Auditing/accounting/reporting
    - Community enforcement (neighborhood watch)
    - Regulatory approaches
  - [Other?]
- References

167. UCC-Type Risks

- Challenges
  - The Uniform Commercial Code is a standard body of laws established by NCUSSL and presented to the state legislators for their consideration and passage.
  - The UCC applies to sales, leases, negotiable instruments, bank deposits, funds transfers, letters of credit, bulk sales, warehouse receipts, bills of lading and documents of title, investment securities and secured transactions.
  - The UCC rules were developed to help solidify customs in commercial transactions in physical goods, and it has been difficult to extend its rules to various intangibles and services-based settings
    - See UCC Article 2B discussions of whether "software" (and related digital products) would be treated as "goods" under the UCC.
  - What might UCC issues and rules teach designers and developers of socio-technical systems in online contexts?
  - [Other?]
- References

167. UCC-Type Risks

- Candidate Analytical Frameworks/Metrics/Actions
  - Each of the articles of the UCC has the potential to teach strategies for different emerging aspects of online commerce and interaction
  - Consider UCC strategies for potential guidance on possible integrity strategies for online/information economies based on analogs to "goods" economy
  - Examples:
    - Relationship of warehouse receipts laws on reserve-based cryptocurrencies
    - Relationship of "goods" rules to valuable data and information flows
    - Relationship of "secured transaction" rules to future AI liability insurance
    - Relationship of check and payment rules to online "identity" structures
  - [Other?]
- References

168. Unfocused Response

- Challenges
  - Notwithstanding proper identification of threat or vulnerability, human and/or institutional responses to novel threats might be unfocused (and not capable of being focused) based on
    - lack of pre-existing (and institutionally-recognized) applicable measurements of risk and de-risking efforts, and
    - lack of framing and paradigm to properly and fully understand and assess circumstances, and therefore ineffective as a response as a result of general unfamiliarity of harm mitigation strategies
  - Challenge arises both within and among humans and organizations as a result of the less-direct cause and effect relationships that are present in distributed information networks
  - Compare the misapplication of solutions from other contexts where novelty of new information threats and vulnerabilities may cause parties to mis-perceive effectiveness of existing solutions, leading to the mischaracterization of system vulnerability and false-comfort in yesterday's solutions
    - Difference here is that this is not the reapplication of preexisting response from other contexts, but rather new, but unfocused, responses.
  - [Other?]
- References

168. Unfocused Response

- Candidate Analytical Frameworks/Metrics/Actions
  - Where unfocused response is due to ambiguity in threat and vulnerability assessment, considering parsing ambiguity to create sub-measurements for portions of the problem that may be handled separately.
  - Expand framing of problem in time and space to discern root causes of challenge/problem that may lend itself to more effective/impactful intervention.
  - Note that distributed systems might require centralization of certain functions to help focus the measurement of risk and response.
    - Funnel interactions through gatekeeping metrics to shape risk flows
    - E.g., Enhance traffic safety by teaching centralized/standardized traffic rules.
  - [Other?]
- References

169. Occupied Infrastructures

- Challenges
  - Networked information systems are built on the laws of physics, which are universal.
    - However, the laws of people and organizations are not universal.
    - As a result, technical system elements (and interoperability of those elements) are not naturally bounded by political, legal, economic or other borders.
  - Mechanisms for reinforcing political, economic, legal and social borders and boundaries against unauthorized access by information network functions have been challenging
    - in part because of the confusion of ”data” and “information”
    - also because the physics that supports the technology applies everywhere.
  - The result is that socio-technical infrastructure (including so called “critical infrastructure”) is accessible to parties regardless of borders
  - The degree of intrusion pressure in online environments (caused by 3rd party “insight seeking” behavior) is such that all information-dependent infrastructure is in a permanent state of occupation by un-invited parties. [Other?]
- References

169. Occupied Infrastructures

- Candidate Analytical Frameworks/Metrics/Actions
  - What is the nature of national defense and intelligence where the infrastructure of a nation is already "occupied" by foreign parties, but the extent and nature of that occupation is not directly detectable?
  - Consider the challenges of institutional authority for government divisions charged with protecting populations and infrastructure from hybrid threats that are simultaneously domestic and foreign
  - Be aware that merely acknowledging that the authorities fall "in the gaps" between existing authorities is not sufficient to solve the challenges
  - Examine existing laws to map the edges, and from that to manage the gaps
    - US Posse Comitatis Act
    - [NOTE: Include other relevant military and intelligence constitutional and statutory authorities]
  - [Other?]
- References

170. Inter-Generational Interpretations

- Challenges
  - Consider the challenges of intergenerational change from both “technology” generations and “human” generational perspectives.
    - Changes in either (technology or human generations) can require retraining of users and operators of technology.
  - Is the particular generation of the technology system at issue and its UIs for operators and users equally accessible and functional for people in different generations?
  - Was the system “user testing” performed in a subpopulation in which the intergenerational differences vary from those of other populations of potential users?
  - The pace of information technology adoption and change is such that institutional and human adaptation will always lag the technical reality.
    - Today’s “solutions” are always directed at “yesterday’s” challenges
  - The nature of intergenerational learning is that there are levels of awareness and understanding that vary among subgroups within the larger overall population.
    - Digital ”natives” versus digital “immigrants”
    - Historical information “risk” narratives get lost in subsequent generations.
  - [Other?]
- References

170. Inter-Generational Interpretations

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider piggybacking on effective existing UIs and narratives to engage new populations of users and operators.
    - Beware of narrative “baggage” and metaphors that become misleading outside of the original context.
  - Configure teams involved in design, development and deployment of system so that they include representatives of different generations of technology and humans
  - Consider “backward compatibility” analogy (from introduction of new versions of technology) for strategizing about mitigation of intergenerational challenges.
  - [Other?]
- References

171. Information “Nuisance”

- Challenges
  - Compare map number 86 (Nuisance)
  - Because a given “datum” can be applied simultaneously by multiple parties to generate “information,” (that is relevant to each of them respectively), such uses maybe inconsistent with other users.
  - “Inconsistent” data uses include:
    - *Directly* inconsistent uses can be analyzed with the “insight/intrusion slider”
    - *Indirectly* inconsistent uses include diffusion and dilution of value of information
  - Entropy exhaust to normal and legal operations
  - [Other?]
- References

171. Information “Nuisance”

- Candidate Analytical Frameworks/Metrics/Actions
  - ”Entropy Field” approaches to system risk analysis acknowledge (and seek to mitigate) the hidden costs of disorder (entropy exhaust) that are generated whenever a system de-risks an interaction or set of interactions
  - “Insight/Intrusion” slider analysis forces integrated consideration of information value and potential for harm
  - Information-related “nuisance” has the potential to be weaponized when the “entropy exhaust” is directed toward parties with an adversarial relationship to the system operator
  - [Other?]
- References

172. Transition of De-Risking Solutions From “Lab” to “Market”

- Challenges
  - Technical and policy solutions that are developed in isolation from real-world systems and are not fully and appropriately tested may fail to deliver effective de-risking when introduced into real world settings and markets
  - Reliable performance of information systems depends upon a host of variables that are not amenable to testing in laboratory and non-real-world settings.
    - How can system performance be evaluated in real world settings in advance of deployment?
  - Successful performance against laboratory parameters does not guarantee expected performance in the field.
    - How can stakeholders increase assurance of expected performance in system deployment.
  - [Other?]
- References

172. Transition of De-Risking Solutions From “Lab” to “Market”

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider past ”successes” and “limitations” of university tech-transfer efforts
  - Consider programs to bring together industry/government users/operators with researchers/developers
    - Seek to create direct discussion early in design/development process
    - Review other “sponsored research” and “directed research” models to identify new avenues of potential collaboration/research integration.
  - [Other?]
- References

173. Ignorance of Network Edge "Quantitative" Attributes

- Challenges
  - Prior to development of "Small World" model of networks by Watts and Strogatz, lack of knowledge of the principles guiding the formation of network connections led to assumption that nodes can be connected at random with a given connection possibility.
    - In these "random networks," the average path length between any two nodes (measured by the smallest number of edges needed to connect the nodes,) scaled as the logarithm of the total number of nodes.
    - This approach failed to measure the local "cliquishness of nodes observed in real world networks.
  - Clustering coefficient of a node is defined as the ratio of the number of links between an nodes neighbors and the maximum number of such links.
  - Compare maps number 70 (Network Structures)
  - [Other?]
- References
  - "Twenty Years of Network Science," NATURE Magazine, June 28, 2018, p. 528-529

173. Ignorance of “Network Edge” “Quantitative” Attributes

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider alternative structures of those “network connections” (i.e., among system components, system users, etc.) that are necessary for system function that more fully integrate “small world” and other perspectives on network attributes.
  - Assure that the system under review is capable of addressing network configuration issues both at the inception of the deployment and dynamically during the period of expected operation.
  - [Other?]
- References

174. Ignorance of Network Edge "Qualitative" Attributes

- Challenges
  - Not all relationships are the same, even between identical nodes.
    - A friend may also be a business associate
    - Compare IRC section that imputes extra taxable transactions to a given relationship (gifts by employer to employee, etc.) (Section 111?) Duberstein Case (gift of car to employee is part of salary, not a true "gift")?
  - Mis-understanding of the relationship can result in additional risks
    - Interaction may be recharacterized for various legal purposes (tax, fraud, etc.)
  - Is the technology and system architected to mitigate "off channel" influences on system performance?
    - Operations
    - Audit
  - [Other?]
- References

174. Ignorance of Network Edge "Qualitative" Attributes

- Candidate Analytical Frameworks/Metrics/Actions
  - Prepare/harden the edge of the system to address exposure to external conditions
    - Consider alternatives to "hardening" strategies for resiliency
      - Avoidance
      - Absorption/Integration
      - [Other]
  - Consider whether the system has a "surface tension" akin to that in water (ionic liquid where surface characteristics vary from bulk fluid)
  - Analogy to Musk Oxen survival formation
    - Face outward to anticipate threat
    - Circle the wagons (Conestoga survival strategy)
  - [Other?]
- References

175. "Sym-Info-Genesis" – Engulfment by Abstraction

- Challenges
  - Under the definition of "life" as "auto-catalytic, entropy-secreting forms (with or without physical embodiment), what we perceive as "risks" may in fact be artifacts of inevitable integrative (eukaryotic?) progression into non-physically embodied information space.
    - Violence to existing negentropy living systems as precursor to integration into larger living systems
  - The relationship of information and risk (see slide __ for background), and their origin in system performance expectations, suggests that systems with environmental awareness will continue to engulf/consume their external environment in an effort to reduce external threat.
    - Render the externality innocuous – reduce information differentials
  - [Other?]
- References

175. “Sym-Info-Genesis” – Engulfment by Abstraction

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider potential lower energy states as potential “strange attractors” for system performance challenges
    - Introduce alternative strategies for resilience
      - Acceptance
      - Adoption
      - Absorption
  - Consider alternative identity narratives that can maintain continuity
  - [Other?]
- References

176. Constraint of Possibilities, Bounded Solution Phase Space

- Challenges
  - Institutional artifacts of historical de-risking structures constrain the imagination about both the characterization of current challenges and the potential pathways to their solutions
    - Book - "Doing Money" suggests that one of the functions of "money" is as a risk consolidator in society
    - How might expanded view of monetary systems function open up (by analogy and direct application) potential pathways to de-risking and leverage solutions in future information markets?
  - Traditional institutional norms and measurements are applied to evaluate system performance of both people and technologies, but increasingly are measuring the wrong system elements.
    - Technologies are being deployed in new contexts
    - Contexts in information networks are changing faster than technology.
  - Book - "____ Debt" says money eliminates consideration of alternative possibility.
  - Monetary issuance reflects the monopoly (sovereignty) of power over certain aspects of social and economic power.
    - Blockchain based "power" isn't exclusive (yet), and so is still "pre-sovereign."
  - Future issue of "Computational Sovereignty"
    - If define "sovereign" as entity that doesn't ask for permission or forgiveness
    - What is nature of computational "governance" as "black box" of computational sovereigns recedes further from human oversight and understanding?
  - [Other?]
- References
  - "Doing Money" by _____.

176. Constraint of Possibilities, Bounded Solution Phase Space

- Candidate Analytical Frameworks/Metrics/Actions
  - A significant constraint of current information network de-risking strategy is the undue focus on “data”
    - Most issues relating to security, privacy, liability and other unknowns in networked information systems arise from the failure of systems to meet expectations with regard to “meaning” variables, not data-related variables.
    - Data plus meaning equals information
      - How enhance “information” security BEYOND data security?
      - HIPAA, GDPR, GLB, etc. are based on “data” security concepts.
    - Examples of mechanisms of “meaning” security include:
      - Statutes, regulations, laws
      - Contract duties
      - Industry norms and practices
  - “Smart contract” concept (as proposed in blockchain and other contexts) is not sufficiently flexible to cover sufficient “meaning” security
    - However, effort reflected in smart contracts-related initiatives suggest the right general intuition about how to to address ”meaning” outside of data structures as pathway to more reliable systems.
  - [Other?]
- References

177. Bias – Cognitive – Checklist of Cognitive Biases

- Challenges
  - The concept of "bias" is often cited as an element affecting system performance, but it is rarely unpacked or parsed into various sorts of bias that can affect the expected performance of technology, institutions and people operating together in information networks
    - It is not possible to create and apply effective solutions to problems (such as bias) if the problem is not adequately identified and characterized
  - In the case of "cognitive biases" (those which affect the mental functioning of humans interacting with networked information systems), the sources and characterization of bias is typically written in the languages of psychology, sociology and other disciplines that are not within the purview of designers and builders of technology systems.
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by various forms of cognitive biases
    - Cognitive bias issues can cause system stakeholders to interact with the system (and otherwise act in ways) that are inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of bias can increase system risks and undermine system function.
  - [Other?]
- References
  - https://en.wikipedia.org/wiki/List_of_cognitive_biases

177. Bias – Cognitive – Checklist of Cognitive Biases

- Candidate Analytical Frameworks/Metrics/Actions
  - Be specific on bias:
    - Whenever issue of “bias” is referenced in context of system performance, care should be taken to define the specifics of the bias assertion
      - What is the nature of the bias
      - What is the source of the bias
      - How and who in the system affected by the bias
  - Shared language of bias:
    - Be aware of the challenges associated with implementing de-biasing strategies in socio-technical systems
      - Confirm that the meanings of language and terms used are shared among technical and other members of the extended development and deployment team.
      - Consider characterizing and describing the requirements of legal, policy and other non-technical elements of the system as ”technical requirements” to make it easier to convert them into integrated system elements.
        - » Phrasing the requirements for humans and institutions as “duties” that have corresponding measurements of their performance enables them to be more readily integrated with technical system expectations
  - Survey list of “cognitive biases” in Atlas for examples of cognitive bias.
  - [Other?]
- References

178. Bias – Cognitive – Anchoring

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by cognitive biases associated with Anchoring
    - Anchoring issues can cause system stakeholders to interact with the system (and otherwise act in ways) that are inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - "Anchoring" introduces bias into cognitive processes by tying thinking to the first information received
    - See Wikipedia definition of "anchoring" below
  - Anchoring can be intentional or unintentional
    - Intentional anchoring is present in training and education that seeks to introduce and cultivate in individuals functional and appropriate biases toward broadly adopted cognitive patterns
    - Unintentional anchoring can occur when initial data and information is over weighted in the consideration of later information
  - Anchoring can be contextually appropriate or inappropriate
    - Appropriate anchoring – Where the introduced "bias" is toward broadly adopted and accepted and functional priors that help a stakeholder to join a community of shared knowledge (an "epistemic community")
    - Inappropriate anchoring – Where the anchoring bias is toward a view that is non-functional, inappropriate or contrary to the interests of the receiving party.
  - Anchoring can constrain discretion in operators, users and other stakeholders of socio-technical systems
  - [Other?]
- References
  - Wikipedia provides that:
    - "Anchoring is a psychological heuristic that describes the propensity to rely on the first piece of information encountered when making decisions. According to this heuristic, individuals begin with an implicitly suggested reference point (the "anchor") and make adjustments to it to reach their estimate. For example, the initial price offered for a used car sets the standard for the rest of the negotiations, so that prices lower than the initial price seem more reasonable even if they are still higher than what the car is worth."
-

178. Bias – Cognitive – Anchoring

- Candidate Analytical Frameworks/Metrics/Actions
  - Research on modifying states of ignorance suggests that once knowledge is integrated into an individual mind, it strongly resists revisions/change
    - Awareness of the persistence of knowledge is critical to configuring and delivering effective training (i.e., new knowledge) to stakeholders regarding system operation
    - Assumptions made about user and operator "knowledge" relating to system operation and use should be carefully compared to actual status in an effort to avoid gap
      - Market research/soft release of system can help identify potential gaps in assumptions versus stakeholder reality
  - [Other?]
- References

179. Bias – Cognitive – Pareidolia and Apophenia

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by cognitive biases associated with Pareidolia and Apophenia
  - Pareidolia and Apophenia issues can cause system stakeholders to interact with the system (and otherwise act in ways) that are inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - Anthropologists and psychologists assert that humans evolved to perceive patterns in "noisy" information environments as a protection from predators and other dangers
    - Human behavior is deeply affected by these survival instincts
  - Apophenia is the cognitive bias that arises when false patterns are perceived in random data
  - Pareidolia is the detection of false patterns in sound and sight.
  - Both pareidolia and apophenia involve the perception by humans of patterns in random or noisy data/environments that falsely suggest the presence of a phenomenon or entity that is not actually present.
  - False perceptions can result in "false positives" and other misperceptions that can influence the behavior of humans (and the institutions for which they work) in ways that can be adverse to expected functioning of information networks and other socio-technical systems.
  - [Other?]
- References
  - Wikipedia provides that:
    - "Apophenia, also known as patternicity, or agenticity, is the human tendency to perceive meaningful patterns within random data. Apophenia is well documented as a rationalization for gambling. Gamblers may imagine that they see patterns in the numbers which appear in lotteries, card games, or roulette wheels. One manifestation of this is known as the "gambler's fallacy". Pareidolia is the visual or auditory form of apophenia. It has been suggested that pareidolia combined with hierophany may have helped ancient societies organize chaos and make the world intelligible."

179. Bias – Cognitive – Pareidolia and Apophenia

- Candidate Analytical Frameworks/Metrics/Actions
  - Since both pareidolia and apophenia involve “false perceptions” the negative effects of such perceptions can be mitigated through application of multiple/alternative measurements to “cross check” the results
    - This strategy is limited to those system aspects that are most vulnerable to these mis-perceptions (by reason of likelihood and/or severity), because the costs of multiple checks and “back up” systems can be prohibitive if deployed system wide.
    - Backup systems might employ AI and/or people from different cultural contexts who are less likely to be subject to identical misperceptions.
  - [Other?]
- References

180. Bias – Cognitive – Attribution

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by cognitive biases associated with Attribution
  - Attribution issues can cause system stakeholders to interact with the system (and otherwise act in ways) that are inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of all Encoders, Decoders and Intermediaries can be affected by bias.
    - Bias can affect performance of individuals making them less reliable or predictable in system operations.
  - All Attribution biases occur when an individual creates or adopts various sorts of explanations for the behavior of another individual or themselves
  - Like other biases, attribution biases may be helpful in evaluating the behavior of others, but may be unhelpful if they are applied as a super-factor for behavioral motivation or otherwise obscure other reasons for a particular behavior
  - Multiple types of attribution biases can affect system performance
    - ultimate attribution error – Group level attribution error that is applied to describe the positive behavior of "in group" members and the negative behavior of "out group" members
    - fundamental attribution error – Tendency of people to overemphasize individual's disposition and personality and underemphasize situational explanations for behavior
    - actor-observer bias – Asymmetry in explaining the behavior of self and others where other's behavior is considered to be driven by their personality, while one's own behavior is sensed to be driven by objective situation and setting
    - self-serving bias – The distortion of a cognitive or perceptual process that is driven by an individuals need to maintain self esteem
  - [Other?]
- References
  - Wikipedia provides that:
    - "An attribution bias can happen when individuals assess or attempt to discover explanations behind their own and others' behaviors. People make attributions about the causes of their own and others' behaviors; but these attributions don't necessarily precisely reflect reality. Rather than operating as objective perceivers, individuals are inclined to perceptual slips that prompt biased understandings of their social world. When judging others we tend to assume their actions are the result of internal factors such as personality, whereas we tend to assume our own actions arise because of the necessity of external circumstances. There are a wide range of sorts of attribution biases, such as the ultimate attribution error, fundamental attribution error, actor-observer bias and self-serving bias."

180. Bias – Cognitive – Attribution

- Candidate Analytical Frameworks/Metrics/Actions
  - Identifying and correcting the negative effects of bias in socio-technical system operation requires proper identification and characterization of the sort of bias in operation
  - Attribution bias involves the making of assumptions about the causes of the behaviors of another based on their perceived habits, personality attributes and other non-situational factors
  - Such causative assumptions may be misleading where they are overemphasized, causing system inefficiencies
  - Attribution assumptions might be more appropriate where the "assumptions" being made are not based on individual personality, but rather on the attributes of the role that an individual has undertaken in an organization that are made consistent by institutional policy:
    - E.g., "Staff sergeants always wake up early."
    - E.g., "Lawyers ask too many detailed questions."
  - Where certain demographics of stakeholders are involved with a system, audit the system and its operators to identify any latent sources of attribution bias in the encoders (senders), intermediaries and de-coders (receivers) of communications in interactions.
  - [Other?]
- References

181. Bias – Cognitive – Framing

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by cognitive biases associated with Framing
  - Framing issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - Framing is another word for the application of a comprehensive, overall narrative to supply context to a given situation
    - Where individuals (acting in their individual and employee capacity) apply framings that are inconsistent with the framings applied in the design, development, deployment or operation of a socio-technical system, the difference in framings can result in diminished reliability and predictability of the system.
  - Among the various sorts of biases, ”framing” is often a social construction that is often quite broadly held and comprehensive in its effect on individual behaviors
    - It may be difficult to adjust biased perspectives and views that are part of a larger “framing”
  - [Other?]
- References
  - Wikipedia provides that:
    - “Framing involves the social construction of social phenomenon by mass media sources, political or social movements, political leaders and so on. It is an influence over how people organize, perceive, and communicate about reality. It can be positive or negative, depending on the audience and what kind of information is being presented. For political purposes, framing often presents facts in such a way that implicates a problem that is in need of a solution. Members of political parties attempt to frame issues in a way that makes a solution favoring their own political leaning appear as the most appropriate course of action for the situation at hand. As understood in social theory, framing is a schema of interpretation, a collection of anecdotes and stereotypes, that individuals rely on to understand and respond to events. People use filters to make sense of the world, the choices they then make are influenced by their creation of a frame.
    - Cultural bias is the related phenomenon of interpreting and judging phenomena by standards inherent to one's own culture. Numerous such biases exist, concerning cultural norms for color, location of body parts, mate selection, concepts of justice, linguistic and logical validity, acceptability of evidence, and taboos. Ordinary people may tend to imagine other people as basically the same, not significantly more or less valuable, probably attached emotionally to different groups and different land.”
  –

181. Bias – Cognitive – Framing

- Candidate Analytical Frameworks/Metrics/Actions
  - Given the breadth and comprehensiveness of the effect on individual behavior of "framing" in socio-technical systems, designers and operators should seek to address "framing" biases directly and explicitly
    - System operation as a competing "frame:"
      - Characterize individual behavior when engaged with socio-technical system at issue as its own unique "frame" in which certain behaviors are expressly required, notwithstanding larger social framing for the behavior
      - Compare legal "standards of care" for parties in different roles that they must adopt as behavioral frames when they are "on duty."
    - Emphasize that the system technical specifications and behavioral/policy rules and requirements are themselves a "frame" that is intended to supersede other subjective frames of stakeholders
      - User rules
      - Operator rules
      - Intermediary rules
  - System audit and operations metrics should enable tracking of performance of system stakeholders to enable evaluation of whether external framings are affecting system performance
    - Particularly important in "user centric," "crowd-sourced" and other broadly distributed systems where the population of individual stakeholders is beyond the direct control or influence of the operators and owners of the system.
  - Consider crafting user and operator rules for system to explicitly address and supplant known external framings that could result in stakeholder behavior that is inconsistent with reliable and predictable operation of the technical system.
  - [Other?]
- References

182. Bias – Cognitive – Halo Effect

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by cognitive biases associated with the Halo Effect (positive) and the Horn Effect (negative)
  - Halo Effect and Horn Effect issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - Reliable operation of technical systems requires reliable and predictable behaviors of various system stakeholders
    - User
    - Operator
    - Intermediary
    - Owner
  - System stakeholders may make certain negative or positive assumptions about other system people, organizations, brands or products that may cloud their objective evaluation and use of a socio-technical system and its subcomponents.
  - Designers and developers of technical and socio-technical systems should take account of aspects of system organization and operation that could be influenced by external sources of "halo" and "horn" effect that could alter behaviors and decisions of stakeholders that could in turn affect system operation
    - Effect of "brand name" alternatives in system subassembly purchases
  - Reputational elements affect "build and buy" decisions (positively and negatively) in ways that can influence system operation
  - In new interaction "blank space" traditional brands of technology and socio-technical systems may enjoy B2B and B2C brand familiarity, but their products and services might not be optimized (or even "fit for function") for de-risking and leveraging interactions of the types and in the volumes experienced.
    - E.g., credit card systems competes with "Square."
    - E.g., [insert example of another dominating legacy brand which is not optimized for a certain set of circumstances]
  - [Other?]
- References
- Wikipedia provides that:
  - "The halo effect and the horn effect are when an observer's overall impression of a person, organization, brand, or product influences their feelings about specifics of that entity's character or properties.
  - The name halo effect is based on the concept of the saint's halo, and is a specific type of confirmation bias, wherein positive sentiments in one area cause questionable or unknown characteristics to be seen positively. If the observer likes one aspect of something, they will have a positive predisposition toward everything about it. A person's appearance has been found to produce a halo effect. The halo effect is also present in the field of brand marketing, affecting perception of companies and non-governmental organizations (NGOs)
  - The opposite of the halo is the horn effect, when "individuals believe (that negative) traits are inter-connected." The term horn effect refers to Devil's horns. It works in a negative direction: if the observer dislikes one aspect of something, they will have a negative predisposition towards other aspects.

182. Bias – Cognitive – Halo Effect

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider application of techniques to assure system objectivity
    - Sealed bids for system subassemblies?
    - Multiple bids for system subassemblies?
  - Separately consider whether positive or negative reputation is undermining purchasing activity associated with system design, development and/or operation that might undermine system operation.
    - E.g., system users should be warned against using certain related products and/or services offered by third parties the operation of which will be inconsistent with system function
      - E.g., Warnings not to use certain types of oil for a car
  - Consider "white list" and "black list" of compatible products to guard against stakeholders making buying decisions inconsistent with overall system operation.
    - Be sure to have defensible criteria for inclusion of third party companies on "white list" and "black list."
      - Objective criteria for decision
        - » Resources of third party
        - » Maintenance and continuity of service of third party
        - » Support offered by third party
  - [Other?]
- References

183. Bias – Cognitive – Self-Esteem

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by cognitive biases associated with Self Esteem
    - Self-Esteem issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function
  - The operation of socio-technical systems in the real world depends on the reliable and predictable actions and behaviors of both technologies and people, but when systems fail to operate as expected, it can be difficult to identify the relative contribution of technology failure and human failure to the system problem
    - The absence of definitive causation chains for explaining system failures can have the effect of undermining the self-esteem of stakeholders such as users and operators
    - Unresolved failure causation chains can negatively affect morale and evaluation processes among stakeholder groups to the further detriment of system operations
  - The introduction of new technologies into organizations and societies frequently yields unpredictable and undesirable effects that are perceived as risks by users, operators and intermediaries
    - Stakeholders may not be able to discern he relative contributions of the technology and the humans/organizations to such unreliability, which can affect self esteem of such parties, and reputational attributes of organizations
  -
  - [Other?]
- References
  - Wikipedia provides that:
    - “Self-serving bias is the tendency for cognitive or perceptual processes to be distorted by the individual's need to maintain and enhance self-esteem. It is the propensity to credit accomplishment to our own capacities and endeavors, yet attribute failure to outside factors, to dismiss the legitimacy of negative criticism, concentrate on positive qualities and accomplishments yet disregard flaws and failures. Studies have demonstrated that this bias can affect behavior in the workplace, in interpersonal relationships, playing, sports and in consumer decisions.”

183. Bias – Cognitive – Self-Esteem

- Candidate Analytical Frameworks/Metrics/Actions
  - Clarify the capacities and limitations of the technology in operating and training materials to help stakeholders identify the source of system operating limitations
  - Offer training that emphasizes the expectations of stakeholder activity in various roles
  - Emphasize in training materials that the system continues to develop and that feedback on problems is not a negative, but represents a contribution to the improvement of the system
    - "Suggestion box" analogy
  - Turn user and operator challenges in using system into a positive
    - Offer rewards for identifying "bugs" in system
    - Like "zero day exploits" markets
  - Shared experience among users and operators of technology (including in solving system challenges) can build esprit d'corp that can improve socio-technical system performance
  - [Other?]
- References

184. Bias – Cognitive – Status Quo

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by cognitive biases associated with Status Quo
    - Status Quo issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function
  - In an era of rapid development of information technologies, the "status quo" is an increasingly slippery and anachronistic concept
    - Myriad interacting complex systems resist characterization as "status quo"
    - Desire for status quo is reduced to a generalized feeling of loss
  - The exponential growth of networked information technology has created a world with myriad new types and volumes of interactions for which there are few or no normative leads
    - "Status Quo" perspectives are not useful in the rapidly expanding interaction "blank space"
  - In periods of rapid change, nostalgia for the past is often clouded by fabricated narratives of a past that never existed resulting in feelings of hopelessness and inefficaciousness among stakeholders
  - How can the owners and operators and users of a given socio-technical system identify and mitigate against the potential for system disablement associated with a gap between system stakeholder "status quo" thinking and ever-advancing system capacities
  - Users and operators frequently don't access many of the features of the system, sticking to known functions and capacities
    - Failure to use all system functions decreases ROI associated with the system
  - [Other?]
- References
  - Wikipedia provides that:
    - "Status quo bias is an emotional bias; a preference for the current state of affairs. The current baseline (or status quo) is taken as a reference point, and any change from that baseline is perceived as a loss. Status quo bias should be distinguished from a rational preference for the status quo ante, as when the current state of affairs is objectively superior to the available alternatives, or when imperfect information is a significant problem. A large body of evidence, however, shows that status quo bias frequently affects human decision-making."

184. Bias – Cognitive – Status Quo

- Candidate Analytical Frameworks/Metrics/Actions
  - Policy and operating manuals (and training) for technical systems should be explicit about the anticipated changes in behavior that are required to exploit all the features of the system
  - Benefits of new features should be made obvious to technical system users and operators
    - Critical system features that are expected to encounter resistance in uptake due to status quo thinking and perspectives should be supported by incentives (and penalties as necessary) for implementation (or failure to implement in the case of penalties)
  - In large organizations, traditional change management approaches should be consulted to help shepherd changes in technology
  - [Other?]
- References

185. Bias - Conflict of Interest – Bribery

- Challenges
  - "Bribery" involves the payment of money to a party (either an individual or an institution) to cause them to engage in a certain behavior requested and/or consistent with the interests of the party offering the bribe [check definition of "bribery"]
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Bribery
    - Bribery issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - Bribery can cause the behavior of a party to an interaction or transaction to act in ways that are unexpected by another party or that otherwise affect the performance of a party in a way that is disadvantageous or harmful to the other party
  - International supply chains associated with the construction of information network hardware, software and systems can involve the contributions of international subassemblies and services that may have been secured or assured with bribery or similar payments, raising the possibility of potential criminal prosecution and/or reputational harm to participating companies
    - "Grease money"
    - US Foreign Corrupt Practices Act (or similar legislation) may apply
  - [Other?]
- References

185. Bias - Conflict of Interest – Bribery

- Candidate Analytical Frameworks/Metrics/Actions
  - Bribery involves the provision of economic value to influence the behavior and actions of parties
    - May address bribery with economic or non-economic strategies
  - Economic mitigation
    - Increase compensation to parties potentially subject to bribery influence to decrease amenability to bribes
    - "Neighborhood Watch" - Create "reward" system among stakeholders to incentivize reporting of bribery and other system-inconsistent activities
    - Apply and invoke laws and regulations against bribery
  - Non-Economic mitigation
    - Create policies and rules that compel reporting of bribery (and other such actions)
      - Compare – Code of legal ethics (obligation to report ethical violations of others)
      - Compare – Neighborhood Watch – "If you see something, say something"
    - Protect Whistleblowers who report bribery in system
  - Provide clear guidance on application of "Foreign Corrupt Practices Act" to employees working in cross border supply chains
    - Conceptions of bribery differ in different cultures and under different laws
  - At its margins, bribery-like practices may be more or less acceptable in different cultures
    - Caution and care should be taken in pricing and budgeting associated with international supply chains where local actions may be constrained by informal and discretionary demands by government and other officials
      - Consider behavior at margins of bribery and "selective prosecution" of local codes, etc.
  - [Other?]
- References
  - Wikipedia provides that:
    - "Bribery is giving of money, goods or other forms of recompense to in order to influence the recipient's behavior. Bribes can include money (Including. Tips), goods, rights. In action, property, privilege, emolument, gifts, perks, skimming, return favors, discounts, sweetheart deals, kickbacks, funding, donations, campaign contributions, sponsorships, stock options, secret commissions, or promotions. Expectations of when a monetary transaction is appropriate can differ from place to place. Political campaign contributions in the form of cash are considered criminal acts of bribery in some countries, while in the United States they are legal provided they adhere to election law. Tipping is considered bribery in some societies, but not others."

186. Bias - Conflict of Interest – Favoritism

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Favoritism
    - Favoritism issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - Conflicts of interest associated with "Favoritism" can cause stakeholders to make decisions, take actions and engage in behaviors that may not be optimal for system operation
  - In a time of rapid technology development, favoritism can obscure opportunities to embrace system changes that could be otherwise advantageous
  - [Other?]
- References
  - Wikipedia provides that:
    - "Favoritism, sometimes known as in-group favoritism, or in-group bias, refers to a pattern of favoring members of one's in-group over out-group members. This can be expressed in evaluation of others, in allocation of resources, and in many other ways. This has been researched by psychologists, especially social psychologists, and linked to group conflict and prejudice. Cronyism is favoritism of long-standing friends, especially by appointing them to positions of authority, regardless of their qualifications. Nepotism is favoritism granted to relatives."

