Massachusetts Institute of Technology

Analytics for Cybersecurity of Cyber-Physical Systems

Policy-based Methods for Risk Analysis

Nazli Choucri

Professor of Political Science
Faculty Affiliate, Institute for Data, Systems, & Society (IDSS)

January 15, 2020

Prepared for:
2020 Winter *Science of Security and Privacy* Quarterly Meeting; January 15-16, 2020; Raleigh, North Carolina.

Introduction: Project in Brief

Problem

- Cybersecurity policies & guidelines are in stand-alone *text form.*
- Text encourages "*passive" compliance* – rather than "active" performance.
- Obscures knowledge of risk & creates *opportunity costs*.

Purpose

- *Extend analytics* for CPS cybersecurity to enhance value of guidelines.
- Develop & demonstrate with *Analytics for Cybersecurity of Smart Grid.*
- Create *test-bed* for risk analysis of policy-based assessments.

Approach

- *Multi-methods* for cybersecurity analytics & risk analysis.
- Expected product is *platform* of tools for analytics of cybersecurity.
- Test application to NIST data for *smart grid* of electric power systems.

Policy-based Risk Analysis

Outline & Agenda

1. Introduction – Problem & Methods
2. Create Linked Policy Database (Y1)
3. Construct System Dependency Framework (Y2)
4. Generate Network Model of As-Is System (Y3 Preview)
5. Risk Analysis – Multiple Tasks & Integration (Y4-5 Preview)
6. Contributions to NSA Science of Security and Privacy Program

Policy-based Risk Analysis

Outline & Agenda

1. Introduction – Problem & Methods
2. Create Linked Policy Database (Y1)
3. Construct System Dependency Framework (Y2)
4. Generate Network Model of As-Is System (Y3 Preview)
5. Risk Analysis – Multiple Tasks & Integration (Y4-5 Preview)
6. Contributions to NSA Science of Security and Privacy Program

Problem Defined

Policy guidelines & directives are transmitted in stand-alone text

- Difficult to aggregate or fully understand policy-technology complexities.
- User tends to treat text as if it were a checklist

Much knowledge is generated in process of establishing guidelines.

- Text impedes locating interactions, feedback, specialized views, etc..
- Knowledge of key cybersecurity factors is "lost".

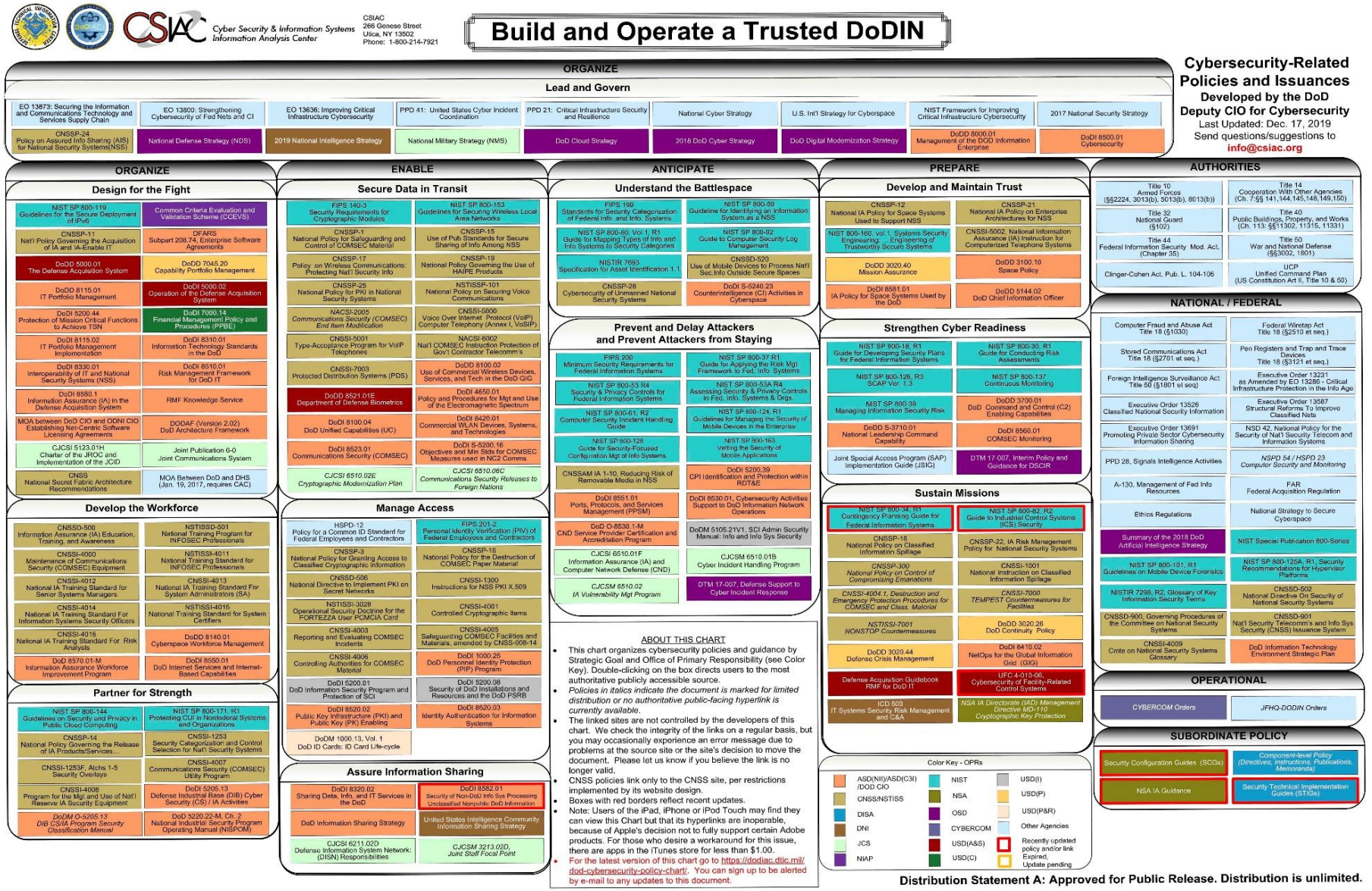
Loss of embedded knowledge creates major opportunity costs.

- It is lost to managers, security experts, & policy analysts who deal with text
- It is lost to all others seeking to increase cybersecurity & reduce risk.

Result:

- Creates undue & unexpected barriers to implementation.
- Impedes operational & pragmatic action.

Cybersecurity Related Policies & Issuances



Support 2020 NDAA* Requirements

Sec. 1648 on Framework to enhance cybersecurity of the United States defense industrial base.

The framework developed pursuant to subsection (a) shall include the following:

(1) **Identification of unified cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements to be imposed on the defense industrial base** for the purpose of assessing the cybersecurity of individual contractors.

(2) Roles and responsibilities of the Under Secretary of Defense for Acquisition and Sustainment, the Under Secretary of Defense for Intelligence and Security, the Chief Information Officer, the Director of the Protecting Critical Technologies Task Force, and the Secretaries of the military departments relating to the following:

(A) Establishing and ensuring **compliance with cybersecurity standards, regulations, and policies.**

(B) **Deconflicting existing cybersecurity standards, regulations, and policies.**

(6) **A plan to provide implementation guidance, education, manuals,** and, as necessary, direct technical support or assistance, to contractors **on matters relating to cybersecurity.**

* **Public Law No: 116-92.**

NDAA on Protection of Critical Infrastructure

2019 John S. McCain National Defense Authorization Act*.

"Pilot program on modeling & simulation in support of military homeland defense operations in connection with cyber-attacks on critical infrastructure." (Sec. 1649)

> *"(A) to **assess defense critical infrastructure vulnerabilities & interdependencies** to improve military resiliency;*
>
> *(B) To **determine** the likely **effectiveness of attacks** described in subsection (a)(1), & **countermeasures, tactics, & tools** supporting responsive military homeland defense operations….";*

2018 National Defense Authorization Act**

"Assessment of Defense Critical Electric Infrastructure." (Sec. 1643)

> "…assess the strategic benefits derived from, & the challenges associated with, isolating military infrastructure from the **national electric grid** & the use of microgrids.''

* Public Law No: 115-232; ** Public Law No: 115-91.

