Forum

GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS

Critical Infrastructure

The current issue of the Georgetown Journal of International Affairs' *Forum - Securing Critical Infrastructure* explores how best to secure critical infrastructure. "Critical infrastructure" is not a novel term; governments have been using it for the past two decades to describe sectors and services such as electricity generation, gas and oil production, telecommunications, water supply, transportation, and financial services that are deemed essential for the functioning of modern society and the economy. For example, the United States has identified sixteen different sectors as critical.[1] The term critical infrastructure itself first emerged in the mid-1990s to define those essential assets, systems, and networks perceived to be becoming uniquely vulnerable through increased automation, interconnectedness, and reliance on the Internet, and as such, susceptible to equipment failure, human error, weather and other naturally caused outage, and physical and cyber attack.[2] Over the last twenty-five years, however, the United States and most other nations have primarily focused their policies and activities on the protection of physical assets and the logical function of infrastructure components rather than on the products or services that the networked infrastructure is providing to society.

The threat to our networked systems and infrastructures is real and growing. Data breaches, criminal activity, service disruptions, and property destruction are becoming commonplace. The resources available to increase the resilience of our infrastructure and decrease the exposure of our nations to damage, however, are finite. In light of this reality, we should probably reconsider what the term "critical" means and whether it truly encompasses so many different sectors. According to the Merriam-Webster Dictionary, "critical" means vital; indispensable; absolutely necessary.[3] Perhaps it is time to ask ourselves: are there really sixteen networked infrastructures that are vital, indispensable, and provide "life-line" services to our society and nation or are there far fewer? For example, telecommunications and power underpin almost every other essential service of a nation. In the aftermath of a hurricane or other major storm, without power, most other critical services stop. This is because the computers and networks that run these services are not be able to function without power. Even with power, if telecommunications services (e.g., Internet) are lost, the free movement of goods, services, capital, and business transactions halts. Might these two key services be more important than other infrastructures that have likewise been deemed critical?

Changing the focus from *critical infrastructure* to *critical service* may change the prioritization and approach to protection, resilience, recovery, and restoration of assets. It may also highlight the interdependencies of networked infrastructures across national boundaries, demanding different approaches to domestic and international security.[4] An interesting example, for instance, is countries' dependence on satellite navigation for many of their essential services, such as e-commerce and transportation. When the European Commission (EC) asked its member states to identify critical infrastructures, however, no nation identified the important shared satellite navigation system of *Galileo.* But if the signals were switched off or failed tomorrow it would have a devastating effect on many critical services in Europe and beyond.[5] Perhaps the nations that responded to the EC's survey assumed that the other would nominate the service. Likewise, National Grid, the power company that delivers energy to communities in Massachusetts, New York, and Rhode Island may be overlooked as a critical asset or service in those states. Similarly, the financial markets may not identify AT&T or Verizon's services as critical to Wall Street and the stability of the global financial system. Preserving the security and resilience of these connected infrastructures requires an understanding of their interdependencies. Once they are understood and acknowledged, it allows for a stronger alignment of security measures and the resource requirements necessary to reduce exposure.

Unfortunately, that is not what most nations are doing right now. National strategies and policies do not prioritize the services and infrastructures that are most at risk—rather they treat the infrastructures equally; they are all deemed "critical". Because there is no hierarchy of importance, governments issue general guidance and broad regulatory requirements to protect infrastructures across the board. For example, the National Institute of Standards and Technology published the *Framework for Improving Critical Infrastructure Cybersecurity 1.0* in February of 2014.[6] The *Framework* provides guidelines to help critical infrastructure owners and operators as well as other businesses understand and assess their cybersecurity capabilities, readiness, and risks from cyber threats. The United Kingdom initiated the *Cyber Essentials* framework that is designed to help businesses protect themselves from cyber threats. The European Commission has developed regulations, currently in draft form, known as the *European Network and Information Security (NIS) Directive*. This directive requires affected organizations to implement security measures to guarantee a level of security appropriate to their risk, and to notify the relevant authorities in the event of a serious security incident. The draft will likely become law in Autumn of 2015. As a final example, the German government recently passed legislation ordering institutions listed as "critical infrastructure," such as transportation, health, water utilities, telecommunications providers, as well as finance and insurance firms, to implement new minimum information security standards or face penalties if they fail to do so within two years.[7]

Instead of reinforcing the status quo, nations should focus on the top two or three critical services, rather than infrastructures, if they want to make measurable progress in increasing the resilience of a broader set of networked infrastructures, and hence the nation as well. Basic guidance and broad regulation may yield incremental improvements, but likely will lead to a sub-optimal allocation of limited resources (e.g., political will, money, time, and people) available in an already hyper-exposed and exploited environment. If we are going to get serious about securing the critical infrastructure then we should prioritize the few critical services from the many infrastructures to advance the safety, security, and resilience of our digitally dependent societies and nations.