186. Bias - Conflict of Interest – Favoritism

- Candidate Analytical Frameworks/Metrics/Actions
  - Favoritism can affect behaviors of many different stakeholders at any stage of technical system design, development, deployment, operation and auditing
    - Documentation and auditing of decision-making at all stages can help to identify and address the effects of favoritism
  - Favoritism in a human behavioral trait that can subtly affect decision making in ways that can undermine objectively-defensible decisions associated with system organization and operation
    - Strategic and significant procurement decisions can be made with input from various groups within the organization to mitigate the potential negative effects of favoritism on decision making
  - Disclosure of potentially conflicting relationships by employees and outside contractors can help to identify potential subjects of favoritism and invite the putting in place of mechanisms to guard against it
  - [Other?]
- References

187. Bias - Conflict of Interest – Lobbying

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Lobbying
    - Lobbying issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - In the context of rapid social change, complex issues, and new framings, representatives of the legislative, executive and judicial branches of government often rely on expertise and advice of non-governmental officials to provide insight into the effects of such changes to help inform their governmental decision making and activities
  - Newly powerful large information network service providers typically do not recognize the benefit and value of lobbying activity in influencing the social and economic setting in which their products are organized and operated until several years after it is initially deployed
    - Many challenges in implementation and operation can be implemented with changes in the law.
  - [Other?]
- References
  - Wikipedia provides that:
    - "Lobbying is the attempt to influence choices made by administrators, frequently lawmakers or individuals from administrative. agencies. Lobbyists may be among a legislator's constituencies, or not; they may engage in lobbying as a business, or not. Lobbying is often spoken of with contempt, the implication is that people with inordinate socioeconomic power are corrupting the law in order to serve their own interests. When people who have a duty to act on behalf of others, such as elected officials with a duty to serve their constituents' interests or more broadly the common good, stand to benefit by shaping the law to serve the interests of some private parties, there is a conflict of interest. This can lead to all sides in a debate looking to sway the issue by means of lobbyists."

187. Bias - Conflict of Interest – Lobbying

- Candidate Analytical Frameworks/Metrics/Actions
  - New socio-technical information systems are rapidly changing the interaction landscape for a variety of stakeholders in society, leading to a widening gap between the realities of technology and the past-realities of law
    - Increased pressure to bridge the gap of law and technology results in increased lobbying activity
  - International supply chains of subassemblies and services associated with technology systems should consult with the local lobbying/bribery laws of relevant jurisdictions to confirm the scope of allowable activities involving government officials
  - Recognize that lobbying affects only ”public laws” (i.e., legislation, regulation, court cases (in “common law” jurisdictions)
    - Public lawmaking is a slow and unpredictable process
  - Lobbying to establish duties and rights in public law should be supplemented by simultaneous efforts to instantiate “private” (contract) law that can create structures of duties and rights that are enforceable as contracts in courts
    - Mass contracts can create duties and rights that apply across large populations
  - Participation in trade associations can support lobbying efforts that may be beyond the resources capacities of many organizations
    - Trade associations work in standards of various sorts serve to create normative “standards of practice” that may be adopted by courts and legislatures as “industry standards” to inform legal “duties of care”
      - Conformity to duties of care can provide potential relief from negligence liability (“reasonable person” test under common law and many statutes)
  - [Other?]
- References

188. Bias - Conflict of Interest – Shilling

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Shilling
    - Shilling issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - Shilling has taken on new dimensions online
    - Includes influencers driving sales and also false metrics on "likes" that mislead business decisions of other parties
    - Generation of false "ratings" and "reviews" online for payment is an example of the expanded state of shilling online
  - [Other?]
- References
  - Wikipedia provides that:
    - "Shilling is deliberately giving spectators the feeling that one is an energetic autonomous client of a vendor for whom one is working. The effectiveness of shilling relies on crowd psychology to encourage other onlookers or audience members to purchase the goods or services (or accept the ideas being marketed). Shilling is illegal in some places, but legal in others. An example of shilling is paid reviews that give the impression of being autonomous opinions."
    - https://www.ftc.gov/news-events/blogs/business-blog/2019/02/ftc-advertisers-bills-shills-product-reviews-are-no-go

188. Bias - Conflict of Interest – Shilling

- Candidate Analytical Frameworks/Metrics/Actions
  - See FTC Notice on disclosure by paid actors shilling merchandise in retail establishments
  - Disclosure of paid promoters on advertising
  - [Other?]
- References
  - FTC notice number ____

189. Bias - Conflict of Interest – Extortion/Blackmail

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Extortion and Blackmail
    - Extortion and Blackmail issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - Extortion/blackmail can be applied to influence the actions and behavior of information network stakeholders in ways that are detrimental to the operation of the system and/or one or more of its stakeholders
  - New forms of extortion are growing online
    - Incidental transparency resulting from death of secrecy under pressure from information seeking behavior of mass populations has revealed patterns of human behavior that are inconsistent with historical norms
      - Cross cultural normative differences also offer opportunities for extortion
  - Extortion/blackmail may be engaged in for a variety of purposes, including pure economic gain, desire to undermine competitor business, etc.
    - Understanding the motivations of the extortionist can help to develop more effective organizational defenses against the threat posed by extortion
  - "Extortion/Blackmail" are:
    - Extortion is the practice of obtaining something of value through force, compulsion or threat. To obtain a benefit through coercion.
    - Blackmail is a type of extortion. Blackmail is the action of demanding payment or other benefit from another person in return for not revealing compromising or damaging information about them
  - [Other?]
- References

189. Bias - Conflict of Interest – Extortion/Blackmail

- Candidate Analytical Frameworks/Metrics/Actions
  - Where the object of the threat is content and functionality of computer systems, steps taken to protect computer content and functionality can help to mitigate the potential for extortion
    - Backup files to protect against erasure or third party encryption
  - Growth in potential sources of "threat" increases in step with the growth of interaction volumes
    - Interactions are sources of risk if expectations of one or more parties is not met
    - 5th order effect of Moore's law increases interaction volumes AND threats in networks
      - Each threat is a potential source of extortion
      - E.g., new threats online based on extortion/blackmail
    - Exponential increase renders "prevention" strategies uneconomic – they are complex systems that exhibit non-linear behaviors the cost of which is unsustainable
    - Alternative approaches to prevention include:
      - Communication among subsystems
      - Process-based solutions
      - Interdependence in operations and enforcement drives cooperation and compromise in rulemaking
  - Provide guidance to stakeholders on actions if they are subject to online extortion
    - Make sure to screenshot and preserve all relevant evidence and communications,
    - Have a trusted friend or family member support party in the documentation process (as this can help refute claims of evidence tampering by the opposing party),
    - Stop engaging with the online blackmailer and cyber-extortioner,
    - Do not pay them any amount of the ransom or try and negotiate,
    - Change up the privacy settings on your social media accounts so that no personal and sensitive information (including contacts) is publicly available,
    - Set up an alerts account to receive notifications anytime your name is mentioned online, and
    - Contact an attorney as soon as possible
- References

190. Bias - Conflict of Interest – Nepotism

- Challenges
  - "Nepotism" is "Favoritism" (see "Favoritism" slide in Atlas) granted to relatives
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Nepotism
    - Nepotism issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - The problem with "nepotism" in the organization and operation of networked information systems is that the parties occupying critical roles in the organization that gained their positions through "nepotism" may not have the needed skills and capacities required for the position, potentially undermining system function and operation
  - Nepotism raises issues of fairness in an organization, potentially affecting trust and morale in other employees
  - [Other?]
- References

190. Bias - Conflict of Interest – Nepotism

- Candidate Analytical Frameworks/Metrics/Actions
  - Nepotism can be difficult to address since it often reflects power relationships in an organization
    - Instances of nepotism are single instances of larger power relationships
    - Consanguinity has been demonstrated to be significant variable in sustaining power
      - Economist article on long term superior performance of family owned business
      - Instances of political families demonstrate ubiquity of phenomenon
      - Biological origins of the behavior may be difficult to eradicate
  - Policies of organizations that seek to minimize the potential negative impacts of nepotism should consider rules that are explicit regarding:
    - The hiring of non-relatives by managers
    - Written guidelines on acceptable hiring and contracting behavior and enforcement of those rules
    - Clear rules and requirements for employees to work their way up in the organization
    - Establish reasonable earnings and compensation levels an apply them fairly
    - Provide appropriate job training opportunities fairly
    - Require employees and contractors to document specific incidents of any perceived nepotism.
  - For parties dealing with organizations that are characterized by nepotism relationships
    - Stick to facts, but recognize potential for intransigence in organization valorized by nepotism relationships.
  - [Other?]
- References
  - Wikipedia provides that: **Nepotism** is the granting of jobs to one's relatives or friends in various fields, including business, politics, entertainment, sports, religion and other activities. Nepotism is the act of using one's power to secure better jobs or unfair advantages for a family member when they may not have the right skill, experience or motivation compared to others.

191. Bias - Conflict of Interest – Horse Trading

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Horse Trading
    - Horse Trading issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - "Horse Trading" refers to negotiations characterized by shrewd bargaining and reciprocal concessions
    - The presence of reciprocal concessions can involve the present negotiation and/or other related and unrelated negotiations directly or indirectly involving the parties
      - The reference to variables from other negotiations may be unknown to parties in instant transactions resulting in varying and unexpected motivations of the parties to the instant transaction
  - [Other?]
- References

191. Bias - Conflict of Interest – Horse Trading

- Candidate Analytical Frameworks/Metrics/Actions
  - Where the same parties repeatedly engage in transactions and interactions together, there is a potential for parties to trade advantage and disadvantage from one transaction to another
    - Regulated markets
    - Litigators
    - Politicians
    - Rulemaking/standard setting stakeholder groups
  - Where the negotiating parties engaging in horse trading owe duties to third parties, ”horse trading” may harm the interests of represented parties if the “gives” are taken from represented parties’ benefits and the “gets” benefit unrelated parties.
    - Fiduciaries (Investment advisers, bankers, etc.)
    - Politicians
  - In the case of interactions that are regularly affected by outside influence of “horse trading,” consider disclosure and audit processes to help identify and evaluate the potential effects of bias associated with the outside influence
    - Political negotiations
    - E.g., B2B interactions in large consumer markets
    - E.g., that are documented by mass contracts (e.g., in insurance, finance, supply chain discipline, etc.)
  - [Other?]
- References

192. Bias - Conflict of Interest – Financial Stake

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by conflict of interest biases associated with Financial Stake
    - Financial Stake issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
    - In "conflict of interest"-prone settings, there are variables that affect the performance of one of the interacting parties in ways not expected or taken into account by the other interacting party.
    - Such unaccounted variables can undermine the evaluation of benefits and/or risks of an interaction or transaction by the non-biased party to their potential harm and detriment
  - "Financial Stake" can result in conflict of interest when one party has an economic interest in an interaction of transaction that is unknown to the other party and which affects the decisions, actions and behaviors of the biased/conflicted party to the interaction in ways that are not known to the other party
  - The extended supply chains of networked information systems (including all intermediary products and services in such chains) offer multiple opportunities for individual investments (and other more subtle forms of financial stake) that may affect the decision making and actions of individuals involved in design, purchasing, systems integration and other "buy or build" decisions.
  - [Other?]
- References

192. Bias - Conflict of Interest – Financial Stake

- Candidate Analytical Frameworks/Metrics/Actions
  - As with other economic sources of conflict of interest, financial stake can be potentially mitigated through financial and non-financial approaches
    - Financial approach
      - Positive financial approach –
        - » Organizations may offer rewards for employees and contractors that identify conflicts of interest, including those associated with financial stake
        - » Organizations may offer assistance in creation of Chinese walls and/or "blind trusts" so that parties with pre-existing financial interests can continue to hold those interests after the time that they are employed or retained by the organization.
      - Negative financial approach – Organizations may limit the investments and financial stakes taken by their employees and independent contractors to help limit and avoid the conflicts of interest associated with financial stake
    - Non-financial approach
      - Disclosure - Employees, independent contractors, counterparties to contracts, and other parties the actions and behavior of which will affect the reliable and predictable performance of the technical system can be required to provide disclosure of financial interests that might affect their decisions in the organization and operation of a technical system
      - "Chinese Wall" – Parties that disclose financial stake that may be inconsistent with expected behaviors for a given system can be isolated from the interactions in a given account or decision process to prevent their conflict of interest from affecting system performance.
  - [Other?]
- References

193. Bias – Analytical/Statistical – Selection Bias

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases associated with Selection Bias
    - Selection Bias issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The behavior of socio-technical systems depends on the reliable and predictable performance of both people/institutions and technologies.
  - In "selection bias" settings parties apply inappropriate or incomplete data to the analysis of one or more system functions [NOTE: Seek improved definition]
  - Selection bias may be intentional or inadvertent
    - Intentional selection bias reflects a decision by a stakeholder to influence a process through the constraint of information taken into account in decision making
      - Cherry picking
    - Inadvertent selection bias arises when the selection of data for system analysis is erroneously assumed to be representative of the object of the study
      - Frequently results where causation relationships are confused with correlation, in which case the selected data is not
  - [Other?]
- References
  - Wikipedia provides that:
    - "Statistical bias is a systematic tendency in the process of data collection, which results in lopsided, misleading results. This can occur in any of a number of ways, in the way the sample is selected, or in the way data are collected. It is a property of a statistical technique or of its results whereby the expected value of the results differs from the true underlying quantitative parameter being estimated.
    - Wikipedia provides that: Selection bias is the, conscious or unconscious, bias introduced into a study by the way individuals, groups or data are selected for analysis, if such a way means that true randomization is not achieved, thereby ensuring that the sample obtained is not representative of the population intended to be analyzed. This results in a sample that may be significantly different from the overall population."

193. Bias – Analytical/Statistical – Selection Bias

- Candidate Analytical Frameworks/Metrics/Actions
  - Selection bias is an experimental error that occurs when the participant pool, or the subsequent data, is not representative of the target population
  - Identifying the specific source of selection bias is important to mitigating this form of bias
    - Sampling Bias source – be aware of self-selection among participants which can be addressed by using a sample that is not self selecting
    - Pre-screening – prescreening of data/participants can distort sample population
    - Insufficient data or participants can also affect research results
    - Cherry picking can affect results
      - The result of intentional selection bias
  - Transparency and clarity can help to identify and address selection bias problems
    - NIH (NSF) and NGO requirements that all data from studies be published and made available for review
  - [Other?]
- References
  - Definition of ”selection bias” above is from https://imotions.com/blog/selection-bias/

194. Bias – Institutional – Academic

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases associated with academia and academic organizations
    - Academia related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
  - When technical and socio-technical systems are developed in whole or in part in academic settings, bias can arise from a variety of institutional, individual, systemic, social and financial sources.
  - Academic bias is particularly important in evaluating information technology systems, since significant academic research forms the basis for design, development, deployment and operation of modern computing, telecommunications and information processing systems.
    - How can implementers, operators, relying parties and other stakeholders detect the presence of various forms of academic bias that can affect the threat and vulnerability profile of a given system that incorporates technical and research output of such academic institutions?
  - [Other?]
- References
  - Wikipedia provides that:
    - "Academic bias is the bias or perceived bias of scholars allowing their beliefs to shape their research and the scientific community. Lately, claims of bias in the US are often linked to claims by conservatives of pervasive bias against political conservatives and religious Christians. Some have argued that these claims are based upon anecdotal evidence which would not reliably indicate systematic bias and have suggested that this divide is due to self-selection of conservatives choosing not to pursue academic careers. There is some evidence that perception of classroom bias may be rooted in issues of sexuality, race, class and sex as much or more than in religion."

194. Bias – Institutional – Academic

- Candidate Analytical Frameworks/Metrics/Actions
  - Many of the sources of bias that can influence meaning and risk in academic settings and studies are not limited to academic settings
    - Academia is characterized by particular dynamics that may enhance the effect of certain types of bias
    - Academic institutions (and entities dealing with academic institutions) should review the general bias slides to identify the extent to which one or more of these sources of bias may be present
  - Academia represents a particular sector of society that is characterized by some unique sorts of relationships and interactions that give rise to certain unique forms of bias
    - The "Bias-Institutional – Academic" slides in this Atlas identify and catalog a subset of academic biases that may cause information risks in a system.
  - [Other?]
- References

195. Bias – Institutional – Academic - Experimenter

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases associated with academia and academic organizations, including "Experimenter Bias"
    - Experimenter Bias-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
  - When technical and socio-technical systems are developed in whole or in part in academic settings, bias can arise from experimenters and other researchers having certain expectations regarding their results that influence their design, operation and observations in an experiment
    - Experimenter bias is a form of "expectancy" bias that occurs outside of the academic setting
  - [Other?]
- References
  - Wikipedia provides that:
    - In science research, experimenter bias occurs when experimenter expectancies regarding study results bias the research outcome. Examples of experimenter bias include conscious or unconscious influences on subject behavior including creation of demand characteristics that influence subjects and altered or selective recording of experimental results themselves.

195. Bias – Institutional – Academic - Experimenter

- Candidate Analytical Frameworks/Metrics/Actions
  - If and to the extent that experimenter bias is viewed as an academic version of "expectancy bias," it can invite the application of some of the mitigation strategies suggested in this Atlas of "expectancy bias"
  - Some of the systems and processes for curbing and mitigating Experimenter bias are already present in the time tested processes
    - Result of "self-testing" "self correcting" systems of scientific method
    - Peer review
    - Reproducibility
    - Publication of negative data
    - Calls for publication of original research question as well as final research question
  - Pre-review of methods and results can help curb propagation of bias through academic channels
  - [Other?]
- References

196. Bias – Institutional – Academic - Funding

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases associated with academia and academic organizations, such as Funding
    - Academic funding-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
  - When technical and socio-technical systems are developed in whole or in part in academic settings, bias can arise from funding considerations can affect the decisions and judgment of researchers, designers and developers in ways that could affect their judgment, research direction, etc.
  - Funding bias in academia is related to "financial stake" bias in broader, non-academic, contexts
    - See "Financial Stake" slides in Atlas
  - The application of academic papers and research to the broader economy and society invites more specific attention and resources into the work of curbing funding biases
    - Academic studies may be perceived as more authoritative and neutral than other materials, and hence the effects of funding bias can be more broadly detrimental to the variety of organizations and individuals that may rely on such materials
  - [Other?]
- References
  - Wikipedia provides that:
    - "Funding bias refers to the tendency of a scientific study to support the interests of the study's financial sponsor. This phenomenon is recognized sufficiently that researchers undertake studies to examine bias in past published studies. It can be caused by any or all of: a conscious or subconscious sense of obligation of researchers towards their employers, misconduct or malpractice, publication bias or reporting bias."

196. Bias – Institutional – Academic - Funding

- Candidate Analytical Frameworks/Metrics/Actions
  - Please see Atlas slides for "financial stake" for related mitigation approaches, metrics and actions
  - In academic settings, funding and financial stake bias takes forms that reflect some of the unique funding structures of academia, and invite consideration of some particular approaches to mitigation
    - Donor/funder oversight – maximum leverage is available to funders who can establish stipulations and prerequisites to funding
    - Academic institution oversight – Universities as employers of professors (even tenured professors) can create policies and rules to govern their employees, including rules on acceptance of outside funding
      - Tech transfer rules and approaches of universities reflect the dynamics of university/professor/third-parties in situations where there is protectable (and potentially valuable) IP (patents, copyrights, trade secrets, etc.)
      - Employer oversight of outside funding relationships may be less developed outside of the tech transfer context
  - [Other?]
- References

197. Bias – Institutional – Academic - FUTON

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases associated with academia and academic organizations
    - Academia related issues associated with "FULL TEXT ON NET" (FUTON) can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
  - When technical and socio-technical systems are developed in whole or in part in academic settings, bias can arise from a unique form of unintentional selection bias that arises based on the relative ease of access online to open access journals (versus charged-access publications) and the resort by researchers to abstracts rather than complete articles (the latter called NAA (No abstract available) bias.
  - These forms of bias can perpetuate inadvertent misinformation to the extent it is then picked up and referenced in later publications
  - [Other?]
- References
  - Wikipedia provides that:
    - Full text on net (or FUTON) bias is a tendency of scholars to cite academic journals with open access—that is, journals that make their full text available on the. internet without charge—in their own writing as compared with toll access publications. Scholars can more easily discover and access articles that have their full text on the internet, which increases authors' likelihood of reading, quoting, and citing these articles, this may increase the impact factor of open access journals relative to journals without open access.
    - The related bias, no abstract available bias (NAA bias) is scholars' tendency to cite journal articles that have an abstract available online more readily than articles that do not.

197. Bias – Institutional – Academic - FUTON

- Candidate Analytical Frameworks/Metrics/Actions
  - FUTON is a form of inadvertent "Selection bias" that arises in academic settings when time and resource-constrained researchers rely on the ease of accessing electronic publications (and abstracts in the case of NAA bias) in performing literature searches and other background research
    - Reference the Atlas slides relating to "selection bias" for potential mitigation strategies associated with FUTON
  - FUTON affects academic and scientific research integrity by introducing data and information into analysis that is based on ease of access to online materials, often at the expense of more probative and relevant authorities (that may be more difficult to find offline, or more expensive to access online)
    - Economic support of academic institutions offering mass licenses to professors and students can help to offset negative effects of constrained set of materials available FUTON
  - [Other?]
- References

198. Bias – Institutional – Academic - Publication

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases associated with academia and academic organizations, including those arising from publication concerns.
    - Academia related publication issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
  - When technical and socio-technical systems are developed in whole or in part in academic settings, bias can arise from the pressures associated with publication
  - Publication success is a "currency" in academia, and academic enthusiasm for the accomplishment of publishing an academic paper can incentivize actions and behaviors that can "bias" the analyses and results of academic work.
  - Pressures of publication can manifest in actions such as:
    - Desire to demonstrate significant findings
    - Disincentive to publication of studies showing negative results
    - Tendency to iterate popular paradigms and suppress negative findings that vary too greatly from accepted doctrine
      - This latter bias can suppress truth for years or decades
        - » See, e.g., research on Heliobactor pylori as cause of ulcers
        - » See, e.g., Copernicus
  - [Other?]
- References
  - Wikipedia provides that:
    - "Publication bias is a type of bias tat arises with regard to what academic research is likely to be published because of a tendency of researchers, and journal editors, to prefer some outcomes rather than others e.g. results showing a significant finding, leads to a problematic bias in the published literature. This can propagate further as literature proof of claims about support for a hypothesis will themselves be biased if the original literature is contaminated by publication bias. Studies with significant results often do not appear to be superior to studies with a null result with respect to quality of design. However, statistically significant results have been shown to be three times more likely to be published compared to papers with null results."

198. Bias – Institutional – Academic - Publication

- Candidate Analytical Frameworks/Metrics/Actions
  - If and to the extent that "publication" is recognized as the equivalent of currency in academic research, publication biases can be seen as related to "financial stake."
    - See the Atlas of risk map slides on "financial stake" for potential mitigation strategies
  - Funders, publishers and universities are gatekeepers for academic publishing and in a position to create and enforce rules that could mitigate the information risk effects of "publication" bias, if it can be demonstrated to be in their respective interests to do so
    - Funder sourced controls
      - Research funders can create contractual requirements in funding documentation that creates duties imposed on authors, researchers (and indirectly to publishers and universities) designed to curb sources of of publication bias
    - Publisher sourced controls
      - Publishers/Journals can adapt acceptance and publication criteria that is designed to curb publication bias
    - University sourced controls
      - University employment policies can establish rights and duties for professors and researchers to curb publication biases
  - The aforementioned publication gatekeepers are bound together in various historical, normative and IP (Intellectual property) drenched agenda that constrains their ability to change
  - Derive, describe and iterate lessons at organizational change management from settings in which the behaviors that introduce publication and other academic biases were altered dramatically in exigent circumstances
    - "Break the glass" settings such as public health research in epidemic disease, emerging headline issues in reproductive health and other high profile, high risk settings breaks down the traditional relationships in the publication ecosystem
    - Consider how the exceptions that naturally arise in extreme/exigent circumstances might be generalized in whole or part
      - Derive from acute settings those risk mitigation strategies and tactics that could apply in chronic risk settings
      - See Atlas of Risk slides based on "time" for challenges of translating solutions from the short term acute to the long term chronic
      - Note that increased pace and volume of interactions creates perception of increased interaction density and relative "speed" of interactions in an institution
        - » The increase in relative interaction speed can serve to cause successful solutions from acute settings to the service of derisking chronic settings
  - [Other?]
- References

199. Bias – Sectoral – Security - Profiling

- Challenges
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Security Profiling-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function
  - Profiling involves the application of heuristics to decision making regarding people
    - Heuristics are simple strategies applied for decision making that trade accuracy for practicality
  - Profiling (as a form of heuristic) may introduce generalizations into decision making that could bias organizational and individual decision making away from objectively testable and defensible decisions
  - Profiling by one set of stakeholders of another set of stakeholders may result in the organization and operation of information network integrity strategies and tactics that are ineffective in real world contexts
    - E.g., Economists assumptions about the behavior of consumers obscures multiple variables that then cause economic analysis to be inappropriate as a controlling variable in social structure planning
    - E.g., profiling of usage behavior of different cultural populations in international supply and consumption chains can influence investment and technology development in ways that may be inefficient and risk-causing.
  - _____
  - [Other?]
- References
  - Wikipedia provides that:
    - "Racial profiling, or ethnic profiling, is the act of suspecting or targeting a person of a certain race on the basis of racially observed characteristics or behavior, rather than on individual suspicion.[1]Racial profiling is commonly referred to regarding its use by law enforcement and its leading to discrimination against minorities."
    - Heuristics definition from Wikipedia https://en.m.wikipedia.org/wiki/Heuristics_in_judgment_and_decision-making

199. Bias – Sectoral – Security - Profiling

- Candidate Analytical Frameworks/Metrics/Actions
  - Profiling, like other biases associated with inter-stakeholder judgment and evaluation, can affect decision making in the context of myriad different stakeholder relationships, each of which must be separately analyzed and addressed to facilitate resilient and sustainable solutions
    - Profiling of users
      - Encoders/Sender users – Information system inputs affect the quality of the operation and outputs of the system itself
        - » Create "neighborhood watch" among stakeholders engaging in different roles in the system to encourage collective monitoring of user/encoder/sender information inputs in system to improve power of the technology system to de-risk and leverage interactions by decreasing bias effect of profiling and increasing objective measurement
          - Shared interest in good function
      - Decoders/Receivers users – Provide decoders/receivers with the ability to audit and test the output of the system to help
    - Profiling of socio-technical system operators
      - Profiling of operators
      - Profiling by operators
    - Profiling of socio-technical system intermediaries
      - Profiling of intermediaries
        - » Carefully consider application of "black lists" and "white lists" that are applied to making decisions about benefits and access to system
        - » Defensible criteria for inclusion and inclusion should be based on defensible factors that do not discriminate (either in action or effect)
          - Capability based decisions
          - Capacity based decisions
          - Resource – based decisions
      - Profiling by intermediaries
        - » a
  - Be cautious of unintended potential exclusions based on latent or hidden profiling
    - E.g., decisions made based on economic resources may mask historical discriminations
      - Evaluation of historical levels of medical insurance of African Americans as lower than other populations reflect historical unavailability of health care for those populations, not an objective economic/investment by these populations
  - [Other?]
- References

200. Bias – Sectoral – Media
Agenda Setting, Gatekeeping and Sensationalism

- Challenges
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Agenda Setting, Gatekeeping, and Sensationalism-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - Bias in the form of agenda setting/gatekeeping and sensationalism (collectively called "Media bias" in this slide") can affect system performance in ways that are not expected by one or more parties that depend on the system.
  - Media bias arises when the demands of mass media and journalism affect the content and manner of the presentation of data and information.
    - These mass media demands that affect the communication of information may not be known to other stakeholders and hence may serve as a source of bias
  - Stakeholders may not have other sources of information beyond the mass media upon which to base their future decisions
    - Even if bias is recognized, it may be difficult to access additional and corrective information
  - [Other?]
- References
- Wikipedia provides that:
  - "Media bias is the bias or perceived bias of journalists and news producers within the mass media in the selection of events, the stories that are reported, and how they are covered. The term generally implies a pervasive or widespread bias violating the standards of journalism, rather than the perspective of an individual journalist or article. The level of media bias in different nations is debated. There are also watchdog groups that report on media bias.
  - Practical limitations to media neutrality include the inability of journalists to report all available stories and facts, the requirement that selected facts be linked into a coherent narrative, government influence including overt and covert censorship, the influence of the owners of the news source, concentration of media ownership, the selection of staff, the preferences of an intended audience, and pressure from advertisers.
  - Bias has been a feature of the mass media since its birth with the invention of the printing press. The expense of early printing equipment restricted media production to a limited number of people. Historians have found that publishers often served the interests of powerful social groups."

200. Bias – Sectoral – Media
Agenda Setting, Gatekeeping and Sensationalism

- Candidate Analytical Frameworks/Metrics/Actions
  - Establish and consistently apply standards of publication to create resource of trust
    - New York Times – "All the news that fit to print"
  - Disclose the pressures such as advertising that affect content
  - Review the Ph.d. thesis by Andrew Gruen, (now at Facebook) entitled "Accountability Journalism in the Digital Age," relating to the collapse of journalism as advertising revenues moved from paper to online social networks
    - Journalism is a necessary element of democratic governance, and its demise undermines sustainable democracy
    - Consider the governance of the technical system and whether the stakeholders subjet to that governance have access to sufficient information.
  - [Other?]
- References
  - Wikipedia provides that:
    - "Agenda setting describes the capacity of the media to focus on particular stories, if a news item is covered frequently and prominently, the audience will regard the issue as more important. That is, its salience will increase.
    - Gatekeeping is the way in which information and news are filtered to the public, by each person or corporation along the way. It is the "process of culling and crafting countless bits of information into the limited number of messages that reach people every day, and it is the center of the media's role in modern public life. [...] This process determines not only which information is selected, but also what the content and nature of the messages, such as news, will be."
    - Sensationalism is when events and topics in news stories and pieces are overhyped to present skewed impressions of events, which may cause a misrepresentation of the truth of a story. Sensationalism may involve reporting about insignificant matters and events, or the presentation of newsworthy topics in a trivial or tabloid manner contrary to the standards of professional journalism."

201. Bias – Algorithmic and Inductive

- Challenges
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies
  - The actions and behaviors of stakeholders AND technology in socio-technical systems can be affected by biases
    - Algorithmic and Inductive-related issues can cause system stakeholders AND technologies to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders AND also contrary to the functioning of other system technical elements
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - System bias can arise in both non-technical AND technical aspects of a system
  - Algorithmic and inductive bias arises when the performance of either technology or non-technical elements is affected by process for engaging with inputs that is inappropriate for the circumstances. [check paragraph]
  - If system stakeholders are not aware of the presence of algorithmic and inductive bias, they may make assumptions about the output of the technical system that is flawed or overbroad.
  - [Other?]
- References
  - Wikipedia provides that:
    - "Inductive bias occurs within the field of machine learning. In machine learning one seeks to develop algorithms that are able to *learn* to anticipate a particular output. To accomplish this, the learning algorithm is given training cases that show the expected connection. Then the learner is tested with new examples. Without further assumptions, this problem cannot be solved exactly as unknown situations may not be predictable. The inductive bias of the learning algorithm is the set of assumptions that the learner uses to predict outputs given inputs that it has not encountered. It may bias the learner towards the correct solution, the incorrect, or be correct some of the time. A classical example of an inductive bias is Occam's Razor, which assumes that the simplest consistent hypothesis is the best."

201. Bias – Algorithmic and Inductive

- Candidate Analytical Frameworks/Metrics/Actions
  - The field of machine learning is still in its infancy and the processes and techniques are undergoing continued development
    - Reinforcement vs. Imitation Learning - “Traditional” ”Reinforcement” machine learning is being improved with new approaches to “Imitation” learning
      - “Reinforcement” learning is characterized by programs trying millions of random actions through trial and error approach to solve a problem
      - “Imitation” learning uses “built up learning” to “bootstrap” learning
        - » Be careful of possible biases in the “priors” that are offered to train the system
  - Different elements of algorithmic systems may be more or less amenable to auditand review
    - Audit of training data may be possible to identify potential sources of bias
    - Audit of algorithm in operation may or may not be auditable due to various “black box” challenges
  - [Other?]
- References
  - Nature Magazine (28 November 2019), p.583 entitled “AI Versus Minecraft.”(Discusses the increased attention to Imitation Learning as supplement or replacement for techniques of Reinforcement Learning

202. Bias – Conflict of Interest – Insider Trading

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases arising from conflicts of interest
    - Insider Trading-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies
  - Insider trading can affect the behavior of stakeholders because it reflects the extraction by one stakeholder (the insider trader) of value from a sociotechnical information system (most typically a stock exchange or other market) based on the taking of actions based on information that is intended to be secret.
  - The difference between fraud and arbitrage is subtle
    - In arbitrage, a party discovers an information differential and then exploits it for value
    - In fraud, a party creates a false information differential and then exploits it for value
    - Insider trading exists at the boundary of fraud and arbitrage
      - A "Perfecg market" incorporates all relevant stakeholder information
      - In insider trading, information is available to some stakeholders before others, undermining fairness
  - [Other?]
- References
  - Wikipedia provides that:
    - "Insider trading is the trading of a public company's stock or other securities (such as bonds or stock options) by individuals with access to non-public information about the company. In various countries, trading based on insider information is illegal because it is seen as unfair to other investors who do not have access to the information as the investor with insider information could potentially make far larger profits that a typical investor could make."