On Importance of Analytics & Metrics

2019 US National Intelligence Strategy*.

"…develop **quantitative methods & data analysis techniques** & tradecraft to improve the IC's **ability to identify, analyze, & forecast changing conditions** & emerging trends across multiple portfolios."

2018 US DoD Cyber Strategy**.

"…The Department will work … to reduce the risk that malicious cyber activity targeting U.S. critical infrastructure ….. We will streamline our **public-private information-sharing mechanisms** & strengthen the resilience & cybersecurity of critical infrastructure networks & systems."

* https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf;
** https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

What is Needed?

Methods to capture full-value of policy texts end-to-end.

1	**Problem**	Recognize that policies & guidelines texts obscure dynamics, feedback, delays, obscure risk & other critical policy features.
2	**Challenge**	Construct “text-to-data” for cybersecurity analyses based on logic & evidence in *sector-specific* & *sector-independent* policy reports
3	**Research Design**	Create “data-to-metrics functions & capabilities to capture “as is” system, vulnerabilities, risks, & manage capability maturity gap.
4	**Expected Products**	Platform for cybersecurity analytics with customized tools to support user needs
5	**Mission Specific**	Provide a generic approach with linked data & method to manage cybersecurity risks for mission-specific requirements

Policy-Focused Approach

High level view.

PURPOSE

1 **Support Presidential Executive Orders & NIST CSF**

"Support the cybersecurity risk management efforts of the owners and operators of the critical infrastructure."

LOGIC

2 **Metricize Existing Policies, Standards, and Guidelines**

Draw on analyses & empirical evidence provided by NIST reports and databases.

PLATFORM

3 **Construct Platform for Cybersecurity Analytics**

Develop tool suite for various analyses of system architecture.

PROCESS

4 **Platform Use for Pragmatic Applications to Cybersecurity**

Establish "ground truth" using platform & tool suite

DECISION SYSTEM

5 **Steps to Identify Targets & Manage Impacts of Damages**

Identify critical gaps, select preferred future system state, & define corrective measures.

Research Design – Operational View

1	2	3	4	5
Create Foundations for Cybersecurity Analytics	**Establish Information Flows in System-wide Operations**	**Explore System Networks & Dependencies in Architecture**	**Apply Interactive Drill-Down Tools for in-Depth Analysis**	**Formalize SoS Policy Analytics & Applications Of Pragmatics**
Identify policy relevant ecosystems.	**Analyze system wide information flows.**	**Examine dependencies of information flows & system architecture.**	**Undertake targeted analysis of system cybersecurity.**	**Conduct & expand SoS for cyber-physical system cybersecurity**
Base Period (Year 1)	**Mid-term (Year 2-3)**	**Mid-Long term (Year 3-4)**		**Long-term (>Year 4)**
1. **Formalize rules** to extract data from text. 2. **Identify missing pieces** for policy implementation. 3. **Design internally** consistent structure to organize & metricize, critical texts	1. **Create dependency structure matrix** (DSM) of CPS by first level information dependencies. 2. **Cluster & partition** DSM to reveal "hidden features".	1. **Generate** visual representations of information flows with graph theory & network methods. 2. **Use visuals** to identify critical control points & distinguish human vs. technical functions.	1. **Provide interactive** tools for on-demand targeted analysis. 2. **Examine functions & security** of nodes & assess vulnerabilities. 3. **Explore resilience of** system whole and parts.	1. **Use Live-Virtual-Constructive** environment for evaluation & validation. 2. **Formalize properties of disturbances** to assess potential system impacts.

Application for Risk Analysis

- **Linked Database**
  Text to Data (Y1)
- **Dependency Framework**
  Data to Metrics (ongoing Y2)
- **Metrics to Model**
  Network System (planned Y3)
- **Risk Analysis**
  Mapping Parameters (options Y4-5)

Policy-based Risk Analysis

Outline & Agenda

1. Introduction – Problem & Methods
2. **Create Linked Policy Database (Y1)**
3. Construct System Dependency Framework (Y2)
4. Generate Network Model of As-Is System (Y3 Preview)
5. Risk Analysis – Multiple Tasks & Integration (Y4-5 Preview)
6. Contributions to NSA Science of Security and Privacy Program

Cybersecurity Policy Ecosystem for Smart Grid CPS

① NIST CSF*

Framework for Improving Critical Infrastructure Cybersecurity

- Functions
  - Categories & Sub-Categories
- Mapping of Security Requirements

② NIST SP 800-37 Rev. 1*

Guide for Applying the Risk Management Framework to Federal Information Systems

- NIST Risk Management Framework

③ NIST SP 800-53 Rev. 4*

Security & Privacy Controls for Federal Information Systems & Organizations

- Data on 18 families of Security Controls,
  - Controls
  - Supplemental Guidance
  - Control Enhancements
  - Priority & Baseline Allocation

④ NISTIR 7628r1#

Guidelines for Smart Grid Cybersecurity

- Smart Grid Conceptual Model
- Security Objectives
- Impact level for Security Objectives
- Security Requirements
- Vulnerability Classes

⑤ NIST SP 1108 Rev. 3#

NIST Framework & Roadmap for Smart Grid Interoperability Standards, Release 3.0

- "Smart grids are viewed from the perspective of cyber-physical systems (CPS)

⑥ NERC CIPs

North American Electric Reliability Corporation critical infrastructure protection

- Set of requirements designed to secure assets required for operating North America's bulk electric system.

⑦ NIST NVD*

National Vulnerability Database

- Standards based vulnerability management data represented using the Security Content Automation Protocol

⑧ DoE/DHS C2M2 Model#

Cybersecurity Capability Maturity Model

- Implementation & management of cybersecurity practices for information technology & operational technology assets & their environments

⑨ NIST CVSS*

Common Vulnerability Scoring System

- Open framework for communicating the characteristics & impacts of IT vulnerabilities
- Calculating the severity of vulnerabilities discovered on one's systems

*** Sector-All**

 # Sector-specific (electricity smart grid)

Function of Linked Data Base

- **Linked Data base is a necessary condition for data-to-metrics**
- **Data-to- metrics is foundation for framework**
- **Framework is the basis for system model**

Linkage data base includes all the relevant elements of system "as is" as well as all variables reflecting system vulnerabilities and correctives

Multi-dimensional Linked Data Base: Scale & Scope

Over 15 interdependent dimensions –smart grid application

- Spread over multiple dimensions in over 600+ pages
- Current text burdens to reader to extract information.

Smart Grid CPS	Count
Core Elements	
Domain	7
Actor	47
Logical Interface between Actors	122
Logical Interface Categories	22
Security Objectives for Smart Grid	
Types {Confidentiality, Integrity, Availability}	3
Impact Level {Low, Moderate, High}	3
Security Requirements identified	180
Families of Security Requirements	19
Types of Security Requirements	3

Smart Grid CPS	Count
Vulnerability	
Types of Logical Interface	53
Categories of Vulnerabilities	4

NIST Cybersecurity Framework	Count
Core Data	
Functions	5
Categories	23
Sub-Categories	414

Distributed Linked Policy Database

Documents for text-to-data utuilized in different research phases

	1 Create Foundations for Cybersecurity Analytics	2 Establish Information Flows in System-wide Operations	3 Explore System Networks & Dependencies in Architecture	4 Apply Interactive Drill-Down Tools for in-Depth Analysis	5 Formalize SoS Policy Analytics & Applications Of Pragmatics
2017-2019 Executive Orders 2017-2019 NDAA 2018-2019 Security Strategies	Identify National Security Requirements & Mandates				Revisit National Security Requirements & Mandates
① NIST CSF*	Cybersecurity Framework	Framework Functions		Framework Functions Applicability	Enterprise Cybersecurity Profile
② NIST SP 800-37 Rev. 1*					Enterprise Risk Management
③ NIST SP 800-53 Rev. 4*				Security & Privacy Controls	
④ NISTIR 7628r1#		Logical Interface, Vulnerabilities Types, & Impacts on Security Objectives		Security Requirements	
⑤ NIST SP 1108 Rev. 3 #		Smart Grid Reference Model			
⑥ NERC CIPs#		Federal Compliance Requirements			
⑦ NIST NVD*				Vulnerability Identification	
⑧ DoE/DHS C2M2 Model#					Smart Grid Cyber Capability Maturity
⑨ NIST CVSS*				Impact & Vulnerability Quantification	

