# Live Free or Die Hard: U.S.–UK Cybersecurity Policies

KRISTAN STODDART*

IN THE 2007 MOVIE *Live Free or Die Hard,* Detective John McClane, played by Bruce Willis, has to tackle a former U.S. intelligence operative turned terrorist who has gained control of U.S. critical national infrastructure (CNI) through a three-stage synchronized attack on transportation, telecommunications, financial, and public utility computer systems.[1] The plot was based in part on John Carlin's *Wired* magazine article "A Farewell to Arms." That article dealt with a U.S. Department of Defense scenario called "The Day After," in which a series of cyberattacks on the United States mean that "Georgia's telecom system has gone down. The signals on Amtrak's New York to Washington line have failed, precipitating a head-on collision. Air traffic control at LAX has collapsed." and other similar events had taken place.[2]

Whether the reality matches the fiction is open to question, but it is notable that upon the release of *Live Free or Die Hard,* Eugene Kaspersky,

*This article was coauthored with Kevin Jones and Hugh Soulsby of Airbus Group Innovations, Andrew Blyth and Peter Eden of the University of South Wales, and Peter Burnap and Yulia Cherdantseva of Cardiff University.

[1]*Live Free or Die Hard* (20th Century Fox, 2007). The movie was released as *Die Hard 4.0* outside North America.

[2]John Carlin, "A Farewell to Arms," *Wired,* May 1997, accessed at http://archive.wired.com/wired/archive/5.05/netizen.html, 3 February 2015.

**KRISTAN STODDART** is a Senior Lecturer at the Department of International Politics at Aberystwyth University. He is the author or co-author of four books and many articles. He has spoken at a wide number of conferences national and internationally and for various forms of media, including the BBC.

POLITICAL SCIENCE QUARTERLY | Volume 131 Number 4 2016–17 | www.psqonline.org

DOI: 10.1002/polq.12535

the chief executive officer of Kaspersky Lab—one of the world's largest information and communications technology (ICT) security companies—proclaimed, "thank you Hollywood, you opened my mouth."[3] He went on to add, "We live in digital world, a cyber-world, and these systems are all around us, unfortunately they are very vulnerable, we live in a very vulnerable world."[4] The degree to which we live in this "vulnerable world" is the subject of this article.

It will concentrate mainly on the United States and the United Kingdom. Both are liberal democracies, with the United States a lead power and the United Kingdom a mature European nation with global-level responsibilities. This does not mean that other states are ignored, but a wider study that takes these into account is a large and complex task requiring a book-length treatment. Many of the problems and questions that the United States and the United Kingdom face are common to other developed and developing liberal democratic states in a number of ways. Indeed, authoritarian states might be better placed in combatting the threats now being faced because accountability and concerns of civil society in these states are subservient to perceived national interests. This inquiry invites wider discussion of cyber espionage and cyber crime, which are not ignored in this article but deserve focused attention in their own right. The article will begin by outlining SCADA (supervisory control and data acquisition) systems. It will then critically analyze U.S. and U.K. policy in the area of CNI. It will demonstrate that national approaches to CNI breaches, as with many other areas of cybersecurity, need to be concerted internationally where practicable while acknowledging that the needs and concerns of private industry and civil society are taken into consideration.[5]

This is reflective of Lucas Kello's belief in the dispersion of power away from governments in cyberspace, which reflects a growing body of literature on cybersecurity issues.[6] Most notably, cybersecurity concerns have emerged in computer science, political science/international relations, and

[3]"Eugene Kaspersky Talks Cyber Threats, the Future of Security," New York University, Tandon School of Engineering, 4 December 2012, accessed at http://engineering.nyu.edu/news/2012/12/04/eugene-kaspersky-talks-cyber-threats-future-security, 3 February 2015.
[4]Ibid.
[5]For an interesting discussion of these issues in the context of international relations theory, see Madeline Carr, *U.S. Power and the Internet in International Relations: The Irony of the Information Age* (London: Palgrave Macmillan, 2016).
[6]Lucas Kello, "The Meaning of the Cyber Revolution Perils to Theory and Statecraft," *International Security* 38 (Fall 2013): 7–40, at 36.

international law.[7] While this article draws on all three disciplines, it also draws significantly on the technical and industrial base. Scholarship in computer science, driven by technological innovation and industry, has long concerned itself with CNI vulnerabilities. While computer science has underplayed political and strategic factors, international law scholars and political scientists have tended to focus on broader conceptual discussions of cyberattacks and whether fears of cyber war are real or unrealistic, without systematically addressing underlying vulnerabilities.[8] From a security studies perspective, Kello is correct to suggest that theoretically informed discussions of cybersecurity are somewhat embryonic and polarized, with many skeptical of cyber war as a potential reality.[9]

The nature and extent of an attack on CNI and whether this is a single event or part of a broader war-like campaign would dictate the speed of any recovery, as would the capabilities, resource base, and will of the actor(s) involved. Cyberattacks have escalatory potential and could be accompanied by military force. Although this article is not explicitly directed to add to the theorization of contested conceptions of "cyber war," it firmly makes the case that vulnerabilities in CNI make cyber war possible. This is possible not only by "war on [or over] the Internet," as Erik Gartzke claims.[10] It is more in line with the thinking of Jon R. Lindsay, who sees "the pragmatic value of rules of engagement that distinguish reversible damage to code versus irreversible damage to equipment, [which] all

[7]Jack Goldsmith, "How Cyber Changes the Laws of War," *European Journal of International Law* 24 (January 2013): 129–138; Michael Robinson, Kevin Jones, and Helge Janicke, "Cyber Warfare: Issues and Challenges," *Computers & Security* 49 (March 2015): 70–94; Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007); and Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *Journal of Law and Policy for the Information Society* 8 (Fall 2012): 325–340.

[8]The *International Journal of Critical Infrastructure Protection* has existed since 2008 and is technically driven. In political science, the first dedicated cybersecurity journal, the *Journal of Cybersecurity,* published its first issue in September 2015. Conceptual examples from political science/international relations and international law include Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35 (February 2011): 5–32. Balanced approaches can be found in Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35 (June 2012): 401–428; Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22 (September 2013): 365–404; and Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11," *Journal of Peace Research* 51 (September 2014): 347–360.

[9]Kello, "The Meaning of the Cyber Revolution," 9–14, 22. In addition to the foregoing examples, theoretical and conceptual debate abound. See, for example, David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed," *Journal of Strategic Studies* 35 (October 2012): 689–711; Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *Journal of Strategic Studies* 36 (January 2013): 125–133; Adam P. Liff, "The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio," *Journal of Strategic Studies* 36 (January 2013): 134–138; and Erik Gartzke, "The Myth of Cyberwar Bringing War in Cyberspace Back Down to Earth," *International Security* 38 (Fall 2013): 41–73.

[10]This is a phrase repeated throughout his article. See Gartzke, "The Myth of Cyberwar."

imply that the physical boundary is very important to strategic and pragmatic analysis."[11]

## SCADA AND INDUSTRIAL CONTROL SYSTEMS

In the real world, both John McClane and the hackers who assisted him in thwarting the terrorists would have to be aware of SCADA, a type of industrial control system (ICS). These systems date back to the 1940s and their use in the electric utilities sector. Most current SCADA systems date to the advent of cost-effective 8- and 16-bit minicomputers and then microcomputers in the 1970s, 1980s, and 1990s. These are increasingly seen as legacy systems, and they are an attack vector for computer-controlled CNI, which includes public utilities such as electricity, water, and transport. These affect every area of developed societies; disruption or damage to these sectors would have profound effects on developed societies that are used to electricity on demand, traffic systems that are safe, and water supplies that are uncontaminated and always available.