202. Bias – Conflict of Interest – Insider Trading

- Candidate Analytical Frameworks/Metrics/Actions
  - The securities laws of many jurisdictions provide rules for addressing insider trading
    - Securities rule 10-b5 under US Securities Laws
  - Note that laws, rules and enforcement standards for insider trading varys from one jurisdiction to another
  - Whatever the legal characterization of the activity, when a party trades on insider information it will affect the behaviors of other stakehodlers who are not party to the same information
  - [Other?]
- References

203. Bias – Systemic – Technology Platform ”Lock In”

- Challenges
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Technology Platform “lock in”-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function
  - Where organizations and individuals integrate a technology system into their lives and operations, they develop dependencies, habits and other patterns of behavior and relationships that can make it difficult to integrate future changes
  - Sociotechnical systems can be “normalized” within and among organizations so that they become “de facto” standards
    - Standards can save costs and lower risk in future intereactions
    - Standards can be anticompetitive, and resistant to further innovation
  - The expense and effort of replacing various systems and subassemblies can cause non-optimal systems and structures to remain in use due to high costs of replacement
  - [Other?]
- References

203. Bias – Systemic – Technology Platform ”Lock In”

- Candidate Analytical Frameworks/Metrics/Actions
  - Strategic considerations: Evaluate “centrality” of third party sociotechnology systems as part of overall operations when making buy-or-build decisions
    - Is the system “plug and play”
      - Technology links to operations
      - People/institutiuonal links to operations
        - » E.g., retail sales on Amazon “depend” on that platform and may have less power to negotiate or switch to new retail platform
  - Competition: consider the platform dependencies of competitors
  - Compare to ”traditional” outsourcing analysis of 1980s
    - Purchase outside expertise
    - Less employee control
    - More contractual control
    - Ability to expand and contract operations more readily.
  - When to act: Consider various future transition strategies at the time of acquisition of a new system
    - Maximum leverage to get concessions from vendor PRIOR to closing purchase
    - What is required for termination of service agreements, etc.?
  - Exit strategies: Consider “portability” of various intangible assets associated with operaiton of the system
    - IP rights (patent, copyright, patent, trade secret) associated with continuing system development during operating phase
    - Data rights associated with data generated during operating period of the technology.
  - [Other?]
- References

204. Bias – Systemic – Bureaucratic “CYA”

- Challenges
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Bureaucratic CYA-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function
  - The phrase “CYA” (derived from the vulgar “cover your ass”) is the heading fofr a category of behaviors in which an individual acts in a manner to acvoid future criticism
    - CYA frequently results in conservative decision-making
    - CYA may result in favoring standards and contracting with established suppliers to avoid potential for accusation of mistake
      - Significant mistakes by corporate officers and directors can lead to assertions of breach of duty of care or other fiduciary duties
  - In periods of rapid technological devellpment, CYA behaviors could curtail appropriate exploration of available innovations that could benefit design, development, deployment or operation of technical systems
  - CYA behavior that delay organizational decision making can have the result of slowing technology “buy or build” decisions in ways that can increase the ultimate costs of system acquisition
    - Ironically, in rapidly changing technology markets, delay can have the advantage of allowing “the dust to settle” on new innovations so that more informed decisions can be made based on the operating experience of other similarly situated parties trying the technology.

- References
  - William Safire defines “CYA” as "the bureaucratic technique of averting future accusations of policy error or wrongdoing by deflecting responsibility in advance"

204. Bias – Systemic – Bureaucratic "CYA"

- Candidate Analytical Frameworks/Metrics/Actions
  - Bureaucratic hesitancy and risk-averse behaviors can crimp the ability of large organizations to adopt new technologies (and the new organizational structures that such technologies engender)
    - Bureaucracies make good and bad decisions slowly
  - Craft agreements associated with design, development, deploymewnt and operation of the technology with clear delineation of respective duties, risks and responisibilitiies of the parties
  - Recognize additional support obligations associated with reality of supporting deployment of new technology in excxisting organizations
    - Structure pricing to accommodate different support profiles
  - Consider offer of transition support from existing systems
  - Seek support for technology change from high levels of organization
    - Power laws of bureaucracies instruct that absence of high level support will be fatal to initiatives since the number of bureaucratic interaction sign offs increases more rapidly than the usefulness of the innovation (power law of bureaucracies).
  - [Other?]
- References

205. Subjective and Un-auditable Performance Expectations

- Challenges
  - Performance expectations and evaluations are most easily communicated, measured and enforced through objectively measurable criteria and metrics.
  - Subjective, hidden, unstated or other poorly communicated requirements and expectations for system performance result in ambiguity in the relationship of parties involved with a system in ways that can create risks for all parties.
  - [Other?]
- References

205. Subjective and Un-auditable Performance Expectations

- Candidate Analytical Frameworks/Metrics/Actions
  - Parties establishing new relationships can benefit from normatively cross referencing definitions, standards, best practices, policies, rules, etc. of third parties
    - Reference to established rules reduces the negotiation, implementation of new systems
    - Order provided by external rules stabilizes parts of system, permitting resources to be applied to new system components.
  - Statutes and regulations are sources of external "objective" metrics that can help to reduce ambiguity of organization and operation in new systems design, development and deployment.
  - Care must be taken when referencing and applying metrics produced by a system
    - Does the measurement, in fact, provide insight into the elements of system operation that it purports to measure?
      - Is the measurement a. good or poor surrogate for the system performance element?
  - Subjective and other measurements should be supported by other metrics and observations that can verify the subjective measurement.
  - [Other?]
- References

206. Vulnerability to Failure Cascade – Dependency Risk

- Challenges
  - Modern information networks are increasingly dependent for their organization and operation on multiple parties.
    - Compare information “service” supply chains to the extended supply chains for goods and their many participants
  - Coordination of information networks is frequently restricted to multiple bilateral contracts and relationships, rather than overall multilateral planning
    - The result of these chains of bilateral agreements is that de-risking negotiations among parties rarely involve all of the parties required to coordinate “end to end” performance expectations.
- The lack of coordination among stakeholders in extended information network ”supply chains” creates a lack of transparency regarding risks elsewhere in the system that can affect remote parties that depend on their expectations of system performance being met.
  - [Other?]
- References

206. Vulnerability to Failure Cascade – Dependency Risk

- Candidate Analytical Frameworks/Metrics/Actions
  - Failure cascades can be propagated (and their risk effects aggravated) by combinations of Attack, Accident, Acts of Nature and AI/ML
    - See slide on "AAAA Risk"
  - Parties dependency on extended supply chains (including extended information network supply chains) should be subject to stress test analysis that includes failures beyond first order relationships.
    - May be difficult to get information about such remote risks
    - Seek information during negotiation stage, when leverage is greatest
  - If information on remote supply chain risks is not available, consider alternative approaches to de-risking
    - Insurance
    - Third-party guarantees and other forms of security
  - Note that creditworthiness of counterparty is relevant in establishing mechanisms for addressing risk.
  - Be aware of the distinction between "assignment of rights" and "delegation of duties" in contract
    - Delegation of duties does not relieve the original obligor of their obligations under a contract in the absence of a release by the party benefitted.
      - In the case of a unilateral delegation by a party of their duties (without a release), the original obligor becomes, in essence a "guarantor" of the performance of the party to which the duties were purported to be delegated.
  - [Other?]
- References

207. Conflict of Interest – Breach of Fiduciary Obligation / Overreaching

- Challenges
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies.
    - Where parties (whether individual or institutional) engage other parties to act on their behalf in one or more interactions, an agency relationship is formed
    - There are many types of agency relationship, each formed to accomplish certain specific purposes.
  - "Fiduciary" obligations arise in that subcategory of agency arrangements in which the "agent" party is expected to put the interests of the other ("principal") party ahead of their own (agent's) interests
  - Examples of "fiduciary" arrangements include:
    - Investment advisers (under the 1940 Investment Advisers Act)
    - Attorney/client relationships
  - When parties with fiduciary obligations act in ways contrary to the interests of their beneficiaries/principals that gives rise to a conflict of interest that can result in the presumed "fiduciary" tngageing in actions and behaviors that are contrary to the expectations of the other stakehodlers in related interactions.
  - Problems can arise when the agent and principal are unsure of their relationship.
    - Scope
    - Timing
  - Absence of established norms and duties in areasof data, information, etc. create many "gray areas" in the provision of agency-related services
    - What is scope of "self dealing" when information is derived fro data handled in an agency capacity
    - Is the same true of meta-data?
  - [Other?]
- References

207. Conflict of Interest – Breach of Fiduciary Obligation / Overreaching

- Candidate Analytical Frameworks/Metrics/Actions
  - Fiduciary obligations are a subset of agency relationships
    - Fiduciary and agency law are well developed
    - Existing law cannot answer many new questions arising for agency relationships in new networked interactions, but it is the right place to start when designing a system that is intended to support the proiviosn of fiduciary type duties and similar duties
  - Agency law is established by the states in the US and references uniform agency laws
    - May have variotions among states
    - Also, be aware of agency and fiduciary laws of various countries in multi-jurisdictional supply chains
  - Agency relationships can be flexibly created and maintained by contract as long as the contract terms are consistent with applicable law
  - Conflict of interest rules and cases have developed fiduciary law that may be applicable to current networked information activities.
  - [Other?]
- References

208. Bias – Cognitive – Confirmation

- Challenges
  - The performance of socio-technical systems (including but not limited to information networks) depends on the reliable and predictable performance of both people/institutions and technologies
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Confirmation bias-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - Unfamiliar user interfaces and uncertain risks cause stakeholders to resort to ascribing causal relationships to familiar and comfortable explanations, analytical framings and stories.
    - Reliance on familiar explanations may cloud awareness of other risk causation chains.
  - [Other?]
- References
  - Wikipedia provides that:
    - "Confirmation bias is the tendency to search for, interpret, favor, and recall information in a way that confirms one's belief's or hypotheses while giving disproportionately less attention to information that contradicts it. The effect is stronger for emotionally charged issues and for deeply entrenched beliefs. People also tend to interpret ambiguous evidence as supporting their existing position. Biased search, interpretation and memory have been invoked to explain attitude polarization (when a disagreement becomes more extreme even though the different parties are exposed to the same evidence), belief perseverance (when beliefs persist after the evidence for them is shown to be false), the irrational primacy effect (a greater reliance on information encountered early in a series) and illusion correlation (when people falsely perceive an association between two events or situations). Confirmation biases contribute to overconfidence in personal beliefs and can maintain or strengthen beliefs in the face of contrary evidence. Poor decisions due to these biases have been found in political and organizational contexts."

208. Bias – Cognitive – Confirmation

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

209. Protection of Vulnerable Stakeholder Populations

- Challenges
  - Does the system lend itself to protection of interests of users and stakeholders who cannot adequately protect themselves from system risks
    - Elderly
    - Children
    - Infirm
    - Victims of overt or implicit/structural discrimination
  - What is the nature of the harms for each group?
  - What are the mechanisms of that protection?
  - How expensive will it be to include the needed protections?
  - [Other?]
- References

209. Protection of Vulnerable Stakeholder Populations

- Candidate Analytical Frameworks/Metrics/Actions
  - Consult with groups that purport to represent vulnerable populations
  - Consult directly with individuals in vulnerable populations
  - Stress test the distribution of benefits of the technology system by running system simulations (in multiple dimensions such as time, economic benefit, insight/intrusion, etc.) swapping the beneficiaries with the burdened parties to reveal system power assumptions
  - Run user groups to gain insight on attitudes directly from affected parties.
  - Permit open narrative to encourage discovery of still-unmeasured risks
    - Don't confuse guidance and curation of process with accidental constraint of response possibilities.
  - Create processes to receive feedback of adequacy of system operation for vulnerable populations DURING OPERATING PHASE
  - [Other?]
- References
  - Jacques Derrida suggested, as an exercise in considering alternative power structures, inverting the center and edges of bell curves of social resource allocations. The "Stress test" suggested above applies this mental experiment to social policy framings

210. Enhancement of Individual Self-Security

- Challenges
  - The architecture of the internet renders hierarchical institutions (with centralized internal information flows) unable to perceive or communicate behavioral and performance standards that would otherwise enhance de-risking.
  - In the absence of centralized institutional initiatives for security, privacy and liability avoidance, individual “nodes” in a system can no longer depend entirely on institutional solutions for security.
  - The volume of online interactions continues to increase exponentially, rendering any institutional or other centralized solution quickly anachronistic, ineffective and potentially counter-productive.
  - How can massively distributed information networks be made more reliable, secure, and private?
  - [Other?]
- References
  - RAND Corporation paper by Paul Baran (1966)

210. Enhancement of Individual Self-Security

- Candidate Analytical Frameworks/Metrics/Actions
  - A first step to improving the security of information networks and other highly distributed sociotechnical systems is to recognize when existing strategies and tactics lose their effectiveness
    - This is a challenge in the absence of alternative or additional measures of system performance
  - Create additional and alternative measurements of system performance that can be applied by individuals and institutions that use the system
  - Neighborhood watch
    - Distributed system
    - Stakeholders with a “stake” in system performance are incentivized to participate in individual and community de-risking activities.
  - [Other?]
- References

211. Amenability to Value Creation, Extraction, Appropriation

- Challenges
  - Does a given technology system anticipate the ways in which value will be created and made available to stakeholders to support adoption and maintenance of the system.
  - Value creation, extraction and appropriation can be functional or dysfunctional.
    - Functional – Enables energy of markets and other systems of exchange to power adoption
    - Dis-functional – May enable exploitation of stakeholders and harm proportional to value generated.
  - If and to the extent that the system does not itself generate extractable value, the cost and resources needed to design, develop and deploy the system must be derived from alternative sources
    - Systems that are not “self funding” (in whole or part) place a greater burden on implementers and users, that might not have the resources to deploy the system.
  - [Other?]
- References

211. Amenability to Value Creation, Extraction, Appropriation

- Candidate Analytical Frameworks/Metrics/Actions
  - Understand and evaluate the precise value proposition of the technology
    - Can the value be achieved through other simpler, less expensive means?
  - Analyze the purported stakeholder benefits of the system
    - What are the mechanisms through which the stakeholder beneficiaries can enjoy the benefits?
      - Are the prerequisite to that enjoyment realistic?
      - What is the incentive for stakeholders to apply the system in the way that can yield such benefits?
  - [Other?]
- References

212. ”WEIRD” UIs

- Challenges
  - Psychological studies that inform some policy and technical system requirements are based on behaviors of test subjects who are typically drawn from ”WEIRD” student bodies at academic institutions:
    - **W**estern
    - **E**ducated, and from countries that are
      - **I**ndustrialized
      - **R**ich and
      - **D**emocratic
  - If and to the extent that the results of any such studies are referenced (directly or indirectly) in the organization and operation of information networks, the performance expectations associated with such systems may be skewed toward anticipation of operator and user performance that is not characteristic of the population in which the system is deployed.
  - Also, replicability crisis in psychology suggests questions about efficacy and predictability of studies.
  - [Other?]
- References

212. “WEIRD” UIs

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the various frameworks and strategies suggested for addressing cognitive bias in technical system organization and operation.
    - View psychological studies as ”snapshots” of human behaviors that are potentially affected by “WEIRD” biases
  - Consider possibility that historical focus on “WEIRD” populations as source of metrics for establishing system requirements has had the result of causing ALL non-WEIRD populations to be potential “vulnerable” populations with respect to the operation of the technology.
  - [Other?]
- References
  - Economist article on bias in health cost data reflecting racially-determined access histories

213. ADA/PDR/DSM Stress Testing

- Challenges
  - Human behaviors can affect both individual and institutional actions in the context of technical system operation
    - Each setting and context for system operation anticipates a different range of acceptable human and institutional behaviors in which it is expected to function within system parameters
  - Human behaviors respond to a wide variety of prompts, triggers and variables, each of which can elicit behaviors along a wide spectrum of predictability
  - Some behaviors are strongly psycho-somatic, meaning that they have a physical prompt/trigger
  - ADA – Americans with Disabilities Act – describes statutory requirements for accommodation of persons with disabilities
  - PDR – Physicians Desk Reference – Lists medications prescribed to patients in the US
  - DSM – Diagnostic and Statistical Manual of _____ - Lists parameters for diagnosis of psychological conditions.
  - The ADA, PDR and DSM all describe physical and behavioral causative factors that can affect the performance of people (acting in their individual and/or institutional capacities)s in ways that are outside of the performance parameters of a system
  - How can system designers and operators de-risk their system from the potential performance disruptions associated with ADA/PDR/DSM variables?
  - [Other?]
- References
  - ADA [citation here]
  - Physician's Desk Reference
  - Diagnostic and Statistical Manual

213. ADA/PDR/DSM Stress Testing

- Candidate Analytical Frameworks/Metrics/Actions
  - The ADA/PDR and DSM each offer detailed and relatively-objectively testable metrics associated with human behaviors that might be helpfully applied in the context of describing the steps needed to de-risk a given socio-technical system deployment.
  - For example:
    - ADA – Aircraft flight systems might not be most safely operated by blind people
    - PDR – Security systems might not be most effectively operated by people taking sleeping pills
    - DSM – [insert example here]
  - Where information networks and other technical systems are being deployed in a population (of operators and/or users) that experiences a high level of a given behavioral trait that is associated with conditions referenced in one or more of the ADA/PDR/DSM, the parties responsible for design, development and deployment of the system can anticipate the presence of that population in their user testing.
  - [Other?]
- References

214. Culturally-Variable Decision Trees

- Challenges
  - The variables that inform decisions can vary from one culture (or even one economic sector) to another.
    - These cultural variables may be reflected in part in local legal systems, but the non-legal variables that affect decision making are more difficult to research and incorporate in system organization and operational requirements.
  - Where a system is dependent on predictability of a given decision tree, it might not perform reliably in settings where the decision tree is different
  - For example, recent MIT study illustrated three different, culturally bound, responses to the classic “trolley car” problem
    - How can AI developers provide training data or otherwise program systems to respond appropriately in systems that will be deployed in cross cultural contexts when the underlying human and social values differ?
  - Is the technology system flexible enough so that it can be reliably operated across multiple cultures and jurisdictions
  - [Other?]
- References
  - See MIT study on ”Trolley Car” problem and variations of response among cultures

214. Culturally-Variable Decision Trees

- Candidate Analytical Frameworks/Metrics/Actions
  - Legal systems offer some (albeit not comprehensive) insight into cultural variables
    - Systems should be designed so that their organization and operation is consistent with the laws of the jurisdictions in which they are operated (and in some cases the laws of the jurisdictions that have laws protecting certain stakeholders – such as individual users of data systems in the EU under GDPR.
  - Beyond legal surrogates for cultural variables it can be difficult for system designers and developers to ascertain the variables to address in localizing their technology systems for the most effective and efficient adoption in a given culture
    - Look at articles on localization
    - Look at Atlas entries on "adaptation studies"
  - Where local cultural variables remain unknown (in whole or part) consider making the critical decision trees explicit in the system organizational and operational materials.
    - Abiding by explicit critical decision trees might be established as a prerequisite to system warranty coverage to encourage operator and user compliance
  - [Other?]
- References

215. Degree of Dependence on Untrained User Base

- Challenges
  - The Internet (and its many subsidiary networked information systems) are widely recognized to be highly distributed systems
    - The term “distributed” describes the characteristics of both operators and users of these systems
  - The continued exponential increase in the growth of interactions that take place over the Internet, results in an exponential increase in the number of people and institutions that are users of the internets ever-increasing functions.
  - If and to the extent that the reliable operation of the Internet (and other distributed information networks) depend on the reliable and predictable behavior of users and operators, such reliability is undermined as the scale and reach of the Internet grows.
  - Does the technical system anticipate the operation and use of the system by ever-less trained populations?
  - [Other?]
- References

215. Degree Of Dependence On Untrained User Base

- Candidate Analytical Frameworks/Metrics/Actions
  - UI development
  - Clarity regarding duties of technology provider
    - Communication of potential harms
  - Training
    - Certification for training as prerequisite to operation of system
  - Help-desk functions
  - Fail safe default states
    - HRO – high reliability organizations ‑ assume failure in operations to maximize de-risking attention
  - Render costs of system failure more predictable
    - Liquidated damages
  - [Other?]
- References

216. Are Elements Of The System Amenable To Commodification In Markets For Scale?

- Challenges
  - Various elements of information networks can be most effectively de-risked at large scales
    - Network effects such as “neighborhood watch” can sometimes de-risk systems in ways that parties cannot achieve unilaterally or at smaller scales
  - For new technologies, it is frequently difficult to predict the scope and degree of future adoption
    - As adoption grows, it is often difficult to make changes to the system that are “backwardly compatible” with earlier versions.
  - What aspects of the socio-technical system (and its individual elements) could present challenges to scaling up?
  - [Other?]
- References

216. Are Elements Of The System Amenable To Commodification In Markets For Scale?

- Candidate Analytical Frameworks/Metrics/Actions
  - Interjurisdictional challenges to scaling
    - Design to operate under a particular legal regime
    - Example – GDPR compliance
  - Operational challenges to scaling
    - Are their operational “bottlenecks” that would impede scaling
  - [Other?]
- References

217. – Constitutional Issues - Generally

- Challenges
  - Constitutional level harms: Among the potential harms that could be caused by the adoption of the technology, are there harms that would attract constitutional scrutiny?
  - Updated Constitutional rights?: Are there potential interpretations (or extensions?) of the bill of rights (however speculative) that might be appropriately entertained to update bill of rights protections for the new technical harms that were unimagined at the time of their original drafting?
  - What mitigations of potential constitutional harms are needed when the government adopts the system of technology?
  - Does the constitutional limitations apply only to government adoptions?
    - Government contractors
    - State governments
    - Private parties
  - What is the nature of the particular constitutional limitation?
- References
  - Book “The Constitution of Risk” (Constitutions generally are contextual government risk mitigation instruments)

217. US Constitution issues - Generally

- Candidate Analytical Frameworks/Metrics/Actions
  - Analyze constitutional issues from both strict constructionist perspective (text says x) AND from a historical risk mitigation perspective.
    - Historical perspective: what was risk that was meant to be prevented, and what is adjustment that is needed to address such risk in later historical context
  - Examine the scope of application of a constitutional provision to see if applicable to parties other than the federal government
  - For each constitutional provision, review case law and other interpretations of constitutional provision to understand potential strategies for mitigation of constitutional harms.
  - [Other?]
- References
  - See book "The Constitution of Risk" in bibliography (for perspectives on constitutions as internal risk balancing narratives – rules for engagement)

218. US Constitution – 1st Amendment – Rights of Religion, Speech, Press, Assembly & Petition

- Challenges
  - Does the adoption and implementation by government of the subject technology system potentially undermine 1st amendment rights?
    - Federal
    - State – Federal 1st amendment guarantees apply to states through 14th amendment ("incorporation doctrine and privileges and immunities clause).
  - Does the adoption and deployment of the information technology system by a US government entity (or government contractor) have the potential to violate US constitutional 1st amendment rights?
  - If the use of the IT system does NOT violate such US Constitutional rights, does it have the potential to cause harms that are similar to those addressed in the constitution?
  - Does the technology result. In the intrusion on the input or output information channel of an individual or organization that impedes their:
    - Input: access to information (freedom of the press)
    - Output: expression of information (freedom of speech)
  - [Other?]
- References
  - Text: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

218. US Constitution – 1st Amendment – Rights of Religion, Speech, Press, Assembly & Petition

- Candidate Analytical Frameworks/Metrics/Actions
  - Review cases and laws under first amendment and how they might apply to new technology system
  - Consider the importance of the first amendment for privacy and identity issues
    - Integrity of “Input” and “output” channels as ultimate source of harms labelled
      - Privacy
      - Security
      - Liability
  - How might individual information and organizational rights be constructed from operation of first amendment with other amendments, such as:
    - 4th Amendment
    - 5th & 14th Amendment
  - Note that US states are bound to US Constitution 1st amendment under the ”Incorporation Doctrine” of the 14th amendment.
  - [Other?]
- References

219. US Constitution – 2st Amendment - Right to Bear Arms

- Challenges
  - Does the adoption and implementation by government of the subject technology system potentially undermine 2nd amendment rights?
    - Federal
    - State – See, Dist. Of Columbia v. Heller in references
  - As control systems in society shift from physical to informational emphasis, does the definition of "arms" need to be revisited and reconsidered to accomplish the original goals of the Second Amendment?
  - The text of of the Second Amendment remains controversial regarding the question of the individual citizens right to bear arms extends beyond the duties as part of government sanctioned militia.
    - If citizens are prevented from possessing certain information capacities that are potentially weaponizable, does the second amendment potentially support citizen access to these functions?
  - [Other?]
- References
  - Text: A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.
  - District of Columbia v. Heller (S. Ct. 2008)(Local, state and federal governments have rights to regulate arms in some instances)

219. US Constitution – 2st Amendment – Right to Bear Arms

- Candidate Analytical Frameworks/Metrics/Actions
  - The scope of the meaning of "arms" has been relevant in the debates relating to the nature of weapons possessed by individuals
    - Automatic weapons
  - Research is needed into question of whether possession of other forms of weapons (biological, nuclear, non-ballistic, etc.) by citizens have been tested under the Second Amendment.
  - Query whether weaponization of information systems might in some future cases be considered "arms" that invite analysis under the Second Amendment.
  - Query whether future forms of encryption and quantum based computing systems might offer such superior capacities to their operators as to be considered "weapons" or arms that would invite consideration of treatment under the second amendment.
    - Second amendment relates to issue of sovereign as having the "monopoly of legitimated violence" in society
    - Consider issues of encryption "back doors," encryption export, etc. in weapons context
    - Consider "weaponized" information issues and regulatory questions relating to private ownership of zero-day exploits
  - [Other?]
- References

220. US Constitution – 3rd Amendment – Quartering Soldiers

- Challenges
  - Does the adoption and implementation by government of the subject technology system potentially undermine 3rd amendment rights?
    - Federal
    - State –
  - 3rd Amendment was passed in response to the attempts to forced Americans to provide lodging for British troops
  - The amendment does allow government to use private homes for lodging "its" soldiers in times of war
  - As conflict has become digitized, and kinetic elements controlled through telepresence, soldiers may be remote from effect.
    - E.g., in "occupied infrastructure"
    - E.g., in "occupied Internet"
    - E.g., in bot nets and other "zombie computers"
  - Where citizen and private company computers and/or infrastructure are involved in national security attack, what is the status of sending in digitized agents of military to do battle with foreign attacker on the computers and accounts of private citizens and entities.
    - Is 3rd amendment invoked?
    - Is Posse Comitatis invoked?
  - The 3rd Amendment, along with the 4th, 5th and 9th have been interpreted as giving rise to a "Right to Privacy"
    - How might the changing face of conflict in the information age (and the movement of the "theaters" of war online) affect the interpretation of the 3rd amendment, and of privacy rights generally
  - [Other?]
- References
  - Text: No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

220. US Constitution – 3rd Amendment – Quartering Soldiers

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the relevance of the third amendment in two separate analyses:
    - First, the literal proscription on quartering of soldiers
      - Is that extendable to other non-US government intrusions?
        - » What about a foreign computer virus or data placed on a citizens computer at the behest of the US government?
    - Second, the interpretation of the 3rd amendment as offering support for a general right to privacy
      - The implied right to "privacy" in the US Constitution has been interpreted to be based on the 3rd, 4th, 5th and 9th amendments
  - Under case law and other interpretations in the privacy line of authority, consider the nature of the harms described in each of the amendments and the respective duties that are applied to eliminate those harms
    - Consider how such existing descriptions of the harms and duties might be updated or modified to address updated privacy harms
  - [Other?]
- References

221. US Constitution – 4th Amendment – Search and Seizure

- Challenges
  - Does the adoption and implementation by government of the subject technology system potentially undermine 4th amendment rights?
    - Federal
    - State – Under the incorporation doctrine, police at all levels of government must have probable cause before stopping or searching someone suspected of a crime.
  - Does the operation of the technology by government entities potentially violate the limitations of the 4th amendment
    - How do the recognized exceptions to the 4th amendment affect the analysis
      - Plain view
      - Administrative Search
      - Borders
  - What is the line between collection of evidence of a crime and general surveillance of citizens?
    - How do concepts of "probable cause" and "search" apply in the massively networked information system of the Internet?
  - Question of scope of data collected for evidentiary use
    - Carpenter case – Warrant applies to cell phone pole information.
  - New forms of searches
    - e.g., all google account holders near crime scene to narrow suspects number
  - ECPA (Electronic Communications Privacy Act) unclarity
    - Increasingly unclear what is an ECS, or RCS, under statute.
    - If not have core business in electronic communications, are you covered by ECPA?
      - e.g., Airbnb as platform that makes it an ECS for that purpose.
      - Courts are looking at services, not whole companies.
        - » Cruise ship that provides Wi-Fi is ECS.
        - » Tricky areas of statutory and constitutions application.
        - » Different procedures, rules, rights, duties, etc.
  - Concerns with using 4th amendment as basis for general privacy right
    - 4th amendment is evidentiary proscription associated with criminal procedure.
    - Is it appropriate starting point for citizen general privacy rights?
  - [Other?]
- References
  - Text: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

221. US Constitution – 4th Amendment – Search and Seizure

- Candidate Analytical Frameworks/Metrics/Actions
  - 4th Amendment may be inadequate framework for citizen "privacy" rights when testing new technologies
    - 4th Amendment is an evidentiary proscription
    - Result of government violations of the 4th amendment is limited to suppression of evidence seized in violation of the provisions
    - No other recovery by citizens is prescribed by the 4th amendment
      - Consider limitations of statutory recovery
      - Consider issues of sovereign immunity from damages
  - 4th amendment provides protection to citizens in the context of a criminal case.
    - Caution against relying on 4th Amendment alone for citizen "privacy" since it has the effect of "criminalizing" the population
      - 4th amendment in effect is a minimum "floor" on citizen rights, rather than an aspiration for citizen freedoms
      - Consider 1st amendment as potential support for privacy
        - » See "identity" and "Privacy" as forms of communication integrity (of input and output channels) and therefore more potentially aspirational
  - [Other?]
- References

222. US Constitution – 5th Amendment – Grand Jury, Due Process, Self-Incrimination, 2x Jeopardy

- Challenges
  - Does the adoption and implementation by government of the subject technology system potentially undermine 5th amendment rights?
    - Federal
    - State – Not all states require grand juries
  - How might the technology affect the citizen's right against self incrimination?
    - Does the technology store data in ways that might undermine this right?
  - How might the technology undermine the rights and procedures associated with "due process?"
    - Does operation of the technology function to undermine the rights of notice, hearing and tribunal?
  - Since "data" is not generally recognized as "property," how might its "taking" be compensated for – other than through operation of the 5th amendment?
  - [Other?]
- References
  - Text: No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

222. US Constitution – 5th Amendment – Grand Jury, Due Process, Self-Incrimination, 2x Jeopardy

- Candidate Analytical Frameworks/Metrics/Actions
  - Self-incrimination
    - Put in place safeguards against the unauthorized access by government to citizen data
  - Consider relationship of “double jeopardy” to the EU GDPR (General Data Protection Regulation) “right to be forgotten.”
  - Structure data pooling arrangements with governments in ways the limit access to citizen data
  - [Other?]
- References

223 US Constitution – 6th Amendment – Rights of Accused, Jury Trial, Confront Witnesses, Counsel

- Challenges
  - Does the adoption and implementation by government of the subject technology system potentially undermine 6th amendment rights?
    - Federal
    - State – Generally applies to states through the Incorporation Doctrine (14th amendment)
  - The 6th amendment is the basis for US criminal procedure
  - How might the technology affect information systems associated with the criminal processes that are intended to preserve rights of accused?
  - In an interconnected world of high speed news, is it possible to identify an impartial jury?
  - In trials involving highly technical systems and materials, such as the technology, is it possible to maintain the availability of competent counsel?
  - [Other?]
- References
  - Text: In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

223 US Constitution – 6th Amendment – Rights of Accused, Jury Trial, Confront Witnesses, Counsel

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the ways in which the effects of the technology on public attitudes might be tested to ascertain whether a jury is impartial?
    - Fake news and viral misinformation
    - Social network research on voting and public attitudes
  - Create jury instructions guidance for judges to assure that "facts of case" presented in courtroom are basis for decisions
  - Where the technology is implemented as part of system involved in processing criminal defendants, what measures are needed to assure conformity to constitutional requirements?
  - Create training modules for Attorney CLE that help to raise awareness of effects of technology on criminal procedure issues
    - Also, consider ethical rules for attorneys relating to competent counsel
  - [Other?]
- References

224. US Constitution – 7th Amendment – Jury Trial

- Challenges
  - Does the adoption and implementation by government of the subject technology system potentially undermine 7th amendment rights?
    - Federal
    - State – Incorporation Doctrine of the 14th Amendment has NOT been applied to the 7th amendment, and so civil suits tried in state and local courts can follow procedures that differ from those developed under the 7th amendment.
  - The 7th Amendment extend some of the protections of the 6th amendment to civil cases
    - Criminal cases are brought by the state
    - Civil cases are brought by one citizen against another
  - How does the technology affect the processes and procedures of civil law such as:
    - Discovery – How is information captured, stored and retrieved in the system?
  - [Other?]
- References
  - Text: In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.

224. US Constitution – 7th Amendment – Jury Trial

- Candidate Analytical Frameworks/Metrics/Actions
  - How is data (including metadata) captured, stored and retrieved in the technology system?
    - In companies, sectors, jurisdictions and other contexts where litigation is prevalent, consider how the technology can serve user needs in the context of litigation from both defendants and plaintiff's perspectives
  - Research authorities relating to "discovery" to identify the ways in which the technology may aid or hinder litigation processes for users and clients
    - Consider promotion of helpful features in litigation contexts.
  - [Other?]
- References

225. US Constitution – 8th Amendment – Excessive Bail, Cruel & Unusual Punishment

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 8th amendment protections?
    - Federal
    - State
  - The 8th amendment requires proportionality of punishment and crime.
    - How can the shifting sources of sovereignty affect the protections that were sought to be crafted in the 8th amendment.
  - Speculative: How does the technology system avoid imposing "cruel and unusual punishment" on its users as part of its normal enforcement of terms
  - Since online space is largely commercial space, as an increasing portion of social, economic and political interactions migrate to that space, should they be tested by the standards of governments, such as in the US constitution?
    - There is a governance gap, without obvious candidates for filling it
  - If "social networks," "search engines," and other online commercial information service offerings are understood to be critical infrastructure for maintaining modern society (and a citizen's ability to navigate that society), is the experience of being kicked off such an online platform equivalent of imposition of "cruel and unusual punishment?"
    - Banishment, excommunication, interdict from the interaction realm maintained by a "computational sovereign"
  - [Other?]
- References
  - Text: Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.