* Sector-All # Sector-Specific (Electricity smart grid)

***Note*: Planned project <u>phase-based</u> uses of "Cybersecurity Document Ecosystem for Smart Grid CPS" ,slide 16. Circled numbers identify document .**

Policy-based Risk Analysis

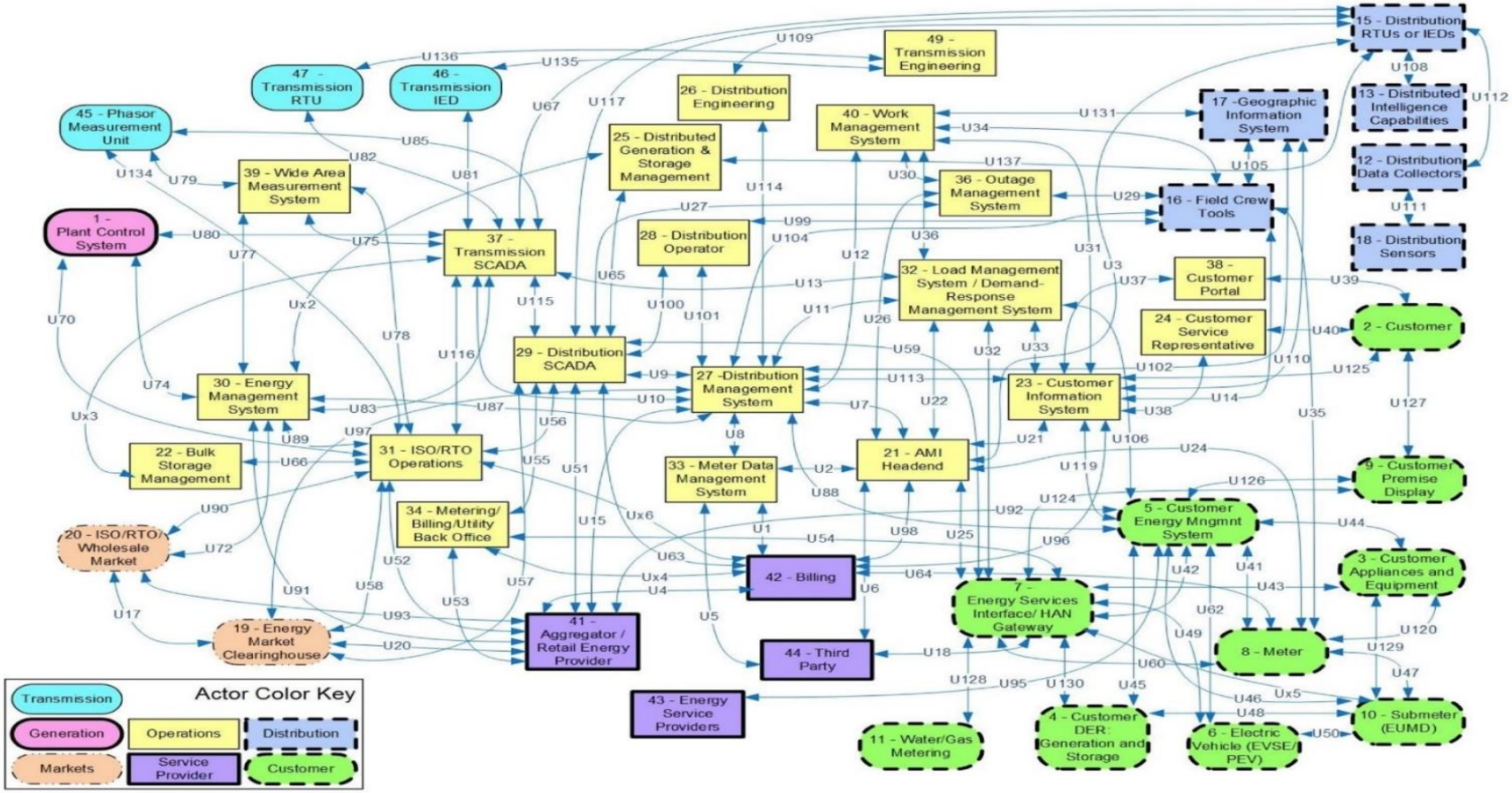
Outline & Agenda

1. Introduction – Problem & Methods
2. Create Linked Policy Database (Y1)
3. **Construct System Dependency Framework** (Y2)
4. Generate Network Model of As-Is System (Y3 Preview)
5. Risk Analysis – Multiple Tasks & Integration (Y4-5 Preview)
6. Contributions to NSA Science of Security and Privacy Program

Source of System Dependency Framework

NIST Smart Grid Reference Model – "As-Is"

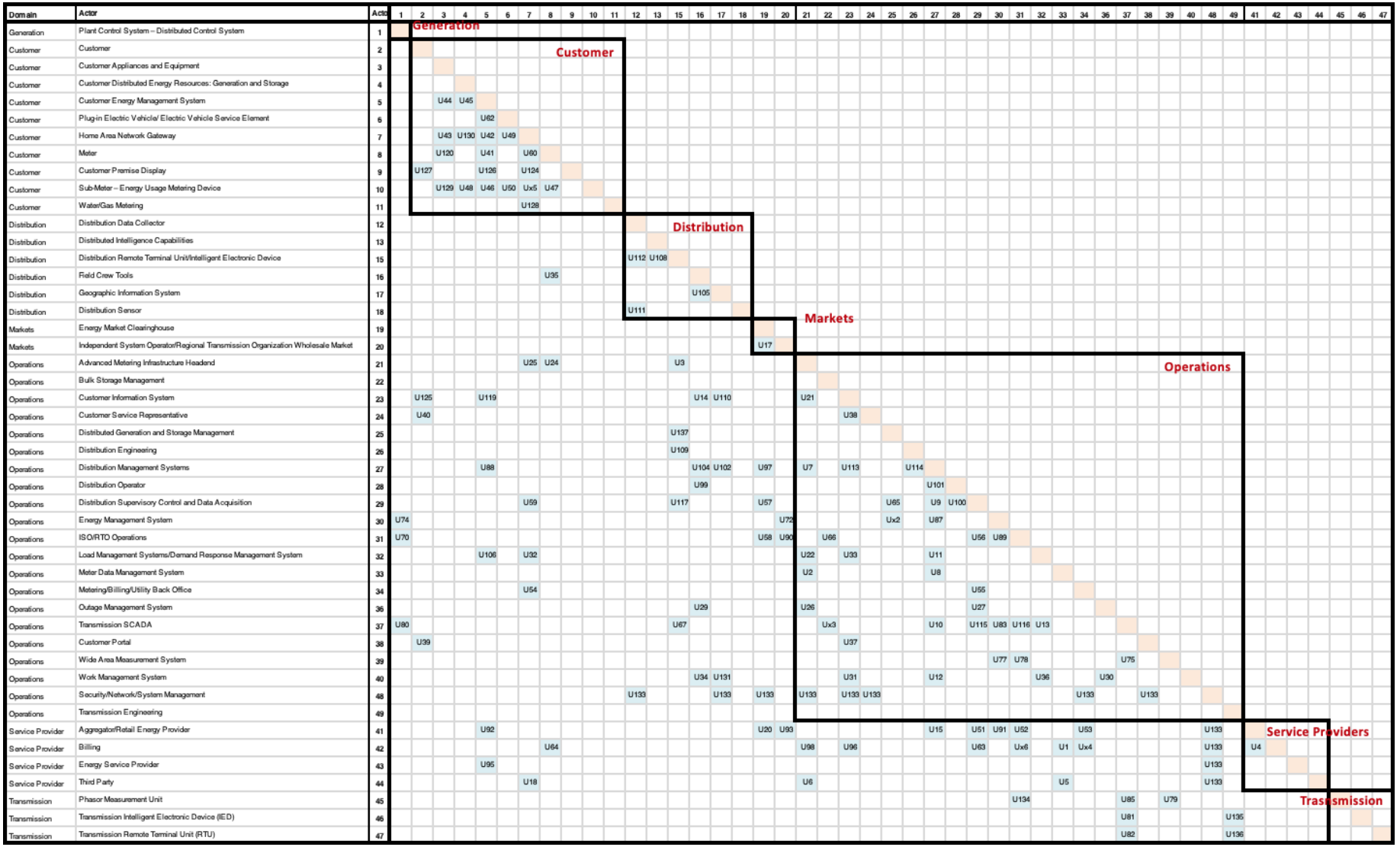
"Reflects the consensus-based process the Smart Grid Interoperability Panel (SGIP) uses to coordinate and accelerate the development of smart grid standards."*



*Source: NIST. "*Guidelines for Smart Grid Cybersecurity-Volume 1*," NISTIR 7628 Revision I, September, 2014. p. x.
Image Source: NIST. "Guidelines for Smart Grid Cybersecurity-Volume 1," NISTIR 7628 Revision I, September, 2014; doi: NIST.IR.7628r1, p17.