The main purpose of SCADA systems is to monitor, physically control, and alarm plant or regional systems from central locations in real time.[12] This includes the operation of local, regional, national, and, in some cases, supranational parts of CNI. Disruption or damage to these systems could affect global critical infrastructure through a cascade effect, such as the economic crash of 2008. As a 2010 U.K. parliamentary report made clear, "national infrastructure is a highly interconnected network both within and between sectors. Failure in one area can spread unexpectedly to others."[13] SCADA systems also have unique sets of properties:

> due to their continuous operation, [SCADA] are not updated or redesigned in some cases for decades. The nature of SCADA systems requires them to be operational 24 hours 7 days a week. This makes the regular patching and upgrading of both SCADA software and a hosting operating system difficult, if not impossible . . . patching of a SCADA system is complicated by the facts that the system is time-critical, there is no test environment and patching may introduce new unknown vulnerabilities or ultimately break the system. Legacy SCADA

[11]Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39 (Fall 2014): 181–192, at 186.
[12]"SCADA Systems," accessed at http://www.engineersgarage.com/articles/scada-systems, 22 July 2014.
[13]Houses of Parliament, Parliamentary Office of Science and Technology, "Resilience of UK Infrastructure," *Postnote,* no. 362 (October 2010), accessed at http://www.parliament.uk/documents/post/postpn362-resilience-of-UK-infrastructure.pdf, 23 July 2014.

> systems may end up relying on operating systems and software that are no longer supported by vendors.[14]

In the water utilities sector, SCADA can control plant systems such as wastewater treatment facilities, while "regional" systems include intake and/or effluent structures, pumping stations, chlorination stations, control valve stations, and so on. For electricity generation, SCADA systems can detect current flow and line voltage, monitor the operation of circuit breakers, or take substations off or onto national grids. SCADA is an embedded technology in developed and developing states across a wide range of sectors and industries.[15] Developed societies now have a high degree of dependency on the computerized control of these sectors, and that dependency is deepening with the introduction of various "smart" technologies and the ever-growing "Internet of things." (IoT). In the meantime, legacy systems will still be operating.

The degree of vulnerability is felt in all developed and developing nations and has been the subject of active debate for national governments and private industry.[16] Numerous cyberattacks on SCADA systems have taken place.[17] There are already publicly discussed fears of a "cyber Pearl Harbor," a "cyber 9/11," or even a statewide "Cybergeddon" attack, as in *Live Free or Die Hard*, aimed at crippling or seriously damaging a nation but which could cascade to other states. This could be both a precursor to and a part of conflicts.[18]

There are three main elements of SCADA systems: various remote telemetry units (RTUs), communications that relay information, and a human machine interface (HMI) that displays that information in the form of graphics or alphanumeric readouts. The HMI is essentially a personal computer system running graphic and alarm software programs. At the facilities themselves, programmable logic controllers (PLCs), which are industrial computer control systems, "continuously monitor the state of input devices and make decisions based upon a custom program to control

---

[14]Yulia Cherdantseva, Peter Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart, "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Computers & Security* 56 (February 2016), 1–27, at 5.

[15]"What Is SCADA?," accessed at http://www.dpstele.com/dpsnews/techinfo/what_is_scada.php, 22 July 2014.

[16]The two most polarized examples of these debates are found in Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (London: Ecco Press, 2010); and Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

[17]Bonnie Zhu, Joseph Anthony, and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (Washington, DC: IEEE Computer Society, 2011), 380–388.

[18]See, for example, Clarke and Knake, *Cyber War;* and Elisabeth B. Miller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times,* 12 October 2012, accessed at http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0, 23 July 2014.

the state of output devices."[19] PLCs can be used to control timing for output devices and operations, such as opening and closing water treatment valves or managing and determining electricity current. The operating systems used by these RTUs and PLCs, including VxWorks and Enea OSE, have exploitable vulnerabilities.[20]

If these systems are running proprietary software such as Windows (especially older versions such as Windows NT or XP, neither of which is supported or patched by Microsoft[21]), then their security flaws are already well known and understood in the hacking community, by ICT specialists, and by states such as China (which itself has these problems).[22] Other operating systems used in ICS include Unix and the more widely used Unix-like Linux OS.[23] Defending against these vulnerabilities is problematic. As Cherdantseva and colleagues argue,

> For over forty years confidentiality, integrity and availability—also referred to as the CIA-triad—have been defining the set and priorities of security goals for corporate information systems. In ICS and SCADA systems, the priorities among the goals are different. Among the triad, integrity and availability are highly paramount, while confidentiality is secondary for SCADA systems. In reality, security goals, in what ever order they appear, are often preceded in SCADA systems by safety, reliability, robustness and maintainability (which are the supreme goal of critical systems).[24]

SCADA systems are often customized rather than bought commercially off the shelf. Furthermore, SCADA systems are component based, and

---

[19]"What Is a PLC?," accessed at http://www.amci.com/tutorials/tutorials-what-is-programmable-logic-controller.asp, 22 July 2014.

[20]Eric Byres, "PLC Security Risk: Controller Operating Systems," accessed at https://www.tofinosecurity.com/blog/plc-security-risk-controller-operating-systems and https://ics-cert.us-cert.gov/advisories/ICSA-13-259-01B, 17 February 2016. See also "Overview of Cyber Vulnerabilities," accessed at https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities, 17 February 2016. For greater detail and thought-provoking insights, see Jane LeClair, ed., *Protecting Our Future,* vol. 2, *Educating a Cybersecurity Workforce* (Albany, NY: Hudson Whitman/Excelsior College Press, 2015).

[21]Microsoft, "Windows XP Support Has Ended," accessed at http://windows.microsoft.com/en-gb/windows/end-support-help, 27 July 2014.

[22]Windows XP is widely pirated in China, and 70 percent of security flaws are never patched. This has led to high-level discussions with the Chinese authorities over continued support for the operating system. See, for example, Michael Kan, "Windows XP Will Continue Receiving Security Support in China," *PC World,* 3 March 2014, accessed at http://www.pcworld.com/article/2103680/chinas-windows-xp-users-to-still-get-security-support.html, 27 July 2014 and Mark Ward, "XP—The Operating System That Will Not Die," BBC News, 5 March 2014, accessed at http://www.bbc.co.uk/news/technology-26432473, 27 July 2014.

[23]Michael Mimoso, "Patching Bash Vulnerability a Challenge for ICS, SCADA," Threatpost, 25 September 2014, accessed at http://threatpost.com/patching-bash-vulnerability-a-challenge-for-ics-scada, 26 September 2014.