225. US Constitution – 8th Amendment – Excessive Bail, Cruel & Unusual Punishment

- Candidate Analytical Frameworks/Metrics/Actions
  - The provisions of the 8th amendment are not enforceable against commercial companies, including those that organize and operate large third party networks of social networks, search engines, online apps, etc.
  - As online information based services become increasingly depended upon by people and institutions, it is clear that their commercial foundation is limiting their mission
    - Consider new community-aware SRO (self-regulatory organization) forms.
      - Organized around communities of interest aligned around shared risks
  - How might death penalty jurisprudence with regard to the "cruel and unusual prohibition (which at present in the US permits federal and states to apply the death penalty in their discretion, help inform questions of "cruel and unusual" punishment in information systems that are deemed to be critical infrastructure.
  - [Other?]
- References

226. US Constitution – 9th Amendment – Non-Enumerated Rights

- Challenges
  - The bill of rights exists because the framers were worried that a protracted discussion of rights might delay implementation of the constitution.
    - When the bill or rights was enacted buy the first congress, there was concern that a listing of rights might be perceived as being exclusive under the legal doctrine ”Espressio Unias Est Exclusio Alterius” (Roughly “The expression of one is the exclusion of the other”).
    - The 9th amendment is intended to clarify that the rights described in the bill of rights are not all of the rights to which people might be entitled
  - Does the adoption and implementation by government of the subject technology system potentially undermine 9th amendment rights?
    - Federal
    - State
  - [Other?]
- References
  - Text: The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

226. US Constitution – 9th Amendment – Non-Enumerated Rights

- Candidate Analytical Frameworks/Metrics/Actions
  - Over the years, US courts have formulated several ”unenumerated” rights:
    - Right to vote
    - Right of free movement
    - The right to privacy
  - How might the history and current configuration of judicially developed “non-enumerated” rights (such as those listed above) inform the development and implementation of future “unenumerated rights” to help protect citizens in the era of networked information systems?
  - Does the notion of rights “retained by the people” invite consideration of the “negative” space not covered by the constitution for new de-risking structures built through new organizations and configurations of “the people?”
  - The right to “contract” enables the right to reach out and form formal de-risking and leverage structures with people and organizations in other countries, etc. [Other?]
- References

227. US Constitution - 10th Amendment – Rights Reserved To States

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 10th amendment protections?
    - Federal
    - State
  - The 10th amendment was intended to address fears that the federal government had too much power relative to the states
    - Would the adoption and operation of the technology by the federal government have the potential to shift the balance of insight and power toward the federal government in a way that is adverse to the power of the states?
  - Consider powers reserved to the states individually:
    - Police Power
      - Insurance regulation
      - Liquor regulation
      - Data breach legislation
      - Education systems
    - Taxation power
    - Eminent domain

- Consider pre-emption and dormant commerce clause effects on power allocations.

  - [Other?]
- References
  - Text: The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

227. US Constitution - 10th Amendment – Rights Reserved To States

- Candidate Analytical Frameworks/Metrics/Actions
  - Analyze relationship of federal and state governments WITH RESPECT TO stakeholders in information networks
  - Be aware of the traditional allocation of powers
    - Police power is lodged in states
      - Provides basis for "remote" applications of data breach and data security laws that affect residents of the respective states.
      - How might states continue to be laboratory of solutions for information risk solutions based on its police power responsibilities
  - Corporate law is state based
    - How might corporate law reform affect information risks experienced by information network stakeholders
  - [Other?]
- References

228. US Constitution – 12th Amendment – Election of President and Vice President

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 12th amendment protections?
    - Federal – The party system that arose during the Jefferson/Burr election of 1800 challenged the method of presidential elections.
    - State
  - Does the technology system affect the manner in which presidential elections are conducted as interpreted under the 12th Amendment?
    - Where the technology is applied in voting contexts (directly or indirectly) are the information flows auditable to permit confirmation of conformity to the 12th amendment.
  - [Other?]
- References
- Text: The Electors shall meet in their respective states and vote by ballot for President and Vice-President, one of whom, at least, shall not be an inhabitant of the same state with themselves; they shall name in their ballots the person voted for as President, and in distinct ballots the person voted for as Vice-President, and they shall make distinct lists of all persons voted for as President, and of all persons voted for as Vice-President, and of the number of votes for each, which lists they shall sign and certify, and transmit sealed to the seat of the government of the United States, directed to the President of the Senate; -- the President of the Senate shall, in the presence of the Senate and House of Representatives, open all the certificates and the votes shall then be counted; -- The person having the greatest number of votes for President, shall be the President, if such number be a majority of the whole number of Electors appointed; and if no person have such majority, then from the persons having the highest numbers not exceeding three on the list of those voted for as President, the House of Representatives shall choose immediately, by ballot, the President. But in choosing the President, the votes shall be taken by states, the representation from each state having one vote; a quorum for this purpose shall consist of a member or members from two-thirds of the states, and a majority of all the states shall be necessary to a choice. [And if the House of Representatives shall not choose a President whenever the right of choice shall devolve upon them, before the fourth day of March next following, then the Vice-President shall act as President, as in case of the death or other constitutional disability of the President. --]* The person having the greatest number of votes as Vice-President, shall be the Vice-President, if such number be a majority of the whole number of Electors appointed, and if no person have a majority, then from the two highest numbers on the list, the Senate shall choose the Vice-President; a quorum for the purpose shall consist of two-thirds of the whole number of Senators, and a majority of the whole number shall be necessary to a choice. But no person constitutionally ineligible to the office of President shall be eligible to that of Vice-President of the United States.

228. US Constitution – 12th Amendment – Election of President and Vice President

- Candidate Analytical Frameworks/Metrics/Actions
  - Confidence in the election systems and processes is fundamental to the maintenance of the social contract through which parties bind themselves to rules of behavior that serve to de-risk and leverage group interactions.
  - The information flows at each step of the electoral college process should be isolated and evaluated to check their integrity against emerging information risk parameters
    - Atlas of risks lists potential integrity challenges at nodes and edges.
  - [Other?]
- References

229. US Constitution – 13th Amendment – Abolition of Slavery & Involuntary Servitude

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 13th amendment protections?
    - Federal
    - State
  - Do Slavery practices, that functioned to treat slaves as property, ignoring the various human rights of the enslaved party echo in current commercial online practices that treat data about people as owned by companies (via the accumulation of various "rights equivalent to ownership").
    - Slavery represents the appropriation/enclosure of individual "self" and the treatment of people as inventory without attention to their needs
      - compare involuntary servitude to misappropriation of valuable data.
      - Misappropriation is a long standing recognized privacy tort
        - » The use of name or likeness for economic purposes without compensation
        - »
  - Is "servitude" in the form of economic, informational, data or other dis-empowerment arise to a form of "slavery" or "involuntary servitude" sufficient to invite constitutional scrutiny.
  - [Other?]
- References
  - Text:
    - Section 1.
      Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction.
    - Section 2.
      Congress shall have power to enforce this article by appropriate legislation.

229. – US Constitution - 13th Amendment – Abolition of Slavery & Involuntary Servitude

- Candidate Analytical Frameworks/Metrics/Actions
  - Research scope of application of terms “slavery” and “involuntary servitude” to ascertain the extent to which they have been applied to the private “ownership” of individual rights beyond traditional slavery.
  - Consider aspects of the tort of “misappropriation” when applied to modern Terms of Service (Terms of Use).
    - Based on banking model/Network TV model, but more intimate information infrastructure.
    - Functional “ownership” of data and insight by companies precludes exercise of certain individual rights by humans
    - If and to the extent that online service provider TOU/TOS are deemed “unconscionable” they are not enforceable contracts, and therefore don’t convert tort analysis to contract analysis.
      - Note that, despite frequent reference to TOUs as “adhesion” contracts, it seems that “Unconscionability “is a more appropriate description of their failings.
      - Constitutional rights cannot be contracted away, so finding of involuntary servitude on social networks would not be defeated by the contract argument.
  - [Other?]
- References

230. US Constitution -14th Amendment – Privileges & Immunities, Due Process, Equal Protection

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 14th amendment protections?
    - Federal – 14th amendment is the basis for applying the principles of the Declaration of Independence (e.g., life, liberty, property) to constitutional law
    - State – 14th amendment is source of authority through which the Supreme Court held that federal constitutional guarantees apply to the residents of the various states.
  - Is "data" or "information" property (for 14th amendment purposes) such that its access constitutes a "taking" for 14th Amendment purposes?
    - If sol then does government access to private or commercial proprietary insights through operation of the system giver rise to a claim of eminent domain and corresponding compensation claims?
  - Do government applications of the technology have the potential to violate equal protection guarantees?
  - Section 2 of the 14th Amendment relates to voting rights of citizens
    - Will the application of the technology undermine the operation and protections of the 14th amendment voting provisions?
  - see also 5th amendment – process and fairness prongs
  - [Other?]
- References
  - Text:
    - Section 1.
      All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.
    - Section 2.
      Representatives shall be apportioned among the several States according to their respective numbers, counting the whole number of persons in each State, excluding Indians not taxed. But when the right to vote at any election for the choice of electors for President and Vice-President of the United States, Representatives in Congress, the Executive and Judicial officers of a State, or the members of the Legislature thereof, is denied to any of the male inhabitants of such State, being twenty-one years of age,* and citizens of the United States, or in any way abridged, except for participation in rebellion, or other crime, the basis of representation therein shall be reduced in the proportion which the number of such male citizens shall bear to the whole number of male citizens twenty-one years of age in such State.
    - Section 3.
      No person shall be a Senator or Representative in Congress, or elector of President and Vice-President, or hold any office, civil or military, under the United States, or under any State, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any State legislature, or as an executive or judicial officer of any State, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof. But Congress may by a vote of two-thirds of each House, remove such disability.
    - Section 4.
      The validity of the public debt of the United States, authorized by law, including debts incurred for payment of pensions and bounties for services in suppressing insurrection or rebellion, shall not be questioned. But neither the United States nor any State shall assume or pay any debt or obligation incurred in aid of insurrection or rebellion against the United States, or any claim for the loss or emancipation of any slave; but all such debts, obligations and claims shall be held illegal and void.
    - Section 5.
      The Congress shall have the power to enforce, by appropriate legislation, the provisions of this article.

230. US Constitution -14th Amendment – Privileges & Immunities, Due Process, Equal Protection

- Candidate Analytical Frameworks/Metrics/Actions
  - The 14th amendment punished states that deprived newly freed slaves of the right to vote by reducing their representation in the House of Representatives.
  - Section 1 of the 14th amendment has provided the foundation for various legal doctrines, each of which should be separately tested against the deployment of the technology by governments (federal and state)
    - Privileges and Immunities
    - Equal Protection
    - Due Process (with 5th amendment)
  - Section 2 of the 14th Amendment provides various voting protections.
    - The operation of the technology system should be tested to confirm that it will not undermine the protections of the 14th amendment through "virtual Gerrymandering," unintended dis-enfranchisement, etc.
  - [Other?]
- References

231. US Constitution – 15th Amendment – Voting Rights

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 15th amendment protections?
    - Federal
    - State
  - While the 15th amendment prohibits the limitation of voting by reasons of race, are those protections preserved or undermined as voting (and voting related processes) move online
    - Does the "digital divide" have the effect of dis-enfranchising minority populations based on race?
    - Compare the variety of ways that states of the former confederacy limited rights of African Americans to vote (prior to the Voting Rights Act of 1965)
      - Poll Taxes
      - Literacy Tests
    - Note that biases that are reflected in "historical" training data for AI become foundational to future AI decision making (See Science magazine in "references").
  - [Other?]
- References
  - Text:
    - Section 1.
      The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude--
    - Section 2.
      The Congress shall have the power to enforce this article by appropriate legislation
  - Science Magazine (10/25/190, p. 421 "Assessing Risk automating racism (A health care algorithm reflects underlying racial bias in society)"

231. US Constitution – 15th Amendment – Voting Rights

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider "disparate impact" of application of technology system to voting-related systems
    - Does system result in dis-enfranchisement of individuals due to its complexity? Its cost?
    - Is the system UI designed, developed and deployed to accommodate the variety of citizen capabilities and capacities and access to online resources to vote.
    - Are alternative methods for voting offered?
    - Can the training data for any algorithms applied by the system be reviewed or audited for evidence of unintended biases?
  - [Other?]
- References

232. US Constitution – 16th Amendment – Federal Income Tax

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 16th amendment protections?
    - Federal - - Does the technology permit the relocation of economic activity in a way that affects the "nexus" analysis for taxation purposes?
    - State
  - Income taxes are typically imposed on net income from various identified economic activities
    - As the value propositions associated with online information networks evolve, Is the tax base appropriate for enterprises that apply the technology?
    - How can "nexus'" for activity (such as tele-present surgery, etc.) be appropriately determined?
    - How can double taxation be avoided with new sourcing rules?
      - Consider standard terms of OECD model income tax treaty
    - Be aware of distinguishing the base and processes for income tax from that of other taxes
      - VAT/Sales Tax
      - Property Tax
      - Other
  - [Other?]
- References
  - Text: The Congress shall have power to lay and collect taxes on incomes, from whatever source derived, without apportionment among the several States, and without regard to any census or enumeration.

232. US Constitution – 16th Amendment – Federal Income Tax

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the traditional bases for finding ”nexus” and “taxing jurisdiction” for income tax purposes and how the adoption and operation of the technology will affect the imposition of tax
    - Ownership of property
    - Performance of services (dependent services and independent services)
    - Receipt of dividends, interest, royalties
    - Other activities
  - Consider new use cases enabled by the system under review that can potentially shift nexus and tax base variables.
    - Coin-based investment (services or dividends received)
    - Distributed enterprises
      - Where does income generating activity of eBay, Airbnb, UBER take place?
  - Do decisions made about deployment of the system affect the tax treatment of the system in operation?
    - Server location
    - Support location
    - Data location
  - [Other?]
- References

233. US Constitution – 19th Amendment – Women's Right to Vote

- Challenges
  - Does the adoption or operation of the technology by government in the context of voting systems potentially undermine 19th amendment protections?
    - Federal
    - State
  - Is the technology and its UI suitable for application in voting contexts
    - Will the technology have disparate impact of individuals based on gender?
  - Is the relative dearth of female participation in technology design, deployment, development and implementation a potential source of disparate impact where such technologies are applied in voting contexts?
  - Did the training data that was used to develop the algorithmic, machine learning, and/or AI components of the system introduce biases in the system that have a disparate impact on female participation in voting?
  - [Other?]
- References
  - Text:
    - The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of sex.
    - Congress shall have power to enforce this article by appropriate legislation.

233. US Constitution – 19th Amendment – Women's Right to Vote

- Candidate Analytical Frameworks/Metrics/Actions
  - Although voting is only a single use case for information networks, its importance as a type of interaction raises the stakes of assuring equal access for all persons.
  - Be aware that critiques of differential benefits and effects of technology based on gender differences can take on constitutional dimensions when the technology is employed in voting contexts
  - Be aware of the different platforms that are used by different genders
  - Be aware of the different ways that genders use technology
  - Does the design and/or operation of the technology make an assumption about binary gender identification that could be inconsistent with user/operator realities?
    - Are UIs, use cases, operating instructions, etc. attentive to issues that might arise?
  - [Other?]
- References

234. US Constitution – 24th Amendment – Abolition of Poll Tax in Federal Elections

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 24th amendment protections?
    - Federal
    - State – Supreme Court ruled that equal protection clause (14th amendment) applied the 24th amendment to the states.
  - The 24th amendment was intended to end the practice of states to impose poll taxes to prevent poor populations from voting
  - As the processes of voting migrate to technical devices (such as mobile devices), does this create an economic barrier to voting by poor people who might not have the technology or resources?
    - Will alternative voting methods (such as the use of paper ballots at centralized polling places) be as readily available as voting through the technology system?
    - [Other?]
- References
- Text:
  - Section 1.
    The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States or any State by reason of failure to pay poll tax or other tax.
  - Section 2.
    The Congress shall have power to enforce this article by appropriate legislation.

234. US Constitution – 24th Amendment – Abolition of Poll Tax in Federal Elections

- Candidate Analytical Frameworks/Metrics/Actions
  - While poll taxes reflect specific state action to create unfavorable economics with the intention to dis-enfranchise poor populations, the exclusions of the poor from voting processes can also take other forms of economic prerequisites
  - If and to the extent that the technology system is applied in the context of voting, will access to the technology be limited such that it has the effect of making voting less available to poor populations
    - E.g., voting app that can only be used on expensive smart phone
  - [Other?]
- References

235. US Constitution – 26th Amendment – Right to Vote at Age 18

- Challenges
  - Does the adoption or operation of the technology by government potentially undermine 26th amendment protections?
    - Federal
    - State
  - The 26th amendment is typically viewed as applicable to voting by younger people
    - Can the 26th amendment support the argument that voting not be not denied on account of older age
    - Are systems used for voting and their User Interfaces confusing for older and elderly citizens?
    - [Other?]
- References
  - Text: Section 1.
    The right of citizens of the United States, who are eighteen years of age or older, to vote shall not be denied or abridged by the United States or by any State on account of age.
  - Section 2.
    The Congress shall have power to enforce this article by appropriate legislation.

235. US Constitution – 26th Amendment – Right to Vote at Age 18

- Candidate Analytical Frameworks/Metrics/Actions
  - Where the technical system is to be deployed directly or indirectly with respect to voting systems, user interfaces (UIs) of the technical system should be subject to testing to confirm that they are equally useful and understandable to citizens of various ages.
  - [Other?]
- References

236. Sovereign Immunity

- Challenges
  - The concept of “sovereign immunity” shields government entities for liability associated with their pursuit of government activities
  - Does the deployment of the technology system involve the engagement in activities that would not be covered by concepts of sovereign immunity
    - What is the nature of the liability that might be experienced by a governmental user or operator of the technology?
  - Is deployment among federal government agencies replicable where other factors are absent (like SI)
  - Is the implementation of the technology system dependent upon the responsibility/liability of a role-player in the system, such that where. A government party pursuing government functions. (such that it can enjoy some form of sovereign immunity) is placed in that position it upsets the balance of responsibility necessary to make the system sustainable.
    - If the system depends on potential liability to prompt stakeholder action, is that present in a government implementation.
  - [Other?]
- References

236. Sovereign Immunity

- Candidate Analytical Frameworks/Metrics/Actions
  - Examine the performance expectations and dependencies of the system to identify potential liability dependencies
    - Include internal components of the system
    - Review external dependencies of the system
  - Where governmental agency with sovereign immunity from liability is present as a stakeholder in a particular system deployment, and is engaged in a role in the system where their performance is critical to the operation of the overall system, are there other ways to compensate for their immunity from liability that are still consistent with system operation?
    - Insurance
    - Guarantees
  - [Other?]
- References

237. Cloud (Contract) Dependency?

- Challenges
  - Users of cloud services are typically unable to negotiate their terms of service for using cloud services
    - The “fixed” nature of cloud contracts has the result that cloud service users must find different ways to address any risks to which they are exposed under such contracts
  - If the terms of service of the cloud. Services provider are altered or modified unilaterally by the cloud service provider, the cloud. Service customer might not be able to achieve corresponding and compensating adjustments in their other customer and supplier agreements to address or absorb any new risks caused by such change.
  - [Other?]
- References

237. Cloud (Contract) Dependency

- Candidate Analytical Frameworks/Metrics/Actions
  - Cloud customers should be particularly attentive to reducing their risks to unilateral cloud contract modification
    - Include modification and termination provisions that reference changes to required cloud arrangements as trigger events
    - Consider provisions that facilitate change in cloud provider if needed to address new liabilities
      - Data portability
      - Assistance in transition
  - Cloud customers should assure that availability and consistency of service and service terms match their needs and that future changes to cloud terms are bounded by safeguards
    - Prior notice of change
    - Backward compatibility of future service?
  - [Other?]
- References

238. Non-Domestic Content

- Challenges
  - Where systems are dependent directly or indirectly on non–domestic (aka “imported”) content, subsystems, or components, additional potential system integrity risk issues (and corresponding interruptions in service) are introduced associated with that cross-border dependency
    - Potential interruptions from import controls imposed in user’s country
    - Potential interruptions from export controls imposed in producer’s country
    - Potential interruptions from boycotts, cartel policies, embargoes, etc. engaged in by mixes of public and private parties
  - [Other?]
- References
  - Issues with Huawei asserted by US government
  - Issues with US social network content asserted by Chinese government

238. Non-Domestic Content

- Candidate Analytical Frameworks/Metrics/Actions
  - All socio-technical systems are dependent on other socio-technical systems for operation within expected performance parameters
  - Providers and buyers of sociotechnical systems (Including sociotechnical information systems) should ”map out” the domestic and international components of both the supply chain and the customer/user base that is anticipated to host a given system
    - Any system interactions that cross a geo-political “border” should be closely examined to identify the potential for risk associated with that border
    - Borders are unique because they involve sovereigns, which are entities that can Unilaterally create duties for other parties without their permission or forgiveness
    - Sovereigns are “present” (behind the scenes) in EVERY human interaction
      - Where multiple sovereigns are involved (as in a cross border agreement and supply chain), there may be no pathways for appeal or recourse for other stakeholders that are negatively affected by sovereign decisions and actions
      - “When elephants fight, it is the grass that gets crushed”
  - A helpful strategy for solutions in cross border interactions is to create a “third space” in between the sovereigns that can be organized in a manner that is not adequately informed by either sovereign’s practices/policies/norms
    - De-risk. New threats and vulnerabilities in the “third space” in ways that none of the parties, including the sovereigns themselves, can achieve unilaterally
    - Self-regulatory entities and structures
    - Third party monitoring
  - [Other?]
- References

239. Risk Under Other Risk Frameworks - Generally

- Challenges
  - Is there risk of failure or default under another applicable risk framework?
  - When technical systems are deployed and operated in contexts in which other systems also operate, there can be clashes between the systems
    - The operation of one system intended to reduce system risk may cause threats or affect vulnerabilities of other related or contiguous systems
  - Sub-systems of the same larger system might operate with inadequate coordination, causing undue interaction friction and cost
  - Risk frameworks take many forms, and are embedded and foundational to every socio-technical system upon which humans currently rely
    - How can a single entity (Human or institutional) hope to address the myriad complexity of other risk frameworks, embedded in systems that they rely upon?
  - How resolved?
  - [Other?]
- References

239. Risk Under Other Risk Frameworks - Generally

- Candidate Analytical Frameworks/Metrics/Actions
  - Current institutional, normative, legal and other social structures reflect a functionally ”balanced” (homeostatic) state among historical power structures
    - Historical structures optimized for entities that had power in those earlier contexts
      - Historical structures might not all be fit-for-function in new interaction environments in which they are depended upon to act
      - “Risk frameworks” expressed in policy, technology deployments, of archaic institutions might produce levels of “risk exhaust” that is excessive in relation to the benefit of those organizations
    - Consider applying co-management structures to address the “risk commons” that arise when mitigation of a risk in a system creates risk in another system(s)
  - Map the duties/rights, or benefits/burdens dyads to address balancing multiple simultaneous threats
    - Consider whether the mitigation of risk is limited by the 4 color problem in cartography
      - Is there a mathematical limitation on the number of different solutions (colors in the original problem) that can be applied to systems in contact with one another?
  - [Other?]
- References

240. What Are *Commercial* Concerns With Widespread Adoption By *Government* Entities?

- Challenges
  - Governments can create environments that favor one technology system over another in several ways:
    - Government legislation and regulation can create environments that are more conducive to a given technology/policy
    - Government use/purchase/adoption of a given technology/policy. Can. Push entities that. Deal. With. Government to adopt compatible solutions. (aka. Government "power of the purse")
    - Government adoption of a given socio-technical information system can give rise to a form of "de-facto" standardization relating to the technology and policy that are foundational to the adopted system
  - Such de-facto standardization may have far ranging implications that were not considered or analyzed in the design/development/deployment of the system
    - Governments have different operational needs than private entities (individuals and organizations)
    - De-facto standard created by government adoption may be harmful to other stakeholders
      - More costly
      - Riskier
  - Consider notion of government "mandate" implicit in adoption as akin to Kant's "categorical imperative"
    - Just because individuals (or a single actor" acts rationally, it doesn't mean that society will act rationally in gross or that the decision will not harm other stakeholders
  - [Other?]
- References

240. What Are *Commercial* Concerns With Widespread Adoption By *Government* Entities?

- Candidate Analytical Frameworks/Metrics/Actions
  - Help government to understand issues and implications of proposed rules
    - This requires coordination and common purpose across stakeholders to avoid dilution of multiple messages
    - Potentially harmful and aspects of government "de-facto" standards (established by legislation/regulation and/or "power of the purse") can be anticipated and mitigated by active normative engagement by non-governmental stakeholders
    - Standard setting
    - Industry and civil society organizations
  - Non-governmental entities can get out ahead of government entities
  - [Other?]
- References

241. What Are *Regulatory/Government* Concerns With Widespread Adoption By *Commercial* Entities?

- Challenges
  - If the technology system under review is widely adopted by commercial entities, could it lead to:
    - Antitrust concerns about system users P2P behaviors
    - Intrusions on traditionally governmental functions by commercial entities that are not subject to discipline in the polls.
      - Monetary controls
        - » Alternative currency systems
      - Police power/adjudication of disputes
      - Loss of public space
      - Other
  - [Other?]
- References

241. What Are *Regulatory/Government* Concerns With Widespread Adoption By *Commercial* Entities?

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

242. Risk Under Other Risk Frameworks - UN SDGs - Generally

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals": Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with the SDGs?
    - Coordination among multiple SDG "Verticals": Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG "Targets" and "Indicators" at
  - [Other?]
- References

242. Risk Under Other Risk Frameworks – UN SDGs - Generally

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

243. Risk under other risk frameworks - UN SDGs – SDG 1 - No Poverty

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment decisions to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 1?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 1 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg1

243. Risk under other risk frameworks - UN SDGs – SDG 1 – No Poverty

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

244. Risk under other risk frameworks - UN SDGs – SDG 2 – Zero Hunger

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 2?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 2 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg2

244. Risk under other risk frameworks - UN SDGs – SDG 2 – Zero Hunger

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

245. Risk under other risk frameworks - UN SDGs – SDG 3 – Good Health and Well Being

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 3?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 3 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg3
  - [Other?]

245. Risk under other risk frameworks - UN SDGs – SDG 3 – Good Health and Well Being

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

246. Risk under other risk frameworks - UN SDGs – SDG 4 – Quality Education

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 4?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 4 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg4
  - [Other?]
- References

246. Risk under other risk frameworks - UN SDGs – SDG 4 – Quality Education

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

247. Risk under other risk frameworks - UN SDGs – SDG 5 – Gender Equality

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 5?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 5 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg5
  - [Other?]
- References

247. Risk under other risk frameworks - UN SDGs – SDG 5 – Gender Equality

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

248. Risk under other risk frameworks - UN SDGs – SDG 6 - Clean Water and Sanitation

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 6?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 6 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg6
  - [Other?]
- References

248. Risk under other risk frameworks - UN SDGs – SDG 6 – Clean Water and Sanitation

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

249. Risk under other risk frameworks - UN SDGs – SDG 7 – Affordable and Clean Energy

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 7?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 7 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg7
  - [Other?]
- References

249. Risk under other risk frameworks - UN SDGs – SDG 7 – Affordable and Clean Energy

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

250. Risk under other risk frameworks - UN SDGs – SDG 8 – Decent Work and Economic Growth

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 8?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 8 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg8
  - [Other?]
- References

250. Risk under other risk frameworks - UN SDGs – SDG 8 – Decent Work and Economic Growth

- Candidate Analytical Frameworks/Metrics/Actions
  - Insert link (as normative cross reference) to existing “Targets” and “Indicators” based on work done regarding this SDG to date
    - Existing SDG metrics reflect cumulative synthesis of work done to date on this SDG
    - For purposes of information risk, these metrics offer de-risking benefits of “de-facto” standardization
      - Just as stoplight could be red or purple – it is the agreement that “red means stop” which de-risks the crossroads
      - So too can “agreement” of multiple stakeholders to consume and apply a shared metric “de-risk” (and leverage) many other sorts of interactions in which multiple stakeholders are involved
      - The benefits of de-risking can be available even if the stakeholders consume the same metric for different purposes
        - » E.g., patient temperature relevant to doctor, insurance carrier, patient, etc.
  - Identify existing performance metrics for SDG and compare horizontally across SDGs
    - For those metrics that are relevant in multiple SDGs, consider the stakeholders in those groups to be in the same “risk community,” and consider opportunities to strengthen links across SDG stakeholder communities to enhance resilience and sustainability of system solutions and to decrease inadvertent “entropy exhaust” from causing harm to related SDGs
  - [Other?]
- References

251. Risk under other risk frameworks - UN SDGs – SDG 9 – Industry Innovation and Infrastructure

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 9?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 9 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg9
  - [Other?]
- References

251. Risk under other risk frameworks - UN SDGs – SDG 9 – Industry, Innovation and Infrastructure

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

252. Risk under other risk frameworks - UN SDGs – SDG 10 – Reduced Inequalities

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 10?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 10 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg10
  - [Other?]
- References

252. Risk under other risk frameworks - UN SDGs – SDG 10 – Reduced Inequalities

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

253. Risk under other risk frameworks - UN SDGs – SDG 11 - Sustainable Cities and Communities

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 11?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 11 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg11
  - [Other?]
- References

253. Risk under other risk frameworks - UN SDGs – SDG 11 – Sustainable Cities and Communities

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

254. Risk under other risk frameworks - UN SDGs – SDG 12 – Responsible Consumption and Production

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 12?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 12 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg12
  - [Other?]
- References

254. Risk under other risk frameworks - UN SDGs – SDG 12 – Responsible Production and Consumption

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

255. Risk under other risk frameworks - UN SDGs – SDG 13 – Climate Action

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 13?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 13 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg13
  - [Other?]
- References

255. Risk under other risk frameworks - UN SDGs – SDG 13 – Climate Action

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

256. Risk under other risk frameworks - UN SDGs – SDG 14 - Life Below Water

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 14?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 14 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg14
  - Many ocean based resources require various sorts of management, based on multiple, simultaneous variables
    - Gradients of state power
    - Migration/senescence of resource
    -
  - [Other?]
- References

256. Risk under other risk frameworks - UN SDGs – SDG 14 – Life Below Water

- Candidate Analytical Frameworks/Metrics/Actions
  - To the extent that the framing of the information network challenges under review lend themselves to a “risk commons” analysis, the area of fisheries management offers a host of well developed use cases where previously-adverse parties developed a system of mutually-dependent incentives and penalties to create new and other-wise unavailable risk mitigation structures
    - The prerequisite to embracing these structures is to conceive of them as “risk commons” rather than ”asset” commons
      - It is not about the ”fish,” “water,” or “forest,” per se, but about the risk of the absence of the asset that provides the incentive for participation.
    - Once co-management/commons structures are understood to be risk rather than asset commons, the exercise of borrowing risk mitigation structures from those settings is more forthright and fruitful
  - [Other?]
- References

257. Risk under other risk frameworks - UN SDGs – SDG 15 – Life on Land

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with “reasonable duties of care,” and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG “Verticals:”
      - Does the technology system help to further and/or measure the “Targets” and “Indicators” associated with SDG 15?
    - Coordination among multiple SDG “Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against “Targets” and “Indicators” in multiple SDG “verticals” to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 15 ”Targets” and “Indicators” at https://sustainabledevelopment.un.org/sdg15
  - [Other?]
- References

257. Risk under other risk frameworks - UN SDGs – SDG 15 - Life on Land

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

258. Risk under other risk frameworks - UN SDGs – SDG 16 - Peace, Justice and Strong Institutions

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 16?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 16 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg16
  - [Other?]
- References

258. Risk under other risk frameworks - UN SDGs – SDG 16 – Peace, Justice and Strong Institutions

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

259. Risk under other risk frameworks - UN SDGs – SDG 17 – Partnerships for the Goals

- Challenges
  - Member states of the UN developed and adopted the SDGs as a guide to development, investment and policy for the benefit of all humanity and the planet.
    - Technology systems that operate inconsistently with the SDGs will more likely encounter resistance to adoption, challenges of interoperability, assertions of inconsistency with "reasonable duties of care," and other challenges from nations and companies that are aligning their strategic and investment strategies to be consistent with the SDGs.
  - How does the technology system under review address and/or support (or undermine) the UN Sustainable Development Goals (UN SDGs), that were adopted by the member states of the UN as a shared framework for global development?
    - Coordination within SDG "Verticals:"
      - Does the technology system help to further and/or measure the "Targets" and "Indicators" associated with SDG 17?
    - Coordination among multiple SDG "Verticals:"
      - Does the technology system generate metrics and/or other data that can help to measure, analyze and coordinate the performance against "Targets" and "Indicators" in multiple SDG "verticals" to mitigate or eliminate conflict among SDGs?
  - [Other?]
- References
  - Link to SDG 17 "Targets" and "Indicators" at https://sustainabledevelopment.un.org/sdg17
  - [Other?]
- References

259. Risk under other risk frameworks - UN SDGs – SDG 17 – Partnerships for the Goals

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

260. Risk Under Other Risk Frameworks – Nation State Branches - Legislative

- Challenges
  - [Other?]
- References
  - ”The Constitution of Risk”

260. Risk Under Other Risk Frameworks – Nation State Branches - Legislative

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

261. Risk Under Other Risk Frameworks – Nation State Branches - Judicial

- Challenges
  - [Other?]
- References

261. Risk Under Other Risk Frameworks – Nation State Branches - Judicial

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

262. Risk Under Other Risk Frameworks – Nation State Branches - Executive

- Challenges
  - [Other?]
- References

262. Risk Under Other Risk Frameworks – Nation State Branches - Executive

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

263. Risk Under Other Risk Frameworks – Nation State Agencies - General

- Challenges
  - [Other?]
- References

263. Risk Under Other Risk Frameworks – Nation State Agencies – General

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

264. Risk Under Other Risk Frameworks – Nation State Agencies – Defense - Army

- Challenges
  - [Other?]
- References

264. Risk Under Other Risk Frameworks – Nation State Agencies –Defense - Army

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

265. Risk Under Other Risk Frameworks – Nation State Agencies –Defense - Navy

- Challenges
  - [Other?]
- References

265. Risk Under Other Risk Frameworks – Nation State Agencies –Defense - Navy

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

266. Risk Under Other Risk Frameworks – Nation State Agencies –Defense – Air Force

- Challenges
  - [Other?]
- References

266. Risk Under Other Risk Frameworks – Nation State Agencies –Defense – Air Force

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

267. Risk Under Other Risk Frameworks – Nation State Agencies –Defense - Marines

- Challenges
  - [Other?]
- References

267. Risk Under Other Risk Frameworks – Nation State Agencies –Defense - Marines

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

268. Risk Under Other Risk Frameworks – Nation State Agencies –Defense - Cyberforce

- Challenges
  - [Other?]
- References

268. Risk Under Other Risk Frameworks – Nation State Agencies –Defense - Cyberforce

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

269. Risk Under Other Risk Frameworks – Nation State Agencies – Intelligence Agencies – Foreign Intelligence

- Challenges
  - [Other?]
- References

269. Risk Under Other Risk Frameworks – Nation State Agencies – Intelligence Agencies – Foreign Intelligence

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

270. Risk Under Other Risk Frameworks – Nation State Agencies – Intelligence Agencies – Domestic Intelligence

- Challenges
  - [Other?]
- References

270. Risk Under Other Risk Frameworks – Nation State Agencies – Intelligence Agencies – Domestic Intelligence

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

271. Risk Under Other Risk Frameworks – Nation State Agencies – Intelligence Agencies – Defense Intelligence

- Challenges
  - [Other?]
- References

271. Risk Under Other Risk Frameworks – Nation State Agencies – Intelligence Agencies – Defense Intelligence

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

272. Risk under other risk frameworks – Nation State Agencies – Intelligence Agencies – Other Intelligence Agencies

- Challenges
  - Nature of intelligence operations is changing rapidly as information is more ubiquitous and accessible across broadly interconnected and interoperable networks
  - Power is exerted through multiple political, economic and social vectors
    - Internal – How decipher an discern “voice” and shared ideas of the population in modern networked information context?
    - External - How ”speak with one voice” as nation interacting with other nations when setting and implementing policy?
    - How
  - [Other?]
- References

272. Risk under other risk frameworks – Nation State Agencies – Intelligence Agencies – Other Intelligence Agencies

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider DIME PMESII framework for analyzing extensions of national power
    - Defense
    - Information
    - Military
    - Economic
    - P
    - M
    - E
    - S
    - I
    - I
  - [Other?]
- References

273. Risk under other risk frameworks – Nation State Agencies – Trade/Commerce Agencies

- Challenges
  - [Other?]
- References

273. Risk under other risk frameworks – Nation State Agencies – Trade/Commerce Agencies

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

274. Labor Laws and Rules

- Challenges
  - [Other?]
- References

274. Labor Laws and Rules

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

275. Bias – Sectoral – Regulatory Effect

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Sectoral – Regulatory Effect-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - [Other?]
- References
- Wikipedia provides that: Self-regulation is the process whereby an organization monitors its own adherence to legal, ethical, or safety standards, rather than have an outside, independent agency such as a third party entity monitor and enforce those standards.[81] Self-regulation of any group can create a conflict of interest. If any organization, such as a corporation or government bureaucracy, is asked to eliminate unethical behavior within their own group, it may be in their interest in the short run to eliminate the appearance of unethical behavior, rather than the behavior itself.
- Regulatory capture is a form of political corruption that can occur when a regulatory agency, created to act in the public interest, instead advances the commercial or political concerns of special interest groups that dominate the industry or sector it is charged with regulating.[82][83] Regulatory capture occurs because groups or individuals with a high-stakes interest in the outcome of policy or regulatory decisions can be expected to focus their resources and energies in attempting to gain the policy outcomes they prefer, while members of the public, each with only a tiny individual stake in the outcome, will ignore it altogether.[84] Regulatory capture is a risk to which a regulatory agency is exposed by its very nature.