Result: Base Framework of "As-Is" Smart Grid System.

Design Structure Matrix (DSM) for Actors, Domains, & Logical Interfaces.



Domain	Actor	Acts	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	36	37	38	39	40	48	49	41	42	43	44	45	46	47
Generation	Plant Control System – Distributed Control System	1																																															
Customer	Customer	2																																															
Customer	Customer Appliances and Equipment	3																																															
Customer	Customer Distributed Energy Resources: Generation and Storage	4																																														
Customer	Customer Energy Management System	5			U44	U45																																										
Customer	Plug-in Electric Vehicle/ Electric Vehicle Service Element	6					U62																																									
Customer	Home Area Network Gateway	7			U43	U130	U42	U49																																								
Customer	Meter	8			U120		U41		U60																																								
Customer	Customer Premise Display	9		U127			U126		U124																																								
Customer	Sub-Meter – Energy Usage Metering Device	10			U129	U48	U46	U50	Ux5	U47																																							
Customer	Water/Gas Metering	11							U128																																								
Distribution	Distribution Data Collector	12																																															
Distribution	Distributed Intelligance Capabilities	13																																															
Distribution	Distribution Remote Terminal Unit/Intelligent Electronic Device	15												U112	U108																																		
Distribution	Field Crew Tools	16								U35																																							
Distribution	Geographic Information System	17															U105																																
Distribution	Distribution Sensor	18												U111																																			
Markets	Energy Market Clearinghouse	19																																															
Markets	Independent System Operator/Regional Transmission Organization Wholesale Market	20																		U17																													
Operations	Advanced Metering Infrastructure Headend	21							U25	U24						U3																																
Operations	Bulk Storage Management	22																																															
Operations	Customer Information System	23		U125			U119										U14	U110				U21																										
Operations	Customer Service Representative	24		U40																				U38																									
Operations	Distributed Generation and Storage Management	25														U137																																
Operations	Distribution Engineering	26														U109																																
Operations	Distribution Management Systems	27					U88										U104	U102		U97		U7		U113			U114																				
Operations	Distribution Operator	28															U99											U101																				
Operations	Distribution Supervisory Control and Data Acquisition	29							U59							U117				U57						U65		U9	U100																		
Operations	Energy Management System	30	U74																		U72					Ux2		U87																			
Operations	ISO/RTO Operations	31	U70																	U58	U90		U66							U56	U89																
Operations	Load Management Systems/Demand Response Management System	32					U106		U32													U22		U33			U11																				
Operations	Meter Data Management System	33																				U2					U8																				
Operations	Metering/Billing/Utility Back Office	34							U54																					U55																	
Operations	Outage Management System	36															U29					U26								U27																	
Operations	Transmission SCADA	37	U80													U67							Ux3				U10		U115	U83	U116	U13															
Operations	Customer Portal	38		U39																				U37																								
Operations	Wide Area Measurement System	39																													U77	U78				U75											
Operations	Work Management System	40															U34	U131						U31				U12					U96			U30										
Operations	Security/Network/System Management	48												U133				U133		U133		U133		U133	U133										U133		U133									
Operations	Transmission Engineering	49																																														
Service Provider	Aggregator/Retail Energy Provider	41					U92													U20	U93							U15		U51	U91	U52		U53							U133						
Service Provider	Billing	42								U64												U98		U96						U63		Ux6		U1	Ux4						U133	U4					
Service Provider	Energy Service Provider	43					U95																																		U133						
Service Provider	Third Party	44							U18													U6												U5							U133						
Transmission	Phasor Measurement Unit	45																													U134					U85		U79								
Transmission	Transmission Intelligent Electronic Device (IED)	46																																		U81					U135					
Transmission	Transmission Remote Terminal Unit (RTU)	47																																		U82					U136					

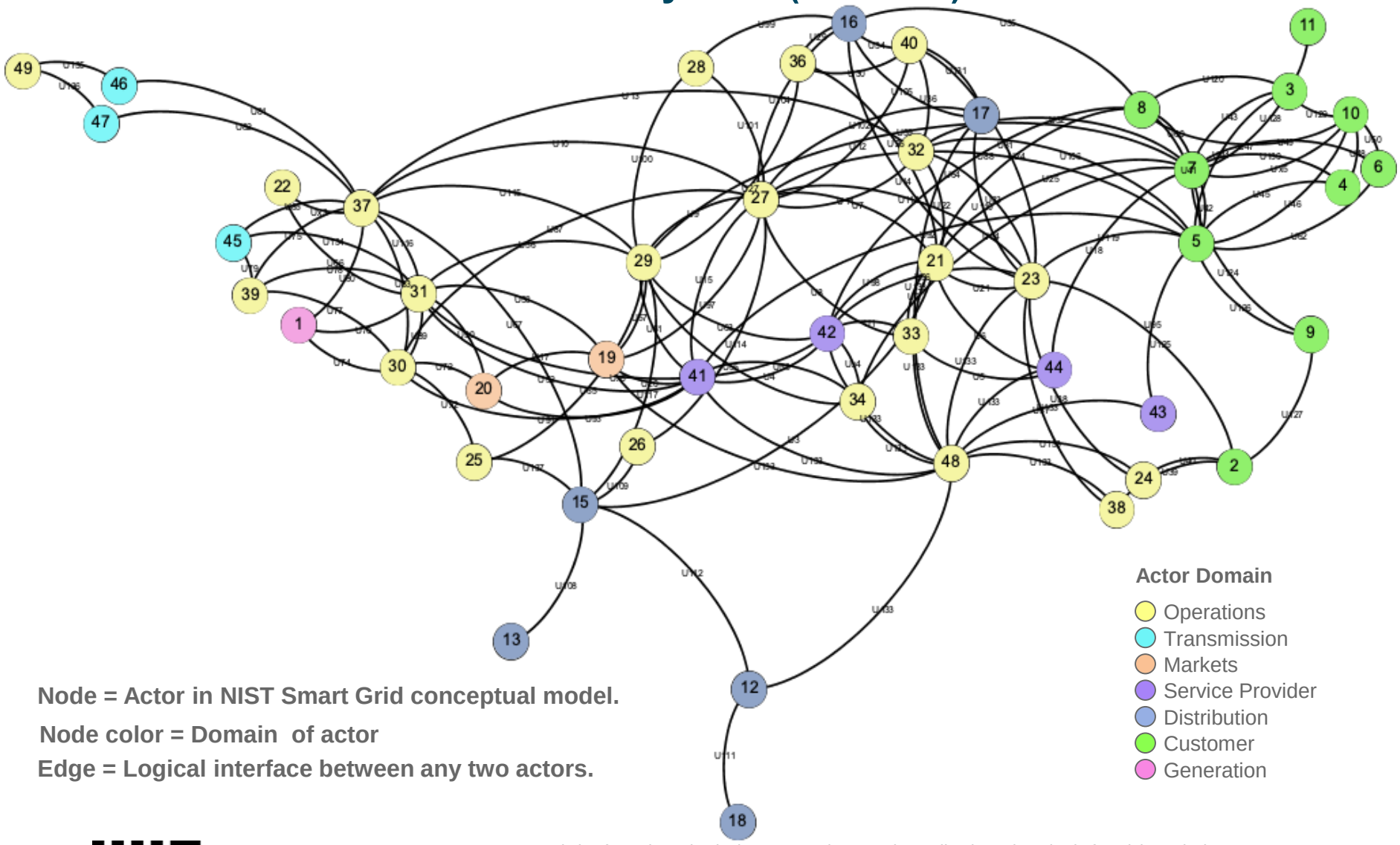
Policy-based Risk Analysis

Outline & Agenda

1. Introduction – Problem & Methods
2. Create Linked Policy Database (Y1)
3. Construct System Dependency Framework (Y2)
4. **Generate Network Model of As-Is System (Y3 Preview)**
5. Risk Analysis – Multiple Tasks & Integration (Y4-5 Preview)
6. Contributions to NSA Science of Security and Privacy Program

Model of As-Is Smart Grid System

Network view of DSM for “as-is” system (Preview).