The articles in this edition of *Forum - Securing Critical Infrastructure* provide a useful addition to the discourse on critical infrastructure protection and provide alternative, and at times overlapping, suggestions to secure and protect critical infrastructure.

The first article, by David P. Fidler, entitled, "Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection," explores the role of international law to protect critical infrastructure from cybersecurity threats. After assessing the historical rationale for the development (and lack thereof) of international law within a cybersecurity context, Fidler goes on to apply the role that international law plays in protecting critical infrastructure from different threat groups, including criminals, terrorists, and the intelligence agencies and militaries of states. Fidler concludes with an exploration of the strengths and weaknesses of cyber norms and international law, particularly as U.S. policy changes to emphasize cyber deterrence.

Myriam Dunn Cavelty and Reimer A. Van Der Vlugt analyze why current security solutions to protect critical infrastructure are falling short of societal needs. Their article, "A Tale of Two Cities: Or How the Wrong Metaphors Lead to Less Security," assesses how concepts (and metaphors) of attack and defense often lead to the conceptualization of the wrong types of security concepts, which may be detrimental to certain critical infrastructure protection efforts. The authors conclude by providing an alternative metaphor for some critical infrastructure protection conceptualization—open cities.

In "Trusted Information Brokerage in the Times of the Snowden- Effect Dilemma: Private- Public Data Sharing in Cyber Security in Austria, Germany, and Switzerland," Gerd Gensbichler assesses the incentives private sector entities have for information sharing with the government in the post-Snowden era. He recognizes that business and government networks are interlinked, and that often cyberattacks against a government network can spill over to business networks and vice versa. Gensbichler argues that this underscores the importance of public-private information sharing, using a survey of national banking, critical infrastructure, and information communication technology firms in Austria, Germany, and Switzerland to provide first hand information on the incentives that drive private actors to participate in public-private information sharing agreements.

In their article, "Securing Telecommunications Infrastructure Against Cyber Attacks," Tarek Saadawi and Haidar Chamas assess the scale and frequency of cyberattacks and recommend the establishment of an International Cyber Union (ICU). They argue that an ICU would monitor, collect, and verify international cyber illegality and hacks; would carry out necessary legal actions; and would provide a platform for international cooperation in the cyber domain. Moreover, the authors propose an architectural model for protection mechanisms that they believe will minimize cybersecurity threats to telecommunications infrastructure.

Finally, in "Power and Energy Infrastructure: Cyber Security, Defense, and Resilience," Massoud Amin argues that the power industry should focus on a 'holistic asset management approach' to address grid resilience against cyber threats. To make his case, Amin assesses this approach from a resilience, security, and vulnerability angle. Amin then concludes by analyzing current initiatives, issues, and security needs moving forward, while providing recommendations to enhance security in power and energy infrastructure.

As we network and interconnect our systems, the services they provide become inherently important—some more important than others. The importance of those services is what should define the notion of "critical services." This issue will challenge the reader to define what is most important is to determine whether it is an infrastructure or a service and share knowledge from experienced authors whose papers aim to fix the problems of today.

Melissa E. Hathaway is President of Hathaway Global Strategies, LLC and a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. In addition to spearheading the national cybersecurity agendas for both President George W. Bush and President Obama, she is a Distinguished Fellow at the Centre for International Governance Innovation in Canada, the Chair of the Council of Experts for the Global Cyber Security Center in Italy, and serves on the Board of Regents at Potomac Institute for Policy Studies.

NOTES

[1] Presidential Policy Directive 21 signed by President Obama in February 2013 highlights sixteen critical infrastructure sectors including: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and waste water systems. The White House, "Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience," February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[2] Presidential Policy Directive 63 signed by President Clinton in May of 1998 recognized vulnerabilities to core infrastructures present a threat to domestic and international security. The White House, "Presidential Decision Directive/NSC-63," May 22, 1998, http://fas.org/irp/offdocs/pdd/pdd-63.htm.

[3] Merriam-Webster Dictionary, "Critical," http://www.merriam-webster.com/dictionary/critical.

[4] Melissa Hathaway, Book Chapter, Best Practices in Computer Network Defense: Incident Detection and Response, pages 3-18, February 2014.

[5] ibid.

[6] National Institute of Standards and Technology, "NIST Releases Cybersecurity Framework," *Press Release*, February 12, 2014, http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[7] RT, "Germany Passes Strict Cyber Security Law to Protect 'Critical Infrastructure'," July 11, 2015, http://www.rt.com/news/273058-german-cyber-security-law/.