Center for a New American Security

MARCH 2014

Securing the Grid
Opportunities and Risks in Operational Technology

POLICY BRIEF

By Robert J. Butler

The smart grid – "a planned nationwide network that uses information technology to deliver electricity efficiently"[1] – will make the delivery of electricity in the United States not only vastly more efficient but also potentially more vulnerable to cyberattack and, thus, potentially less reliable. Indeed, the very features that make this new grid smarter than the system it is replacing will open new avenues for adversaries to access the grid, as well as new ways for them to disrupt grid operations once they gain access. In August 2003, a blackout that began in northern Ohio when a high-voltage power line brushed against overgrown trees cascaded across the grid. It ultimately affected 55 million people, contributed to six deaths in New York, caused 4 million Detroit residents to boil their drinking water for four days and cost between $7 billion and $10 billion.[2] If a natural threat can cause that type of disruption and destruction, just imagine the cascading negative effects of a planned cyberattack against an interconnected smart -grid network over an even larger geographic region with focused targeting against critical U.S. infrastructure.

Two important sets of security initiatives are currently underway to respond to this risk. First, industry and the U.S. government have been partnering to develop a cybersecurity framework and guidelines for smart grid cybersecurity.[3] The second set of initiatives focuses on strengthening security standards for the industrial control systems (ICSs) that control circuit breakers and other operational technology (OT) components such as air-handling and power-distribution systems.[4] The first initiative deals with controls on information technology (IT) – cybersecurity. The second deals with controls on the physical operation of industrial control systems. These realms are obviously connected.

To a dangerous extent, however, these efforts in cybersecurity and ICS security constitute two separate "silos of excellence." Unless they are better integrated, the gaps between them will create new risks to the grid and overall digital infrastructure – especially by enabling attacks on data centers and the critical information they contain. In fact, the data centers deployed today are the foundation for IT enterprise processing and cloud computing in a virtualized environment. Failure to secure data centers through integrated IT and OT security puts American businesses, their operations around the world and the nation's overall economic security at risk.

To respond to this threat and to secure the multileveled infrastructure, the U.S. government should partner with industry to develop a holistic strategy that focuses on expanded information sharing between IT and OT groups. Furthermore, to close vulnerabilities more rapidly and create better situational awareness of the infrastructure foundation, the nation should move to new, secure, on-demand construction of standardized digital infrastructure. Finally, the government and private sector should jointly develop and implement capabilities to mitigate residual risk in the event of an unforeseen attack to the digital infrastructure; this should include risk insurance for all levels of infrastructure.

The Grid Will Power the Nation's Data Centers and Digital Infrastructure

The grid has three levels of infrastructure, with multiple operators at each level.

- **IT infrastructure** is the cybernetwork that makes the smart grid "smart." It is the digital interconnection of grid assets, from power plants to substations to smart meters. This digital infrastructure includes software, communications devices and hardware such as servers. At this layer, converted industrial power is used to drive computing, storage and network processes.
- **OT control systems** include industrial control systems, supervisory control and data acquisition (SCADA) systems, distributed control systems and other control configurations that are often found in the industrial sector and critical infrastructures. OT control systems control the grid infrastructure and are connected to the digital infrastructure to enable automated and remote control.
- **Power infrastructure** is the physical (as distinct from digital) infrastructure that generates, transmits and distributes power. It includes all forms of power generation (power plants fueled by coal or natural gas, wind and solar farms, nuclear plants, etc.), as well as the wires, substations, transformers and switches that bring power to consumers. This level includes the equipment owned and operated by the utility companies themselves, as well as the control centers that manage the grid.

OT control systems connect to the IT infrastructure and power infrastructure. The lack of integrated cybersecurity and OT security at this area of convergence represents one of the most significant challenges for the nation's critical energy infrastructure. In this model, it is critical to secure the entire environment holistically. To date, the government and private sector have not adequately addressed the need for integrated intelligent control across these infrastructure layers.