[24]Cherdantseva, et al., "A Review of Cyber Security Risk Assessment," 5.

although there are industry standards, no two SCADA systems are likely to be the same. SCADA forms the backbone of CNI in an age when ICT of various types underpins much of the world's industrial, economic, and social interests. Through websites such as Shodan, Internet-facing SCADA systems can be targeted by both "Black Hat" hackers who can gain access to these systems to alter the computer code for malicious intent or by "White Hat" hackers who highlight these vulnerabilities for owner-operators and governments.[25] SCADA vulnerabilities also include communications traffic managed within a plant or geographically dispersed site, which is often by data cable, wire, or fiber-optic, while regional systems most commonly utilize radio. SCADA systems will indicate the nature and degree of a problem, with the ability to remotely control site equipment providing an entry point or back door.[26]

The software security provider FireEye-Mandiant alarmingly warned in a report titled "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model" that "attackers got through organizations' cyber 'Maginot Line' at least 97 percent of the time. They compromised more than 1,100 critical systems spanning a wide gamut of geographies and industries. This suggests that thousands upon thousands of organizations around the world may be breached and not even know it."[27] Their analysis of real-world data, taken from more than 1,216 organizations in 63 countries and more than 20 major industries (making it a global and multisector study), is a worrying signpost.

The most widely known, and most widely reported, attack to date on a SCADA system was Stuxnet. Stuxnet adversely affected the centrifuges in the Natanz nuclear processing plant in Iran, unbeknownst to the operators.[28] A lesser known but disturbing attack was made on the SCADA systems of a German steel mill in 2014, which caused the blast furnace to shut down, resulting in massive damage but no loss of life.[29] A further attack occurred in December 2015 in Ukraine that

[25]See Shodan, accessed at http://www.shodanhq.com/, 2 February 2015 and Kim Zetter, "10K Reasons to Worry about Critical Infrastructure," *Wired,* 24 January 2012, accessed at http://www.wired.com/2012/01/10000-control-systems-online/, 2 February 2015.

[26]For more information, see https://www.cpni.gov.uk/scada/, accessed 22 July 2014.

[27]FireEye and Mandiant, "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model," accessed at http://www2.fireeye.com/rs/fireye/images/fireeye-real-world-assessment.pdf, 27 September 2014.

[28]For an excellent synopsis of Stuxnet, see Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy,* 19 November 2013, accessed at http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/, 10 October 2016. See also Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Business, 2014).

[29]"Hack Attack Causes 'Massive Damage' at Steel Works," BBC News, 22 December 2014, accessed at http://www.bbc.co.uk/news/technology-30575104, 3 January 2015.

precision-targeted three regional power distribution companies through external attack. Although it lasted only a few hours, 225,000 customers were affected.[30] Whether governments (or private industry) will ever be able to prevent these "intelligence failures" is disputed.[31]

There are many gateways and back doors into systems. Hardware, for example, often has passwords hardwired into its firmware that are widely available on the Internet. A multiplying myriad of known and unknown ("zero day"[32]) software vulnerabilities mean that ideas of perimeter defenses through firewalls are insufficient by themselves. Moreover, human operators can be a weak link, and insider attacks are difficult to defend or see coming.[33] Externally, if investigations by the director of the U.S. National Cybersecurity and Communications Integration Center in the U.S. Department of Homeland Security (DHS) are a guideline, then not only are ICS connected to the corporate/enterprise network, which is Internet facing, but also they are connected through multiple pathways with air-gapped systems (not being Internet connected) a myth.[34] With all of this in mind, better bottom-up practices have to be further encouraged and enabled by private industry in the specific area of ICS and SCADA.[35] This should be combined, through a joint approach, by central governments in the United States, United Kingdom, and elsewhere through top-down education programs and industry incentives and regulation.

---

[30]"Cyber-Attack against Ukrainian Critical Infrastructure," Industrial Control Systems Cyber Emergency Response Team, 25 February 2016, accessed at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01, 28 June 2016. The activities of ICS-CERT and related organizations provide a valuable protective barrier.

[31]See, for example, Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31 (October 1978): 61–89; and David Omand, *Securing the State* (London: Hurst & Co., 2012).

[32]Martin C. Libicki, Lillian Ablon, and Tim Webb, *The Defender's Dilemma: Charting a Course towards Cybersecurity* (Santa Monica, CA: RAND Corporation, 2015), 44–49. The authors offer an extremely good assessment of "zero days" and the "hacking community" but distinctly underplay how these can be used against CNI targets.

[33]Libicki, Ablon, and Webb, *The Defender's Dilemma,* 33; and Cherdantseva et al., "A Review of Cyber Security Risk Assessment," 5.

[34]Bill Lydon, "Cyber Security Threats: Expert Interview with Eric Byres, Part 1," 28 August 2011, accessed at http://www.automation.com/automation-news/article/cyber-security-threats-expert-interview-with-eric-byres-part-1, 28 September 2014 and Eric Byres, "ICS and SCADA Security Myth: Protection by Air Gap," accessed at https://www.tofinosecurity.com/blog/1-ics-and-scada-security-myth-protection-air-gap, 28 September 2014.

[35]One technical approach could be to integrate these risks and produce a business process model. See, for example, Remco Dijkman, Irene Vanderfeesten, and Hajo A. Reijers, "Business Process Architectures: Overview, Comparison and Framework," *Enterprise Information Systems* 10 (2016): 129–158.

## SCADA AND CRITICAL NATIONAL INFRASTRUCTURE

Business needs are a vital consideration in the United States, the United Kingdom, and around the world. The applications of increasing connectivity and the boon that technology brings are readily apparent. Many of us will need no reminder of the world before the Internet. However, increasing connectivity without commensurate thought towards cybersecurity ignores the issues we now face. While safety is already an established part of business practice in the sectors that encompass CNI, cybersecurity has been a latecomer.

The original designers of modern CNI simply did not anticipate the rise of the Internet and the increasing levels of connectivity we increasingly demand, or how the world of CNI now has back doors and booby traps that can be exploited remotely in what were hitherto considered physically safe and secure sites. With around 80 percent of CNI owned and operated by private industry and neoliberal economic practices prioritizing minimum state intervention in the United States, the United Kingdom, and many other liberal democracies, this poses a problem of responsibility. Improving resilience requires a mutual undertaking between government and private industry. This mutual undertaking is embedded in states such as Germany and Estonia, among many others.[36] Already there have been several attacks on SCADA systems including the following:

- In August 2003, the "Slammer" worm infected "more than 90 percent of vulnerable hosts within 10 minutes, causing significant disruption to financial, transportation, and government institutions and precluding any human-based response."[37] This included the Davis-Besse nuclear power plant in Ohio, which led to a five-hour shutdown of computer systems.
- In August 2006, the city council of Los Angeles temporarily blocked engineers from accessing the computers controlling traffic signals during a strike by city

[36]Details of U.S. and U.K. policies in this area are provided in the following sections. For German policy, see "CIP Implementation Plan of the National Plan for Information Infrastructure Protection," 2009, accessed at http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.html, 25 January 2016. For Estonia, see "2014–2017 Cyber Security Strategy," 2014, accessed at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world, 14 February 2016. The website of the European Union Agency for Network and Information Security contains information on many valuable practises in the field of CNI protection across the European Union and worldwide.