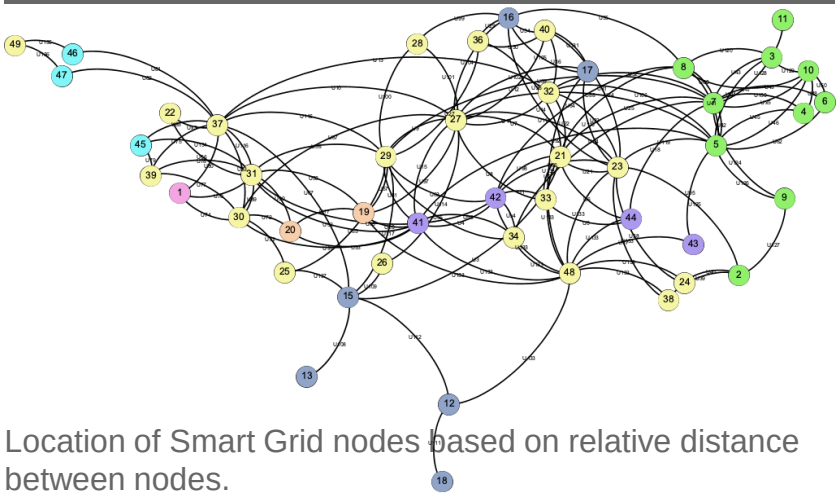
Node = Actor in NIST Smart Grid conceptual model.

Node color = Domain of actor

Edge = Logical interface between any two actors.

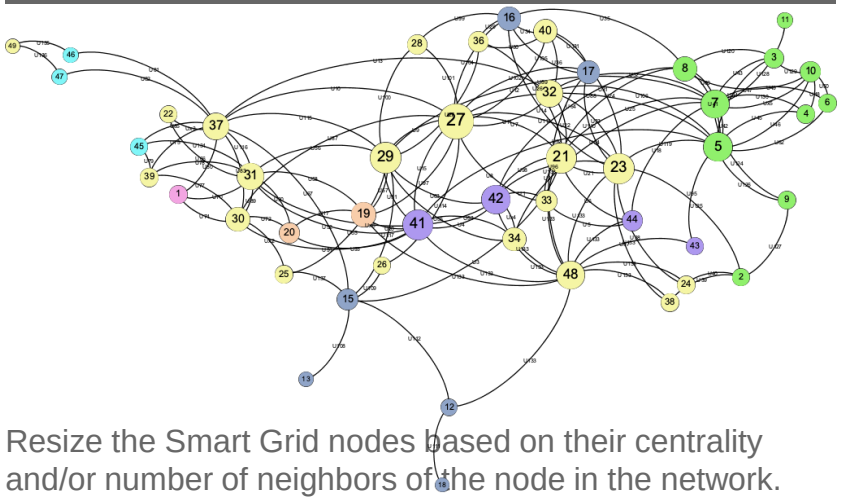
Exploratory Analysis: User Defined Views (examples)

1 Core Network Map



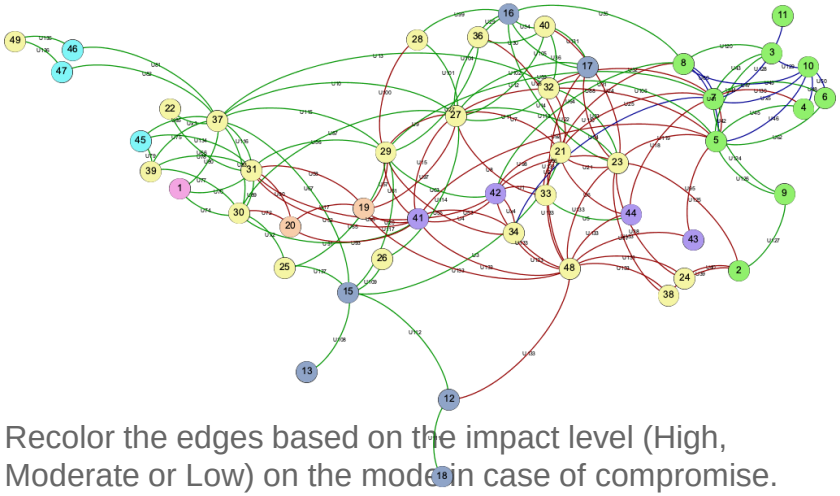
Location of Smart Grid nodes based on relative distance between nodes.

2 Resize the Nodes



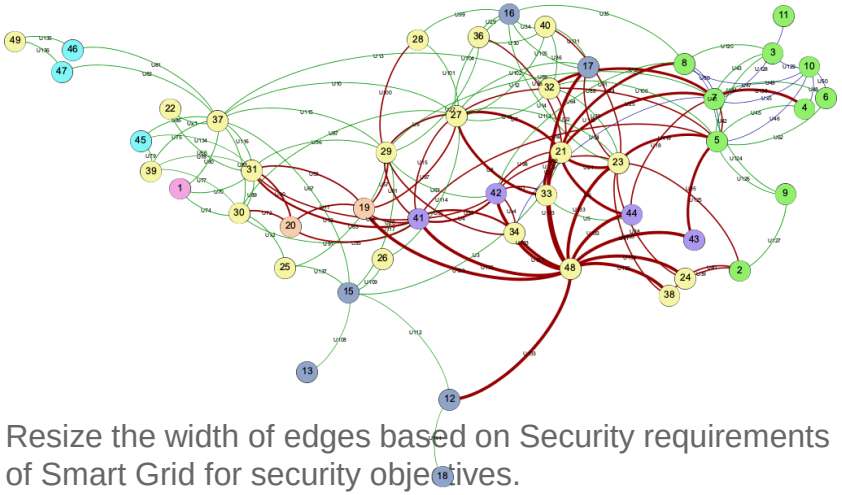
Resize the Smart Grid nodes based on their centrality and/or number of neighbors of the node in the network.

3 Recolour the Edges



Recolor the edges based on the impact level (High, Moderate or Low) on the mode in case of compromise.

4 Resize the Edges



Resize the width of edges based on Security requirements of Smart Grid for security objectives.

Policy-based Risk Analysis

Outline and Agenda

1. Introduction – Problem & Methods
2. Create Linked Policy Database (Y1)
3. Construct System Dependency Framework (Y2)
4. Generate Network Model of As-Is System (Y3 Preview)
5. **Risk Analysis – Multiple Tasks & Integration** (Y4-5 Preview)
6. Contributions to NSA Science of Security and Privacy Program

Steps for Risk Analysis
Anchored in Network Model

(1) Map Risk Properties, Impact Levels, & Vulnerabilities.

(2) Apply NIST CVSS Logic for Risk Aggregation.