This converged smart grid needs to power our data centers, which in turn control the grid. As a senior official at the Department of Energy recently noted, "It's also important to recognize that the data centers that control the ICS (or the grid) are also dependent upon the operation of the systems they control. It's a complete dependency circle of powering the data center to control the electrical grid to deliver the electricity to power the data center."[5] Therefore, the security of critical data in the country's data centers depends on how well cybersecurity and OT security are integrated within the grid. The new data center infrastructure needs to be a secure, integrated system that supports the deployment of enterprise applications and data and provides network interfaces for power distribution, energy recovery, the environment and IT. This infrastructure must always be "on" and secure across all of these interfaces, and it needs to guarantee the continuous availability, confidentiality and integrity of data and processing.

The Convergence of Information Technology and Operational Technology is Transformational and Creates New Challenges

> *In the past we were able to keep our control systems protected because they were separated from our business systems and the control systems were so unique (and old in many cases) that they were difficult to attack and there were not many ways to attack a large number of systems efficiently. That is no longer the case as we move to implement a smart electric grid and begin connecting smart devices to the grid that are also connected to the Internet. … This opens up new vectors our adversaries can use to gain access to our control systems. These attack methodologies include Aurora, Stuxnet and Duqu; and this is just the beginning. Like the "I Love You" virus that raised awareness in the public about the vulnerabilities exploited by email, these latest events show us that we need to think about security in a new way for our critical infrastructure as well.*[6]
>
> GIL VEGA, FORMER CHIEF INFORMATION SECURITY OFFICER, DEPARTMENT OF ENERGY

We have witnessed numerous breaches of digital infrastructure at the layer of operational control systems, including the Stuxnet attack in 2010 and the Saudi Aramco breach in 2012. These and other attacks point to weaknesses in the interface between the IT and the OT layers. By hacking into gateways or edge devices that link operational controls to the IT layer, an adversary could reprogram the control systems. Such reprogramming could be designed to cause the system to self-destruct (as was the case with Stuxnet) by commanding equipment to operate at unsafe speeds or valves to open when they should be closed. Thus, in the context of the smart grid, security is about more than protecting data.

Analysts at the Center for a New American Security have noted that "increasingly, cyber technologies can have real effects in the physical world. The well-reported Stuxnet attack against Iranian nuclear facilities provided an early example of this potential."[7] In other words, plans for data center security in the smart grid must involve not only security in the classic IT security sense, but also the reliability and safety of physical OT control systems.

Threats against digital infrastructure at both the physical and logical layers are known as cyber-physical, or blended, attacks. The National Institute of Standards and Technology (NIST) reports that these attacks "are executed by an adversary or result from inadvertent action that causes a greater impact and/or different consequences than a cyber or physical attack could cause individually."[8] Cyber-physical attacks include physical attacks that are informed by cyber reconnaissance of a network, cyberattacks that enhance physical attacks and the use of a cybersystem to cause physical harm. The last type of attack is most threatening from the standpoint of national security and safety.[9] The GridEx II exercise recently concluded by the North American Reliability Corporation posited a combined cyber-physical attack that disrupted the grid for weeks across large portions of the United States.[10]

Cyber-physical attacks are also increasingly easy to execute. Zero-day threats – attacks that exploit a previously unknown vulnerability – are of particular concern. They close the gap between rogue adversaries without significant technical resources and adversaries (such as nation-states) that are not willing or able to launch attacks directly but have the technical capacity to develop and sell zero-day exploits. The actors behind advanced persistent threats require situational awareness of system configurations within the target. Solid targeting and predictable access for such an actor depends on persistent access to, and awareness of, changes to a networked infrastructure.

In 2007, Idaho National Laboratory conducted an experiment to determine whether the United States was susceptible to cyberattacks on OT control systems. In the experiment, dubbed "Project Aurora," researchers built a miniature industrial city plan and sent a red team to attack it. The red team rewrote the OT control system computer code for one of the diesel generators, directing the generator to destroy itself. It did, and the notion that cyber commands alone could destroy physical OT control equipment was confirmed.

As in the smart grid, too many data center operators think about cybersecurity and physical security as separate issues.