[37]On the "Slammer" worm, see David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, "Inside the Slammer Worm," *IEEE Security and Privacy,* July/August 2003, 33–39, accessed at http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf, 23 August 2014.

employees. Nevertheless, two employees, engineers Kartik Patel and Gabriel Murillo, hacked in and programmed signals so that red lights would stay on for an extended length of time on the most congested roads, causing gridlock.[38]

- In October 2006, a foreign hacker planted malware in the water filtration system in Harrisburg, Pennsylvania.[39]
- In June 2008, the Hatch nuclear plant in Georgia was closed for two days after an engineer installed a software patch for a business network that rebooted the plant's power control system.[40]
- In April 2009, it was reported in the *Wall Street Journal* that foreign actors had infiltrated the U.S. electrical grid and managed to install software that could be used to disrupt the system. It was reported that the hackers were from China and Russia in what should be assumed were separate attempts to map the U.S. electrical grid.[41]

In 2013, a pair of U.S. researchers found more than two dozen vulnerabilities in products that are used in CNI that would permit attackers to hijack a SCADA system to crash servers controlling electricity substations and water systems.[42] Although their findings were specific to North American electrical grid systems, this is unlikely to be a regional issue given global supply chains in ICS.[43] The aforementioned case of the German steel mill and the Ukrainian power outage are but the latest examples with public disclosures able to shake public confidence and harm stock prices.

## U.S. GOVERNMENT CYBERSECURITY ACTIVITIES AND THE PRIVATE SECTOR

As far back as 1997, the vulnerability of U.S. CNI to cyberattack and catastrophic failure was recognized in a report by the President's

[38]Luckily, no reported accidents occurred. See "Engineers Who Hacked into L.A. Traffic Signal Computer, Jamming Streets, Sentenced," *L.A. Now* (*Los Angeles Times* blog), 1 December 2009, accessed at http://latimesblogs.latimes.com/lanow/2009/12/engineers-who-hacked-in-la-traffic-signal-computers-jamming-traffic-sentenced.html, 19 August 2014.

[39]U.S. Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (Washington, DC: U.S. Government Printing Office, 2007), accessed at http://www.gao.gov/assets/270/268137.pdf 11 October 2016.

[40]Brent Kesler, 'The Vulnerability of Nuclear Facilities to Cyber Attack', *Strategic Insights* 10 (Spring 2011): 21-24.

[41]Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal,* 8 April 2009. See also Maggie Shiels, "Spies 'Infiltrate U.S. Power Grid,'" BBC News, 9 April 2009, accessed at http://news.bbc.co.uk/1/hi/technology/7990997.stm, 29 September 2014.

[42]Kim Zetter, "Researchers Uncover Holes That Open Power Stations to Hacking," *Wired,* 16 October 2013, accessed at http://www.wired.com/2013/10/ics/, 15 July 2014.

[43]Ibid.

Commission on Critical Infrastructure Protection.[44] In 2003, President George W. Bush established the United States Computer Emergency Readiness Team (US-CERT) under the DHS. Within the DHS, this is a branch of the Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center.[45] Its remit is to lead "efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans."[46]

US-CERT has 24/7 reporting mechanisms through a dedicated operations center that invites reporting of cybersecurity incidents or software vulnerabilities. Threat information is analyzed and disseminated through the National Cyber Awareness System, and US-CERT operates a Vulnerability Notes Database that provides technical descriptions of system vulnerabilities. Crucially, "US-CERT partners with private sector critical infrastructure owners and operators, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local partners, and domestic and international organizations to enhance the Nation's cybersecurity posture."[47]

The Protected Critical Infrastructure Information (PCII) Program is designed to protect sensitive or proprietary information, including that deemed to be commercially sensitive, that is passed by owner-operators to the DHS and state governments. PCII is then used to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures. This allows the DHS to help protect America's CNI through the vulnerability data it collects through programs such as the Enhanced Critical Infrastructure Protection security surveys along with Site Assistance Visits (SAVs) and risk management tools such as the Computer-Based

---

[44]Dana A. Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat* (Washington, DC: Congressional Research Service, 21 February 2003), accessed at http://fas.org/irp/crs/RL31534.pdf, 15 July 2014. See also Michael Warner, "Cyber-Security: A Pre-History," *Intelligence and National Security* 27 (October 2012): 781–799. On U.S. efforts in this realm, see Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age* (London: Routledge, 2008); and Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace 1986–2002* (Vienna, VA: Cyber Conflict Studies Association, 2013), 14–88.

[45]In October 2010, a memorandum of understanding between the Departments of Homeland Security and Defense was signed to increase interdepartmental collaboration. See James Andrew Lewis and Götz Neuneck, *The Cyber Index: International Security Trends and Realities* (Geneva: United Nations Institute for Disarmament Research, 2013), 53, accessed at http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf, 11 October 2016.

[46]United States Computer Emergency Readiness Team (US-CERT), "About Us," accessed at https://www.us-cert.gov/about-us, 17 January 2015.

[47]Ibid.

Assessment Tool, the Voluntary Chemical Assessment Tool, and the Automated Critical Asset Management System. Under PCII, through the Critical Infrastructure Information Act (2002), owner-operators are legally protected from the Freedom of Information Act; state, tribal, and local disclosure laws; use in regulatory actions; and use in civil litigation.[48]

Given the potential harm that could result from damage or disruption to CNI, this is a major incentive for companies to report breaches and vulnerabilities. Access to PCII is restricted to trained and certified federal, state, and local government employees or contractors on a "need to know" basis.[49] However, this remains a voluntary system of reporting rather than a legally mandated one that makes nonreporting a civil or criminal act.[50]

Through the SAVs, advice is provided on identifying vulnerabilities alongside subject-matter experts from the National Guard who deal with physical security. This takes place at the request of owner-operators rather than through government intervention.[51] Responsibility for cybersecurity is also vested in the Federal Bureau of Investigation (FBI) and the Department of Defense. This includes the U.S. Cyber Command, which coordinates with the National Security Agency (NSA), alongside the Departments of State and Commerce, which take the lead on international negotiations and development of cybersecurity standards.[52] In addition, there is the long-standing National Institute of Standards and Technology (NIST) within the Department of Commerce.[53] An additional federal-level program is administered by the National Cyber Response Coordination Group, which is a joint enterprise between the Defense and Justice Departments for coordinating the 13 federal agencies under their authority in the event of a major national cyber incident.[54]

---

[48]For the relevant legal statutes, see 6 CFR Part 29, "Protected Critical Infrastructure Information," accessed at http://www.law.cornell.edu/cfr/text/6/part-29, 19 January 2015.

[49]In addition, PCII can only be accessed "in accordance with strict safeguarding and handling requirements." See U.S. Department of Homeland Security, "Protected Critical Infrastructure Information (PCII) Program," accessed at http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program, 19 January 2015. See also U.S. Department of Homeland Security,. "Receive PCII Authorized User Training," accessed at https://www.dhs.gov/pcii-authorized-user-training, 14 October 2016.

[50]An early commentary on these issues can be found in James J.F. Forest, ed., *Homeland Security: Critical infrastructure* (Westport CT: Praeger, 2006), 69–75.

[51]U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency are Evolving but Program Management Could Be Strengthened* (Washington, DC: U.S. Government Printing Office, 2010).

[52]Lewis and Neuneck, *The Cyber Index,* 52–54.

[53]NIST's latest guidance can be accessed at http://www.nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf, 1 February 2015.

