Editor-in Chief's Letter

Richard M. Krieg, PhD

Of the 25 authors whose articles populate this issue—in addition to those who are university-based—we are pleased by the contributions of those working at nationally prominent strategy development and research organizations. These include Idaho National Laboratory (INL), the Stimson Center, the Naval Postgraduate School, the Johns Hopkins University Applied Physics Laboratory (APL), the Naval Information and Warfare Center (NIWC), Savannah River National Laboratory (SRNL), the InfraGard National Members Alliance (INMA) and other organizations. The *Journal* has collaborated in the past with INL, and we are pleased to see that partnership grow.

I am happy to announce the appointment of four new *JCIP* Associate Editors: Noah Dormady, PhD; Judith (Cooksey) Krieg, MD, MS; Thomas Sharkey, PhD; and Camille Palmer, PhD. They will continue to play important roles in Journal Development, and I thank them. We are very grateful for our peer reviewers, and appreciate the efficient staff of our publisher, the Policy Studies Organization (PSO), and editorial assistant Tabor French.

In this issue, we launch a new *Strategic Perspectives* section with **David Woods'** and **David Alderson's** thought provoking "Progress toward Resilient Infrastructures: Are we falling behind the pace of events and changing threats?" The authors describe a Strategic Agility Gap evidenced by the regular occurrence of unforeseen failures at the organizational, regional, national scales—breakdowns that trigger or threaten widespread service outages with substantial financial and human costs. The Gap is the difference between the rate at which an organization can adapt to change and the rise of unexpected challenges at a larger industry or society scale. Using events occurring in 2021 as a counterpoint, the case is made that there are practical limits to current strategies for building critical infrastructure resilience. A pivot—facilitated by scientific advances—is warranted, intended to increase strategic agility across critical infrastructure sectors.

Debra Decker and **Kathryn Rauhut**, in "Incentivizing Good Governance Beyond Regulatory Minimums: The Civil Nuclear Sector," report the findings from a multi-year project to determine how a well-conceived "Good Governance Template" can be used as the basis for potential market rewards, with the framework being tested and refined across many stakeholder groups. The large-scope, nuanced process used to identify how market incentives could be used as a force multiplier to incentivize nuclear security has broad applicability to other critical infrastructure sectors. The authors report that judgments of rating agencies, insurers, courts, and financiers can motivate good security performance of a nuclear facility operator

 doi: 10.18278/jcip.2.2.1

by affecting public reputation and by modifying potential liability of the facility's owners/operators in the event of an incident. Demonstrating good performance may also affect the availability of financing/investment and financing terms and conditions. Insurance availability, especially for cyber coverage, will become a more important incentive for good governance as owners and operators have expanded exposure to more complex technologies and an enlarged threat surface.

In "Evolution and Trends of Industrial Control System Cyber Incidents since 2017," **Robert Grubbs**, **Jeremiah Stoddard**, **Sarah Freeman**, and **Ron Fisher** use selected publicly reported cyber incidents to analyze and dissect the continued and growing threat to industrial control systems (ICS) and the operational technology (OT) environment. The perceptive article reviews each incident and, when available, provides information on the cyber actors, the vulnerabilities exploited, and any guidance the US Government provided in response. Data from the Department of Homeland Security (DHS) is used to highlight quantitative trends concerning ICS incidents. A more proactive US-facing policy framework is necessary to protect critical infrastructure. Cyber actors have learned that they do not need to compromise the OT environment to disrupt OT services; the convergence of IT and OT has blurred that line. Similarly, cyber actors lacking ICS/SCADA-specific knowledge have realized that an IT intrusion can be just as effective as an OT disruption, lowering the sophistication necessary to target OT environments. This trend has increased the vulnerability to OT systems since both IT and OT exploits can be used to impact OT systems.

George Baker, **Ian Webb**, **Klaehn Burkes**, and **Joseph Cordaro**, in "Large Transformer Criticality, Threats and Opportunities," respond to the reality that large power transformers (LPTs) represent a critical "tent-pole" in national electric power grid and national resiliency. The seminal article notes that they are essential to both the generation and transmission sectors of the nation's electric power grid—and they are known to be targets in adversaries' plans to debilitate US critical infrastructures. Their high cost and supply chain issues involving months to years of replacement time dictate the importance of survivability assurance. The authors recommend an important test effort to determine LPT vulnerabilities and to develop effective protection approaches. They delineate electromagnetic, physical, and cyber threats, emphasizing the critical importance of rigorous testing. While programs have been undertaken for transformer and transformer substation cyber and physical resiliency, it is essential that a vigorous effort to test LPTs under real load conditions occur and that effective resiliency measures for electromagnetic threats be implemented as a national priority.