Furthermore, reporting from the ICS-Computer Emergency Response Team at the Department of Homeland Security (DHS) over the past two years has caused even greater concern about the number of ICS vulnerabilities accessible from the Internet. The team states that Project Shine (Shodan Intelligence Extraction), an ongoing project to identify industrial control systems that are connected to the Internet, has discovered well over a million such systems.[11]

These same issues exist within the digital infrastructure of the traditional data center. There, too, the cyber and the physical converge. The data center sits on a foundation of IT infrastructure, reliant on OT control systems (like power distribution units and cooling systems) and the digital infrastructure of connected hardware and software above them. And as in the smart grid, too many data center operators think about cybersecurity and physical security as separate issues.

Our financial exchanges and service firms rely on interconnected data center infrastructure. Imagine, for example, a power or digital infrastructure failure in the northeast that included the New York financial district. Such a failure could result not only in financial service data centers going off line but also in cascading disruption to hub transportation systems, communications systems, hospitals and other "lifeline" infrastructure. The consequence would be a significant homeland security and safety issue, possibly including loss of life.

The Risks Generated by Converged Infrastructure

The United States government is clearly aware of the need to address cyber-physical security. In March 2013, President Obama issued *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity*[12] and *Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience*.[13] Their implementation will "drive action toward system and network security and resiliency, and will also enhance the efficiency and effectiveness of the U.S. government's work to secure critical infrastructure and make it more resilient."[14]

NIST's 2013 revision of the *Guidelines for Smart Grid Cybersecurity* proposes a logical architecture for the smart grid and represents an important step forward.[15] But a fundamental vulnerability remains: The guidelines do not address a better way of implementing a secure foundational layer at the level of OT control systems to provide the data center security required for secure grid operations. After implementation of the NIST framework, DHS is charged with developing infrastructure-specific implications of preferred target profiles. These are the logical "container" for cyber-physical risk-management and best-practice guideposts. Because this process is just beginning, it provides a ready opportunity for public-private collaboration to address the IT layer's overlap with the OT control plane.[16]

Additional resources that attempt to address cyber-physical attack include NIST SP 800-82, *Guide to Industrial Control Systems Security*, and ISA 99, *Industrial Automation and Control Systems Security*[17] Although NIST SP 800-82 can provide a starting point, future efforts need to address the fact that control system security operates on industrial campuses, an environment that lacks the scale, complexity and distributed nature of a smart grid or large-scale, globally interconnected, digital infrastructure.

The Growing Need for Secure Converged Infrastructure

As the nation moves toward the Internet of Things, in which just about everything is connected to the Internet, private sector entities are increasingly realizing that the "divide" between IT and OT is closing. However, innovation in information technologies has far outpaced innovation at the level of OT control systems. For consumers, innovation above the OT infrastructure level is tangible and exciting. What they don't know is that those innovations are sitting atop foundations that are crumbling.

One of the most significant vulnerabilities of the smart-grid digital infrastructure is the challenge of maintaining security in OT control systems that have one foot in the past – as isolated systems using specialized hardware and software – and one foot in the present, connected to the network for remote access. That leaves the OT control systems vulnerable to security breaches.

Several actions are critical to securing the nation's digital infrastructure at the level of OT control systems. These actions must combine a focus on hardware standardization with software-enabled intelligent control.

Recommendations and Conclusion

NIST, as the premiere standards body, and DHS, as the government's lead implementation arm, need to build on current standards to develop a holistic strategy for securing digital infrastructure and data centers that focuses on expanded information sharing and learning between information technology and operational technology groups. This effort will require several components:

- Building off the Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which will serve as an implementation of the recently published NIST Cybersecurity Framework, NIST and DHS should convene a group in which the public and private sectors work together to develop a model for data center security. This recommendation builds on the recommendations of the recent Bipartisan Policy Center report addressing cybersecurity in the North American electric grid.[18] This data center security "community of interest" should go beyond simple information sharing to the actual construction of converged solutions for integrating and securing IT and OT systems, thereby providing a foundation for data centers and cloud computing.
- Expanded security guidelines should extend beyond a focus on threats to include threat mitigation capabilities. A government and private sector partnership should work proactively to actually build campaigns to counter advanced persistent threats.
- The threats to data centers extend beyond the United States and are, in fact, a global problem. Thus, the United States should work with other nations and standards bodies to ensure security standards, best practices, threat sharing and workable solutions to close seams around the globe. This recommendation is directly aligned with the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity.*[19] The International Organization for Standardization and International Electrotechnical

Commission (ISO/EC) 27001:2005 framework provides a good foundation for nations to work together on continual innovation and risk mitigation.

