Policy-Governed Secure Collaboration: Toward Analytics for Cybersecurity of Cyber-Physical Systems

Nazli Choucri
Professor
Political Science Department
Massachusetts Institute of Technology

Gaurav Agarwal
Alumnus
Sloan School of Management
Massachusetts Institute of Technology

Xenofon Koutsoukos
Professor
Computer Science Department
Vanderbilt University

March 13, 2018

Abstract

Mounting concerns about safety and security have resulted in an intricate ecosystem of guidelines, compliance measures, directives and policy reports for cybersecurity of all critical infrastructure. By definition, such guidelines and policies are written in linear sequential text form that makes them difficult to integrate, or to understand the policy-technology-security interactions, thus limiting their relevance for science of security. We propose to develop text-to-analytics methods and tools focusing on CPS domains such as smart grids.

Keywords

Science of security, cyber-physical systems, critical infrastructure, smart grid.

Citation: Choucri, N., Agarwal, G, & Koutsoukos, X. (2018). *Policy-governed secure collaboration: Toward analytics for cybersecurity of cyber-physical systems* [Conference session]. SoS Lablet Kickoff and Quarterly Meeting, College Park, MD, March 13–14, 2018.

Unique Resource Identifier: https://cps-vo.org/SoSLabletQtrlyMeeting_2018

Version: Author's final manuscript.

Policy-Governed Secure Collaboration: Toward Analytics for Cybersecurity of Cyber-Physical Systems

1 Problem Statement

1.1 Context and Motivation

Almost everyone recognizes the salience and power, and ubiquity of cyber-physical systems (CPS), engineered systems where functionality derives from networked interaction of computational and physical processes. The tight integration of physical and computational features already created new generations of smart systems whose impacts are revolutionary, pervasive, and system transforming in the broadest sense of the term.

A profound revolution is driven by technology and market forces that already turns whole industrial sectors into producers of CPS. We have seen autonomous vehicles, military platforms, intelligent buildings, smart energy systems, intelligent transportation systems, robots, and smart medical devices. Industrial platforms as the Internet of Things are becoming household items.

Such complexity comes with critical correlates – notably new and emerging vulnerabilities, threats and attacks, and diffused uncertainty. We are dealing with the merging or coupling of computing and networking with physical systems that create new capabilities, produces, and processes. We recognize that physical systems can now be attacked through cyberspace, and cyberspace can be attacked through physical means. But even networks of networks that enable cyberspace are anchored in physical properties.

The entanglements are complex and pervasive – and do little justice to current idioms, such as spaghetti plate, for example. And society is responding with a wide range of policies, guidelines and directives designed to reduce risk, enhance safety and ensure security – for the social order broadly defined and for the built systems upon which it depends.

Central to all critical infrastructure is smart grid technology. Increasingly ubiquitous in power systems, it represents a highly complex cyber-physical system. Mounting concerns about safety and security resulted in an intricate ecosystem system of guidelines, compliance measures, directives and policy reports for cybersecurity of all critical infrastructure. By definition, such guidelines and policies are written in linear, sequential text format that makes them difficult to integrate, or to understand the policy-technology-security interactions, thus limiting their full use for policy implementation as well as their potential for contributions to science of security. Missing is the value-added of analytics for smart grid cybersecurity and risk assessment. To capture full

benefits and opportunity costs embedded in guidelines and policy documents. We propose to develop text-to-analytics methods and tools, applied initially to Cybersecurity Framework [1] and NIST Guidelines for Smart Grid Cybersecurity [2].

1.2 Technical Problem

Policy directives and guidelines texts for cybersecurity carry their own constraints. Some are explicit; others are not. It is not clear if the dilemma lies in design and substance of the policies, the paucity of metrics, or in the absence of informative analytics. RAND concluded that "…the policies governing cybersecurity are better suited to simple, stable, and predictable environments, leading to significant gaps in cybersecurity management." [3]. More important, they are not based on any precepts we would consider as bearing on a science of security.

1.3 Technical Barriers

Several technical barriers impede full understanding of the cyber-physical properties of a smart grid enterprise. Among these are: (a) locating policy relevant decision points, (b) identifying vulnerabilities embedded in organizational process and technical operations (c) Differentiating intents of threat actor vs. vulnerability of system, (d) tracking damages and diffusion effects, (e) characterizing potential unknown-unknowns, or (f) metricizing functional relationships – to note the most obvious.