[54]Lewis and Neuneck, *The Cyber Index,* 52–54; and US-CERT, "DHS Cyber Security," accessed at https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf, 1 February 2015.

In 2007, the FBI established the National Cyber Investigative Joint Task Force (NCIJTF), based near Washington, DC. The NCIJTF has agents drawn from across the intelligence communities, including the U.S. Secret Service, and several federal agencies from across government. Shawn Henry, then the deputy assistant director of the FBI's Cyber Division, publicly noted that the NCIJTF encompasses "all cyber threats" but especially "organizations that are targeting U.S. infrastructure." Henry added, "We're sharing investigative and threat information . . . looking at the attacks [each agency is] seeing and the methodologies being used."[55] The NCIJTF is seen as one of the cornerstones for a whole-of-government approach to protecting the United States from cybersecurity threats and operates under the 2008 Comprehensive National Cybersecurity Initiative.[56] This does not mean the FBI is the lead organization for CNI protection by default, and this is not dependent on the actor(s) involved. Instead, there is multiagency participation.[57]

In October 2012, the FBI also launched its Next Generation Cyber Initiative in response to the Office of the Inspector General report of April 2011, which expressed concern over the FBI's ability to address cyber intrusion threats to the United States. This has seen the FBI shift its focus from reacting to cyber intrusions to "predicting and preventing them."[58] The FBI currently ranks cyber-based attacks third on its list of priorities, after counterterrorism and counterintelligence. In 2012, Robert S. Mueller, the former director of the FBI, stated before Congress that he anticipated that cyber threats would surpass terrorism in the coming years.[59] Information sharing between the FBI and the private sector remains problematic, a situation exacerbated by the Edward Snowden revelations.[60]

With these problems in mind, the Barack Obama administration tabled some controversial cybersecurity legislation after 2012 and found it blocked by the Republican-controlled Congress, which believes this will

[55]"FBI Organizes Defense against Cyber-Attacks," *Washington Times,* 21 April 2008, accessed at http://www.washingtontimes.com/news/2008/apr/21/fbi-organizes-defense-against-cyber-attacks/, 29 May 2016.
[56]Federal Bureau of Investigation, "Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity," accessed at https://www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view, 10 October 2016.
[57]Remarks made during presentations at the 8th International Conference on Cyber Conflict, Tallinn, Estonia, 1–3 June 2016.
[58]U.S. Department of Justice, Office of the Inspector General, "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative," July 2015, i–ii, accessed at https://oig.justice.gov/reports/2015/a1529.pdf, 29 May 2016.
[59]Ibid., i.
[60]Ibid., ii–iii, 17–22, 28.

unduly impinge on the private sector to share information with federal government.[61] The Obama administration was also at odds following the appointment of Howard Schmidt as "cyber czar" from 2009 to 2012. Schmidt publicly repudiated the concept of cyber war and doubted that public utilities such as the U.S. electrical grid could be hacked.[62] He found himself contradicting stated military policy, with Admiral Mike McConnell, the former director of national intelligence, testifying to the U.S. Senate in February 2010 that "[i]f the Nation went to war today in a cyber war, we would lose . . . We're the most vulnerable. We're the most connected. We have the most to lose.[63]

With this NSA-spiked warning in mind, the Obama administration introduced Presidential Policy Directive 20 (PPD-20) in October 2012, which set the parameters for defensive and offensive cyber operations conducted by the U.S. government and formed part of the disclosures of intelligence subcontractor turned whistleblower Edward Snowden. PPD-20 helped formulate new rules of engagement and strengthened the U.S. Cyber Command for this end alongside the military branches it oversees.[64] It also included Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." This sought to promote further voluntary "sharing of actionable threat information and warnings between the private sector and the U.S. Government and to spread industry-led cybersecurity standards and best practices to the most vulnerable critical infrastructure companies and assets."

This was followed up by a further framework document in 2014, while the breach of Sony later in the year focused attention on state-based threats to private industry.[65] The personal data of 21 million Americans hacked

---

[61]Dominic Rushe and Spencer Ackerman, "Obama Plans for Cybersecurity Aim 'To Make Internet Safer Place,'" *The Guardian,* 21 January 2015, accessed at http://www.theguardian.com/us-news/2015/jan/20/obama-cybersecurity-state-of-the-union-address-speech, 1 February 2015.

[62]Ryan Singel, "White House Cyber Czar: There Is No Cyberwar," *Wired,* 4 March 2010, accessed at http://www.wired.com/2010/03/schmidt-cyberwar/, 15 February 2016.

[63]U.S. Senate, Committee on Commerce, Science, and Transportation, *Cybersecurity: Next Steps to Protect Our Critical Infrastructure,* 111th Cong., 2nd sess., 23 February 2010, accessed at https://fas.org/irp/congress/2010_hr/cybersec.pdf, 15 February 2016. McConnell repeated his remarks in an opinion piece, "Mike McConnell on How to Win the Cyber War We're Losing," *Washington Post,* 28 February 2010, accessed at http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html, 15 February 2016.

[64]Lewis and Neuneck, *The Cyber Index,* 52–54. See also Glenn Greenwald and Ewen MacAskill, "Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks," The Guardian, 7 June 2013, accessed at http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text, 1 February 2015.

[65]White House, "Cybersecurity," accessed at http://www.whitehouse.gov/issues/foreign-policy/cybersecurity, 1 February 2015 and Michael D. Shear, "Obama to Announce Cybersecurity Plans in State of the Union Preview," *New York Times,* 10 January 2015, accessed at http://www.nytimes.com/2015/01/11/us/politics/obama-to-announce-cybersecurity-plans-in-state-of-the-union-preview.html?_r=0, 2 February 2015.

from the U.S. Office of Personnel Management in 2015 also highlighted that vulnerabilities that exist within government.[66] The approach of the Obama administration to cybersecurity pays heed to these breaches and warnings issued by the NSA. Its views were summarized by Philip D. Quade, chief of the NSA Cyber Task Force, who said in the fall of 2015,

> Cyber resilience is a critical business and social issue for our nation. America's national security and economic prosperity are increasingly dependent upon critical communications infrastructures that are at risk from a variety of hazards, including cyber-attacks. These infrastructures are the backbone of our nation's economy, security, and health and requires a unified whole-of-nation, whole-of-community effort to maintain secure, functioning, and resilient critical infrastructures. Safeguarding the physical and cyber aspects of critical infrastructures is a national priority that requires information sharing and partnerships at all levels of government and industry. While the majority of our nation's critical infrastructure is privately owned and operated, both the government and the private sector have a shared interest to prevent and reduce the risks of disruptions to critical infrastructures. The need to prepare for all types of events shifts the focus from asset protection to one of overarching system resilience.[67]

How this is accomplished is a complex matter. Private industry finds the legislative proposals on the table "burdensome" and unnecessarily intrusive, while the U.S. federal government sees merit in this approach to combat valid national security concerns.[68] It is also unhelpful that the NSA and DHS have crosscutting remits in cybersecurity—especially concerning CNI protection.[69] The legislative record of the Obama administration in the field of cybersecurity is patchy (pun intended). In 2013, Obama issued

---

[66]Tal Kopan, "OPM Hit for Mishandling Data Breach Cleanup," CNN, 10 December 2015, accessed at http://edition.cnn.com/2015/12/10/politics/opm-data-breach-contract-improper-ig/, 15 February 2016.

