Environ Syst Decis (2013) 33:469–470
DOI 10.1007/s10669-013-9484-z

EDITORIAL

Four domains of cybersecurity: a risk-based systems approach to cyber decisions

Zachary A. Collier · Igor Linkov · James H. Lambert

Published online: 23 November 2013

1 Overview

With pervasive reliance on information technology, the robustness and security of these systems are critical to diverse infrastructure systems and particularly to resilience of industry, military, society, community, etc. As safeguards evolve and are implemented, adversaries develop novel ways to breach information technology systems, access sensitive data, and disrupt critical infrastructure. While significant advances in the field of cybersecurity have been achieved, solutions have focused more on the technical issues at component levels such as threat detection, encryption, and other mitigation procedures and technologies and less on how to address overall cyber-influenced risk and to support decisions at level of large-scale systems.

This issue explores the theory, methods, and applications of systems analysis for cybersecurity (including software and hardware and other perspectives) with linkages to other subject areas such as risk management, systems engineering, and strategic decision-making. In particular, there is a need to approach cybersecurity risks from a multi-scale, systems perspective, recognizing the diverse interactions among cyber, physical, and human systems (Lambert et al. 2013). In this direction, our first paper frames the rest of the issue in terms of *cyber-resilience*, wherein Linkov et al. (2013) discuss how decision-makers require the ability to plan for threats and absorb, recover, and adapt to threats after they occur along the physical, information, cognitive, and social domains in which these systems exist. The remaining articles are organized by these domains respecting that several of the articles cross domains.

2 Physical domain

The physical domain includes hardware and software and networks as building blocks of cyber infrastructure. Gilmore et al. (2013) outline the risks posed by counterfeit electronic parts in the context of hardware security. They discuss a validation strategy based on infrared analysis and blind source separation to authenticate suspected counterfeit parts and stop counterfeits from moving downstream in the supply chain.

3 Information domain

Monitoring, information storage, and visualization are features of the information domain. The issue features several articles that focus on risks within the information domain. First, Baiardi and Sgandurra (2013) discuss a simulation-based risk assessment methodology that models adaptive threat agents as well as identifies effective countermeasures. Cam and Mouallem (2013) then describe a model that dynamically models mission assurance through monitoring of cyber assets and includes a risk management scheme to mitigate risks to acceptable levels. Finally, Ezell et al. (2013) describe a framework to model the risks and impacts of cyber attacks on traffic control systems.

4 Cognitive domain

Information should be properly analyzed and sensed as well as used for decision-making in the cognitive domain.

Z. A. Collier · I. Linkov (✉)
US Army Engineer Research and Development Center, Concord, MA, USA
e-mail: Igor.Linkov@usace.army.mil

J. H. Lambert
University of Virginia, Charlottesville, VA, USA

Rosoff et al. (2013) explore the mental decision-making heuristics that people use when faced with a cybersecurity dilemma. They present the results of two experiments in which gain-loss framing was modified for participants when presented with cybersecurity scenarios.

5 Social domain

Decisions on cybersecurity should be consistent with social, ethical, and other considerations that are characteristic of their enveloping societal domain. Four articles discuss cybersecurity within the social domain. First, Sheppard et al. (2013) approach cybersecurity from an organizational perspective, describing how organizations can be better prepared to respond to cyber threats and provide a survey and scorecard to measure preparedness levels. Pawlak and Wendling (2013) then explore the existing and future trends in governmental policies related to cybersecurity and identify gaps and potential paths forward. Next, Kelic et al. (2013) describe an agent-based decision framework for modeling the macroeconomic impacts of cyber attacks on vulnerable industry sectors, such as the oil and gas industry. Finally, Vaishnav et al. (2013) outline a novel framework connecting cybersecurity and international relations as a single system and comment on the properties of such a system.

6 Closure

The readers of ES&D are encouraged to respond to this issue and its articles via notes to the editors and authors, and to provide more formal responses in the way of follow-on articles and discussion notes that can be considered for publication in future issues of the journal. Proposals for follow-on special issues on cybersecurity and related topics are welcomed by the editors and editorial board at any time.

References

Baiardi F, Sgandurra S (2013) Assessing ICT risk through a Monte Carlo method. Environ Syst Decis. doi:10.1007/s10669-013-9463-4

Cam H, Mouallem P (2013) Mission assurance policy and risk management in cybersecurity. Environ Syst Decis. doi:10.1007/s10669-013-9468-z

Ezell B, Robinson EM, Foytik P, Jordan C, Flanagan D (2013) Cyber risk to transportation industrial control systems and traffic signal controllers. Environ Syst Decis. doi:10.1007/s10669-013-9481-2

Gilmore ET, Frazier PD, Collins IJ II, Reid W, Chouikha MF (2013) Infrared analysis for counterfeit electronic parts detection and supply chain validation. Environ Syst Decis. doi:10.1007/s10669-013-9482-1

Kelic A, Collier ZA, Brown C, Beyeler WE, Outkin AV, Vargas VN, Ehlen MA, Judson C, Zaidi A, Leung B, Linkov I (2013) Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks. Environ Syst Decis. doi:10.1007/s10669-013-9479-9

Lambert JH, Keisler JM, Wheeler WE, Collier ZA, Linkov I (2013) Multiscale approach to the security of hardware supply chains for energy systems. Environ Syst Decis 33(3):326–334

Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A (2013) Resilience metrics for cyber systems. Environ Syst Decis 33(4). doi:10.1007/s10669-013-9485-y

Pawlak P, Wendling C (2013) Trends in cyberspace: can governments keep up? Environ Syst Decis. doi:10.1007/s10669-013-9470-5

Rosoff H, Cui J, John RS (2013) Heuristics and biases in cyber security dilemmas. Environ Syst Decis. doi:10.1007/s10669-013-9473-2

Sheppard B, Crannell M, Moulton J (2013) Cyber first aid: proactive risk management and decision-making. Environ Syst Decis. doi:10.1007/s10669-013-9474-1

Vaishnav C, Choucri N, Clark D (2013) Cyber international relations as an integrated system. Environ Syst Decis. doi:10.1007/s10669-013-9480-3