275. Bias – Sectoral – Regulatory Effect

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

276. Bias – Analytical/Statistical - Forecast

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
  - Security Profiling-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - [Other?]
- References
  - Wikipedia provides that: A forecast bias is when there are consistent differences between results and the forecasts of those quantities; that is: forecasts may have an overall tendency to be too high or too low.

276. Bias – Analytical/Statistical - Forecast

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

277. Bias – Analytical/Statistical – Observer-Expectancy Effect

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Analytical/Statistical bias-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - [Other?]
- References
  - Wikipedia provides that:
    - The observer-expectancy effect is when a researcher's expectations cause them to subconsciously influence the people participating in an experiment. It is usually controlled using a double-blind system, and was an important reason for the development of double-blind experiments.

277. Bias – Analytical/Statistical – Observer-Expectancy Effect

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

278. Bias – Analytical/Statistical – Reporting Bias and Social Desirability Bias

- Challenges
  - The actions and behaviors of stakeholders in socio-technical systems can be affected by biases
    - Reporting Bias-related issues can cause system stakeholders to interact with the system (and otherwise act in ways that are) inconsistent with the baseline requirements and specifications for optimal socio-technical system function and are contrary with the expectations of other system stakeholders
    - Reliability of users, operators, intermediaries, designers, developers, etc. may be affected
    - In such cases, the behavioral effects of this form of bias can increase system risks and undermine system function.
  - [Other?]
- References
- Wikipedia provides that:
  - “In epidemiology and empirical research, reporting bias is defined as "selective revealing or suppression of information" of undesirable behavior by subjects or researchers. It refers to a tendency to under-report unexpected or undesirable experimental results, while being more trusting of expected or desirable results. This can propagate, as each instance reinforces the status quo, and later experimenters justify their own reporting bias by observing that previous experimenters reported different results.
  - Social desirability bias is a bias within social science research where survey respondents can tend to answer questions in a manner that will be viewed positively by others. It can take the form of over-reporting laudable behavior, or under-reporting undesirable behavior. This bias interferes with the interpretation of average tendencies as well as individual differences. The inclination represents a major issue with self-report questionnaires; of special concern are self-reports of abilities, personalities, sexual behavior and drug use.”

278. Bias – Analytical/Statistical – Reporting Bias and Social Desirability Bias

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

279. Machine-Learning Vulnerabilities – Adversarial Attacks

- Challenges
  - [Other?]
- References

279. Machine-Learning Vulnerabilities – Adversarial Attacks

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Science Magazine, March 22, 2019 p. 1287
    "Adversarial attacks on medical machine learning"

280. Machine-Learning Vulnerabilities - Unprovability

- Challenges
  - [Other?]
- References

280. Machine-Learning Vulnerabilities - Unprovability

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

281. Algorithmic Radicalization

- Challenges
  - [Other?]
- References

281. Algorithmic Radicalization

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - “The Making of a YouTube Radical” (New York Times, June 9, 2019, Section 1, page 1.
  - “Some Extremist Groups See Porn as a Conspiracy” (New York Times, June 9, 2019, Section 1, p. 19

282. Capacity for Scaling via Separation of System Governance Functions

- Challenges
  - Do the system operating requirements and parameters (which constitute a set of system rules) enable large scale system deployment?
  - Rules that are centralized (to ensure system component interoperability, coordination, central control, etc.) inhibit large scale deployment and adoption of systems
  - [Other?]
- References

282. Capacity for Scaling via Separation of System Governance Functions

- Candidate Analytical Frameworks/Metrics/Actions
  - Governance structures that include or allow for separation of 3 functions can scale faster
    - Rulemaking – legislative function
    - Operations – executive function
    - Enforcement – judicial function
  - Most private/proprietary owners of technology/systems will want to maintain the "control" of the system, which typically includes all 3 functions listed above.
    - Rulemaking is the most "existential" of the functions
    - Operations is the function that is most amenable to outsourcing
      - Expectations of performance of outsourcers can be detailed in specifications to enable contractual control of third party performer
    - Enforcement is in-between –
      - In common law jurisdictions and dynamic interaction environments, enforcement of rules has the potential to contribute (through various feedback loops) to rulemaking/legislative processes
      - In code-based law jurisdictions and static interaction environments , enforcement of rules is more consistent and stable, and more closely resembles operations/executive functions.
  - [Other?]
- References

283. Risk Under Other Risk Frameworks – EU GDPR

- Challenges
  - [Other?]
- References

283. Risk Under Other Risk Frameworks – EU GDPR

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

284. Risk Under Other Risk Frameworks – California Consumer Privacy Act (CCPA)

- Challenges
  - [Other?]
- References

284. Risk Under Other Risk Frameworks – California Consumer Privacy Act (CCPA)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

285. Optimization for User/Operator Perception - General

- Challenges
  - With integration of technology into various immersive and augmented reality systems, how are positive and negative system effects of human natural sensory systems (and natural variation in acuity across human populations) taken into account in system performance metrics
  - [Other?]
- References

285. Optimization for User/Operator Perception - General

- Candidate Analytical Frameworks/Metrics/Actions
  - Unpack 7 human senses to identify challenges and optimization opportunities for a given sensory system
    - Visual
    - Auditory
    - Tactile/Haptic
      - Heat, pressure, pain,
    - Aroma/Taste
    - Vestibular - (Balance and Movement)
    - Proprioception - (Body awareness)
  - [Other?]
- References

286. Optimization for User/Operator Perception - Visual

- Challenges
  - Visual perception is a dominant form in humans
    - Text
    - Graphic
    - Photographic
    - Video
  - Many historical pathways to altering meaning of visual cues that affect risk
    - Mimicry, counterfeiting, impersonation, “false light” in publishing, forgery, sleight of hand, etc.
  - [Other?]
- References

286. Optimization for User/Operator Perception - Visual

- Candidate Analytical Frameworks/Metrics/Actions
  - Review strategies and defenses against visual misdirection in other settings to assemble toolkit of possible approaches
    - Review methods of distraction, approaches in stage magic, propaganda,
  - [Other?]
- References
  - Compare works on processing of false information (slide __ and bibliography)

287. Optimization for User/Operator Perception - Auditory

- Challenges
  - [Other?]
- References

287. Optimization for User/Operator Perception - Auditory

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

288. Optimization for User/Operator Perception – Tactile/Haptic

- Challenges
  - Tactile sense includes sensory neurons responsive to multiple sensations
    - Pressure
    - Heat
    - Pain
  - [Other?]
- References

288. Optimization for User/Operator Perception – Tactile/Haptic

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

289. Optimization for User/Operator Perception – Aroma/Taste

- Challenges
  - Aromas can be used to induce emotional states that can affect human performance
  - Body has “good” and “bad” taste channels
    - Sugar and Umami are good channel
      - Indicate presence of nutritious carbohydrates and proteins
    - Bitter and Sour are “bad” channel
      - Indicate presence of poisons
    - Salt uses ”good” channel until certain level of blood salinity then switches to ”bad” channel
  - How might natural taste signaling channels be applied to inform operators and users of a given technology
  - [Other?]
- References
  - Nature article on taste neuron structure

289. Optimization for User/Operator Perception – Aroma/Taste

- Candidate Analytical Frameworks/Metrics/Actions
  - Mercaptan is added to odorless, colorless natural gas to enable leaks in highly decentralized distribution systems to be detected easily
  - Consider additions to food stocks to guard against certain weaponizations
  - [Other?]
- References

290. Optimization for User/Operator Perception – Vestibular (Balance and Motion)

- Challenges
  - Augmented and virtual reality interfaces and user and operator experiences rely on digital creation and representation of analog ("real world") experience where the faithfulness/filtering/amplification of representation can lead to inaccurate morphological responses that can affect sociotechnical system performance
  - How does choice of UI (visual, auditory, tactile/haptic, other) affect
  - How does user/operator proprioception affect the performance of systems that rely on telepresence
    - Remote surgical procedures
  - Feeling of nausea/headaches and other performance-degrading responses in Virtual Reality-based systems based on lag in movement and display refreshing
  - [Other?]
- References

290. Optimization for User/Operator Perception – Vestibular (Balance and Motion)

- Candidate Analytical Frameworks/Metrics/Actions
  - Incorporate user testing of UIs early in design/build process to confirm absence of vestibular/balance-based performance degradation
  - Consider inclusion of “back up” or secondary systems or other compensating controls to account for vestibular/vertigo/balance-induced user/operator performance deficiencies
  - Consider application of various proprioception resetting protocols and practices
    - Use UI design (color/pattern/etc.) to correct or offset user/operator orientation challenges in using system
    - Consider presentation of warnings and posting of notices in virtual environments/landscapes to suggest that users/operators have a safe physical working environment in which to operate/gesticulate:
      - Use of safety tape around factory machines and robots
      - Wearing of safety equipment by users/operators to protect from personal injury when operating in VR.
  - [Other?]
- References
  - [Cite for: RAND CORPORATION – Robotic Safety Book – 1980s]

291. Optimization for User/Operator Perception – Proprioception (Body Position)

- Challenges
  - Augmented and virtual reality interfaces and user and operator experiences rely on digital creation and representation of analog ("real world") experience where the degree of (or relative lack of) faithfulness/filtering/amplification of representation can lead to inaccurate morphological or psycho-somatic responses in users and operators that can affect sociotechnical system performance?
  - How does choice of UI (visual, auditory, tactile/haptic, other) for a given information/technical system affect user/operator proprioception and therefore overall socio-technical performance?
  - How does user/operator proprioception affect the performance of systems that rely on telepresence
    - Remote surgical procedures
  - Feeling of nausea/headaches and other performance-degrading responses in Virtual Reality-based systems based on lag in movement and display refreshing
  - [Other?]
- References

291. Optimization for User/Operator Perception – Proprioception (Body Position)

- Candidate Analytical Frameworks/Metrics/Actions
  - Incorporate user testing of UIs early in design/build process to confirm absence of latency-based performance degradation
  - Consider inclusion of “back up” or secondary systems or other compensating controls to account for lag-induced user/operator performance deficiencies
  - Consider application of various proprioception resetting protocols and practices
    - Submariners get to look out the periscope once a week
  - Consider presentation of warnings and posting of notices in virtual environments/landscapes to engage perception of user/operator and periodically disengage immersive experience, for example:
    - Banking regulatory warnings posted in early online game “second life”
    - Notices provided when user moves from one online website to another
      - Disavow content – Disclaimers
  - [Other?]
- References

292. System Processing of False Information

- Challenges
  - False information can be intentionally or accidentally introduced into system and organizational operations, where it can skew decision making and undermine optimal system performance and operations
  - How vulnerable is the technology system to accidentally or intentionally introduced mis-information inputs during the various stages of its design, development, deployment, operation and performance testing (DDDOPT)?
    - How can system sub-systems be tested for the application of mis-information in their respective DDDOPT?
  - Does the system support the ability of system users and operators to discern and appropriately process false information?
  - [Other?]
- References

292. System Processing of False Information

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

293. Bias – Systemic – “Fail Safe” Default States

- Challenges
  - When system operation is ”broken,” does the system default to a state that is harmful/disadvantageous to one or more system stakeholders?
  - What are system mechanisms for users and operators to discern system failure?
  - What is the ”lag-time” between onset of system failure and user or operator notification for various sorts of system failure?
  - [Other?]
- References

293. Bias – Systemic - ”Fail Safe” Default States

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider total and partial failure of system and the implications of that failure for dependent system operations
    - Compare traffic lights – Cannot default to green/green.
  - [Other?]
- References

294. Bias – Systemic – Bias in Bias Detection System Itself

- Challenges
  - [Other?]
- References

294. Bias – Systemic – Bias in Bias Detection System Itself

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

295. Bias – Promotion Bias of Engineers - Revenue

- Challenges
  - [Other?]
- References

295. Bias – Promotion Bias of Engineers - Revenue

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

296. Ability to Disconnect As Security/Privacy “Fail Safe”

- Challenges
  - Connected IoT, Mobiles and other sensor-enabled devices can encode, collect and transmit data that, once collected, can be received, decoded, and reviewed remotely and repeatedly making it difficult or impossible to test system for access controls and integrity of transfers to 3rd parties.
  - There is no standardization of signals or marks for users/consumers that a product or service has features that are undetectable to the consumer, such as
    - System universal Data collection and transfer capacities
    - Autonomous Operating mode
  - Business models based on secondary use of data will need to change their revenue model to account for loss of free data feedstock
    - Will people pay for social network and search services that previously received free of fee (with service payment based on data)
  - In B2B settings, consider whether system can be isolated from mission critical systems and how
  - [Other?]
- References

296. Ability to Disconnect As Security/Privacy “Fail Safe”

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider “fail safe default state” of no data collection
    - Turning “on” data collection mode is like physical “opt in”
  - Brexit test
    - What happens if installed system is pulled from larger organizational or set of systems?
    - Technical implications
  - Compare concept of “cover” under UCC
    - Steps to mitigate harm of non-performance of system
    - Implications of bespoke or made to order systems
  - [Other?]
- References

297. System Design Informed By Flawed “Theory of Change”

- Challenges
  - [Other?]
- References

297. System Design Informed By Flawed “Theory of Change”

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

298. Misapprehension of Conduct and Effects of Sovereignty

- Challenges
  - [Other?]
- References

298. Misapprehension of Conduct and Effects of Sovereignty

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

299. Incomplete System Adoption and Marketing Plan

- Challenges
  - [Other?]
- References

299. Incomplete System Adoption and Marketing Plan

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

300. Consistency With Stakeholder "PEN" (Principles, Ethics and Norms)

- Challenges
  - [Other?]
- References

300. Consistency With Stakeholder "PEN" (Principles, Ethics and Norms)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

301. Amenability to Audit of Operation

- Challenges
  - [Other?]
- References

301. Amenability to Audit of Operation

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

302. Prevalence-Induced Concept Change in Human Judgment

- Challenges
  - [Other?]
- References

302. Prevalence-Induced Concept Change in Human Judgment

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

303. Machine Learning Limitations

- Challenges
  - [Other?]
- References

303. Machine Learning Limitations

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

304. Machine Learning Limitations

- Challenges
  - [Other?]
- References

304. Machine Learning Limitations

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

305. Machine Learning Limitations

- Challenges
  - [Other?]
- References

305. Machine Learning Limitations

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

306. Reliance on Random Numbers

- Challenges
  - Quality of random number
  - Latent patterns of system
  - Is system subject to attack by introduction of non-random (but apparently random) numbers in substitution of random numbers?
  - [Other?]
- References

306. Reliance on Random Numbers

- Candidate Analytical Frameworks/Metrics/Actions
  - If the system is dependent on random numbers (or subsystems that depend on random numbers),
    - is the quality of such random numbers testable?
  - [Other?]
- References

307. Reliance on Non-Verified System Metrics

- Challenges
  - Unique or otherwise non-verifiable system metrics can yield illusory performance effectiveness and promote impression of causation and system efficacy
  - Are system metrics random, or weakly correlated undermining usefulness of system.
  - Is there random phenomenon or environmental variables that threaten system performance?
    - False signals
  - [Other?]
- References
- G.K. Chesterton said: “Exactitude is obvious, but inexactitude lies hidden”

307. Reliance on Non-Verified System Metrics

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

308. Reliance on Third-Party Certifications of System Components

- Challenges
  - [Other?]
- References

308. Reliance on Third-Party Certifications of System Components

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

309. Reliance on Biometrics

- Challenges
  - Various sorts of biometrics are being integrated into technology systems as part of system access controls, operating protocols, etc.
  - Different sorts of biometrics pose different potential security and operational challenges.
  - Once data from biometric has been captured, how prevent its reuse for access (even in absence of actual biometric signal)?
  - [Other?]
- References

309. Reliance on Biometrics

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider adding another “factor” to biometrics to improve their integrity
    - Time stamp hashed with biometrics data as generated to prevent reuse of data generated from biometric
  - [Other?]
- References

310. Disinformation Defenselessness

- Challenges
  - Concern that, since the Internet was developed without an identity layer, the source, provenance, etc. of information cannot be ascertained with sufficient assurance to help process “good” from ”bad” information.
  - Notably, this problem is not entirely new in human society, but the traditional strategies and tactics to help curb and mitigate the negative effects of misinformation are no longer effective in highly interconnected social and information networks
  - Concern that if volume of disinformation is increased, even debunking will still result in people doubting that they can trust ANY news or official signal.
  - [Other?]
- References
  - “Combating Fake News – Lie detector” (Economist Magazine. (Oct. 26, 2019, p.70)

310. Disinformation Defenselessness

- Candidate Analytical Frameworks/Metrics/Actions
  - Lithuanian ”Demaskuok” (“de-bunk”) searches for sources (“patient zero’s”) in fake news
    - Applies ”dis-information” likelihood scores
      - Economist notes bases for scoring include:
        - » Look at propogandist style wording and themes
          - poverty, rape, environmental degradation, military shortcomings, war. Games, societal rifts, viruses and health scares, political blunders, poor governance and uncovering of deceit, gossip and scandal
        - » Emotional terms:
          - Children, immigrants, sex, ethnicities, animals, national heroes, injustice
        - » Virality: number of shares and times read
        - » Timing: Disinformation posted often on Friday
        - » Recurring use of fake names and re-used. Pictures
        - » Reputation of website for posting disinformation
    - Debunk EU: can spot some ”broken mirrors,” i.e., disinformation presenting accurate facts misleadingly (compare to “False Light” Risks elsewhere in Atlas)
    - Demaskuok technical assessments are reviewed by humans and institutional actors
  - Noted in Economist article that “Officials say that abundant debunking has cultivated healthy skepticism in most Balts.”
    - Consider volume of Debunking signals as relevant in citizen education about self-filtering
  - [Other?]
- References
  - “Combating Fake News – Lie detector” (Economist Magazine. (Oct. 26, 2019, p.70)

311. Smooth Fractals?

- Challenges
  - Can visualization of
  - Between fractals and regular surfaces.
  - [Other?]
- References

311. Smooth Fractals

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

312. Challenge of measuring symmetry in analog human systems

- Challenges
  - Math is ultimately about symmetry
    - Reference to philosophy magazine article
  - Difficult to discern symmetries in humanities
  - Difficult too “resolve” paradoxes in absence of measurements.
  - [Other?]
- References
  - Reference to philosophy magazine article

312. Challenge of measuring symmetry in analog human systems

- Candidate Analytical Frameworks/Metrics/Actions
  - Draw “graph-theory” style diagrams to discern unbalanced relationships
    - See if ”edges” balance
    - Is each stakeholder offered a balanced bargain in the structure?
  - [Other?]
- References
  - ”Doing Money” by (one of the functions of money is as a. risk consolidation tool).

313. Encoding and Decoding Meaning – Rhetorical Information Payloads

- Challenges
  - It is not just the “signal” that must be encoded and decoded (separate from the channel ”noise”), but also the meaning that must be decoded.
    - “Meaning signal” and “meaning noise” are determined by such things as context, priors, etc.
  - In what ways does the technology support the encoding and decoding of meaning?
    - Are controls for meaning encoding made available. To both sender and receiver
  - [Other?]
- References

313. Encoding and Decoding Meaning – Rhetorical Information Payloads

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

314. Encoding and Decoding Meaning – Censorship Laws

- Challenges
  - Jurisdictions impose varying ”duties of care” on information network intermediaries
    - Is the technology system able to support the conformity of use to the patchwork of different requirements
  - [Other?]
- References
  - “The Splinternet” - Economist article (Nov. 9, 2019, p. 53)

314. Encoding and Decoding Meaning – Censorship Laws

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

315. Encoding and Decoding Meaning – Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived and analyzed can influence the development and deployment of strategies and tactics to mitigates its negative influence on socio-technical system operation
  - Ignorance impacts on information risk, but the ambiguity of the term can be a source of additional and aggravating risk when systems are designed, hardened to mitigate the negative system effects of ignorance
  - Ignorance in its various manifestations can negatively affect the performance of entities that encode signals (senders), intermediaries and those who decode signals (receivers) in interaction networks
  - The treatment of the topic of ignorance in this Atlas applies the. Analytical framing of DeNicola's "Understanding Ignorance" (see below)
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

315. Encoding and Decoding Meaning – Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the negative system performance impact of various forms and iterations of “ignorance” when manifested in different roles in interactions
    - Sender
    - Intermediary
    - Receiver
  - Structure of Atlas of Risk Maps “Ignorance” discussion is based on DeNicola book
  - Structure applied is not exclusive approach, but allows for unpacking of concept to make it operational
  - [Other?]
- References
  - “Understanding Ignorance - The surprising impact of what we don’t know” by DeNicola (MIT Press, 2017)

316. Encoding and Decoding Meaning – Ignorance - Images of Ignorance – The impact of ignorance*

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - Ignorance of stakeholders of a socio-technical system can undermine expected performance of the system
    - Designer ignorance
    - User ignorance
    - Operator ignorance
  - Ignorance has many sources and connections with interactions that make it a difficult problem to address
  - Goethe said "There is nothing more frightening than ignorance in action."
  - "Understanding" of problem is necessary prerequisite to addressing/solving it
    - Ignorance is a many faceted "problem" that must be disambiguated prior to formulating solutions
  - Ignorance of stakeholders is more than mere void of lack of knowledge
    - Ignorance is also rooted in various complex and dynamic interactions
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

316. Encoding and Decoding Meaning – Ignorance - Images of Ignorance – The impact of Ignorance*

- Candidate Analytical Frameworks/Metrics/Actions
  - Analysis and approach to mitigating effects of various sources of “ignorance” of stakeholders (users, operators, designers, intermediaries, etc.) that can affect performance of technical systems in operation should consider strategies and tactics in dynamic interaction environment of ignorance
    - Not problem of ignorance in isolation
    - Ignorance in context of interactions
    - Dynamic elements of ignorance
  - Integrate concepts of ”ignorance” and “knowledge” to best understand, characterize and address ignorance.
  - [Other?]
- References
  - “Understanding Ignorance - The surprising impact of what we don’t know” by DeNicola (MIT Press, 2017)

317. Encoding and Decoding Meaning – Ignorance – Images of Ignorance – Conceiving Ignorance*

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - Ignorance may be conceived of as a "negative" (aka "privative") which suggests a gap, lack
    - Like abstraction like crack in sidewalk, hole in donut, deficiency of vitamin D
    - Can conceive of ignorance as absence of knowledge, or knowledge as absence of ignorance
      - Confusing and ambiguous terms obscure possible approaches
  - Paradox of ignorance is that it is difficult to conceive of how to know about what is not known
  - Paradox in fact that it requires knowledge to identify ignorance
    - Ignorance does not recognize itself – need system to help us identify when we are ignorant in operating a system in a given context
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

317. Encoding and Decoding Meaning – Ignorance – Images of Ignorance – Conceiving Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Where ignorance is treated as a "privation/gap" in knowledge it invites the consideration that it also suggests a capacity to learn
    - Category confusion to say that "bowling ball" is "ignorant" since it has no capacity to learn
  - Once ignorance is recognized as implying the capacity to learn, invites consideration of strategies to promote learning
    - See slides on "Processing Inaccurate Information" for unpacking of the mechanisms and challenges associated with revising prior knowledge
  - Can manage the "paradox" of ignorance (i.e., how to convert "unknown unknowns" into "known unknowns") by distinguishing between the concept of ignorance and understanding that which is not yet understood
    - Scope - Since vectors of ignorance are vast, consider "contiguous" knowledge requirements in operating the system to help define "front lines" of ignorance that can be most helpfully addressed
  - Can narrow paradox by considering "whose" ignorance is being addressed
    - Roles, backgrounds, training, etc. all relevant
    - Not "one size fits all" solutions
  - Distinguish ignorance from "error"
  - "error" is by an action – ignorance requires no action
  - Consider parsing ignorance based on parsing of types of knowledge
    - Knowing "that" includes knowledge of factual expressions expressible as propositions ("S knows that P")
    - Knowing "how" refers to skills
    - Knowing by Direct Acquaintance – Immediate memory of unmediated experience ("I know Mr. Jones")
  - In these slides, based on "Understanding Ignorance" by DeNicola, apply 4 metaphors to help enclose concept of ignorance for analysis
    - Strategies and tactics for addressing ignorance-based challenges may benefit from application of similar metaphors.
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

318. Encoding and Decoding Meaning – Ignorance – Ignorance as Place – Dwelling in Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - Metaphors of ignorance to places can affect the manner in which ignorance is addressed in deploying and operating a technical system
  - Plato's cave analogy presents "ignorance" as place of ignorance that created a fundamental incapacity to understand in its occupants
    - See only shadows of reality
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

318. Encoding and Decoding Meaning – Ignorance – Ignorance as Place – Dwelling in Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Capacity for knowledge is embedded in ignorance
  - If ignorance is pervasive default state of humans (as suggested in Plato's allegory of the cave), then technical systems should be designed and deployed with attention to mechanisms to dissipate this state, vis a vis operation of the system
    - Include training
    - Include attentive UIs
    - Provide metrics for system that can be referenced for periodic audit of operation
  - Do not rely on stakeholder initiative to self train for system role
    - Muslim philosopher Al-Ghazzali said, "Heedlessness is an illness of which the afflicted person cannot cure himself."
  - Apply Kerwin's 4 categories of ignorance (Rumsfeld cited 3)
    - Known knowns: what I know I know
    - Known unknowns: What I know I don't know
    - Unknown unknowns: What I don't know I don't know
    - Unknown knowns: What I don't know I know
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

319. Encoding and Decoding Meaning – Ignorance – Innocence and Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - Conceptions of ignorance as a form of innocence can obscure needs and benefits of knowledge
    - Compare biblical story of Garden of Eden
  - Innocence is a state of dependence that results in potential vulnerability of a person and the system in which they are acting
  - Falsely perpetuating or prolonging innocence/ignorance of the operations of a system can signal motives and agenda that are not ignorant
    - Ignoring external harms caused by system operation
  - Structures and systems of perpetuated ignorance/innocence can become places of dependence and oppression that can interfere with socio-technical system function
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

319. Encoding and Decoding Meaning – Ignorance - Innocence and Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Patterns of ignorance and innocence remind us that we are members of multiple "epistemic communities" (communities of shared understanding)
    - Based on language
    - Based on education
    - Based on belief
    - Etc.
  - Community nature of knowledge and ignorance invites consideration of community-based approaches to addressing ignorance
  - Recognize that willful ignorance/innocence of harm of system operation does not absolve parties of responsibility
    - Legal "know or should have known" test for reasonable knowledge
    - Doctrine of "unclean hands" in equitable remedies
  - Consider ignorance/innocence claims in light of the "Insight/Intrusion" slider
    - Any insight is accompanied by a potential "intrusion" on others
    - Innocence of that harm of intrusion might not be reasonable in a given context – supporting liability
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

320. Encoding and Decoding Meaning – Ignorance – Ignorance as Boundary ‗ Mapping our Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - Despite frequent references to "boundaries" and "borders" between ignorance and knowledge, it is difficult to understand and analyze ignorance directly
    - Limits potential responses to mere examination of ignorance in general
  - It is difficult to operationalize and implement programs to constrain general ignorance
    - But also difficult to identify specific areas of ignorance and to weight their relative importance
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

320. Encoding and Decoding Meaning – Ignorance – Ignorance as Boundary - Mapping our Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Distinguish concept of "general ignorance" from self-created ignorance
    - See slide 321 for constructed ignorance
  - Even though boundary of general ignorance is nebulous, to gain insight into ignorance, consider differences among some object types of ignorance, including, for example, ignorance of:
    - Facts
    - Data and quantities
    - Entities (substances, objects, creatures, places)
    - Persons, names, roles or relationships
    - Concepts, principles, laws, theories
    - Errors or discrepancies
    - Clusters and systems of all of the above, including subjects, fields and disciplines
  - The successful operation of each deployed technical system will depend, to a greater or lesser extent, on addressing the particular "mapping" of ignorance associated with each separate object type of ignorance
    - Mitigation of the negative impacts of ignorance for each involves potentially different strategies and tactics
  - General ignorance is unintentional, and therefore lends itself to more general characterization (in accordance with the types of ignorance above, e.g.,) than constructed ignorance
    - See discussion of "constructed ignorance" in slide 321)
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

321. Encoding and Decoding Meaning – Ignorance – Ignorance as Boundary – Constructed Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - It is necessary to understand and characterize the source and causation pathways of particular ignorance in order to address it
  - Ignorance is typically an undesirable state, but in certain circumstances, entitles may seek to maintain "constructed ignorance" ("Nescience") when it is to their benefit
  - "Nescience" is what we or others *have determined* we are not to know
    - Nescience varies from general ignorance in its intentional maintenance by parties that would otherwise gain knowledge
  - 5 forms of Nescience (see next slide) are of distinct origin and invite different strategies and tactics of mitigation
    - Willful ignorance is a form of nescience that is persistent, in part, because it is based in fear.
  - Within and among organizations, structures of confidentiality, secrecy, and "need to know" information are institutional and contractual forms of "constructed ignorance"
  - Paradox of Nescience is that it requires some knowledge of the area in order to act in a manner to deliberately avoid that information
    - Compare "holographic" principle – Surface of system carries information about the interior. Is deliberate/constructed ignorance an awareness of the "surface" but not the details of an area of knowledge.
    - Compare "constructed ignorance" and "willful ignorance" – the latter requires both ignorance and ignoring the concept
  - Ignorance may be inadvertently constructed due to exercise of individual preference and algorithmic amplification
    - See slides on "echo chambers" and "confirmation bias"
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

321. Encoding and Decoding Meaning – Ignorance - Ignorance as Boundary – Constructed Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Constructed ignorance (or "intentional ignorance") takes several familiar forms
    - Constructed ignorance to serve individual goals (Nescience)
    - Constructed ignorance to serve organizational goals (confidentiality, NDAs, etc.)
  - Distinguish among the 5 different types of Nescience to better craft mitigations:
    - Rational Ignorance – Making conscious decision not to know based on cost/benefit analysis
      - E.g., not reading terms of service for software license
      - Usually a personal decision, but may be made by managers, gatekeepers, etc. for others (ethical considerations)
      - As global information increases exponentially, selective rational ignorance will become increasingly necessary
      - Rational ignorance more readily defensible for individual choices, but less appropriate for public officials, fiduciaries, etc.
    - Strategic/Tactical Ignorance – Maintain ignorance for an advantage. Offers deniability.
      - Avoidance of the responsibility of knowing
        - » Query whether the deliberate cultivation of excludability is itself morally culpable?
      - Avoidance can preserve the benefits of knowing later (avoiding "spoiler alert")
      - Avoidance can preserve fairness (assuring jury does not read about case in newspaper; jury instructions instruct ignoring certain information)
    - Willful Ignorance – Forms of self-deception. Putting one's head in the sand.
      - Differs from strategic/tactical ignorance because caused by "will" rather than rational thought
      - Recognizes that ignorance is not just lack of knowledge, but an active force of psychic and social consequence
      - E.g., Ignoring spousal infidelity, maintaining racial stereotypes
      - Involves bifurcation of self into an "aware" self (that self-deceives) and unaware self (the self that is deceived)
    - Secrecy – Contexts of structured secrecy, privacy, confidentiality all require substantial effort and resources to maintain
      - Privacy suggests a zone of "proper ignorance" that others should not seek to breach
      - Whistle-blowers and subpoenas are examples of breaches of secrecy motivated by public benefits
    - Forbidden Knowledge – Linked asymmetries of knowledge and power can place certain information off limits
      - E.g., Regulations of certain research (gain of function in H5N1), religious taboos
  - Non-disclosure agreements, confidentiality arrangements, and similar agreements are deliberate forms of constructed ignorance that can carve out specific types or areas of information
    - Consider "residual clauses" are "Carve outs" from NDA as forms of "constructed knowledge"
  - Constructed ignorance recognizes ignorance as a strategy, not a liability
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