[67]"In Discussion with Philip Quade, Chief of NSA Cyber Task Force," National Security Agency, 9 October 2015, accessed at https://www.nsa.gov/public_info/news_information/2015/ncsam/NCSAM_Week2.shtml, 15 February 2016. See also Kelly Jackson Higgins, "Former Director of NSA and CIA Says US Cybersecurity Policy MIA," 13 January 2016, accessed at http://www.darkreading.com/attacks-breaches/former-director-of-nsa-and-cia-says-us-cybersecurity-policy-mia/d/d-id/1323888, 15 February 2016.

[68]See, for example, Jody Westby, "The Government Shouldn't Be Lecturing Private Sector on Cybersecurity," *Forbes*, 15 June 2015, accessed at http://www.forbes.com/sites/jodywestby/2015/06/15/the-government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity/#45c2d9df38d6, 15 February 2016; Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions* (Washington, DC: Congressional Research Service, 16 March 2015); and Steve Rosenbush, "Former NSA Chief Mike McConnell Says Culture, Not Tech, Is Key to Cyber Defense," 20 June 2014, accessed at http://blogs.wsj.com/cio/2014/06/20/former-nsa-chief-mike-mcconnell-says-culture-not-tech-is-key-to-cyber-defense/, 15 February 2016.

[69]Colin Clark, "Build a 'Department of Cyber': Former DNI McConnell," 3 March 2015, accessed at http://breakingdefense.com/2015/03/build-a-department-of-cyber-former-dni-mcconnell/, 15 February 2016.

an executive order that tasked NIST with developing cybersecurity standards for CNI through a "Cybersecurity Framework."[70] As Ed Dourado and Andrea Castillo describe, then "a spate of cybersecurity bills were signed into law in late 2014, which separately defined the National Cybersecurity Communications Integration Center as the main federal cyber information sharing hub, authorized NIST to facilitate the Cybersecurity Framework, amended the FISMA reporting processes, and increased cybersecurity workforce examinations and placements."[71]

In his 2015 State of the Union address, President Obama declared that "[n]o foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism."[72] Obama outlined three areas in which bipartisan support from Republicans was possible: increasing the sharing of cyberattack information between private companies and the government, bolstering law enforcement's ability to investigate and prosecute cyber criminals, and establishing a federal mandate for hacked companies to disclose breaches to customers within 30 days of discovering the hack. The last of these proposals would replace the "patchwork quilt" of reporting mechanisms that currently operate in the majority of U.S. states and the relationship of state-level cybersecurity to the federal government.[73]

In February 2016, a further executive order was issued that created a commission to examine the question of how to establish better cybersecurity practices for government and the private sector over the next decade. Part of its broad remit intends to provide "effective private sector and government approaches to critical infrastructure protection in light of current and projected trends in cybersecurity threats and the connected nature of the United States economy."[74] To be successful, this needs to be conducted in a spirit of (relative) harmony for the greater national and

[70]These executive orders can be accessed at https://www.whitehouse.gov/briefing-room/presidential-actions/executive-orders, 16 February 2016.
[71]Ed Dourado and Andrea Castillo, "Poor Federal Cybersecurity Reveals Weakness of Technocratic Approach," Mercatus Center at George Washington University, June 2015, accessed at http://mercatus.org/sites/default/files/Dourado-Poor-Federal-Cybersecurity-MOP.pdf, 16 February 2016.
[72]Julianne Pepitone, "SOTU: Will Obama's Cybersecurity Proposals Actually Protect You?," NBC News, 20 January 2015, accessed at http://www.nbcnews.com/storyline/2015-state-of-the-union/sotu-will-obamas-cybersecurity-proposals-actually-protect-you-n289826, 24 January 2015.
[73]Ibid.
[74]"Executive Order—Commission on Enhancing National Cybersecurity," White House, 9 February 2016, accessed at https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity, 16 February 2016.

international interest. Despite the promise, this raft of legislation goes too far for some, while for others, it does not go far enough. Joel Brenner, a senior cybersecurity adviser at the NSA, claimed in early 2015,

> Our nation is being turned inside out electronically and we seem helpless to stop it. The Russians have broken into a White House network and JPMorgan Chase. The Chinese have stolen blueprints, manufacturing processes, clinical trial results and other proprietary data from more than 140 companies and have utterly penetrated major media. The Iranians attack our banks, our electric grid is assaulted with frightening frequency and North Korea has brought Sony to its knees. Meanwhile, credit card data from big retailers such as Target and Home Depot are for sale electronically by the boatload. Infrastructure is at risk. Last month, attackers disrupted production at a German steel plant and damaged its blast furnaces, using only cyber methods. The fact that network attacks are getting worse, even after vast sums have been invested in defense, should tell us something fundamental about the deeply flawed nature of our networks. Unfortunately, the measures just announced by President Barack Obama do not address these flaws. He's right that better information-sharing between the private sector and the government is overdue; Congress should finally pass legislation to make it possible. But it would not address underlying weaknesses in the Internet. Stiffer sentences for cyber crime may be useful, but they would not make our infrastructure harder to attack or our communications more secure. His proposal for a uniform breach-notification law would simplify companies' legal compliance, but it would do nothing to prevent breaches.[75]

Brenner also added this warning:

> We have been walking backward on cyber defense while ignoring the real issues. First, we adopted a moat-and-drawbridge approach. This didn't work for two reasons. We had barbarians inside the gates, and the gates themselves, which we fancied as "firewalls," were merely flimsy filters . . . All defense strategies are variants on these models, and all of them are variants of Whac-A-Mole. We are playing a losing game.[76]

The legislative proposals put forward by Obama and those advocated by Brenner share commonalities with the Cyber Intelligence Sharing and Protection Act, which has now become the Cybersecurity Information

[75]Joel Brenner, "How Obama Fell Short on Cybersecurity: Under the President's Proposals, We'll Remain America the Vulnerable," Politico, 21 January 2015, accessed at http://www.politico.com/magazine/story/2015/01/state-of-the-union-cybersecurity-obama-114411.html#ixzz3PjrwwEnf, 24 January 2015.
[76]Brenner, "How Obama Fell Short on Cybersecurity." Brenner's wider views on cybersecurity can be found in Joel Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (New York: Penguin 2013).