1.4 Previous Related Work

In our previous work, we reviewed the new trends, contributions, and identifiable limitations in cybersecurity research. We argue that these limitations are due largely to the lack of interdisciplinary cooperation required to address a problem that is clearly multifaceted. We have also provided recommendations for terminology use when writing papers on cybersecurity and lay the ground work for interaction between technical and nontechnical stakeholders [4]. The vision and the objectives of our research and a solution strategy for analytics for smart grid cybersecurity are described in [5].

2 Research Approach

We propose a multimethod modular approach applied to a generic system in a controlled environment. The "raw data" consists of texts of National Institute for Standard and Technology (NIST) guidelines for cybersecurity of power systems [2], augmented by exploration of on user-specific customizations and generalizations.

2.1 Overview

Figure 1 below provides the near-, mid- and long- term project goals, with "Policy Governed Secure Collaboration" as the primary hard problem. The others four hard problems are situated in the work process outlined in Figure 1. A more detailed view connections of hard problems is in Figure 2.

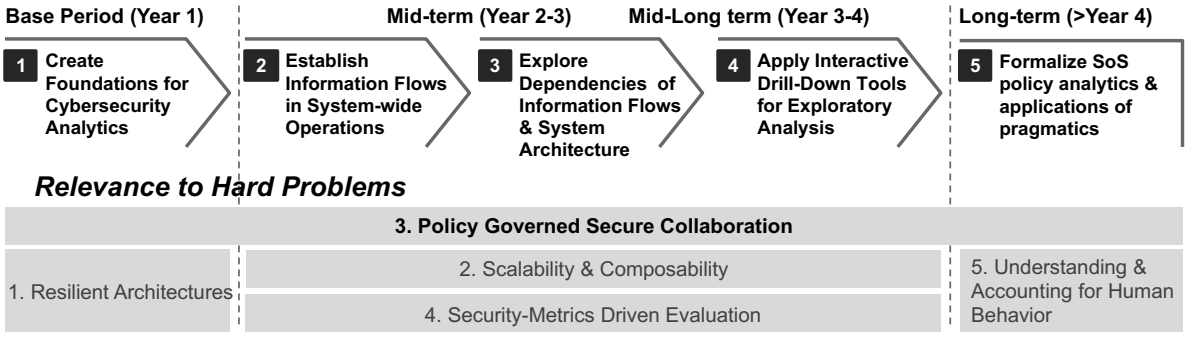

Figure 1. Research Design – Phases

		Focus
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 and time scales.** • Provide methods with tools to deep dive into database for customized insights & analyses. • Create decision supports with methods to identify, analyse and record risk and its responses.
3	**Policy Governed Secure Collaboration**	**Conduct targeted enterprise-relevant analysis** • Resolve the system-level complexity and heterogeneity due to the policy landscape. • Identify points of power and control created by design decisions and policies.
4	**Security-Metrics-Driven Evaluation, Design, Development & Deployment**	**Identify and implement operational responses and actions.** • Use metrics to assess, deploy and develop capabilities - People, Policy and Procedures. • Implement cybersecurity framework– Executive, Business/Process, Operations level.
5	**Understanding & Accounting for Human Behaviour**	**Establish independent monitoring of key enterprise functions.** • Timely, uniform and accurate accounting of business processes. • Identify potential violations of policy directives & systematically prevent their occurrences.

Figure 2. Research Design – Connection to Hard Problems

2.2 Relevance to Science of Security Program:

This work directly addresses the hard problem of "policy-governed secure collaboration" at the enterprise level (for Smart Grid). It is especially relevant to the Science of Security program because the work plan is anchored in a structured system model derived from critical policy texts that is designed to (a) identify major system-wide parameters, (b) situate vulnerabilities (c) map security requirements to security objectives and (d) advance research work on how multiple system features interact with multiple security requirements and affect the cybersecurity critical cyber-physical enterprises.

2.3 Research Design

We now turn to a brief review of the research approach and work plan for each task. Consisting of five tasks, each task represents a distinct phase of inquiry that allows for independent assessment. Each, however, is contingent on products of the other.