322. Encoding and Decoding Meaning – Ignorance - Ignorance as Boundary – The Ethics of Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - Members of communities of constructed ignorance and others who are ignorant for other reasons who become stakeholders in a socio-technical system might skew performance of that system as a consequence of their behaviors based on their erroneous beliefs
    - Moral judgements are made about beliefs, knowledge and ignorance
    - Moral judgments can have legal and liability consequences
    - E.g., Legal test of negligence based on *"what a reasonable person knows of should have known"*
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

322. Encoding and Decoding Meaning – Ignorance - Ignorance as Boundary – The Ethics of Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Design and deploy information systems with attention to producing outputs and metrics that can support the 4 factors that affect moral assessment of knowledge and ignorance
    - Process – means by which one pursues and acquires knowledge or causes of ignorance
      - Ethical violations in research, violations of privacy, theft of proprietary information all unethical forms of knowledge acquisition
    - Content – Intrinsic morality of content
      - E.g., forbidden , harmful, trivial, disgusting content may be salient in ethics of knowledge decision
    - Purpose – Intention and purpose of seeking information is relevant in ethical analysis of knowledge acquisition
      - Purposeful nescience (constructed ignorance) raises ethical questions where knowledge is part of responsibility
    - Context – Moral judgment of ignorance depends on roles and relationships
  - [Other?]
- References
  - “Understanding Ignorance - The surprising impact of what we don’t know” by DeNicola (MIT Press, 2017)

323. Encoding and Decoding Meaning – Ignorance _ Ignorance as Boundary – Virtues and Vices of Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

323. Encoding and Decoding Meaning – Ignorance – Ignorance as Boundary - Virtues and Vices of Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - “Understanding Ignorance - The surprising impact of what we don’t know” by DeNicola (MIT Press, 2017)

324. Encoding and Decoding Meaning – Ignorance – Ignorance as Limit – The Limits of the Knowable

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

324. Encoding and Decoding Meaning – Ignorance - Ignorance as Limit – The Limits of the Knowable

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - “Understanding Ignorance - The surprising impact of what we don’t know” by DeNicola (MIT Press, 2017)

325. Encoding and Decoding Meaning – Ignorance – Ignorance as Limit – Managing Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

325. Encoding and Decoding Meaning – Ignorance – Ignorance as Limit – Managing Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - “Understanding Ignorance - The surprising impact of what we don’t know” by DeNicola (MIT Press, 2017)

326. Encoding and Decoding Meaning – Ignorance – Ignorance as Horizon – The Horizon of Ignorance

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - [Other?]
- References
  - "Understanding Ignorance - The surprising impact of what we don't know" by DeNicola (MIT Press, 2017)

326. Encoding and Decoding Meaning – Ignorance – Ignorance as Horizon – The Horizon of Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

327. Encoding and Decoding Meaning – Ignorance – Ignorance and Epistemology

- Challenges
  - "Ignorance" of stakeholders (users, operators, designers, intermediaries, etc.) can affect performance of technical systems in operation
  - The ways in which ignorance is conceived can influence the development and deployment of strategies and tactics to address ignorance
  - [Other?]
- References

327. Encoding and Decoding Meaning – Ignorance – Ignorance and Epistemology

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - “Understanding Ignorance - The surprising impact of what we don’t know” by DeNicola (MIT Press, 2017)

328. Encoding and Decoding Meaning – Rhetoric and Persuasion - Generally

- Challenges
  - Technical systems are useless if people and organizations do not use them or use them improperly
    - People and organizations are not merely users or operators of technical systems, but also often function as critical 'components" of such systems in operation.
  - Socio-technical systems (i.e., technical systems as deployed and used in real settings) depend upon the reliable and predictable behaviors and performance of both technical and human/institutional components
    - Technical components are rendered reliable by conformity to standard specifications
    - Human/institutional components are rendered reliable by conformity to policies, rules and norms
      - Policies and rules are presented in text form, the language of which is intended to satisfy many requirements, including the conveyance of normative guidance, objectively testable audit and enforcement variables, etc.
  - Adoption rates for new sociotechnology systems depend on multiple variables such as perceived efficacy, ease of use, etc.
  - Many of the variables of humans and institutions in socio-technical system performance settings depends directly and indirectly on the quality of instructional and training text, internal and external communications and interactions, and the quality of the conveyance of relevant system status information to and among stakeholders
    - Information for designers, developers, operators, users, etc.
  - The qualities of the crafting and presentation of written materials to stakeholders is critical to their performance in relations to a new technology system
    - Not just basic "quality" of writing, but recognition of written components as central to performance of human/institutional e=elements of the system
  - [Other?]
- References

328. Encoding and Decoding Meaning – Rhetoric and Persuasion - Generally

- Candidate Analytical Frameworks/Metrics/Actions
  - Recognize need to "calibrate" text presented to relevant stakeholders for consistency with technical system goals
  - Rhetorical elements are those constructed to have an impact on the attitudes, beliefs and actions of its audience
    - System operators, owners and users depend on the reliable and predictable performance of other stakeholders
    - Rhetorical and persuasive elements of communicative elements of the system can help to assure reliability and predictability of human and institutional behaviors and performance with can contribute to overall system reliability
  - Rhetoric is about persuasion – the ability to coax predictable responses and behaviors from others
  - Rhetoric involves many elements/canons of knowledge construction and communication and style is relevant to all of them
    - Invention – the discovery of content and lines of argument
    - Judgment – the selection of content appropriate for the situation
    - Arrangement – the ordering of the selected parts for the audience and situation
    - Memory – the internalization of the text for recall
    - Delivery – the management of voice and body (medium of communication)
  - Based on extension of "situated cognition" to recognition that the mind exists in language and material culture (the brain being equivalent to an antenna that "tunes in" to the mind), rhetoric is a form of compulsion and force used to affect the behavior of others that share the communicative/social mind.
  - Rhetoric in this context is not about style for its own sake, but the power of language (including language associated with eh use of a particular technical system) to force conformity, compliance, reliability and predictability
    - That reliable performance serves to decrease risk and increase leverage across stakeholders interacting with a given technical system.
  - [Other?]
- References

329. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – Language of Origin

- Challenges
  - Socio-technical information systems operate to help humans (and human institutions) convert data-to-information-to-knowledge
    - Each step involves the addition of context, priors, background, norms (collectively meaning) to entrain and guide the development of useful information and knowledge that can offer superior insight which can, in turn, help to de-risk and leverage future interactions.
  - The manner in which "meaning" is applied is not neutral, and can affect the pace and depth of adoption of information systems and their output
    - Meaning manifests in all sorts of text, and also in other communications associated with system operation and deliverables
    - Attention to amplification of desired meaning (and suppression of undesirable meaning) can help to drive the efficacy and efficiency of information system operation
  - Among the recognized rhetorical and persuasive devices is choice of words based on language of origin____
  - How might attention to language of origin in the instructions, training materials, operating instructions, system calibrations, inter-stakeholder communications, system outputs, system audits and other system-related communications affect the overall performance of the system in context?
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

329. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – Language of Origin

- Candidate Analytical Frameworks/Metrics/Actions
  - All textual inputs and outputs to an information system should be subject to rigorous rhetorical analysis to confirm that:
    - opportunities for persuasion consistent with system operations are maximized and
    - intentional and accidental language that undermines system function is minimized
  - For systems operated in English:
    - English core words convey clarity, directness and simplicity
    - English words based on French usage convey elevation, aspiration and innovation
    - English words based on Latin and Greek convey formality, erudition, cognition
  - For international teams working on developing technology it is important to confirm shared definitions AND shared penumbral meanings of team communications to avoid inefficiencies and system breakdowns
  - Compare to international identity federations where weighting of identity attributes from one culture to another
    - Identity is bound up in cultural elements, including language.
    - Trust in systems can be negatively affected by program communications that offend or are unfamiliar to stakeholders from some cultural groups
  - [Other?]
- References

329. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – New Words

- Challenges
  - Both the technical and social elements of new information systems create new relationships, invite new perspectives and introduce new and changing words and jargon into general usage
  - The use of new and changed words in sociotechnical systems communications can introduce both intended and accidental meaning into communications, potentially undermining system operation
  - Massively distributed information networks are sociotechnical systems that depend on large populations of (often untrained) users
    - How can system functions and potential harms be conveyed to large populati0ns of untrained users?
    - How can UIs be developed to minimize the negative impact of ignorance of new and technical words?
  - The technology sector creates new sorts of interactions and conceptions for which existing language is inadequate
    - Tech sector stakeholders readily introduce and adopt "Nonce" words, i.e., words occurring invented or used just for a particular purpose (aka Neologisms)
  - Corporate roots of technical innovation often introduce intellectual property and proprietary considerations into the usage and spread of New Words
    - Trademark law and copyright both require some "originality"
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

329. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – New Words

- Candidate Analytical Frameworks/Metrics/Actions
  - Textual and oral communications that are critical for system operations should be carefully screened to assure that there is shared understanding and meaning among all relevant stakeholders
  - Categories of examples include:
    - Foreign Borrowings – Effect on conveyed meaning depends on whether the term has been assimilated or not.
    - Compounds - xxx
    - Prefix/Suffix
    - Clipping
    - Blends
    - Conversions
    - Catachresis
    - Acronyms
    - Proper Names to Common Names
    - Analogy
    - Fabrication
    - Onomatopoeia
    - Taboo Deformation
    - Doubling
  - [Other?]
- References

330. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – Categories of Choice

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

330. Encoding and Decoding Meaning –
Rhetoric and Persuasion – Word Choice – Categories of Choice

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

331. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – Language Varieties

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

331. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – Language Varieties

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

332. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice - Tropes

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

332. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice - Tropes

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

333. Encoding and Decoding Meaning – Rhetoric and Persuasion – Word Choice – Figures of Word Choice

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

333. Encoding and Decoding Meaning – Rhetoric and Persuasion - Word Choice – Figures of Word Choice

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

334. Encoding and Decoding Meaning – Rhetoric and Persuasion – Sentence Predication

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

334. Encoding and Decoding Meaning – Rhetoric and Persuasion – Sentence Predication

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

335. Encoding and Decoding Meaning – Rhetoric and Persuasion – Sentence Construction: Modification

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

335. Encoding and Decoding Meaning – Rhetoric and Persuasion – Sentence Construction: Modification

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

336. Encoding and Decoding Meaning – Rhetoric and Persuasion – Sentence Architecture

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

336. Encoding and Decoding Meaning – Rhetoric and Persuasion – Sentence Architecture

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

337. Encoding and Decoding Meaning – Rhetoric and Persuasion – Figures of Argument

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

337. Encoding and Decoding Meaning – Rhetoric and Persuasion – Figures of Argument

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

338. Encoding and Decoding Meaning – Rhetoric and Persuasion - Series

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with “Rhetoric and Persuasion” borrow their overall framing (and condensed titles) from the book “Rhetorical Style – The Uses of Language in Persuasion,” (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 (“_____”). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

338. Encoding and Decoding Meaning – Rhetoric and Persuasion - Series

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

339. Encoding and Decoding Meaning – Rhetoric and Persuasion – Prosody and Punctuation

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

339. Encoding and Decoding Meaning – Rhetoric and Persuasion – Prosody and Punctuation

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

340. Encoding and Decoding Meaning – Rhetoric and Persuasion– Interactions – Speaker and Audience Construction

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

340. Encoding and Decoding Meaning – Rhetoric and Persuasion – Interactions – Speaker and Audience Construction

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

341. Encoding and Decoding Meaning – Rhetoric and Persuasion – Interaction – Incorporating Other Voices

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

341. Encoding and Decoding Meaning – Rhetoric and Persuasion – Interaction – Incorporating Other Voices

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

342. Encoding and Decoding Meaning – Rhetoric and Persuasion – Interaction – Situation and Occasion

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

342. Encoding and Decoding Meaning – Rhetoric and Persuasion – Interaction – Situation and Occasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

343. Encoding and Decoding Meaning – Rhetoric and Persuasion – Passage Construction - Coherence

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

343. Encoding and Decoding Meaning – Rhetoric and Persuasion – Passage Construction - Coherence

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

344. Encoding and Decoding Meaning – Rhetoric and Persuasion – Passage Patterns

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

344. Encoding and Decoding Meaning – Rhetoric and Persuasion – Passage Patterns

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

345. Encoding and Decoding Meaning – Rhetoric and Persuasion - Amplification

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with "Rhetoric and Persuasion" borrow their overall framing (and condensed titles) from the book "Rhetorical Style – The Uses of Language in Persuasion," (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 ("_____"). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

345. Encoding and Decoding Meaning – Rhetoric and Persuasion - Amplification

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

346. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References
  - The 18 Atlas slides dealing with “Rhetoric and Persuasion” borrow their overall framing (and condensed titles) from the book “Rhetorical Style – The Uses of Language in Persuasion,” (Jeanne Fahnestock, Oxford University Press, 2011. This slide 328 reflects the discussion in chapter 1 (“_____”). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of for rhetoric and persuasive elements of socio-technical system interactions and outputs.

346. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

347. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

347. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

348. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

348. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

349. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

349. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

350. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

350. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

351. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

351. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

352. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

352. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

353. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

353. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

354. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

354. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

355. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

355. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

356. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Challenges
  - [Other?]
- References

356. Encoding and Decoding Meaning – Rhetoric and Persuasion

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

357. Encoding and Decoding Meaning - Simulacrum - First Order

- Challenges
  - The metric is not the same as the phenomenon
    - First order simulacrum challenges arise in the gap between reality and representation
    - First order question regards the fidelity with which the system representation of reality (expressed in its metrics, parameters, operating assumptions, etc.) reflects an objective reality
      - "objective reality" is one that operates independently of the system stakeholders, and the knowledge and awareness of which can benefit stakeholders
  - How can system stakeholders be confident that the system metrics and representations are a reasonable reflection of reality?
    - "Reality" includes the (physical and relational) operating environment of the system including those parameters that are relevant to system operation
  - What is the "reality" conveyed by the system to system stakeholders?
    - Does that conveyed "reality" appropriately characterize variables that are relevant to the stakeholders?
    - Are there elemenets of "reality" beyond the system generated metrics that would be relevant to stakeholders if they were consumed or measured by the system?
  - the Senders, receivers and intermediaries each encode and decode metrics/signals that they rely upon to inform and de-risk their future interactions with the system
  - To what degree do the metrics provided by the system enhance or detract from the the ability of the sender, receiver or intermediary to perceive the "real" operation of the system
    - "Real" internal system operation perspective
    - "Real" external insight into the relationship of the system to other systems
  - For purposes of this analysis, "Real" environment and operation of the system means "functional reality," i.e., provides a sense of the system, and the environment in which it operratoes that is sufficiently relevant and comprehensive that it allows for the appropriate calibration and tuning of the system so that it can perform within expected parameters
    - Not a matter of sensing "objective reality"
    - Must be empirically testable as part of the reasonable operation of the system.
  - [Other?]
- References

357. Encoding and Decoding Meaning - Simulacrum - First Order

- Candidate Analytical Frameworks/Metrics/Actions
  - Cross-check system metrics with other external sources to confirm fidelity of system first order simulacrum
  - Provide clear "calibration" criteria for confirming that system metrics/output reflect functional reality for edch stakeholder
  - New technology system operation/output/metrics can be "ground-truthed" with respect to informatni generated by other technical and socio-technical systems
    - Operation and metrics of organizational legacy systems can offer familiar "touchpoints" to evaluate new technology operations
      - Where new technologies operate with respct to new inte3ractions and relationships, legacy system metrics might not be available or relevant to evaluate new technology effectiveness in de-risking and leverage.
  - [Other?]
- References
  - Simulations by John Baudrillard (Semiotext - 1983) describes successive phases of abstraction of image and measurement as follows:
    - 1st order - the system representation/metric is the reflection of basic reality
    - 2nd order –the system representation/metric masks and perverts a basic reality
    - 3rd order – the system representation/metric masks the absence of a basic reality
    - 4th order – the system representation/metric bears no relation to any reality whatever: it is Its own pure simulacrum

358. Encoding and Decoding Meaning - Simulacrum - Second Order

- Challenges
  - System representations and metrics are not, themselves, reality, so those outputs may alter/pervert reality
    - Metrics may intentionally alter reality
    - Metrics may un-intentionally alter reality
    - Need different strategies to address intentional versus unintentional application of altered system metrics
  - Consumption and application by system stakeholders of altered reflections/metrics for reality can lead to ill-founded behaviors and strategies
    - Detrimental reliance can lead to legal liability if system operators have a duty to stakeholders
  - [Other?]
- References

358. Encoding and Decoding Meaning - Simulacrum - Second Order

- Candidate Analytical Frameworks/Metrics/Actions
  - See candidate analytical frameworks/metrics/actions for "First Order Simulcrum"
    - Second order and second order simulacrum both assume the existence of a basic reality that is measured by the system and in which the system operates
      - Some strategies to address first order and second order simulacrum overlap
  - If the Second Order Simulcrum is due to intentional action of a stakeholder, consider the nature of the strategies needed to address the "intentional" source of risk
    - Intentional actions are more persistent
    - Agenda of intentional actor may not be obvious to other stakeholders
  - If Second Order Simulcrum is due to accikdent or inadvertence, consider nature of strategies needed to addrees the "accidental" source of risk
    - Accidental actions are less persistent
      - Caused by non-linear behaviors of complex systems
  - In formulating response to the presence of second order simulacrum in system operation, consider the timing and manner in which the metric or system reflection that manifests the second order simulacrum is introduced into the system
    - Design phase
    - Developmemnt phase
    - Deployment phase
    - Operations phase
  - [Other?]
- References
  - Simulations by John Baudrillard (Semiotext. - 1983) describes successive phases of abstraction of image and measurement as follows:
    - 1st order - the system representation/metric is the reflection of basic reality
    - 2nd order –the system representation/metric masks and perverts a basic reality
    - 3rd order – the system representation/metric masks the absence of a basic reality
    - 4th order – the system representation/metric bears no relation to any reality whatever: it is Its own pure simulacrum

359. Encoding and Decoding Meaning - Simulacrum - Third Order

- Challenges
  - A third order simulacrum is a metric, system output, or other system operating element that masks the absence of an external reality
    - Third order (and fourth order) simulacrum does NOT require an external reality
  - Third order simulacrum defies cross-checking because the absence of an actual reality precludes separate measurement of that externality
  - Examples of third order simulacrum appear and proliferate in markets, interaction settings, and communities in which actions, behaviors and decision making of stakeholders involves abstrcactions and heuristics
    - Abstractions are more readily detached from the underlying reality on which they are based, and offer the potential for manipulation, modification and interprestation that is isolated from reality.
  - [Other?]
- References

359. Encoding and Decoding Meaning - Simulacrum - Third Order

- Candidate Analytical Frameworks/Metrics/Actions
  - Unlike 1st and 2nd order Simulcrum, strategies to address and mitigate 3rd order simulacrum cannot be based on cross-checking with other systems that offer reality metrics, since 3rd order simulacrum arises in the absence of an underlying reality
    - Cannot seek to base de-risking and leverage strategies on calibration of system metrics against reality
    - The metrics ARE the reality
  - In 3rd order simulacrum settings, the system that masks the absence of a reality becomes, in effect, its own reality
    - In the absence of an environment/reality in which the system operates, the operation of the system itself creates an environment/externality that can be described as its incidental effect on external stakeholders and externality generally
    - Organized systems seek to externalize entropy/disorder, which affects parties outside the system
    - Creates entropy wasteland outside the systm, that becomes the "reality" of that system, but which the system continues to ignore.
  - Consider application of Kant's "categorical imperitive" to test system risk
    - Consider whether the metric, if applied equally by all stakeoolders, would reveal a sufficiently comprehensive view of reality
  - [Other?]
- References
  - Simulations by John Baudrillard (Semiotext - 1983) describes successive phases of abstraction of image and measurement as follows:
    - 1st order - the system representation/metric is the reflection of basic reality
    - 2nd order –the system representation/metric masks and perverts a basic reality
    - 3rd order – the system representation/metric masks the absence of a basic reality
    - 4th order – the system representation/metric bears no relation to any reality whatever: it is Its own pure simulacrum

360. Encoding and Decoding Meaning - Simulacrum - Fourth Order

- Challenges
  - A fourth order simulacrum is a metric, system output, or other system operating element that bears no relationship to any external reality whatsoever
    - Fourth order (and third order) simulacrum does NOT require an external reality
  - Fourth order simulacrum defies cross-checking because the absence of an actual reality precludes separate measurement of that externality
    - It is important to know the ”order” of the simulacrum to configure de-risking strategies
    - Absence or presence of external reality drives potential de-risking and leverage strategies and tactics
  - Examples of fourth order simulacrum appear and proliferate in markets, interaction settings, and communities in which actions, behaviors and decision making of stakeholders involves abstrcactions and heuristics
    - Abstractions are more readily detached from the underlying reality on which they are based, and offer the potential for manipulation, modification and interprestation that is isolated from reality
  - Detachment of 4th order simulacrum from ANY underlying reality means that when organizations and institutions based on 4th order simulacrum experience a system failure, there is no externality available that can help to stabilize the stakeholder’s interactions previously moderated by the 4th order simulacrum
    - 2008 financial break was example of 4th order simulacrum
      - Financial derivatives “risk” analysis was affected by multiple stkaeholders agenda, and didn’t reflect any underlying reality whatsoever
  - When the narratives of 4th order simulacrum collapse, it releases the “disorder” that they previously stored
    - Like collapse of dam at mining tailings pond
  - [Other?]
- References

360. Encoding and Decoding Meaning - Simulacrum - Fourth Order

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Simulations by John Baudrillard (Semiotext. - 1983) describes successive phases of abstraction of image and measurement as follows:
    - 1st order - the system representation/metric is the reflection of basic reality
    - 2nd order –the system representation/metric masks and perverts a basic reality
    - 3rd order – the system representation/metric masks the absence of a basic reality
    - 4th order – the system representation/metric bears no relation to any reality whatever: it is Its own pure simulacrum

361. Encoding and Decoding Meaning. - Hardening Systems Against Ignorance

- Challenges
  - [Other?]
- References

361. Encoding and Decoding Meaning – Hardening Systems Against Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

362. Encoding and Decoding – Vernacular and Regional Understanding

- Challenges
  - [Other?]
- References

362. Encoding and Decoding – Vernacular and Regional Understanding

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

363. Confusion of Causation and Correlation

- Challenges
  - [Other?]
- References

363. Confusion of Causation and Correlation

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

364. Confusion of Causation and Synchronicity

- Challenges
  - [Other?]
- References

364. Confusion of Causation and Synchronicity

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

365. Logic Flaws in Causation Analysis

- Challenges
  - Even when “causation” demonstrably and predictably affects the operation of elements or components of a given system, the impact of such causation on other elements of the system should not be presumed without being explicitly demonstrated to appropriately extended to such additional components
    - Strong causative factors may affect some system components more than others
  - [Other?]
- References

365. Logic Flaws in Causation Analysis

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

366. Processing Inaccurate Information – Knowledge Acquisition Accuracy

- Challenges
  - How does the technology system detect and protect its operations, operators and users from the negative effects of encountering inaccurate information?
  - Has the technology system been stress tested to confirm that inaccurate information encountered by stakeholders of the system does not form the basis of system operation, and is not duplicated, iterated, valorized or perpetuated by the system?
  - Does the system enhance the normal information seeking behavior of stakeholders
  - Does the system support "Bayesian" (serial error correction) construction of accurate knowledge?
  - Most research into information acquisition focuses on "how people learn valid, accurate information that we hope they will encode into their knowledge base."
    - How does the technology system protect against misinformation, inaccuracies and incorrect information?
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 366 reflects the discussion in chapter 1 ("Accurate and Inaccurate Knowledge Acquisition," by Rapp and Braasch). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.
  - Cite Nature Magazine article on Bayesian knowledge construction in human infants.

366. Processing Inaccurate Information – Knowledge Acquisition Accuracy

- Candidate Analytical Frameworks/Metrics/Actions
  - Most research into cognition and education has focused on the integration of accurate information, without attention to the additional questions raised by encounters with mis-information.
    - Note that research has focused on individual human information integration, not institutional or organizational. Modes
      - Institutional modes. May offer additional, rule. Based, opportunities. To. Address the three big issues
        - » How and. When do users. Realize that they are. Encountering misinformation?
        - » Why do specific. Comprehension difficulties. Occur?
        - » Can particular processes be designed to support processing of information so that they can successfully discount or ignore information?
  - Include fact checking and review processes to help prevent users from integrating misinformation into prior knowledge
  - Design system to enhance the potential for noticing and rejecting misinformation
  - Design system to encourage that people utilize accurate prior knowledge when appropriate to do so.
  - In technology system design, development and implementation separately consider for both the system itself AND the users of the system, the following questions:
    - Detecting and Dealing with Inaccuracies – Behaviors and remediations
    - Mechanisms of Inaccurate Knowledge Acquisition – Identify system components that engage in the activities of processes and products. Of experiences with inaccuracies
    - Mental Models – How does the system establish and employ framings to aid operators and users in the determination. Of whether. Information is inaccurate
    - Emerging models. For identifying when inaccuracies. May lead to comprehension difficulties and how to deal with them.
  - [Other?]
- References

367. Processing Inaccurate Information – Correcting Misinformation

- Challenges
  - Misinformation that has been integrated into a system and/or the cognition of users/operators of a system is persistent and challenging to correct
  - Technical systems enjoy an air of authority, with the result that their information outputs can be perceived as accurate, even in the face of contradictory evidence.
  - Retractions and refutations of misinformation have been shown to be ineffective in correcting misinformation and in fact may reinforce that misconception by repeating the false connection as part of the refutation.
    - That same ironic reinforcement can occur when a correction runs counter to strongly held beliefs
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 367 reflects the discussion in chapter 2 ("Correcting Misinformation – A Challenge for Education and Cognitive Science," by Ecker, Swire and Lewandowsky). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

367. Processing Inaccurate Information – Correcting Misinformation

- Candidate Analytical Frameworks/Metrics/Actions
  - Refutation texts set the stage for strategic conceptual change processing
    - "Refutational texts allow people (in personal and professional settings) to co-activate, align and integrate their misconceptions with corrective evidence which then facilitates the updating of beliefs." (Rapp at 29)
  - Consider variations in refutational strategies for intervention to reduce misconceptions
    - Introduction of refutational texts (correct misinformation with repeating of misinformation)
    - Introduction of non-refutational texts (correct but not repeat the misinformation)
  - Anticipatory refutation: When patterns of misinformation are encountered repeatedly across time or space in a broadly deployed system, it will be more effective to directly address and refute the potential misconceptions than to present the system instructions in standard format
    - Pre-address the reinforcement problems with refutation.
    - Avoid mere refutations as a strategy to correct misinformation and instead focus on comprehensive explanation of why it is incorrect.
      - The Atlas lists multiple bases for challenging misinformation by focusing on the influences on "meaning"
        - » E.g., Wakefield's debunked. Paper linking autism and MMR vaccine was motivated by his receipt of $500k from lawyer preparing class action case against vaccine manufacturer.
  - Be aware of the 4 separate stages of correcting misinformation by applying the "conceptual change model." (see ref)
    - Dissatisfaction with one's own current understanding (instigates cognitive conflict)
    - Proposed replacement needs to be intelligible
    - Proposed replacement needs to be plausible
    - Proposed replacement needs to be fruitful
  - Consider designing system too present "normal" distribution of responses for comparison to output to help "co-activate and align the misconception and the presented evidence in working memory" (Rapp at 28)
  - [Other?]
- References
  - Conceptual change model proposed by Posner, Strike, Hewson and Gertzog (1982) ref. in Processing Inaccurate Information, p. 28.

368. Processing Inaccurate Information – Persistence of Misinformation in Reasoning

- Challenges
  - Misinformation demonstrates robust persistence in memory and its corrosive effects on reasoning.
  - Misinformation can. Also enjoy a separate persistence when it is embodied in institutional and organizational policies that are based on that misinformation.
    - Policies may persist as artifacts of earlier periods, even after individual memory and reasoning has been purged of such misinformation.
    - Policy making lag can offer false disincentive for stakeholders in a system to adopt the corrected information when conformity to the policies forms the basis of the incentive structure in an organization.
  - Misinformation continues to be applied despite explicit correction in proportion to its "causal" role in the understanding of the system or setting
  - Stakeholders seek causal continuity
    - Stakeholders avoid causal gaps in their understanding
      - Stakeholders prefer an incorrect model over an incomplete model
  - Compare desire for "causal completeness" with issue of confusion of correlation and serendipity (slide number ___)
    - Both modes of understanding base comprehension on types of temporal cohesion
      - Causal completeness is temporal cohesion within a single system
      - Synchronicity is temporal cohesion among separate systems
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 368 reflects the discussion in chapter 3 ("The Continued Influence Effect: The Persistence of Misinformation in Memory and Reasoning Following Correction" by Seifert). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

368. Processing Inaccurate Information – Persistence of Misinformation in Reasoning

- Candidate Analytical Frameworks/Metrics/Actions
  - Research demonstrates that the only way to avoid the “Continued Influence Effect” (through which misinformation remains in memory and affects reasoning) is through introduction of “causal alternatives”
  - Misinformation can never be entirely purged from human memory and reasoning and organization policies (and related incentives and penalties) can take time to correct
    - Technical systems should include mechanisms to periodically re-test. The memory and reasoning of users and operators to confirm that the persistence of misinformation in individuals and in institutional policies does not negatively affect the processing of meaning by the system.
      - Check operator. Decisions against historically ”normal” decisions to “red flag” any anomalies for further evaluation.
  - [Other?]
- References

369. Processing Inaccurate Information – Ignorance of Comprehension Failures in Real Time

- Challenges
  - Interacting with static and dynamic information systems (such as conversations, texts, a social networks, advertising, news reports, etc.), comprehension is based on a number of factors present in the source, the medium of communication and the receiver, yielding multiple factors that can negatively affect the degree of comprehension of the receiver.
    - Unless and until a person or organization is aware that they are experiencing a comprehension failure, they will not take appropriate remedial measures
  - Does the technical system provide the people and organizations in its stakeholder community real time error detection and correction capability to signal the occurrence of a comprehension failure as a prerequisite to its correction
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 369 reflects the discussion in chapter 4 ("Failures to Detect Textual Problems during Reading," by Hacker). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

369. Processing Inaccurate Information – Ignorance of Comprehension Failures in Real Time

- Candidate Analytical Frameworks/Metrics/Actions
  - Awareness of comprehension failure is prerequisite to initiating appropriate remedial procedures to support comprehension
  - There are 5 generally recognized sources of stakeholder lack of awareness of comprehension that should be taken into account in the design, development, deployment and operation of a technical system
    - Knowledge Deficit: Stakeholders may lack requisite knowledge to fix the source of the comprehension failure
      - Design system with "hyperlinked" resources to provide real time information to stakeholders to supplement their prior knowledge
    - Process Deficit: Stakeholders may fail to experience "trigger event" so that they do not activate the knowledge at critical times when receiving information
      - Craft policies to invite deliberation by stakeholders so that they can self-test their comprehension in real time
    - Establish Stakeholder goals for information interaction to prompt different "kinds" of information processing by stakeholders
      - Readers and information receivers "goals" can affect their comprehension and error detection capacities
    - Instantiate cues (lexical, text base, and situational) for self-regulated comprehension (met comprehension) in stakeholder experience and UI design
    - Avoid cognitive/comprehension overload
      - Be aware of levels of representation in the information and the additional cognitive and comprehension resources needed to support active inference needed to process information
      - Accuracy is. Compromised when texts are too easy or too difficult
    - Configure information resources and texts to invite active processing of information
      - Active processing is necessary prerequisite to self-regulated comprehension
      - Mindless reading is not comprehension
  - [Other?]
- References

370. Processing Inaccurate Information – Avoiding Semantic Illusions

- Challenges
  - Does the technology system support the discovery and elimination of the data equivalent of semantic illusion?
    - Semantic illusion is a state of misinformation arising in a receiver/listener caused by the qualities of the text itself and the qualities of the reader
      - Intentional introduction of imposter words and/or educational "priors" to listeners represents a weaponization of semantic illusion
      - Unintentional introduction of semantic illusions
        - » Attend to semantic impact of data/text/output at multiple levels of analysis
        - » Compare tort of "false light" in publishing
          - Issue of juxtaposition of text and photos in publications causing harmful effects to person's reputation and identity
  - Semantic Illusions are different than psychological "Priming"
    - Priming has been broadly discredited in replication studies
    - Semantic illusions may be viewed as happening on a shorter time cycle than priming
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 370 reflects the discussion in chapter 5 ("Research on Semantic Illusions Tells Us That There Are Multiple Sources of Misinformation," by Hannon). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

370 – Processing Inaccurate Information - Avoiding Semantic Illusions

- Candidate Analytical Frameworks/Metrics/Actions
  - Address semantic illusions with attention to variables affecting two vectors of semantic illusion
    - The data stream/text/output presented
    - The individual/organization receiving the data stream/text/output
  - For each vector of semantic illusion, consider incentives/penalties.
    - Business
    - Legal
    - Technical
  - In each "BLT" domain, consider strategies and tactics based on each of the theories of semantic illusion
    - Partial Matching - Confusion caused by partial matching of semantic features in data/text stream
    - Structure Node Theory – Activation of external semantic network node by semantic or phonological prompt
    - Partial Processing - Activation of disordered/entropic thought from irrelevant priors by contiguous data/words
  - Consider measurements of information entropy in identifying and evaluating anomalies in data and text output of system
    - Signal in negentropy spike – even if source unknown
      - Tautology because only can register spike if already asked question/calibrated system
      - Research questions bound answers
  - Consider research (see reference text at 98)suggesting that unconscious anomaly detection is more robust than conscious awareness of anomaly
    - Consider use of system prompts of user awareness to help draw unconscious awareness of anomaly to conscious awareness of system users and operators.
    - Apply machine and artificial "ground checking" to conclusions of human users and operators to gain advantage of "unblinking eye" of recruited and intentional objective machine-based biases.
    - Calibrate instruments to address degrees of textual, lexical, and content-based entropy as "red flag" to help users/operators to "snap to" awareness of semantic illusions in real time.
  - Provide training to users and operators to aid in detection of intentional and accidental imposter data/words
    - See Ref. Processing Inaccurate Information, p. 101 et. Seq.
  - Consider "breaking the cadence of system data output to avoid the dulled attention that can lead to semantic illusions
  - [Other?]