Sharing Act (CISA). CISA can be used to force private companies, including industry giants such as Microsoft, Apple, and Google, to share data with the government.[77] This public–private tie-in was brought sharply into focus by the Snowden revelations and the Apple-FBI iPhone dispute. As a 2015 Congressional Research Service report details, "there are many reasons why entities may opt to not participate in a cyber-information sharing scheme, including the potential liability that could result from sharing internal cyber-threat information with other private companies or the government."[78] This has not halted collaboration between the U.S. and U.K. governments, which share mutual security interests with long-standing intelligence coordination between themselves as well as with allied nations.[79]

## U.K. GOVERNMENT CYBERSECURITY ACTIVITIES AND THE PRIVATE SECTOR

There was little direct "governance" of CNI in the United Kingdom in the way national industries were run centrally by government prior to their privatization during the 1980s and 1990s. Instead, as CNI is largely owned and operated by private industry, it resembles more a form of macromanagement in terms of oversight and regulation in the way the National Health Service and National Rail are now run. Micromanagement in the nine sectors that comprise CNI (communications, emergency services, energy, financial services, food, government, health, transport, and water), which are large and complex sets of organizations with enormous budgets, is undertaken through regulation and oversight via formal and informal statutory regulators and legal bodies. Within the context of national security and the protection of CNI, the October 2010 U.K. Strategic Defence and Security Review (SDSR) stated,

> Over the last decade the threat to national security and prosperity from cyber attacks has increased exponentially. Over the decades ahead this

[77]Andy Greenberg, "Congress Slips CISA into a Budget Bill That's Sure to Pass," *Wired,* 16 December 2015, accessed at http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/, 15 February 2016. See also Lewis and Neuneck, *The Cyber Index,* 50–52.

[78]Nolan, *Cybersecurity and Information Sharing,* summary.

[79]This includes a rolling program of "war games" between the two to test their cyber reliance, the first of which simulated an attack on their financial services sectors. Nicholas Watt, "US and UK Plan Cyber 'War Games' to test Resilience," *The Guardian,* 16 January 2015, accessed at http://www.theguardian.com/technology/2015/jan/16/cyber-war-games-uk-us-intelligence, 2 February 2015. See also Warwick Ashford, "Cameron and Obama Plan War Games to Test Cyber Resilience," *Computer Weekly,* 16 January 2015, accessed at http://www.computerweekly.com/news/2240238298/Cameron-and-Obama-plan-war-games-to-test-cyber-resilience, 2 February 2015.

> trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict. We need to be prepared as a country to meet this growing challenge . . . [of] cyber and proxy actions instead of direct military confrontation [and it] will play an increasing part, as both state and non-state adversaries seek an edge over those who overmatch them in conventional military capability. As a result, the differences between state-on-state warfare and irregular conflict are dramatically reducing.[80]

It recognized that cyberattacks can be a force multiplier for weaker nations against stronger, more developed nations and help offset hard military capabilities and the economic and industrial capacity that underpin them. The SDSR ranked cyber threats as one of four Tier One threats to the United Kingdom, alongside terrorism. The potential for disruption or damage of CNI was also recognized in the 2015 SDSR, which again placed cyber threats as a Tier One threat to national security. It warned that a "growing numbers of states, with state-level resources, are developing advanced capabilities which are potentially deployable in conflicts, including against CNI and government institutions. And non-state actors, including terrorists and cyber criminals can use easily available cyber tools and technology for destructive purposes."[81]

Activities to combat threats to SCADA and ICS that are embedded across industries were overseen in the United Kingdom by the national Computer Emergency Response Team (CERT-UK), established in 2014, as well as by the Government Computer Emergency Response Team (GovCERT). These bodies were tasked with providing warnings, alerts, and assistance to public sector organizations. CERT-UK is one of many now set up by national governments. It was designed to "work closely with industry, government and academia to enhance UK cyber resilience."[82] Part of these new initiatives was the formation of the Cyber Security Information Sharing Partnership, which had 750 organizations as members as of 2014.[83] It was intended that "CERT-UK will be able to add the day to day experience of working with critical national infrastructure companies in handling the incidents they face alongside the international dimension."[84]

---

[80]Cabinet Office, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (London: Stationery Office, 2010), 4, 16, see also 47–49.
[81]Prime Minister's Office, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* (London: Stationery Office, 2015), 19.
[82]National Cyber Security Centre, accessed at https://www.cert.gov.uk/, 16 July 2014.
[83]Cabinet Office, *The UK Cyber Security Strategy: Report on Progress and Forward Plans* (London: Stationery Office, 2014), 5.
[84]Cabinet Office, "UK Launches First National CERT," news release, 31 March 2014, accessed at https://www.gov.uk/government/news/uk-launches-first-national-cert, 3 February 2015.

A year prior to the SDSR, the government initiated the United Kingdom's first Cyber Security Strategy, which led to the formation of the Cyber Security Operations Centre. Immediately there were criticisms that there remained a lack of cooperation between central government and the owner-operators of CNI.[85] Although the Cyber Security Strategy was renewed again in 2011 in the wake of the SDSR, concern remained that the government was not doing enough to protect CNI. This led to the reorganization of the Office of Cyber Security as the Office of Cyber Security and Information Assurance (OCSIA), which was provided with a budget of £650 million through 2015. The OCSIA became the lead agency for central government, and a "fast-track route" was provided to the U.K. National Security Council. In essence, the OCSIA's remit was to try to "secure" the United Kingdom's cyberspace.[86] It built on the United Kingdom's 2011 Cyber Security Strategy, which had four main objectives: for the United Kingdom to tackle cyber crime and become one of the most secure places in the world to do business in cyberspace; to be more resilient to cyberattacks and better able to protect U.K. interests in cyberspace; to help share an open, stable, and vibrant cyberspace that the U.K. public can use safely and that supports open societies; and, finally, to have crosscutting knowledge, skills, and capability to underpin U.K. cybersecurity objectives.[87]

Despite these initiatives, a 2011 Chatham House report, "Cyber Security and the UK's Critical National Infrastructure," put forward that "there is currently no publicly available, comprehensive account of the UK national cyberspace stakeholder environment that could provide the basis for the development of a national cyber security regime, culture or policy framework."[88] This remained largely the case in 2016 despite further Whitehall initiatives. The research discovered that there was "no coherent picture or sense of what constitutes a vulnerability, or of the likely severity of the consequences of that vulnerability . . . embracing the public and private sectors."[89] The report also found that although a plethora of information was available to CNI providers, this was fragmented and central

[85]Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *Cyber Security and the UK's Critical National Infrastructure: A Chatham House Report* (London: Chatham House, 2011), vii, accessed at http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r0911cyber.pdf, 21 July 2014.
[86]Shaun Harvey, "Unglamorous Awakenings: How the UK Developed Its Approach to Cyber," in Healey, ed., *A Fierce Domain,* 261–262.
[87]National Cyber Security Centre, accessed at https://www.cert.gov.uk/, 16 July 2014.
[88]Cornish et al., *Cyber Security and the UK's Critical National Infrastructure,* vii–x.
[89]Ibid., viii.

government should do more and be a focal point and not just a point of contact. Simultaneously, the report recognized that "government cannot provide all the answers and cannot guarantee national cyber security in all respects and for all stakeholders."[90]

To evolve resilience beyond Darwinian "survival of the fittest" tests, this needs to be addressed through a multistakeholder approach, which, as in the United States, requires long-term and systematic direction from the board level down and from owner-operators upward in a two-stage continuous process conducted in an honest and constructive manner. However, board-level awareness of the risks and dangers remains deficient, as does board-level technical knowledge of cybersecurity threats. This is the case in many nations and for society at large.