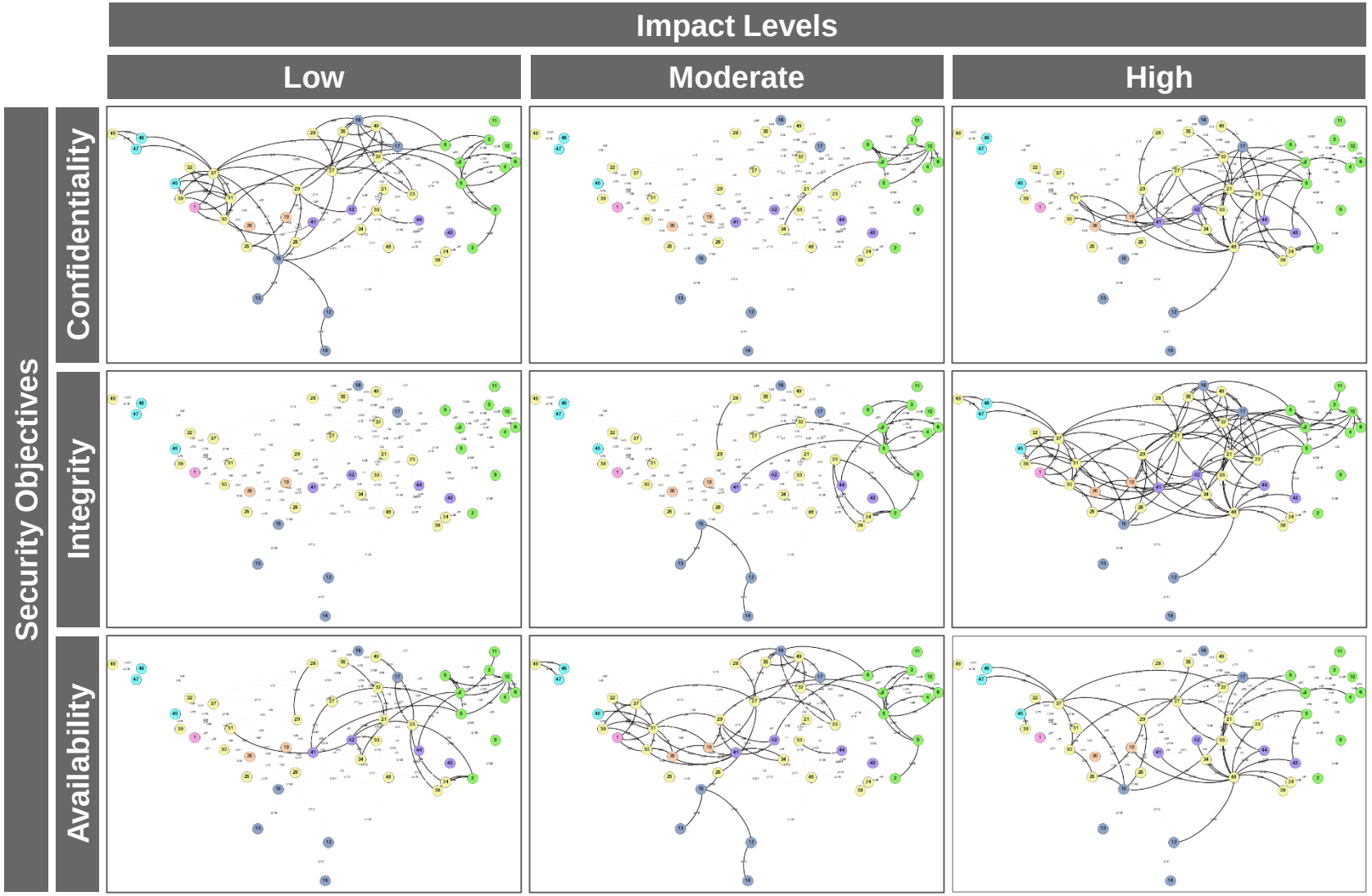
(3) Integrate System-wide Results per NIST CVSS.

(4) Assess Risk Results – for System Parts or Whole.

(5) Tailored Risk Management Analysis.

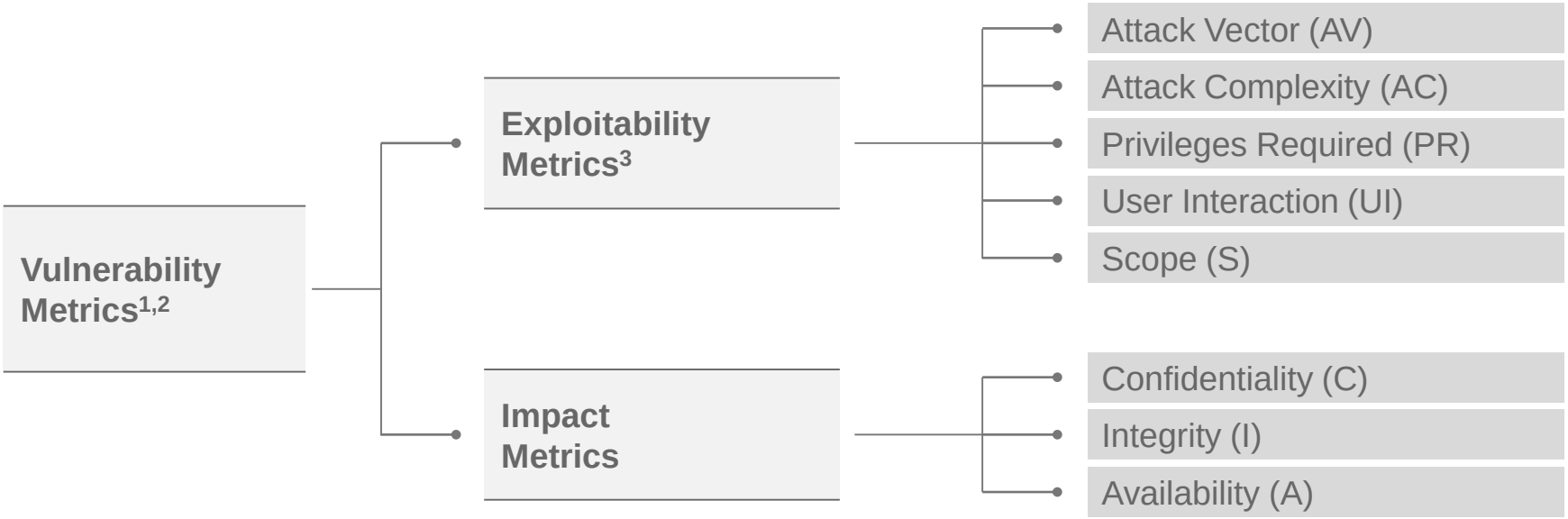
(1) Map Risk Properties, Impact Levels, Vulnerabilities

Based on criticality of information for worst-case system impact.



(2) Apply CVSS Logic for Risk Aggregation

Produce a numerical score of severity (Impact) & exploitability for NIST qualitative assessments of risk.



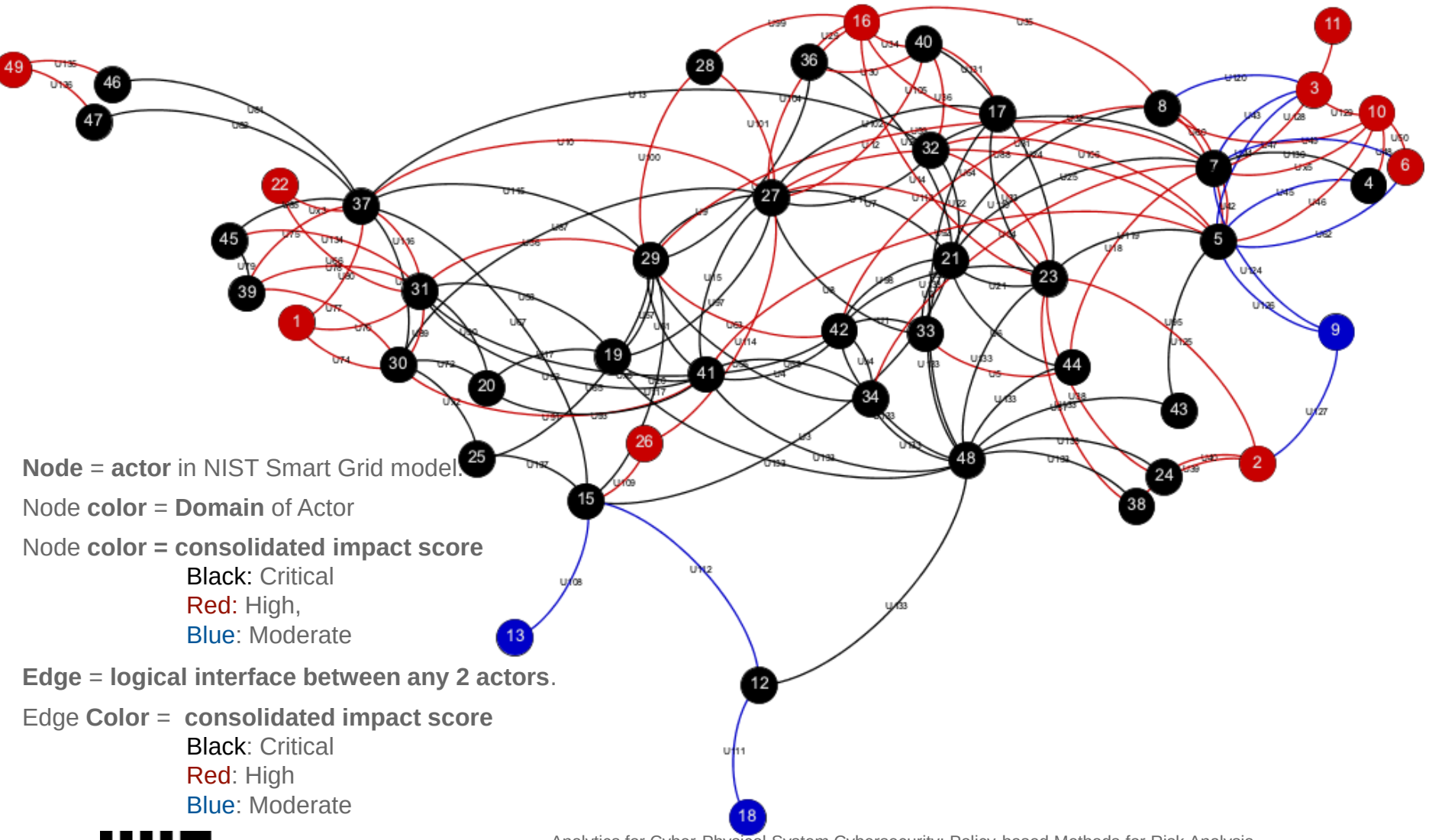
1. See https://www.first.org/cvss/calculator/3.1 to calculate based Impact and Exploitability Scores.
2. Temporal and Environmental Scores are not included in this study.
3. for quantification of enterprise specific vulnerabilities