2.3.1 Task 1: Create Foundations for Cybersecurity Analytics

During Year 1, the focus is entirely on the required foundations for cybersecurity analytics that include: (1) Identify the policy relevant ecosystem; (2) Formalize rules for extracting data from text; (3) Identify missing pieces for implementation of cybersecurity measures; (4) Design internally consistent structure to organize, metricize, and manage critical information. Even the most cursory view of the ecosystem provides information about both human and technical features components.

2.3.2 Task 2: Establish Information Flows in System-wide Operations

Our objective in Year 2-3 is to construct model(s) of the systems structure and information flows represented in the policy texts. A key objective is to create a dependency structure matrix of physical cyber system by identifying first level information dependencies. The dependency matrix can then be transformed into clusters and partitions of structure and process, and will be used to explore properties that reveal feedback dynamics as well as "hidden features".

2.3.3 Task 3: Examine Dependencies of Information Flows and System Architecture

Accordingly, the next step is to examine the dependencies of information flows and technical architecture. Our purpose here is to generate visual representations of information flows throughout the system using graph theory and network methods. These representations are used subsequently for identifying critical nodal or control points, distinguishing between

human/management vs. technical operations and connections, and identifying modalities of interface or integration of human and technical systems.

2.3.4 Task 4: Apply Interactive Drill Down Tools for Exploratory Analysis

As an extension to Task 3, in year 2-3, we must then develop tools for policy analysis of the whole or the parts. Needed are on-demand tools for targeted drill-down of the technical system, information flows, and underlying policy landscape.

2.3.5 Task 5: Formalize SoS Policy Analytics and Application of Pragmatics

The long-term goal (Year 4-5) is to conduct science-based analysis of cybersecurity. We must formalize enterprise- wide system dependencies and, at the initial phase, use a three-fold Live-Virtual-Constructed environment for evaluation and validation:

1. Live: a simulation involving real people using/operating the real system;
2. Virtual: a simulation involving real people using/operating the simulated system; and
3. Constructed: a simulation involving simulated humans and the simulated system.

An essential task at this point is to formalize properties of system disturbances (vulnerabilities and risks) in order to assess potential system impacts and attendant flow of implications.

3 Strategy for Evaluation & Validation:

Strategy for evaluation and validation include (i) completing, validating, & implementing analytics derived from NIST smart grid "conceptual" model [2], (ii) integrating the risk analysis and directives of NIST Cyber Security Framework v.1.1. and (iii) undertaking contingency analysis of security threats, in terms of "what...if..." Concurrently, recognize the importance of applying the core parts of the research design in other contexts and for other types of cybersecurity or other challenges. A combination of (a) portability, (b) robustness, and (b) customization is an essential contribution to the Science of Security.

4 Potential Impacts

Tasks 1-5 summarize a research approach and operational method approach for replicating it in other systems. For example, it supports four focus areas of US DoD CIO [6] by establishing foundations of a resilient cyber defense posture (task 1); buttressing the transformation of cyber defense operations for greater emphasis on adversary activities and intent (task 2); enhancing cyber situational awareness (task 3 and 4) and supporting capabilities to identify and transcend highly-

sophisticated cyber-attacks (Task 5) – all beyond vision and planned scope of the initiative at this time.

5 Integrative Research

The long-term (3-5 years) goal is to disseminate the results, both theory and applications, via Cyber-Physical Systems Virtual Organization platform (https://cps-vo.org) for enterprise use.

References

[1] National Institute of Standards, and Technology. Framework for improving critical infrastructure cybersecurity. 2014.

[2] National Institute of Standards, and Technology. Guidelines for smart grid cybersecurity. NIST Inter- agency/Internal Report (NISTIR)-7628 Rev 1, 2014.

[3] D. Snyder, J. D. Powers, E. Bodine-Baron, B. Fox, L. Kendrick, and M. H. Powell. Improving the cybersecurity of US Air Force military systems throughout their life cycles. Technical report, RAND, 2015.

[4] R. Ramirez and N. Choucri. Improving interdisciplinary communication with standardized cyber security terminology: A literature review. IEEE Access, 4:2216–2243, 2016.

[5] N. Choucri and G. Agarwal. Analytics for smart grid cybersecurity. In 2017 IEEE International Symposium on Technologies for Homeland Security, pages 1–3, 2017.

[6] Chief Information Officer. DoD Strategy for Defending Networks, Systems, and Data. US Department of Defense. 2013. http://iac.dtic.mil/csiac/download/DDNSD_Public_Releasable_11132014.pdf