- References

371. Processing Inaccurate Information – Inaccurate Argumentation From "Accurate" Data

- Challenges
  - Faulty argumentation and assertions drawn from accurate data can cause harm by suggesting causation chains that are, in fact, illusory
    - Data + Meaning = Information
    - Accurate Data + illogical meaning = misinformation
  - How does the technology help protect against faulty reasoning affecting the potential for harm in the input and output of the system?
    - Like question of secondary use of data outside of original context
      - Different meaning = different information
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 371 reflects the discussion in chapter 6 ("Sensitivity to Inaccurate Argumentation In Health News. Articles: Potential Contributions of Readers' Topic and Epistemic Beliefs," by Braasch, Braten, Brritt, Steffens and Stromso). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

371. Processing Inaccurate Information – Inaccurate Argumentation From "Accurate" Data

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider the misinformation effects upon two potential vectors of Inaccurate Argumentation
    - Information input/feedstock for system operation
    - System data output
  - Information input for system operation
    - With system information input, operators are potential sources of inaccurate argumentation.
      - Assumptions made about inputs may be inconsistent with understanding of other stakeholders
      - Like issue of quality of training data for machine learning
        - » Inaccurate argumentation in input is like bias in training data
  - System data output
    - With system data output, users are potential source of inaccurate argumentation
    - Attach equivalent of "warning labels" to system output, warning against using such output as "data" for future inaccurate argumentation
  - [Other?]
- References

372. Processing Inaccurate Information – Conversational Computer Agents For Normative Guidance

- Challenges
  - Human individuals (acting in both individual and institutional capacities) may be unable too detect information anomalies in the inputs and outputs of system operation
  - How does the technology system support the introduction and operation of scalable conversational computer agents that can offer various forms of anomaly detection to mitigate against the introduction and perpetuation of misinformation in system inputs and outputs?
    - Conversational Computer Agents introduce pause and prompts for human deliberation
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 372 reflects the discussion in chapter 7 ("Conversational Agents Can Help Humans Identify Flaws in the Science Reported in Digital Media," by Graesser, Millis, D'Mello and Hu). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

372. Processing Inaccurate Information – Conversational Computer Agents For Normative Guidance

- Candidate Analytical Frameworks/Metrics/Actions
  - Paired human/computer ”dyads” can support scaled conversational agents services that can help humans to identify contradictions in system inputs and outputs
    - To provide artificial social contexts in which human readers/data receivers can be brought along the “gullible/skeptical” continuum
    - Help human users/operators to alleviate cognitive disequilibrium
  - Interventions of conversational computer agents can be supported by a suite of functions similar to that of a ”Human Use Regulatory Affairs Advisor.” (HURA Advisor)(See reference)
    - Didactic lessons
    - Technical document repository
    - Hypertext references
    - Multimedia/video
    - Lessons with relatable scenarios including ethics
    - Query based information retrieval
    - Animated agent
  - [Other?]
- References

373. Processing Inaccurate Information – Knowledge Neglect

- Challenges
  - Knowledge Neglect arises when a human or system fails to retrieve and apply stored knowledge that is appropriate for a given situation or interaction
    - Example is reader who, after reading a story about a plane crash, answers the question "where were the survivors buried?"
  - Does the system help users/operators to "unbelieve" anomalous information presented by the system?
  - Humans don't have processing resources available to the ascertain the truth of everything that is read/presented
  - System may have "computational authority" that can cause humans to question their own judgement and priors, isolating them from prior knowledge that could properly inform their response to current system output
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 373 reflects the discussion in chapter 8 ("Knowledge Neglect: Failures To Notice Contradictions With Stored Knowledge," by Marsh and Umanath). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

373. Processing Inaccurate Information – Knowledge Neglect

- Candidate Analytical Frameworks/Metrics/Actions
  - Knowledge neglect has, to date, proved relatively intractable to scalable solutions
    - Intentionally slowing content presentation to promote reader self monitoring has had mixed effects
  - Consider opportunities for normative consistency (standardization) through use of coherent narratives that can help “script” consistent/predictable responses across system user and operator populations
    - Use cases in training
    - Drills and practices among stakeholder groups
  - [Other?]
- References

374. Processing Inaccurate Information – Misinformation Stickiness

- Challenges
  - Misinformation Taint: Individuals (acting in personal and organizational capacities) default to accepting information they read, only engaging in critical evaluation under specific circumstances, and only after initially encoding potentially inaccurate information
  - How does technology system mitigate tendency of humans (as users and/or operators) to accept and use
    - Information presented
    - Information recently presented
  - Liberal Encoding of misinformation can result in poor decision making.
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 374 reflects the discussion in chapter 9 ("Mechanisms of Problematic Knowledge Acquisition," by Rapp, Jacovina and Andrews). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

374. Processing Inaccurate Information – Misinformation Stickiness

- Candidate Analytical Frameworks/Metrics/Actions
  - Strategies that support compartmentalization of misinformation (apart from general knowledge)
    - Tagging strategies can help isolate harmful effects of misinformation
  - [Other?]
- References

375. Processing Inaccurate Information – Acuity At Discounting Misinformation

- Challenges
  - Does the system aid the human (acting in its personal and/or professional) capacity) in discounting misinformation in real time?
    - Aid to operator discounting misinformation in input stream for system
    - User discounting mis-information output from system
      - Compare to separate information risk from transfer of context (See Atlas Map Number ___)
  - Research suggests that "discounting" is not typically effective as guard against encoding misinformation
    - Misinformation, once encoded into knowledge is difficult to purge
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 375 reflects the discussion in chapter 10 ("Discounting Information: When False Information Is Preserved and When It Is Not," by Schul and Mayo). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

375. Processing Inaccurate Information – Acuity At Discounting Misinformation

- Candidate Analytical Frameworks/Metrics/Actions
  - Considering that misinformation has been demonbstr4ated to be difficult to purge from receiver consciousness/application, how can system be enforced to place appropriate levels of responsibility/liability on providers of information?
  - Consider whether future information network duties/regulations might impose "strict liability" for information outputs of system
    - Owner liability
    - Operator liability
    - User liabilities (for information misuse, secondary use)
  - Encourage move from "resolving" paradox toward "managing paradox."
    - Management of paradox is needed because encoded misinformation is persistent in memory and so will continue to come in contact with correcting new information, precluding resolution
    - Challenges of "discounting" can be mitigated by attention to organizational and policy effects that can help to:
      - Support delays by humans and organizations in arriving at closure regarding encoding of received information
      - Help humans to support tolerance of ambiguities
      - Help humans and institutions to resist resolving inconsistencies
  - [Other?]
- References

376. Processing Inaccurate Information – Updating Mental Models

- Challenges
  - Research demonstrates the challenge experienced by humans in updating their respective mental representations
    - Core elements of mental models are most resistant to updating
  - Failure of humans to update their mental models when acting as users and operators of technological information systems can result in undue reliance on misinformation in personal and organizational decision making by those humans
  - Focus of readers on new and inconsistent information may have negative effect regarding updating
    - May reinforce misinformation
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 376 reflects the discussion in chapter 11 ("The Ambivalent Effect Of Focus On Updating Mental Representations," by Oostendorp). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

376. Processing Inaccurate Information – Updating Mental Models

- Candidate Analytical Frameworks/Metrics/Actions
  - Presentation of background knowledge can be helpful to Humans engaging in the updating of mental models
  - Updating may also be aided by encouragement of particular mental operations
    - Active processing (prompts introduced to encourage questioning of one's own understanding
    - "Chunking of information," (see referenced text)
    - Integrating new information (by retrieving information from previous text in order to contrast that with present information)
  - [Other?]
- References
  - Consider strategy of General _____, who was unusual in briefing his troops extensively on the objects of a particular military engagement so that they could better respond to failures of the "chain of command" in the midst of the "fog of war."

377. Processing Inaccurate Information – Real Time Integration of Comprehension and Validation

- Challenges
  - Strategy of misinformation detection and prevention is affected by question of whether comprehension of text and validation of that comprehension are serial or simultaneous processes.
    - Evaluation of information is broadly considered to be offline, downstream, voluntary process subsequent to comprehension
  - Epistemic monitoring is made more difficult by the variety of vectors of factual violations in comprehension
    - Violations of factual world knowledge ("Soft soap is edible")
    - Implausibility –("Frank has a broken leg. He calls the plumber")
    - Inconsistency with antecedent text ("Mary is a vegetarian, she orders a cheeseburger."
    - Semantic anomalies ("Dutch trains are sour."
    - Validation of self referential statements ("My name is Ira")
    - Validation of statements that refer to person's value system ("Euthanasia is acceptable/unacceptable")
  - Difficulty of performing validation
    - Validation can be based on false/subjective beliefs and contribute to their persistence
    - Validation is moderated by available knowledge/beliefs
    - Routine validation processes may be conditionally automatic
    - Readers can fall victim to false information when it is sufficiently plausible
    - Validation based on quick and incomplete analysis
    - Readers perform validation to the extent that they understand a linguistic message
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 377 reflects the discussion in chapter 12 ("Comprehension. And Validation: Separable Stages of Information Processing? – A Case for Epistemic Monitoring in Language Comprehension," by Isberner and Richter). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing. Text and examples in slides from ref.

377. Processing Inaccurate Information – Real Time Integration of Comprehension and Validation

- Candidate Analytical Frameworks/Metrics/Actions
  - Given the research suggesting the difficulties of changing mental models ”after the fact,” explore whether the technical system can offer opportunities for more “real time” “epistemic monitoring” of information output for benefit of operators and users
  - Consider that the disruption of comprehension by implausible information does not just reflect processing costs of implausibility, but rather a highly purposeful validation process that protects the mental system from false information
    - The “validation process” (called epistemic monitoring) is incremental, immediate, context sensitive and non-strategic
  - Framework for integrating strategies and tactics for comprehension and validation might be supported by projecting them onto a common dimension of plausibility.
    - “Plausibility” is the “goodness of fit with prior knowledge.”
  - Design and deploy technical information systems based on modified two step model
    - Not assume 2 steps of “validation” followed by “comprehension”
    - Assume 2 steps of “evaluative comprehension” (which includes both comprehension and epistemic monitoring, followed by optional stage of epistemic elaboration
  - [Other?]
- References

378. Processing Inaccurate Information – Dealing with Knowledge as a "Complex System"

- Challenges
  - Knowledge is itself a "complex system."
    - Knowledge system driven by myriad components of "intuitive causality" (called "P-Prims") that are loosely coupled
      - P-Prims are abstracted causal relationships that help us understand and efficiently operate in the world.
      - Misapplication of p-prims in inappropriate settings can facilitate misinfrmati0n
    - Knowledge system is driven by multiple mental models ("coordination classes")
      - Set of things that one actually observes (extraction or readout strategies)
      - Set of inferences (inferential net) that are used to get from observations to characteristic features of the coordination class.
  - How does the system enable the use of different extractions and inferences in different circumstances in which the system will be involved
  - Traditional strategy of dealing with misinformation is to:
    - Prevent misconceptions from happening in the first place
    - When cannot prevent their occurrence, can we minimize or eliminate their negative impact
  - However, Epistemological perspective views knowledge as composed of P-Prims
    - P-prims are not wrong or right, but rather are more or less productive
    - P-Prims cannot be eliminated
  - Without functional view of knowledge and its acquisition, it is difficult to diagnose and address mis-information
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 378 reflects the discussion in chapter 13 ("An Epistemological Perspective on Misinformation," by diSessa). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

378. Processing Inaccurate Information – Dealing with Knowledge as a "Complex System"

- Candidate Analytical Frameworks/Metrics/Actions
  - Apply "epistemology" to the study of misinformation
    - "Epistemology" is the study of "knowledge" per se)
    - "Knowledge in Pieces" (KiP) recognizes knowledge as a complex system
    - Engage in complexity, not just make generalizations about it
  - Consider P-Prims and coordination classes approach to misinformation management
    - P-Prims are "phenomenological primitives" – small and simple elements of intuitive causality (e.g., "more effort begets greater result.") and not further reduced in use
  - P-Prims are activated in knowledge acquisition
    - P-Prims may be contextually unhelpful or inappropriate
    - Need to examine the source and activation of P-Prims of operators and users of system to understand how they might be activated in that use context
    - P-Prims should not be eliminated (in fact they cannot), but caution must be taken in system design and operation so that they are not activated in inappropriate contexts and circumstances in which case they will constitute "misinformation"
  - [Other?]
- References

379. Processing Inaccurate Information – Human Error as Percept-Concept Coupling

- Challenges
  - Humans (and the institutions in which they function) are prone error from misinformation when interacting with an information system
  - Systems should anticipate and deal with the linking (or conflict) of user and operator perceptions and conceptions that could otherwise lead to misinformation
    - Percepts are formed in real time from sensory impressions and are continually in flux based on perception
    - Concepts are formed over time in mental space from mental examination or justification and are open to change based on thinking
  - Does the system provide framing, outputs, training opportunities, etc. that can help operators and users to couple system percepts and their existing concepts to address potential performance challenges associated with misinformation that might otherwise arise.
    - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 379 reflects the discussion in chapter 14 ("Percept-Concept Coupling and Human Error," Alexander and Baggetta). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

379. Processing Inaccurate Information – Human Error as Percept-Concept Coupling

- Candidate Analytical Frameworks/Metrics/Actions
  - The system should apply strategies of mitigating misinformation based on the continuous and reciprocal interplay of perception and conception can effectively deal with reducing internal error and also transforming misguided, naïve or unscientific ideas
    - UI strategies
    - Training strategies
    - Audit strategies
  - Note that percepts are built in real time from relational thinking
  - Note that concepts are built later from relational reasoning
  - Relational reasoning strategies involve 4 basic types – all of which open the door to direct intervention in system design and operation
    - Analogical Reasoning – association is based on relationship similarity between two seemingly disparate ideas, objects, representations or situations
    - Anomalous reasoning – involves the recognition of discrepancies or deviations in one idea, object, representation or situations from an established rule or trend in another
    - Antinomous reasoning – involves the recognition that two ideas, objects, representations or situations are incompatible
    - Antithetical reasoning – requires the recognition that two representations are set in direct contrast or opposition – mutually exclusive
  - [Other?]
- References

380. Processing Inaccurate Information – Conscious Ignorance and Meta-Ignorance

- Challenges
  - Problems are only solvable or mitigated to the extent that they are first productively characterized
  - Misinformation and ignorance take many forms and have many roots that can affect human and institutional performance
  - Among the roots of misinformation are various forms of conscious and unconscious ignorance
  - Even a conscious of ignorance can be constrained in ways that can affect the formulation and implementation of performance enhancement for systems
    - Conscious Ignorance – Involves the presence of ”known” unknowns that create gaps in understanding affecting the ability to derive analysis and conclusions that can lead to functional future behaviors involving use and application of the system
    - Meta-Ignorance – Involves the presence of ”unknown” unknowns that create gaps in understanding affecting socio-technical system operation
  - Technical systems operate in numerous environments in which the users and operators are aware of the presence of unknowns and their effect on misinformation that can undermine
  - The scope of system operation may be constrained in a way that reflects conscious ignorance about externalities that can affect the system
    - This does not mean that the system is built to address the externalities, just that they remain unaddressed
    - Technical systems that ignore UIs, deployment contexts, etc. embody conscious ignorance in that they ignore these potential variables in system operation
  - Conscious ignorance can also have social functions
    - Vague statements have higher probability of being true because easier to validate
  - [Other?]
- References
  - The 19 Atlas slides dealing with “Processing Inaccurate Information” borrow their overall framing (and condensed titles) from the book “*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*,” (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 380 reflects the discussion in chapter 15 (“Cognitive Processing of Conscious Ignorance,” by Otero and Ishiwa). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

380. Processing Inaccurate Information – Conscious Ignorance and Meta-Ignorance

- Candidate Analytical Frameworks/Metrics/Actions
  - Develop technical system specifications that also provide requirements for training of operators, external elements in which the system will operate, etc.
    - Convert "known unknowns" into strategies for making these evident for users and operators
  - Various forms of conscious ignorance can lend themselves to alternative forms of mitigation in system design, development, deployment and operation
  - Consider alternative framings of ignorance that might be useful in addition to conscious ignorance and meta-ignorance
    - Kerwin identified 6 forms of ignorance
      - **Conscious Ignorance** - Known un-knowns
      - **Meta ignorance** - Not known not to be known
      - **Errors** - Thought to be known but actually not known
      - **Tacit Knowledge** – thought not to be known, but actually known
      - **Taboos** – not supposed to be known but possibly useful
      - **Denial** – too painful to be known so instead suppressed
  - [Other?]
- References

381. Processing Inaccurate Information – KReC framework for Revising Existing Knowledge Base

- Challenges
  - Research suggests that prior misinformation that is embedded in knowledge is not easily purged
    - Outdated, inaccurate information may be reactivated and disrupt comprehension and slow information uptake
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 381 reflects the discussion in chapter 16 ("The Knowledge Revision Components (KReC) Framework: Processes and Mechanisms," by Kendeou and O'Brien). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

381. Processing Inaccurate Information – KReC Framework for Revising Existing Knowledge Base

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider each component of the Knowledge Revision Components (KReC) Framework in system design and deployment to mitigate the effects of mis-information
    - The Encoding Principle – Once information has been encoded in long term memory, it cannot be deleted.
      - "Erase and replace" strategies are not effective in correcting misinformation
    - The Passive Activation Principle – Inactive information in long term memory becomes active and available via passive activation based on global memory models
      - Resonance model notes that any information related to current contents of working memory has potential to be activated, whether it facilitates or interferes with comprehension
    - The Co-activation Principle – These "passive activation" processes co-activate both previously acquired but no longer correct information and newly encoded information
      - Co-activation is necessary to bring new information into contact with and integrated with previously acquired information
    - The Integration Principle – Knowledge revision can only occur when newly encoded information is integrated with previously acquired information
  - KReC outlines basic comprehension processes and text factors that can be accentuated to increase potential for successful knowledge revisions
  - KReC framework allows parsing of separate and inter-dependent steps associated with correcting misinformation
  - [Other?]
- References

382. Processing Inaccurate Information – Content-Source Integration Model

- Challenges
  - People acting in both their personal and professional capacities frequently encounter conflicting and inconsistent information that they must address prior to integrating it into their decision making for de-risking and leverage of future interactions
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 382 reflects the discussion in chapter 17 ("The Content-Source Integration Model: A Taxonomic Description of How Readers Comprehend Conflicting Scientific Information," by Stadtler and Bromme). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

382. Processing Inaccurate Information – Content-Source Integration Model

- Candidate Analytical Frameworks/Metrics/Actions
  - Systems can help users and operators to identify, address and mitigate the negative effects of misinformation in system inputs and outputs
  - Content-Source Integration Model (CSI) assumes three stages of processing conflicting information
    - Detecting information conflict in real time,
    - Conflict regulation
    - Conflict resolution
  - Systems should include requirements and recommendations relating to the following variables are caused to focus on the three stages
    - Reader characteristics
    - Contextual scaffolds
    - Text characteristics
  - [Other?]
- References

383. Processing Inaccurate Information – Contextual/Situated Inaccuracy

- Challenges
  - Accuracy of text affects comprehension
  - "Accuracy" of text is not just inherent in text, but also affected by the entire environment of the writing and reading, etc. of text
    - Author's intent
    - Readers Strategy
    - Reader's goals
    - Readers epistemic beliefs
    - Reader's meta-cognitive awareness
  - Does the socio-technical system anticipate and address the potential for mis-information from context?
  - Internet text is presented in new complex contexts and environments for which the strategies to address complexity have not yet been fully developed
    - Internet and hypertext present texts from sources of varied expertise and legitimacy
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 383 reflects the discussion in chapter 18 ("Inaccuracy and Reading in Multiple Text and Internet/Hypertext Environments," by Afflerbach, Cho and Kim). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

383. Processing Inaccurate Information – Contextual/Situated Inaccuracy

- Candidate Analytical Frameworks/Metrics/Actions
  - Do the specifications for the technical system include requirements for the socio-technical elements of the system that can help to reduce the complexity of the de-coding environment to reduce overall contextual inaccuracy
  - Consider the distinction of “data” from “information”
    - Information arises from data decoded in a context
      - Contexts provide meaning that converts inert “data” to valuable “information” that can “inform” the decoder
  - Processing of text by reader takes place in complex environments
    - Complex author (encoder) environment
    - Complex reader (decoder) environment
    - Complex intermediary environment
  - Consider texts on “situated cognition” which identifies various mechanisms and vectors through which cognition is “situated” outside of the human brain
    - Inaccuracy arises in cognition
    - Situated inaccuracy arises in situated cognition
  - [Other?]
- References

384. Processing Inaccurate Information – User/Reader "AIR" Strategies

- Challenges
  - Knowledge formation in humans ("epistemic cognition") claims that reliable processes of evaluating information include:
    - A wide variety of belief-producing processes are used to produce knowledge claims
    - The processes used vary in reliability
    - Among reliable processes, certain conditions must be met for those processes to produce true beliefs
    - To evaluate knowledge claims in the real world, people need vast store of schemas for evaluating processes
    - People's schemas vary in validity
  - How can socio-technical systems support and develop the AIR processes?
  - Information systems are designed to accomplish multiple goals
    - A subset of information system goals are directed toward enhancing "epistemic cognition"
      - "Epistemic Cognition" refers to "the complex of cognitions that are related to the achievement of epistemic ends, such as knowledge, understanding, useful models, explanations, etc."
    - The AIR model identifies three components of Epistemic Cognition
      - Readers' "**A**ims and Value" – Aims and the value that they place on Aims.
      - Reader's "Epistemic **I**deals" – Standards applied by reader to determine if their knowledge goals have been met
      - Reader's "**R**eliable Processes – Expected reliable processes used by reader to evaluate veracity
  - Significant elements of processing accurate and inaccurate information involve people's schemas
  - [Other?]
- References
  - The 19 Atlas slides dealing with "Processing Inaccurate Information" borrow their overall framing (and condensed titles) from the book "*Processing Inaccurate Information – Theoretical and Applied Perspectives from Cognitive Science and the Educational Sciences*," (Rapp and. Braasch (eds.), MIT Press, 2014. This slide 384 reflects the discussion in chapter 19 ("Epistemic Cognition and Evaluating Information: Applying the air Model of Epistemic Cognition," by Chinn, Rinehart and Buckland). Please see the individual chapters of the referenced text for a more comprehensive treatment of the risks associated with each different analytical framing of inaccurate information processing.

384. Processing Inaccurate Information – User/Reader "AIR" Strategies

- Candidate Analytical Frameworks/Metrics/Actions
  - Apply modified "AIR" model to frame misinformation processing
  - "**A**ims and Value"
    - Include system resources to assist users/readers/decoders in setting epistemic (knowledge acquisition) goals
    - When users/readers/decoders do apply epistemic goals, are they monitored by the system to assure that desired system information conveyance goals are being achieved?
    - Users/readers/decoders apply both epistemic and non-epistemic goals in processing material
      - Can the system detect user application of non-epistemic goals in processing material and make appropriate modifications in UIs and system interface?
  - "Epistemic **I**deals"
    - How does the system recognize and enlist the user's/reader's/decoder's particular epistemic ideals to support processing of system information without negative influence of misinformation
      - Internal Structure of information
      - Connections to other Knowledge
      - Connections to empirical evidence
      - Standards of presentation and presenter to be believed
      - Clear communication
  - "**R**eliable Processes"
    - Does the system support and promote reliable processes for information production?
    - Demonstrable absence of factors that could result in the production of misinformation
  - [Other?]
- References

385. Use of Vernacular, Regionalisms, and Argot

- Challenges
  - Vernacular and Argot are speech and usage patterns that are generated by and used within a specific community or group
  - Vernacular, argot and heuristics accompany information flows from various sectors and domains
    - Usage may not be familiar to other stakeholders
  - [Other?]
- References

385. Use of Vernacular, Regionalisms, and Argot

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

386. System Externality Co-Management

- Challenges
  - System risks can
  - [Other?]
- References

386. System Externality Co-Management

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

387. Flattening of Stakeholder Consciousness

- Challenges
  - Computerizaiton and commercialization of language and communication has ”dumbed down discourse and flattened content.”
  - [Other?]
- References
- See article “Recovering the Vernacular” by Thomas Fitzgerald in The Hedgehog Review (Summer 2014, p. 85)

387. Flattening of Stakeholder Consciousness

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider whether the narrative associated with most intrinsically human elements of sociotechnical system operations are adequately addressed in system design, development, deployment, operation and training
  - In social, political and economic contexts, consider the de-risking qualities of shared senses of human cognitive/emotional response among stakeholders such as:
    - **W**it
    - **S**ubtlety
    - **A**mbiguity
    - **P**aradox
    - **I**rony
    - **E**motions
    - **N**uturing
  - [Other?]
- References

388. Disabling Authority of Managerial Grammars

- Challenges
  - Managerial Grammars are those that constrain stakeholder behavior and action phase space by speaking in a preemptory and decisive voice
    - Voice issued by disciplined engineers, technicians and accountants
    - Voice of hierarchies and top-down, centralized information flows
  - Vocabulary of business, commerce and administrative agencies precludes significant areas of individual experience, and doesn't elicit human stakeholder input in areas of relevance to sociotechnical system organizqtion and operation
    - Mind and creative thought
    - Awareness and refklection
    - Withes,
    - Expectations
    - Benevolent purposes
    - Interpreted eanings
    - Beliefs and values for guiding judgment
  - Managerial Grammars leave no place for moral or aesthetic input
    - The language of technology is a managerial grammar which doesn't offer ethical guidance
    - Note that "policy" statements in engineered systems often extend only so far as the instructions for huans to use the system correctly based on technological needs, rather than overall "socio0-technical" needs of the system.
  - [Other?]
- References
  - See article "Recovering the Vernacular" by Thomas Fitzgerald in The Hedgehog Review (Summer 2014, p. 85)

388. Disabling Authority of Managerial Grammars

- Candidate Analytical Frameworks/Metrics/Actions
  - Consider that technical and managerial grammars may not be fully relatable by stakeholders or even the most effective mode of communicating
    - Consider use of vernacular to improve relatability of training, instruction and operations signaling associated with socio-technical systems
  - Solicit forms of vernacular from stakehlders as forms of linguistic and grammatical “practice” that can then inform “best practices” and ”standards” for future system builds
  - Consider influence on system-consistent behaviors of:
    - Epigrams
    - Proverbs
    - Obiter dicta (incidental remarks)
    - Jokes
    - Anecdotes
    - Contes morals (morality tales)
  - Assure that vernacular is localized to be accessible to relevant stakeholder communities.
  - [Other?]
- References

389. Multiple Intelligences (Gardner)
Linguistic

- Challenges
  - Human stakeholders and operators require training, education and other forms of curated adaptationxxx
  - [Other?]
- References
  - Insert reference to Gardner's categorization of multiple intelligences including linguistic, musical, logical-mathematical, spatial, bodily-kinesthetic and personal.

389. Multiple Intelligences (Gardner)
Linguistic

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

390. Multiple Intelligences (Gardner)
musical

- Challenges
  - [Other?]
- References
  - Insert reference to Gardner's categorization of multiple intelligences including linguistic, musical, logical-mathematical, spatial, bodily-kinesthetic and personal.

390. Multiple Intelligences (Gardner)
musical

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

391. Multiple Intelligences (Gardner)
logical-mathematical

- Challenges
  - [Other?]
- References
  - Insert reference to Gardner's categorization of multiple intelligences including linguistic, musical, logical-mathematical, spatial, bodily-kinesthetic and personal.

391. Multiple Intelligences (Gardner)
logical-mathematical

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

392. Multiple Intelligences (Gardner)
spatial

- Challenges
  - [Other?]
- References
  - Insert reference to Gardner's categorization of multiple intelligences including linguistic, musical, logical-mathematical, spatial, bodily-kinesthetic and personal.

392. Multiple Intelligences (Gardner)
spatial

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

393. Multiple Intelligences (Gardner)
bodily-kinesthetic

- Challenges
  - [Other?]
- References
  - Insert reference to Gardner's categorization of multiple intelligences including linguistic, musical, logical-mathematical, spatial, bodily-kinesthetic and personal.

393. Multiple Intelligences (Gardner)
bodily-kinesthetic

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

394. Multiple Intelligences (Gardner)
Personal

- Challenges
  - [Other?]
- References
  - Multiple Intelligences (Gardner)
    musical, logical-mathematical, spatial, bodily-kinesthetic and personal

394. Multiple Intelligences (Gardner)
Personal

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

395. Human Encoding
Mental Models - Generally

- Challenges
  - [Other?]
- References

395. Human Encoding
Mental Models - Generally

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

396. Human Encoding
Mental Models - [Several slides here]

- Challenges
  - [Other?]
- References

396. Human Encoding
Mental Models - [Several slides here]

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

397. Direct Evaluation of System Output - Generally

- Challenges
  - The output of technical and socio-technical systems themselves can give rise to information risk
    - May be easier to evaluate system outputs than many “background” factors that contribute to information risk
    - Compare constitutuional analysis of “disparate treatment” vs. ”disparate harm” and other settings where “output” of process and/or system can be independently evaluated for providing various signals of risk
  - Stakeholders in broadly distributed systems tuypically do not have acces to information about the processes involved in system organization and operation, and must rely solely on the outur of the system that is made available to them to peform such evaluation.
    - What guidance can be provided to stakeholders to help them effectively evaluate system outputs ont heir face?
  - Where the output of a system embodies and/or perpetuates vectors of information risk (e.g., as identified in this Atlas), it is a red flag that the threat/vulnerability may be encoded in the output itself
  - There are few frameworks designed to check the integrity of technical system operation (from an information risk point of view) based solely on evaluation of the system output
  - [Other?]
- References
- The 13 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

397. Direct Evaluation of System Output - Generally

- Candidate Analytical Frameworks/Metrics/Actions
  - Atlas slides entitled “Direct Ecvaluation of System Output” provide a 12 part checklist to assist stakeholders in evaluating system output for signs of sources of information risk
  - The checklist was originally created to assist readers and evaluaters of scientific publication, and so certain modifications are necessary to apply the list in broader information risk contexts
    - Substitute word “system output” for the term “publication” wherever it occurs
    - Recognize that not all checklist questions will be relevant to the analysis of all systems
  - [Other?]
- References

398. Direct Evaluation of System Output –Research Governance

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

398. Direct Evaluation of System Output – Research Governance

- Candidate Analytical Frameworks/Metrics/Actions
  - Ask:
    - Are the locations where the research took place specified and is this information plausible?
    - Is a funding source reported?
    - Has the study been registered with any third party source that could provide support/verification?
    - Arte details such as dates and studuy methods in the publication consistent with those in the registration documents?
  - [Other?]
- References
  - Form and content of questions is borrowed from article “Evaluation of System Output” (Nature Magazine, 1/9/20, p.167

399. Direct Evaluation of System Output - Ethics

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

399. Direct Evaluation of System Output - Ethics

- Candidate Analytical Frameworks/Metrics/Actions
  - Ask:
    - Is there evidence that the work has been approved by a specific recognized ethics or toehr vahavioral evaluation committee?
      - Are the reports or any such evaluation bosdy made availablewith the research outputs?
        - » Note, content of ethics and other behavior reports may be needed to support certification mark and other supply chain standard programs.
        - » Form and content of ethican and similar reports should be checed to cinform vconformity with requirements of any external certification authority rules.
    - Are there any concerns about unethical practices raised in the content or circumstances in which the system output is provided?
  - [Other?]
- References

400. Direct Evaluation of System Output – Authorship/Origin

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

400. Direct Evaluation of System Output – Authorship/Origin

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

401. Direct Evaluation of System Output - Productivity

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

401. Direct Evaluation of System Output - Productivity

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

402. Direct Evaluation of System Output – Plagiarism/Infringement

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

402. Direct Evaluation of System Output – Plagiarism/Infringement

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

403. Direct Evaluation of System Output – Research Conduct

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

403. Direct Evaluation of System Output – Research Conduct

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

404. Direct Evaluation of System Output – Analysis and Methods

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

404. Direct Evaluation of System Output – Analysis and Methods

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

405. Direct Evaluation of System Output – Image Manipulation

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

405. Direct Evaluation of System Output – Image Manipulation

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

406. Direct Evaluation of System Output – Statistics and Data

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

406. Direct Evaluation of System Output – Statistics and Data

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

407. Direct Evaluation of System Output – Errors

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstances, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

407. Direct Evaluation of System Output - Errors

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

408. Direct Evaluation of System Output – Data Duplication and Reporting

- Challenges
  - [Other?]
- References
  - The 12 Atlas slides entitled “Evaluation of System Output . . .” incorporate the evaluation framework from the article entitled ”Check for publication integrity before misconduct,” (Nature Magazine, 1/9/20, p. 167). That article provides a checklist of 11 categories of ”red flags” (indicia) of research misconduct drawn directly from publications themselves, rather than having to investigate researcher misconduct itself. In the proper circumstaces, these red flags can signal infotech system outputs that can perpetuate information risks intentionally or inadvertently.

408. Direct Evaluation of System Output – Data Duplication and Reporting

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

409. Inaccurate Human Encoding (Mental Models)
Causal Reductionism

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models) Causal Reduction

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

410. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

410. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

411. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

411. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

412. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

412. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

413. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

413. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

414. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

414. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

415. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

415. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

409. Inaccurate Human Encoding (Mental Models)

- Challenges
  - [Other?]
- References
  - Model defined:
  - For “General” challenges of Mental Models see slide 785
  - Atlas entries 409-784 were brought to the attention of Atlas authors by the excellent book ”Super Thinking - The Big Book of Mental Models” by Weinberg and McCann (Penguin, 2019). The Atlas expands on each such model. The Atlas entries reflect the authors’ order of model presentation to aid readers who would benefit from the delightful narrative through which the authors weave together the various cognitive support structures.

409. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References
  - Entries on slides 409-785 apply titles from (and are presented in the order found in) the book “Super Thinking – The Big Book of Mental Models” by Weinberg and McCann (Portfolio/Penguin 2019).