As part of this work, DHS and the Department of Energy should lead government and business efforts to adopt new, secure and on-demand construction of standardized data center infrastructure with intelligent control for the purposes of achieving greater situational awareness and more rapid development of countermeasures within the growing digital infrastructure. Standardized production of OT control systems will reduce risk to the digital infrastructure.

- The global nature of the supply chain for products assembled in the United States means that the entire chain must be vetted and every component tested. For the infrastructure that drives power to our data centers, that kind of standardized production of assets would help ensure the "up front" implementation of security measures, enable greater levels of quality control and potentially significantly improve interoperability.
- Beyond standardization, the Defense Science Board task force has advocated the use, modular data center infrastructure to rapidly create and secure a robust and elastic layer of digital infrastructure.[20] The same things that make a system expansible and responsive – standardization and visibility – lend themselves to enhanced security and can be applied to create a comprehensive strategy for mitigating risk to the grid and the nation's digital infrastructure. This "build-as-you-need" approach, coupled with an intelligent data center operating system that can "see" legacy system vulnerabilities, will enable efficient "transition strategies" for migrating legacy grid devices to a more secure infrastructure. The Department of Energy's

DHS and the Department of Energy should lead government and business efforts to adopt new, secure and on-demand construction of standardized data center infrastructure with intelligent control for the purposes of achieving greater situational awareness and more rapid development of countermeasures within the growing digital infrastructure.

National SCADA Test Bed should be leveraged implement this approach and help secure multichannel communications between the IT and OT levels.

Finally, to provide additional protection after a compromise (and prior to detection) and as we work to transition to a more secure digital infrastructure, insurance companies should work with data center owners and service providers to provide robust risk insurance in line with best security practices to address breaches across both the IT and OT infrastructures. Risk insurance is just one area for further research and is a good incentive to promote faster adoption of converged security standards. This recommendation also aligns with recent White House discussion about incentives for faster adoption of the recently published NIST Cybersecurity Framework.[21] From a public sector perspective, provisions of the Safety Act should apply to DHS-designated critical infrastructure data centers and will also help to mitigate negative consequences by providing liability protections in the event of a cyberattack on these data centers.

The time to act is now, as a new digital infrastructure is being deployed to power America's national security and business enterprises. A failure to act will jeopardize the nation's economic competitiveness and overall security.

Robert J. Butler is an adjunct fellow at the Center for a New Amercian Security and the vice president of government strategies for IO.

The author would like to thank the following individuals for their contributions to this paper: Joel Brenner of Joel Brenner, LLC; Bob Brese, Chief Information Officer of the Department of Energy; Dr. Chris Bronk, Director of the Program on Energy and Cybersecurity, Center for Energy Studies, Rice University; Andy Bochman of Bochman Associates, LLC; Molly Castelazo of Castelazo Marketing, LTD; Dr. Fred Chang, Lyle Endowed Centennial Distinguished Chair in Cyber Security, Southern Methodist University; Jamie Dos Santos, former Chief Executive Officer of Terremark Federal and member of the President's National Security Telecommunications Advisory Committee; Dr. Matt Fleming of the Homeland Security Studies and Analysis Institute; Dr. Irv Lachow, Principal Cyber Security Engineer at the Mitre Corporation; Dr. David Mussington at the Institute for Defense Analyses; Dr. Paul Stockton, former Assistant Secretary for Homeland Defense at the Department of Defense and Managing Director of Sonecon, LLC; Joe Weiss, Managing Partner at Applied Control Solutions, LLC; Aaron Call and Laura Lauer of IO; and Ben FitzGerald, Liz Fontaine, Dr. Dafna Rand and Shawn Brimley at the Center for a New American Security. As always, the views expressed in this paper are the author's alone.