Ryan Hruska, **Kent McGillivary**, and **Robert Edsall**, in "A Functional All-Hazard Approach to Critical Infrastructure Dependency Analysis," address the inherent difficulty of assessing vulnerabilities, resiliency, and priorities for protecting interdependent critical infrastructure systems from an all-hazards perspec-

tive. The article introduces an All-Hazards Analysis (AHA) methodology, which provides an integrated functional basis across infrastructure systems, through the implementation of a common language and a scalable level of decomposition to effectively evaluate the resilience of interconnected infrastructure systems. The function-based analytical framework is designed to enable the evaluation of critical infrastructure systems and their dependency relationships. The authors use the Colonial Pipeline incident to demonstrate the approach, showing that it provides a consistent, robust and repeatable process for the development and analysis of computable dependency models of interconnected infrastructure systems.

In an important technology transfer article, **Aleksandra Scalco, David Flanigan**, **and Steven Simske** apply concepts undergirding national defense cybersecurity planning to hospitals and healthcare. "Control Systems Cyber Security Reference Architecture (RA) for Critical Infrastructure: Healthcare and Hospital Vertical Example" delineates RA cybersecurity approaches along with related strategies including Zero Trust (ZT), Defense-in-Depth (DiD), network segmentation, and security orchestration. Testing to deploy these concepts in other critical infrastructure sectors are underway. However, based on the current wave of ransomware attacks and the potential for serious patient impacts, there is special need to deploy these approaches in healthcare settings. In addition to improving the current healthcare cybersecurity posture, the adoption of military-grade cybersecurity can provide tools for healthcare policy development. The inherent complexity of healthcare provision coupled with a constant stream of new healthcare modalities and providers add additional challenges to cybersecurity decision-making. Nevertheless, adept application of the strategies laid out can contribute to successful system development by providing a consistent approach to dealing with a complex entity, maintaining traceability from requirements to physical components, and ensuring that all system behaviors are captured and mapped to solution elements.

Eric Cote, in a *Practice Advances* piece, expresses his views on the need to improve awareness of the nation's hospital and healthcare generator fleet. In "National Action Needed to Strengthen the Hospital Emergency Power Infrastructure," he argues that catalytic work undertaken by his organization, Powered for Patients, in Los Angeles and Rhode Island, provides a national model. This includes assembling information on a locality or state's healthcare emergency power generation equipment (such as generator age and lack of redundant emergency power), minimizing risk to healthcare emergency power through the adoption of best practices, upgrading emergency power threat reporting and response protocols, and sharing information among those involved in emergency decision-making regarding the loss of healthcare power supply. For example, in Los Angeles, with support provided by the Department of Homeland Security, a system is being implemented to provide real time generator threat alerts to government emergency managers from single generator hospitals. A working group has also been

established to enhance pre- and post-disaster coordination between government agencies and the generator service, fuel, and rental industries.

In "Automotive Ground Vehicles' Resilience to HEMP Attack: An Emergency Management Mitigation Plan," **Julian LoRusso**, **Mariama Yakubu**, **Wayne Sandford**, **Jeffrey Treistman**, **Ed Goldberg**, and **Matt Van Benschoten** take a deep dive into automotive resilience to—and countermeasures for—this type of emergency. A high-altitude electromagnetic pulse (HEMP) attack would immobilize many critical infrastructure components and sub-systems. Presidential Executive Order 13865 and corresponding National Defense Authorization Act legislation called on the nation to build critical infrastructure resilience to potential electromagnetic pulse (EMP) events. Automotive Ground Vehicles of different types would be essential to maintain a wide array of community lifelines during this type of emergency. From an engineering standpoint, a methodology is presented to help visualize the critical components and potential failure modes from a HEMP event in automotive ground vehicles, and to inform proposed test plan and mitigation proposal strategies. The authors argue that strategic implementation of cost-effective HEMP countermeasures—and emergency management strategies—should be implemented nationwide for automotive vehicles and other critical infrastructure systems facing EMP risk.