410. Inaccurate Human Encoding/Decoding (Mental Models) Ergodicity

- Challenges
  - [Other?]
- References

410. Inaccurate Human Encoding /Decoding (Mental Models) Ergodicity

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

411. Inaccurate Human Encoding /Decoding (Mental Models)

- Challenges
  - [Other?]
- References

411. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

412. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References

412. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

413. Inaccurate Human Encoding /Decoding (Mental Models)

- Challenges
  - [Other?]
- References

413. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

414. Inaccurate Human Encoding /Decoding (Mental Models)

- Challenges
  - [Other?]
- References

414. Inaccurate Human Encoding /Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

415. Inaccurate Human Encoding /Decoding (Mental Models)

- Challenges
  - [Other?]
- References

415. Inaccurate Human Encoding /Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

416. Inaccurate Human Encoding /Decoding (Mental Models)

- Challenges
  - [Other?]
- References

416. Inaccurate Human Encoding /Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

417. Inaccurate Human Encoding /Decoding (Mental Models)

- Challenges
  - [Other?]
- References

417. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

418. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References

418. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

419. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References

419. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

420. Inaccurate Human Encoding/Decoding (Mental Models)

- Challenges
  - [Other?]
- References

420. Inaccurate Human Encoding/Decoding (Mental Models)

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

421.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

422.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

423.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

424.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

425.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

426.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

427.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

428.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

429.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

430.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

431.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

433.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

435.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

438.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

439.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

440.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

441.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

442.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

443.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

444.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

445.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

446.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

447.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

448.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

449.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

450.

- Challenges
  - [Other?]
- References

450.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

451.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

452.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

453.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

455.

- Challenges
  - [Other?]
- References

455.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

456.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

457.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

458.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

459.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

460.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

461.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

462.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

463.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

466.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

467.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

469.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

471.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

472.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

473.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

474.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

475.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

476.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

478.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

480.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

481.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

482.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

483.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

485.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

487.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

488.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

489.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

490.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

491.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

492.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

493.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

494.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

497.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

- Challenges
  - [Other?]
- References

499.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

785.

- Challenges
  - Mental models create cognitive meaning momentum that can lead to invalid conclusions and poor decisions
    - Ambiguity of Model can mislead
    - Misunderstanding of model can lead to application of Model in inappropriate circumstance
  - Mental models and similar cognitive framings that are shared among interaction participants can create false efficiencies in de-risking and leveraging interactions.
    - Parties encoding and decoding interaction signals may not share same mental model or precise configuration and implications of the model.
    - Model may be ambiguous in application to a particular interaction setting
  - [Other?]
- References

500.

- Candidate Analytical Frameworks/Metrics/Actions
  - [Other?]
- References

n. Other?

- Challenges
  - This Atlas can be improved by stakeholder processes to identify new and relevant metrics for various policy goals
    - Atlas is a living policy document
  - New Policy challenges are arising as new perspectives are being brought into the data and identity policy areas.
    - Atlas should be expanded to include new policy frameworks for operations and research.

Theory of Atlas of Risk

- A reference guide to risks in information system-dependent environments

What is the Atlas of Risk Maps?

- The Atlas is a guide to emerging ***non-technical*** threats and vulnerabilities that cause risk for ***technical*** systems, and a risk mitigation tool for the people and institutions that depend on those technical systems.
  - Focus on risks associated with the Internet and networked information systems.

- The Atlas is an emerging community of organizations and individuals who recognize that our best protection against certain emerging online threats, vulnerabilities, and risks is to collaborate on solutions to shared challenges
  - This draft Atlas has been compiled based on input, research, conference conversations, and ideas collected informally from across the global IRRI Community over several years, and this is just the start!

- The Atlas is a checklist of 400+ numbered sections each of which includes a logical grouping of ***non-technical*** threats, vulnerabilities and risks identified by the IRRI Community - that can be immediately helpful in identifying and addressing risks.
  - Many topic overlaps in Atlas highlight areas of hybrid solutions

- The Atlas is a project being built in 4 stages:
  - 1. **Listing** of threats, vulnerabilities and risks
  - 2. **Suggestions** of Metrics to capture listed risks
  - 3. **Visualizations** of Metrics to create "Risk Maps"
  - 4. **Revisions** and updating of Atlas (ongoing)

- The Atlas is a draft currently at stage 1 - **Listing** Risks

When Is The Atlas Useful?

"...and by tomorrow, I'll need a list of specific unknown risks that we'll encounter with this project."

Next Steps for Atlas Community

- The "Atlas of Risk Maps" is a crowd-sourced project that is already available (in this draft) to help you now, and is also ready to invite your participation in the next steps

- Next Step 1: **Browse and Use the Atlas**
  - Atlas is built from community input, and is openly available to anyone for reference even at these early draft stages of development
  - Atlas "maps" (still in text form) are already useful for:
    - Performance testing/auditing/risk-proofing of existing networked information technologies and systems
    - R&D of new ICT product and service conception, design, development, deployment and operation
    - Policy construction through legal and regulatory drafting and contract negotiation and preparation
    - Standards setting efforts within and across sectors, supply chains, and jurisdictions aimed at *non-technical* interoperability
    - Rights management initiatives to support individual rights associated with security, privacy, identity, and information channel integrity.
    - Budgeting and cost analysis in technology systems acquisition and operations
    - Teaching and curriculum development for in-house training, cyber-professionals, K-12 and higher-e/graduate students
    - Risk Analysis for organizations operating or contemplating expanded information network infrastructure

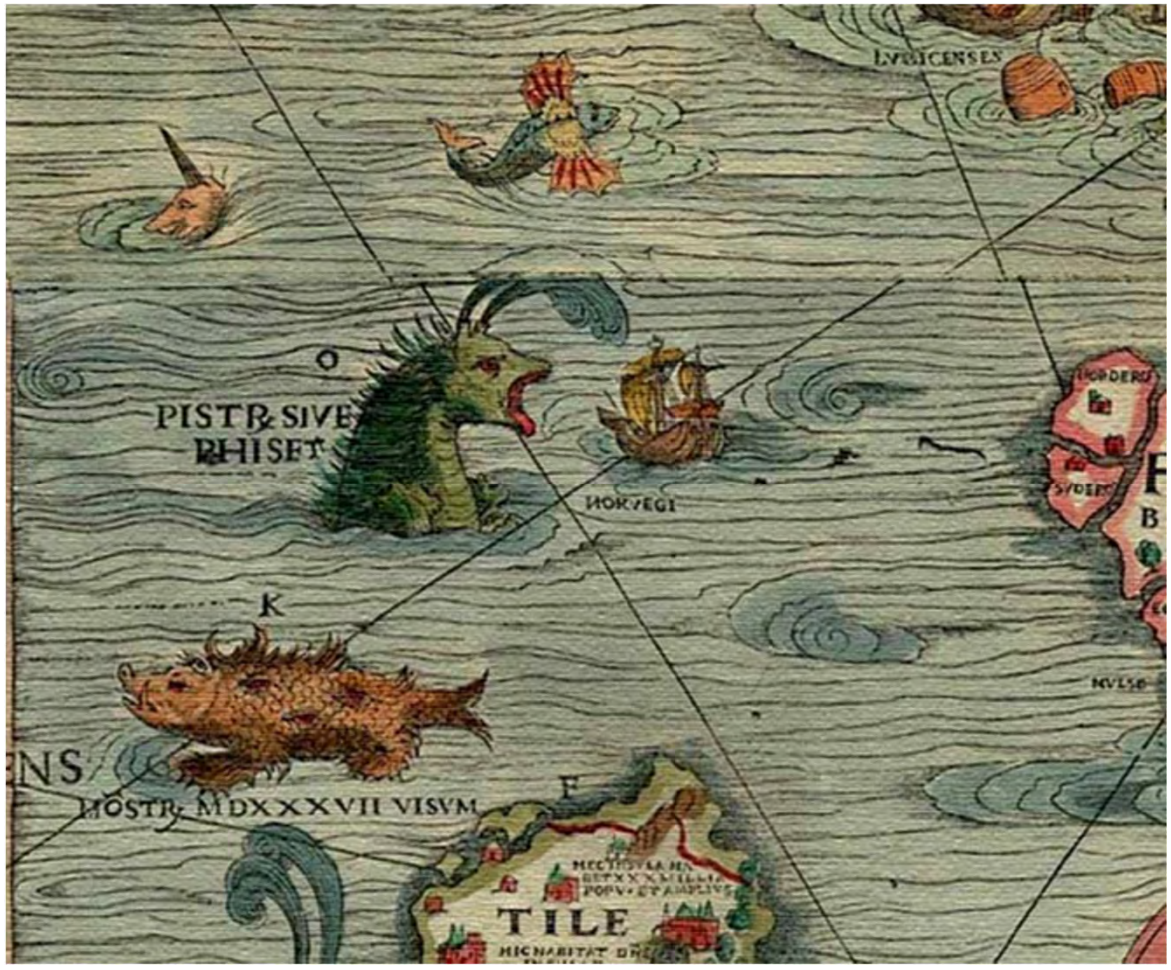
- Next step 2: **Help Build the Atlas**
  - Critique the Atlas – Please tell us how the Atlas (and the Atlas project) can be improved.
    - This is a community project, and we want to address your needs
  - Contribute your comments, thoughts, research links (to your research and others), suggestions of new map portfolios, ideas about new topics within existing maps, normative (and/or informative) cross-references to other metrics and standards, existing analytical structures for maps and metrics, existing processes for trust framework construction to reference, etc.
  - This is your Atlas– we want it to help address your needs, and we need your thoughts to be part of the synthesis of community perspectives on non-technical threats, vulnerabilities and risks that we currently describe as cybersecurity policy, privacy, identity management, risk and liability management and related domains

- Next step 3: **Please Be Patient**
  - This current Atlas draft is in PowerPoint format to ease initial compilation– it is a first "static" version
  - We have future plans to stand up an online interactive form of Atlas (wiki? GitHub? etc.?)
    - Volunteers and resources are welcomed to help accelerate this step 3.

- Please direct criticisms, suggestions, inquiries, pledges of support, etc. to:
  - Scott David, IRRI Executive Director, at sldavid@uw.edu

Introduction to IRRI Atlas of Risk Maps

Uncharted *Physical* Zones are Risky



Uncharted *Interaction* Zones are Also Risky

- Non-physical "interaction zones" within information networks harbor many new un-measured and uncharted non-physical threats, vulnerabilities, and risks
  - Commercial supply chains and financial markets
  - Critical infrastructure operations
  - Social/cultural networks
  - Governance/political structures
  - Training and learning connections
  - Etc.

The potential risks of uncharted/unmeasured threats *Beyond* Internet *Perimeter 1.0* are constraining human social, cultural, and economic progress

An Atlas to Measure and Map Risk *Beyond* Network Perimeter 1.0

- **Information network "*Perimeter 1.0*" was at the measurable edge of our operating systems of technology and institutions**
  - Risk increases as perception dims at the edge of our tech and institutional-enhanced sensory/measurement abilities
    - In this Atlas of Risk Maps, that measurement-of-performance edge is called "Perimeter 1.0"
  - Now new threats and risks are presenting themselves from beyond that old Perimeter 1.0
    - Traditional Cybersecurity, privacy, IM and legal-compliance-based efforts are blind to the new risk vectors.
  - We are experiencing new dimensions of risk of which we were unaware, and for which we are unprepared

- **If we cannot measure a phenomenon: then we cannot see it, anticipate it, or deal with it**
  - Effective "Situational Awareness" is grounded in observation/metrics from multiple perspectives
  - The many threats and vulnerabilities from beyond Perimeter 1.0 are perceived as risky because we cannot yet measure them

- **What gets measured gets done. . . and the opposite is also true**
  - Unknown risks from beyond Perimeter 1.0 are constraining what we can get done in distributed information networks
    - Risk restrains resource deployment and investment
  - For the next wave of innovation in society, culture and economics, and our own growth, we need to break through the "risk boundary" at the edge of Perimeter 1.0 and explore, measure and map the risk borderlands of Perimeter 2.0
  - The "fuel" to power this exploration and mapping is "high octane" individual and institutional "self-interest"
    - Deliver levels of risk reduction and leverage that cannot be achieved unilaterally by any stakeholder
    - Build risk mitigation structures to create new value at the edge of disorder (historical e.g., rule of law, insurance,. etc.)
    - Cultivate "non-zero sum" risk-co-management structures (e.g., rules, norms, markets, etc.)

- **Information network *Perimeter 2.0* is in the hearts and minds of people, and in the programmed responses of technology (derived from specifications) and institutions (derived from foundational documents and contracts)**
  - How can we measure threat correlations and causative factors of risks from these "softer" non-technical sources?
  - Can a broad "systems engineering" approach that embraces "applied social science" and a new enthusiasm for measurement in new domains inform our next-gen risk mitigation architectures and trust frameworks?

Proposal to Map Threats, Vulnerabilities and Risks at Network Perimeter 2.0

- **Problem: Information Network Perimeter 2.0 is unmapped/unmeasured and presents unknown risks**

  - ALL of our systems are vulnerable to threats at Perimeter 2.0
    - Vulnerable to "AAAA Threats" – (Attacks, Accidents, Acts of Nature and AI/Autonomous Systems)
      - We cannot measure/detect AAAA threats beyond security Perimeter 1.0
      - We are all blind to AAAA threats and failures at system Perimeter(s) 2.0
      - We cannot yet provide "distributed security" (or even AAAA threat measurement) at Perimeter(s) 2.0

- **Proposed Solution: Measure and Map Threats, Vulnerabilities and Risks at Perimeter(s) 2.0**

  - Recognize multiple new vectors for "AAAA Threats" in hybrid *socio*-technical information network systems
    - System integrity and performance depends on reliability of BOTH technology AND people/institutions
    - Perimeter 1.0 was the "technical" perimeter at the edge of performance measurement of technology
    - Perimeter(s) 2.0 is the multiple "socio" elements in "Socio-Technical" systems

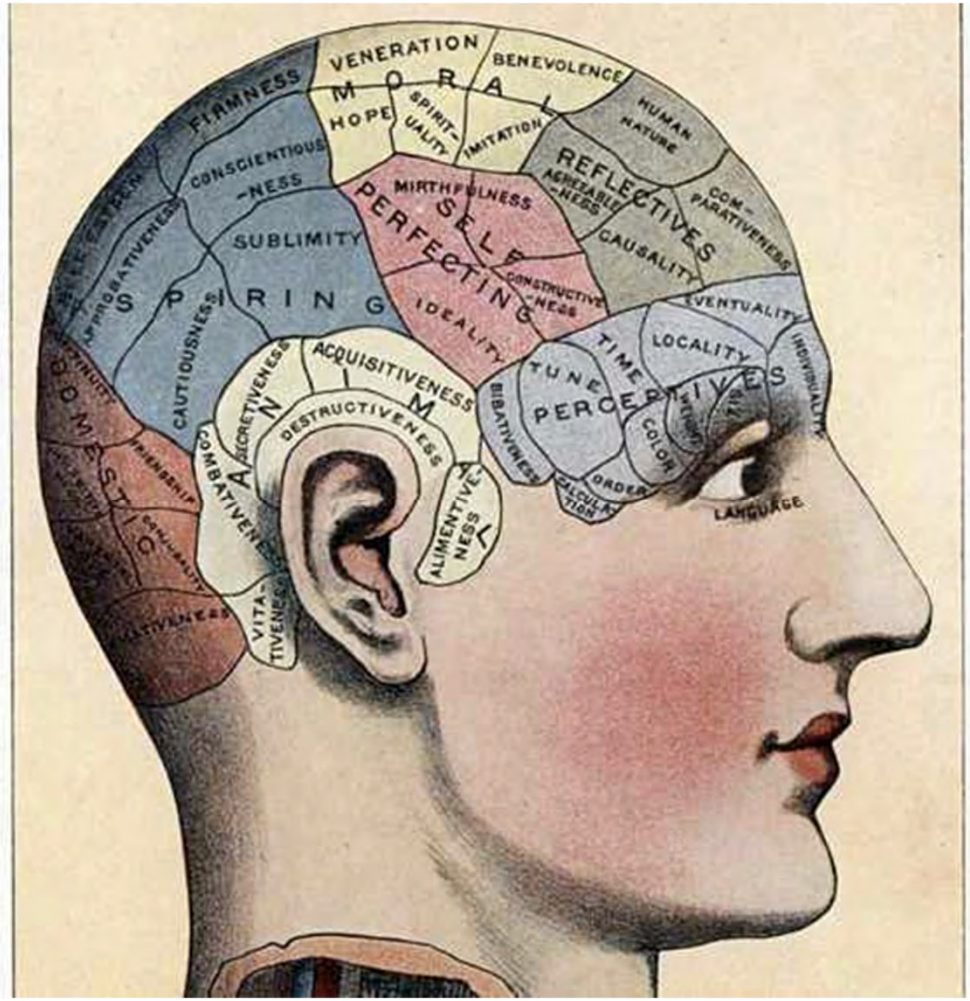
  - **Atlas program will Identify, collect and make available *non-technical* (aka "policy") threat, vulnerability and risk metrics from Perimeter(s) 2.0 to be part of systems-engineering "requirements" for cyber-vulnerable systems**

  - Current draft "Atlas" includes 400+ new cyber system threat/vulnerability/risk dimensions that are (to date) too inadequately measured to be able to fully positively contribute to systemic risk mitigation
    - To enable "Distributed Security for Distributed Systems, this crowd-sourced program creates an open "Risk Atlas" wiki structure for cyber-insecure stakeholder groups to help inform both their joint AND individual R&D and Operations

AAAA threats

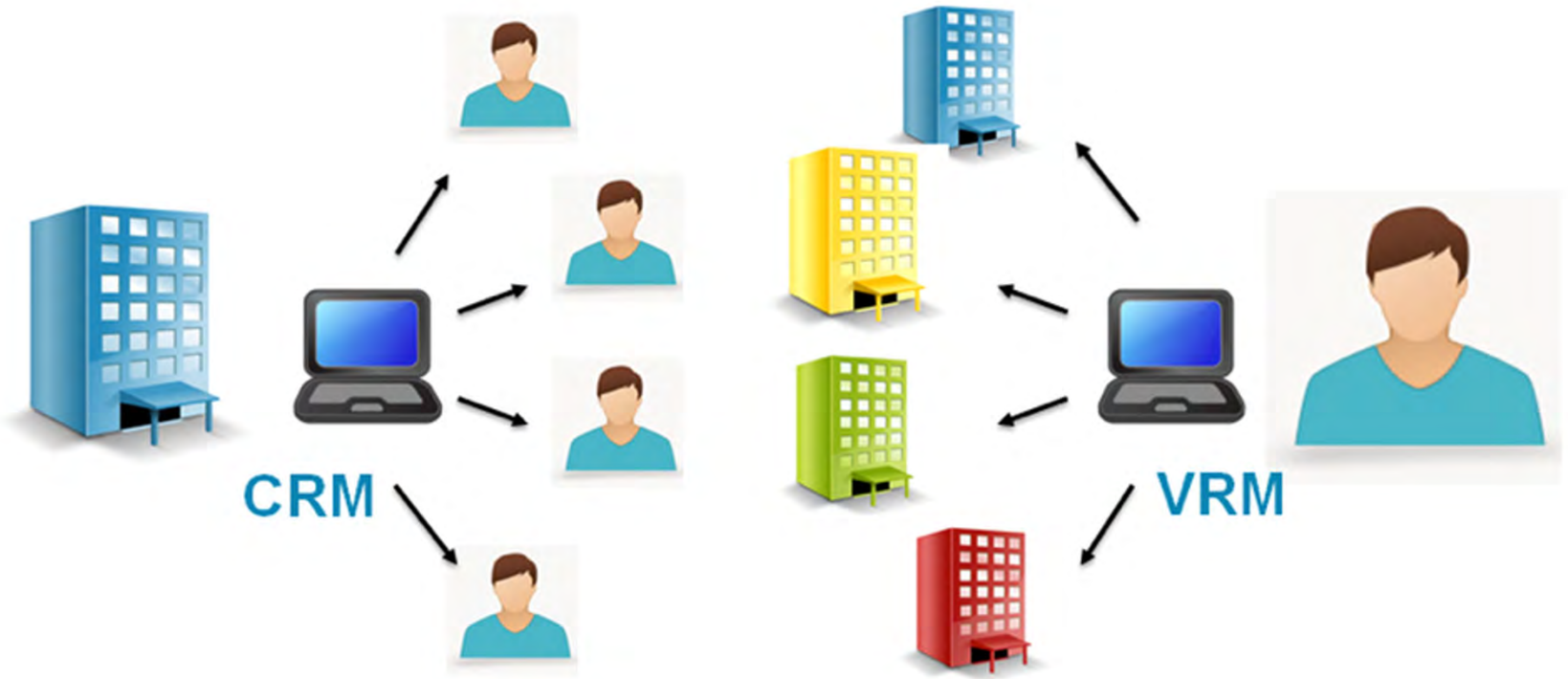
- All known human harms can be assigned to a AAAA threat category
- Atlas is tool for analyzing and mitigating AAAA threats of all types
  - Also used for parsing hybrid threats and analyzing causation chains
- Attack
  - Definition: Intentional acts of individuals and institutions
  - Many of the Atlas risks are currently being weaponized
    - In commerce ”weaponization” is information arbitrage
- Accident
  - Definition: Unintentional acts of individuals and institutions
- Act of nature
  - Definition: Harms not included in Attack or Act of Nature
- Ai/Autonomous systems
  - Definition: Harms caused by AI/Autonomous systems
  - Emerging from inert to independent/discretionary systems. Not yet capable (and legally culpable) for intention and negligence. Currently the liability is with owner or operator of AI/Autonomous system

Humans are information beings.
We define ourselves by our perceptions and expressions in interactions.



Our identity is social.
We act within and among groups.

Hybrid networks link
both organization and individual nodes
via defined interaction edges



We measure and map our relationships to
define our identities and *manage our interaction risks*

How should we measure stakeholder risks and value in highly multi-dimensional relationship networks?

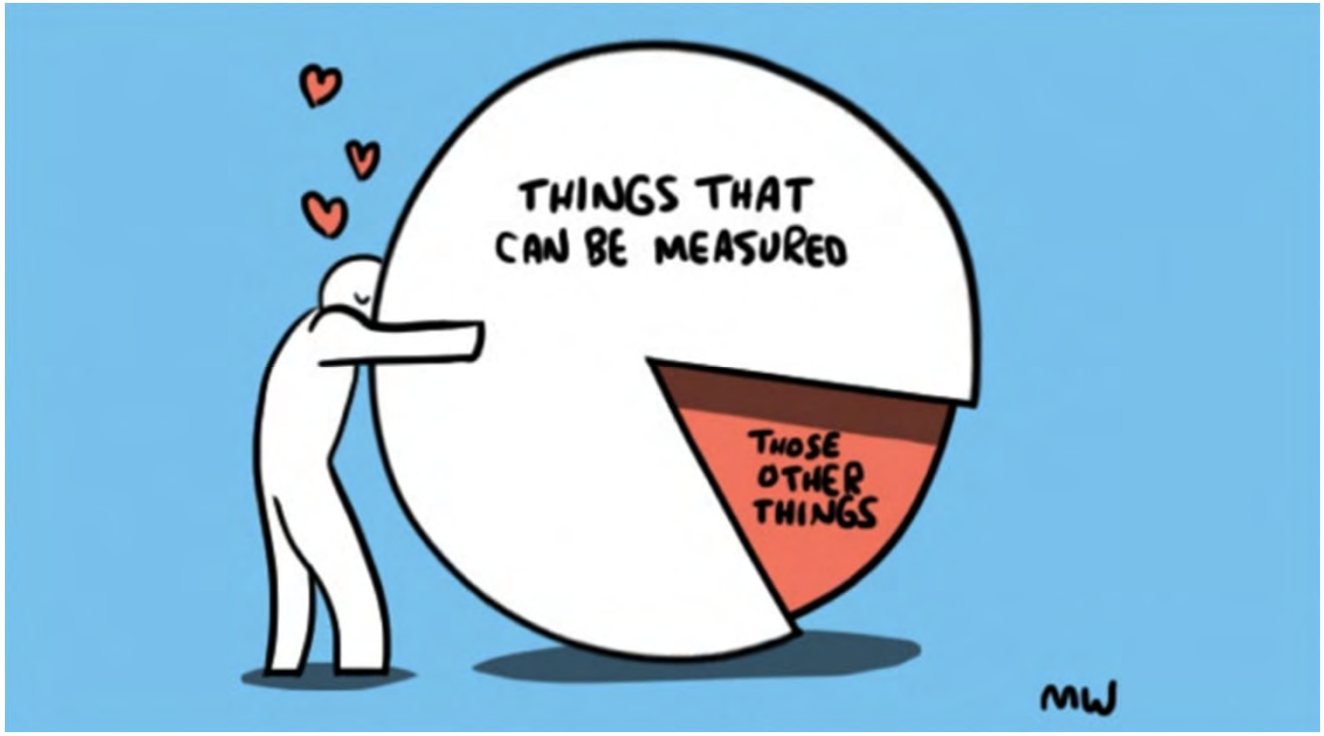
How can we derive stakeholder-defined measurements of risks across multiple contexts?

Stakeholders need reliable and shared *quantitative* metrics to reduce risk

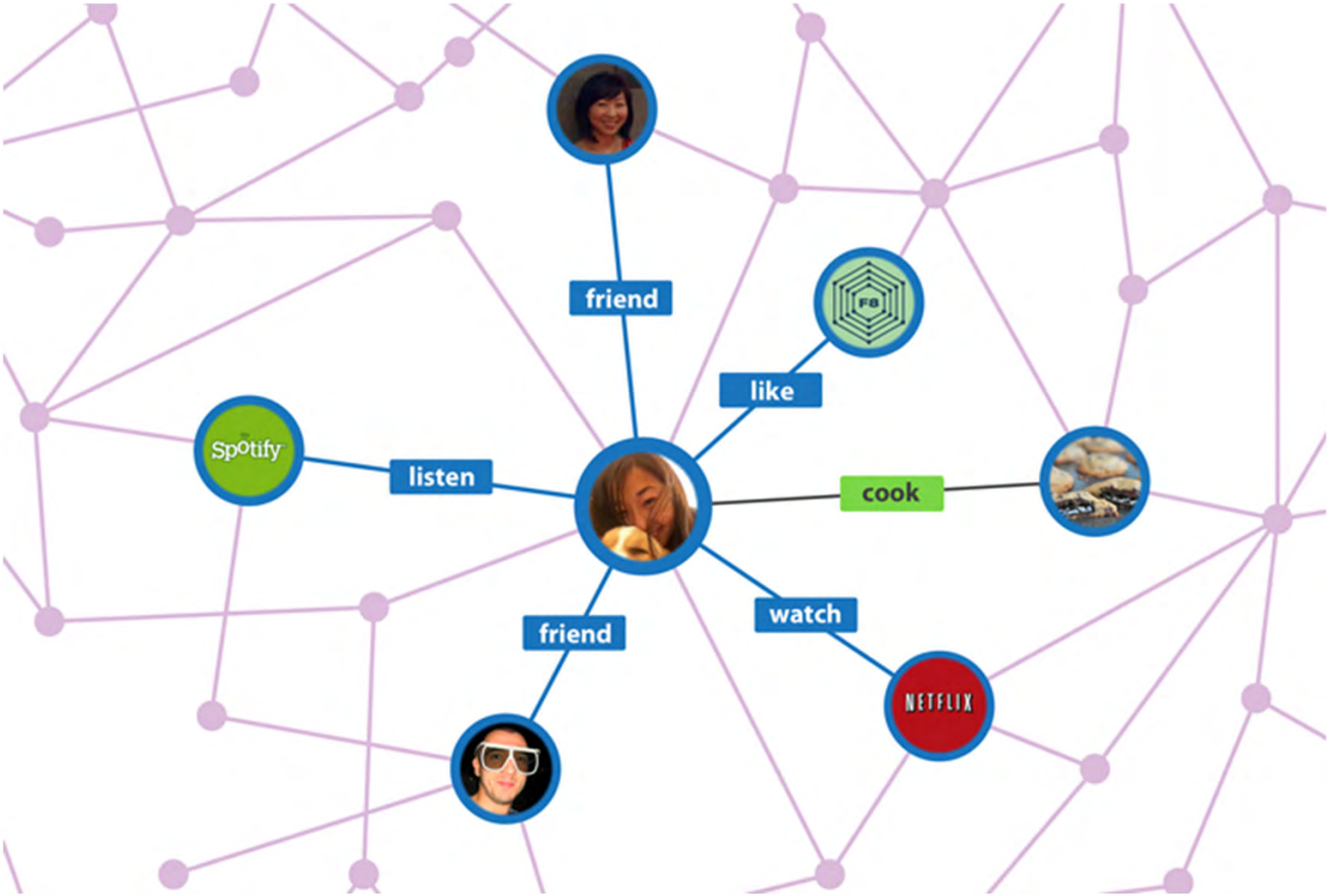
Stakeholders need reliable and shared *qualitative* metrics to reduce risk

So, what specifically should we measure
to reduce emerging non-technical interaction risks?

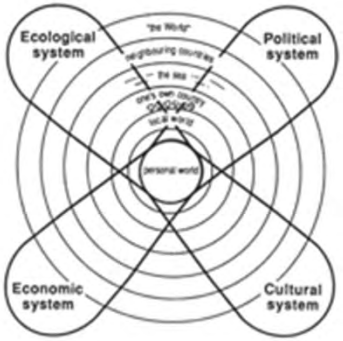
(recalling that “what gets measured gets done”)

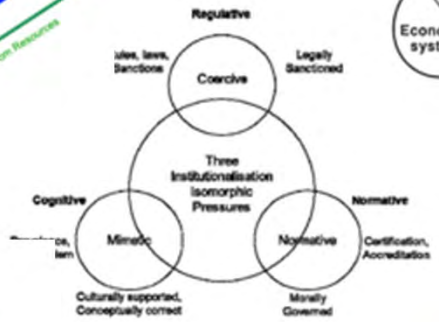


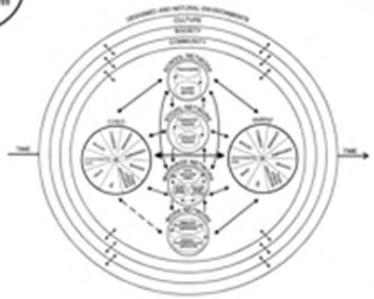
Stakeholders need relationship maps to visualize attribute metrics of BOTH edges AND nodes that together yield “context” where identity, risk, and valuable information all emerge



R&D for new interaction risk maps at Perimeter(s) 2.0 is highly inter-disciplinary







IRRI Perimeter(s) 2.0 Mapping Tool

- **300+ Map Portfolios in the Atlas group metrics based on a type or quality of network nodes or edges**
  - Metrics in each portfolio will be derived from multiple disciplines
    - Atlas helps to bring together interdisciplinary research and development work
  - Map making/metrics visualization will commence as candidate measurements/metrics are derived for given portfolio

- **300+ Map Portfolios are presented in this draft Atlas in random order**
  - Later online wiki format versions of Atlas of Risk Maps will be sortable to match stakeholder relevance
  - Will enable custom presentation of map portfolios in stakeholder-responsive order

- **Entries are color coded in Atlas Table of Contents to indicate relative degree of current metrics development**
  - Blue are "Known Known" Risks
    - Known risks/Known metrics
      - Blue Risks are Known AND some Risk Metrics are available
    - Blue question: what other and/or improved metrics are needed by stakeholders to navigate interactions at their relevant Perimeters(s) 2.0?
  - Green are "Known Unknown" Risks
    - Known risks/Unknown metrics
      - Green Risks are known, but currently available Metrics are indirect, insufficient or not relevant
    - Green question: what new metrics are needed to help inform risk-exposed stakeholders?
  - Red are "Unknown Unknown" Risks
    - Unknown risks/unknown metrics
      - Red Risks are speculative AND no current relevant operating Metrics are available
    - Red question is what is the nature of the risk AND what are relevant metrics

Notes for Atlas Users and "Risk Cartographers"

- **Atlas Focus:** Content of Atlas is currently directed at cybersecurity and information network-related threats, vulnerabilities and risks
  - Particular attention to risks associated with identity management (IM), security and privacy technologies and policies
  - Challenges raised and strategies suggested can also help reduce risk associated with other information technologies.

- **Map Portfolios:** Each numbered "risk map" is really an invitation to create a portfolio of maps/metrics.
  - Maps are currently in form of descriptions of challenges and potential solution structures
  - Example: "Risk map 6 – Individual Bias" anticipates dozens of separate measurements and potential mappings of individual bias-based risks that can affect reliability and predictability of networked information systems
    - See https://en.wikipedia.org/wiki/Bias
  - So, these 400+ "map portfolios" in reality reflect *thousands* of possible measurements of threat, vulnerability and risk that are of potential value to information network stakeholders.

- **Map Portfolio Types:** The initial several hundred map portfolios are grouped by wildly-varying conceptual categories
  - The initial groupings of metrics/maps within each of the map portfolios is intended to invite the consideration of commonalities of measurable qualities among these many different concepts, categories, and abstractions

- **Format:** Each of the hundreds of numbered Map Portfolios is presented on just two slides
  - Slide 1 – "Challenges" initial sketch of the types of risks and concerns that are included in that particular map portfolio
  - Slide 2 – "Candidate Analytical Frameworks/Metrics" suggests some "trial balloons" of possible approaches to identifying and applying measurements that can help to inform the organization and operation of networked information systems.

DRAFT NOTES FOLLOW

NOTES FOR INTRODUCTION: Data is not Information

- Data security is not information security.
- We have focused on data security
- This atlas deals with information security
- The difference is meaning security
  - Same as in crypto
  - Same as in espionage
  - Same as in highlands
  - “Meaning” is critical missing element at present.

Other process themes

- NABC
  - Slide 1=needs, slide 2=approach/practices
- 4 steps of institution construction
  - Practices
    - Plus adoption via rulemaking (legislation) equals:
  - Best practices
    - Plus certification/enforcement (judicial) equals:
  - Standards
    - Plus operational (executive) equals:
  - Institutions
- Note: all second slides present candidate “practices”

Other process themes

- Porter and Ronit 5 stages of rulemaking
- Legal algorithm – (rights - duty-breach-causation-damages-liability-insurance)
- NABC
- BLT
- Tools and Rules
- Data + Meaning =Information