ENDNOTES

1. National Institute of Standards and Technology, "Smart Grid: A Beginner's Guide," nist.gov, May 8, 2013, http://www.nist.gov/smartgrid/beginnersguide.cfm.

2. Executive Office of the President, National Science and Technology Council, *A Policy Framework for the 21st Century Grid: A Progress Report* (February 2013), http://www.whitehouse.gov/sites/default/files/microsites/ostp/2013_nstc_grid.pdf.

3. National Institute of Standards and Technology, "Cybersecurity Framework," nist.gov, March 12, 2014, http://www.nist.gov/cyberframework/index.cfm.

4. Keith Stouffer, Joe Falco and Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security*, Special Publication 800-82 (National Institute of Standards and Technology, June 2011), http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

5. Robert Brese, Chief Information Officer, Department of Energy, personal communication to author, Feb 10, 2014.

6. Gil Vega, "Cybersecurity as a Mission Enabler," PowerPoint presentation, April 2012, San Antonio, TX.

7. Shawn Brimley, Ben FitzGerald and Kelley Sayler, "Game Changers: Disruptive Technology and U.S. Defense Strategy" (Center for a New American Security, September 2013), http://www.cnas.org/files/documents/publications/CNAS_Gamechangers_BrimleyFitzGeraldSayler_0.pdf.

8. Smart Grid Interoperability Panel Smart Grid Cybersecurity Committee, National Institute of Standards and Technology, *Guidelines for Smart Grid Cybersecurity – Revision 1*, NISTIR 7628 (October 2013), http://csrc.nist.gov/publications/PubsNISTIRs.html.

9. Smart Grid Interoperability Panel Cyber Security Working Group, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security* (September 2010), http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf.

10. Jaime Simmons, "GridEx II Simulates Security Breach to U.S. Power Grid," Examiner.com, November 24, 2013, http://www.examiner.com/article/gridex-ii-simulates-security-breach-to-u-s-power-grid.

11. Patrick Coyle, "Reader Comment – 11-02-13 – Project Shine," Chemical Facility Security News blog on blogspot.com, November 5, 2013, http://chemical-facility-security-news.blogspot.com/2013/11/reader-comment-11-02-13-project-shine.html.

12. Exec. Order No. 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register*, 78 no. 33 (February 12, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

13. The White House, *Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience* (February 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

14. Department of Homeland Security, *Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity/Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience Fact Sheet* (March 2013), http://www.dhs.gov/sites/default/files/publications/EO-PPD%20Fact%20Sheet%2012March13.pdf.

15. Smart Grid Interoperability Panel Smart Grid Cybersecurity Committee, National Institute of Standards and Technology, *Guidelines for Smart Grid Cyber Security - Revision 1*.

16. For more information on this developmental path, see National Institute of Standards and Technology, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* (February 12, 2014), http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

17. International Society of Automation, "ISA99, Industrial Automation and Control Systems Security," http://isa99.isa.org/ISA99%20Wiki/Home.aspx

18. Bipartisan Policy Center, *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat*, pp 11-12,February 2014.

19. National Institute of Standards and Technology, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity,* Section 4.7.

20. Defense Science Board, Department of Defense, *Cyber Security and Reliability in a Digital Cloud* (January 2013), http://www.acq.osd.mil/dsb/reports/CyberCloud.pdf.

21. Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," The White House blog on whitehouse.gov, August 6, 2013, http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

About the Center for a New American Security

Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. The views expressed in this report are those of the authors and do not represent the official policy or position of the Department of Defense or the U.S. government.

Center for a New American Security
1152 15th St., NW
Suite 950
Washington, DC 20005

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Contacts
Liz Fontaine
Acting Director of External Relations
and Creative Director
lfontaine@cnas.org, 202.457.9423

JaRel Clay
Communications Associate
jclay@cnas.org, 202.457.9410