Impact metrics reflect direct consequence of a successful exploit & represent consequence to target that suffers the impact.

Exploitability metrics reflect ease & technical means by which vulnerability can be exploited.

(3) Integration: Consolidated Impact Score

Integrate system-wide results (from Step 1) per NIST CVSS (in Step 2)



Node = **actor** in NIST Smart Grid model.

Node **color** = **Domain** of Actor

Node **color = consolidated impact score**

Black: Critical
Red: High,
Blue: Moderate

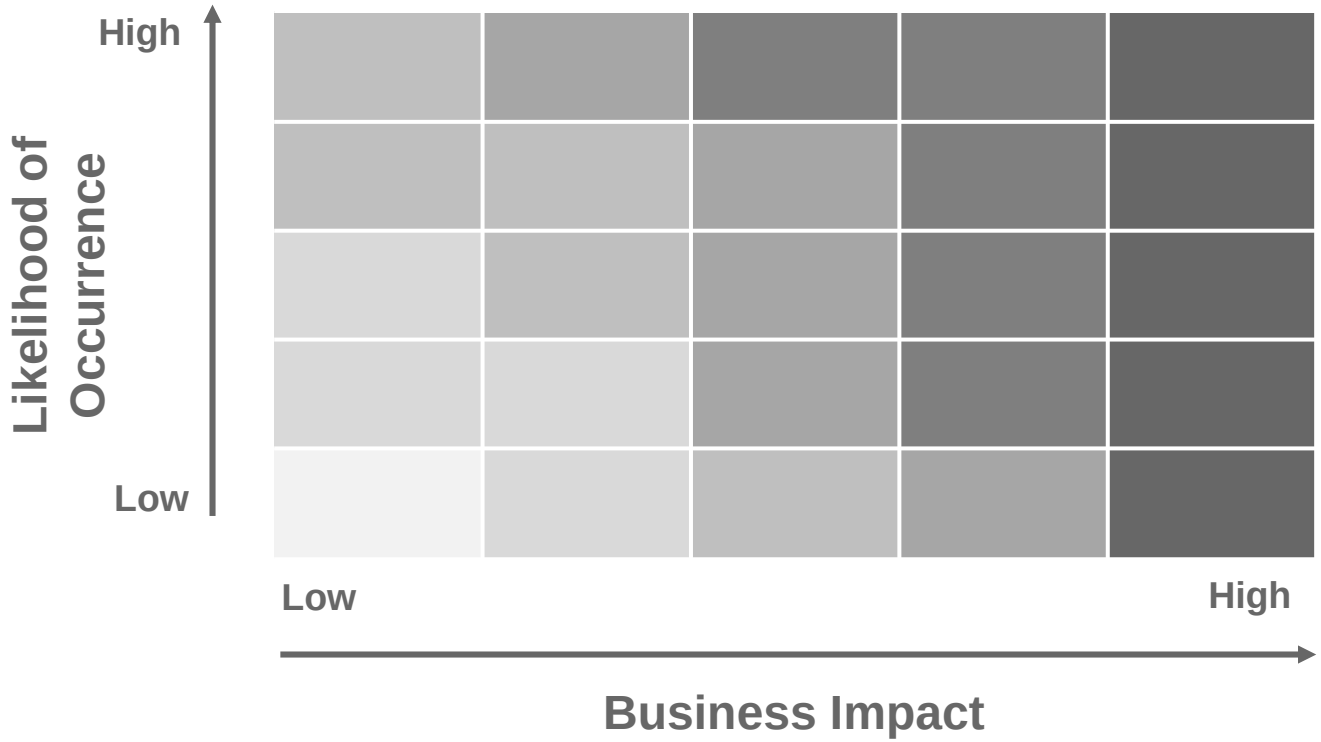
Edge = **logical interface between any 2 actors**.

Edge **Color** = **consolidated impact score**

Black: Critical
Red: High
Blue: Moderate

(4) Assess Risk Results–for System Parts or Whole

NIST framework to transform CVSS metrics into business objectives & to situate individual risks on risk matrix



Likelihood of occurrence based on:

- NIST National Vulnerability Database
- Historic data/ Internal Assessments
- Engineering Risk Benefit Analysis

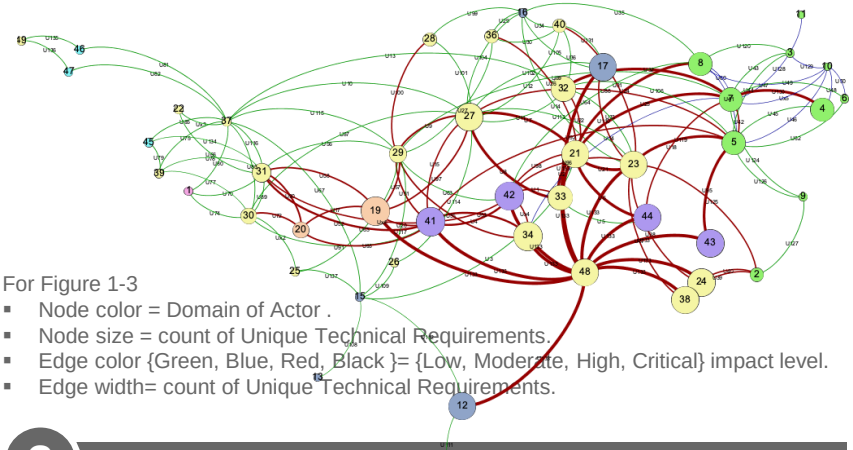
Impact due to system compromise:

- Compromised National Security
- Loss of Business, and/or Loss of Sales
- Cleanup Costs

(5) Tailored Risk Management Guidance (example)

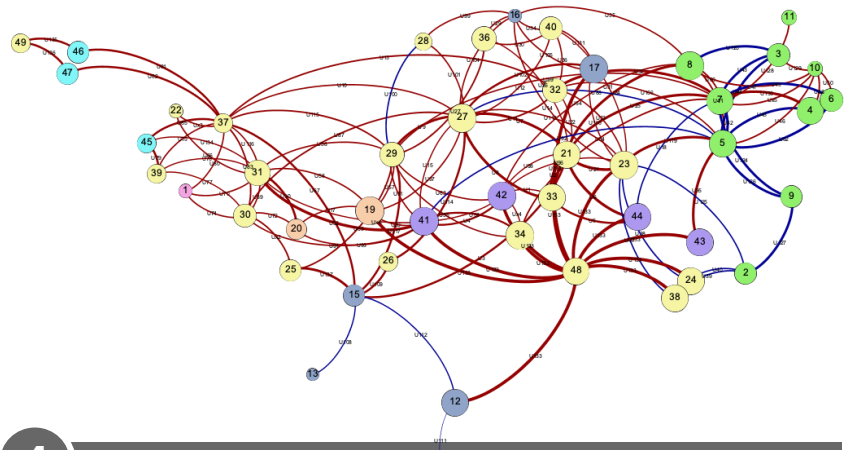
Select baseline security controls from NIST SP 800:53 Rev. 4.

1 *Confidentiality* Security Objective

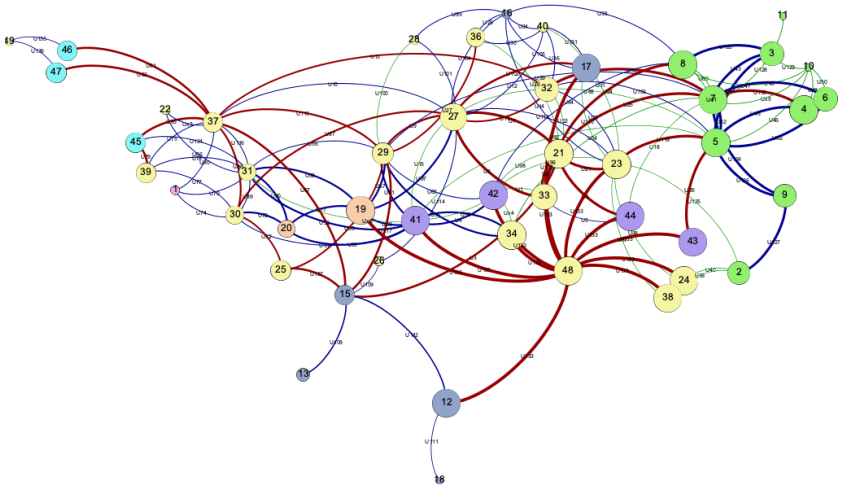


For Figure 1-3
- Node color = Domain of Actor .
- Node size = count of Unique Technical Requirements.
- Edge color {Green, Blue, Red, Black }= {Low, Moderate, High, Critical} impact level.
- Edge width= count of Unique Technical Requirements.

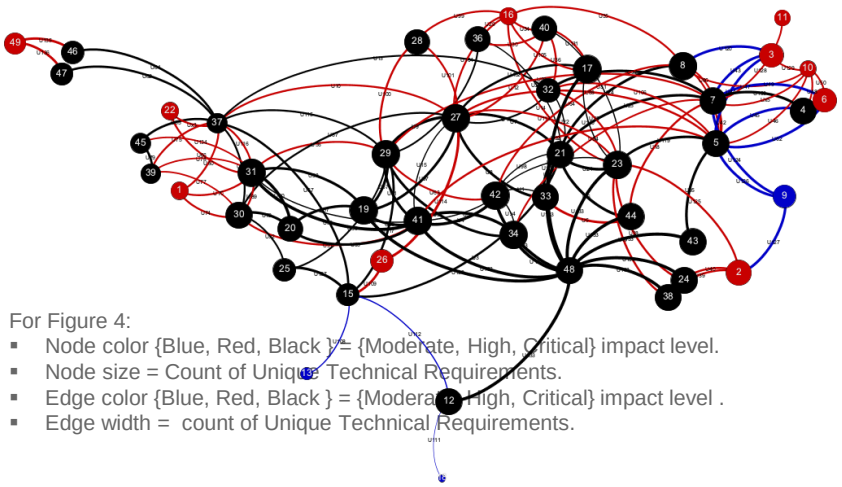
2 *Integrity* Security Objective



3 *Availability* Security Objective



4 *Cumulative* View



For Figure 4:
- Node color {Blue, Red, Black } = {Moderate, High, Critical} impact level.
- Node size = Count of Unique Technical Requirements.
- Edge color {Blue, Red, Black } = {Moderate, High, Critical} impact level .
- Edge width = count of Unique Technical Requirements.

Policy-based Risk Analysis

Outline & Agenda

1. Introduction – Problem & Methods
2. Create Linked Policy Database (Y1)
3. Construct System Dependency Framework (Y 2)
4. Generate Network Model of As-Is System (Y3 Preview)
5. Risk Analysis – Multiple Tasks & Integration (Y4-5 Preview)
6. **Contributions to NSA *Science of Security and Privacy Program***

Relevance of our Linkage Approach to Cyber Security Framework & Privacy Framework

CSF & PF share common features:

Not a one-size-fits-all approach to managing cybersecurity risk

- No **one-solution-full-guidelines** covering all industries & companies.
- No ontological **structure or processes** provide for mapping Frameworks to specific industry activities.

No imposed profile templates & allow for flexibility in implementation

- An entity may select or **tailor** the Privacy/Cybersecurity Framework's **Functions, Categories, & Subcategories** to its specific needs.
- An entity may choose to have multiple Profiles for specific systems, products, services, or categories of individuals (e.g., employees, customers).

Result:

Application is left to implementing entity. Linkage mechanisms are needed to connect risks, vulnerabilities, impacts etc. of (a) industry or system properties to (b) Framework features.

Relevance to US DoD

Sec. 1641 of 2020 NDAA on "role of Chief Information Officer in improving enterprise-wide cybersecurity."

"(a) IN GENERAL.—

In carrying out the responsibilities established in section 142 of title 10, United States Code, the Chief Information Officer of the Department of Defense shall, to the maximum extent practicable, **ensure that the cybersecurity programs and capabilities of the Department**—

(1) **fit into an enterprise-wide cybersecurity architecture**;

(2) are maximally **interoperable with each other**, including those programs and capabilities deployed by the components of the Department;

(3) **enhance enterprise-level visibility and responsiveness to threats**; and

(4) are developed, procured, instituted, and managed in a cost-efficient manner, exploiting economies of scale and enterprise-wide services and **discouraging unnecessary customization and piecemeal acquisition."**

* **Public Law No: 116-92**.

Contributions to *Science of Security* Program

Policy-Bases Analytics

Provide replicable methods to:

- Deconflict existing cybersecurity standards, regulations, and policies.
- Enhance enterprise-level visibility and responsiveness to threats.

Education

Demonstrate multi-methods for cybersecurity policy of complex systems:

- Provide “end-to-end” road map & document all applications step-by step.
- Explore advantages & constraints of multi-method approach.

Outreach

Connect to diverse communities.

- Envisage e-Lab for cybersecurity
- Ongoing discussions with NIST, Air Force and NSA personnel for possible extensions.

Relevance to *Science of Security* Hard Problems

Hard problem is policy-governed secure collaboration (applied to smart grid) & relation to other hard problems

1	**Resilient Architectures**	**Generate linked database of operations, standards & guidelines** ▪ Design approach database to align enterprise functions to generic system-properties. ▪ Provide system-of-system database of critical documents.
2	**Scalability & Composability**	**Enable "full package" for different risk types, levels & time scales.** ▪ Provide methods with tools to deep dive into database for customized insights & analyses. ▪ Create decision supports with methods to identify, analyse & record risk & its responses.
3	**Policy Governed Secure Collaboration**	**Conduct targeted enterprise-relevant analysis** ▪ Address system-level complexity & heterogeneity due to policy landscapes. ▪ Identify points of power & control created by design decisions & policies.
4	**Security-Metrics-Driven Evaluation, Design, Development & Deployment**	**Identify & implement operational responses & actions.** ▪ Use metrics to assess, deploy & develop capabilities – People, Policy & Procedures. ▪ Implement cybersecurity framework– Executive, Business/Process, Operations level.
5	**Understanding & Accounting for Human Behaviour**	**Establish independent monitoring of key enterprise functions.** ▪ Timely, uniform & accurate accounting of business processes. ▪ Identify potential violations of policy directives & systematically prevent occurrences.

How Can We Collaborate?

Next steps?

- Explore further options for cybersecurity risk management methodology as required in 2020 NDAA.
- Initiate SoS cybersecurity risk management project with support of industry or business partner.

Key Questions

- Do you see relevance of our approach for your sector, system, or enterprise?
- How can we jointly contribute to Science of Security?
- What can we do that can be of mutual interest & benefit?

Contact details

Nazli Choucri

Professor of Political Science

+1 (617) 253 - 6198; nchoucri@mit.edu