Illustrating this point are the responses from the organizations that Chatham House surveyed, in which a fundamental contradiction was found.[91] While there was an awareness of cyber threats and cyber vulnerabilities, CNI providers were perceived to be "risk tolerant." This was not helped by the interface between their ICT professionals and the boards, which demonstrated that each was not speaking a language both could readily understand and that "the needs of the business [were] driving ICT security rather than the other way around."[92] Furthermore, in some cases, cybersecurity "was deliberately pushed below the boardroom level in order to remove a complex and baffling problem from sight," with it becoming the sole preserve of a chief information officer or the ICT department."[93] This needs addressing at the boardroom level. To try to keep up to date with the multiplying cyber threats that the United Kingdom is facing, CERT-UK worked with a number of other agencies, including the following:

- The Communications-Electronics Security Group (CESG) was part of the Government Communication Headquarters (GCHQ) and a partner of the NSA in Signals Intelligence. The CESG provided policy and assistance on the security of communications and electronic data, working in partnership with industry and academia.
- The Centre for the Protection of National Infrastructure (CPNI) protected national security by providing protective security advice. Protective security means establishing in building or design, security measures or protocols so that threats can be deterred, detected, or the consequences of an attack

[90]Ibid., viii.
[91]The Chatham House team attempted to survey 100 CNI providers, but only a limited number responded. As a result, some questions need to be raised against their findings.
[92]Cornish et al., *Cyber Security and the UK's Critical National Infrastructure*, viii.
[93]Ibid., 10.

minimized. The CPNI provided advice on physical security, personnel security, and cybersecurity/information assurance.[94]

- GovCertUK operated under the CESG and offered help to public sector organizations in response to computer security incidents and providing advice to reduce exposure to threats. It also gathered data from all available sources to monitor the general threat level with classified and unclassified reporting 24/7.
- MoDCert is the CERT operated by the U.K. Ministry of Defence (MoD). It provides responses to computer security incidents within the MoD.
- The National Cyber Crime Unit s currently part of the National Crime Agency aimed at providing a joined-up national response to cyber crime.[95]
- The Centre for Cyber Assessment (CCA) was established at GCHQ in April 2013. The CCA, whose membership is drawn from across government departments, agencies, and law enforcement bodies, is the cyber equivalent of the Joint Terrorism Analysis Centre. It is funded from the National Cyber Security Plan and designed to provide all-source intelligence driven reports to government customers including "top industry bodies and companies as part of our wider work to protect British national security, our citizens and businesses."[96]

Dialogues with industry are intended to be a partnership among government, regulators, and industry.[97] CERT-UK was intended to be an "honest broker" so that the public and private sectors can share good practice, growing from just 85 staff to 1,100. CERT-UK was not a wholehearted attempt to put the state at the center of U.K. cybersecurity but instead aimed to provide a focal point for good/best practice and good "cyber hygiene." Indeed, it did not have the resources in terms of personnel or finances to be anything more or less than a hub of active advice. However, one of its partner agencies was GCHQ, which has seen heavy investment in its cyber capabilities over recent years. This is evidenced in the 2010 and 2015 SDSRs. Indeed, the 2010 SDSR was key to the formation of CERT-UK and expanded resources in the cybersecurity field.

---

[94]Further information on the CPNI's remit and activities can be accessed at http://www.cpni.gov.uk/about/#sthash.ljdX1wXX.dpuf and http://www.cpni.gov.uk/about/, 16 July 2014.

[95]National Cyber Security Centre, accessed at https://www.ncsc.gov.uk/ /, 18 October 2016. See also the National Crime Agency, accessed at http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit, 16 July 2014; Jisc, accessed at http://www.ja.net, 16 July 2014 and Nominet, accessed at http://www.nominetcyberassist.org.uk/, 16 July 2014.

[96]Government Communications Headquarters, "Foreign Secretary Highlights the Work of the Centre for Cyber Assessment," news release, 29 June 2015, https://www.gchq.gov.uk/news-article/foreign-secretary-highlights-work-centre-cyber-assessment, 12 October 2016.

[97]"Communiqué from the 'Strengthening the Cyber Security of Our Essential Services' Event," accessed at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284085/Communique_-_Strengthening_the_Cyber_Security_of_Our_Essential_Services.pdf, 30 March 2015.

The National Cyber Security Plan, begun in 2011 with funding of £860 million through 2016, is ongoing.[98] This figure was more than doubled in the 2015 SDSR, and the £1.9 billion earmarked for cybersecurity from 2016 to 2020 is a precursor to the second five-year National Cyber Security Strategy and the new National Cyber Security Plan launched in 2016. This includes funding for offensive cyber capabilities through the National Offensive Cyber Programme run jointly by the MoD and GCHQ and strengthened computer networks within government. The 2015 SDSR also makes it clear the U.K. government intends to be more open in sharing information on cyber threats in partnership with the private sector. This includes threats from "lone wolves" through Advanced Persistent Threats associated with nation-states, with some information shared with NATO and allied nations.[99] GCHQ continues to claim the majority of cybersecurity funding to "provide protection at pace and scale to key networks of national significance."[100] Much of its work to protect Britain's CNI from cyberattack remains classified, with government oversight provided through the Parliamentary Intelligence and Security Committee.

Importantly, given the large number of organizations (a number of which are relatively recent creations) dealing with cybersecurity, the 2015 SDSR also announced the establishment of a new National Cyber Security Centre (NCSC) under the leadership of GCHQ, which opened in London in October 2016.[101] This is designed to "manage our future operational response to cyber incidents, ensuring that we can protect the UK against serious attacks and minimise their impact."[102] It is intended that the NCSC will act as a single point of contact against cyber threats. As Chancellor George Osborne recognized, "we need to address the alphabet soup of agencies involved in protecting Britain in cyberspace."[103] The NCSC could significantly improve

[98]Francis Maude, "Written Statement to Parliament UK Cyber Security Strategy: Statement on Progress 3 Years On," 11 December 2014, accessed at https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-3-years-on, 28 March 2015; and National Audit Office, *The UK Cyber Security Strategy: Landscape Review* (London: Stationery Office, 2013), accessed at http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf, 31 March 2015.

[99]"National Cyber Security Strategy 2016 to 2021," 1 November 2016, accessed at https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, 7 November 2016; Prime Minister's Office, *National Security Strategy and Strategic Defence and Security Review 2015,* 24, 40–41.

[100]Cabinet Office, *The UK Cyber Security Strategy,* 13; and Prime Minister's Office, *National Security Strategy and Strategic Defence and Security Review 2015,* 40–41, 73. See also *Cabinet Office, The UK Cyber Security Strategy 2011-2016 Annual Report April 2016.*

[101]Cabinet Office, "New National Cyber Security Centre Set to Bring UK Expertise Together," news release, 18 March 2016, accessed at https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together, 9 June 2016.

[102]Prime Minister's Office, *National Security Strategy and Strategic Defence and Security Review 2015,* 41.

[103]"Chancellor's Speech to GCHQ on Cyber Security," 17 November 2015, accessed at https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security, 29 December 2015.

macro-level tactical and strategic oversight and a positive step. In being the "bridge between industry and government" by "providing a unified source of advice and support" it is intended that the NCSC "will be a single point of contact for the private and public sectors."[104]

Organizations such as the CESG, CERT-UK, the CCA, and the cybersecurity portfolio of CPNI, will be encompassed by the NCSC. The NCSC is aimed squarely at addressing the issue of too many government organizations dealing with cross-cutting issues.[105] These cross-cutting remits are mirrored in the United States especially among the FBI, NSA, and DHS.

The United States aimed to grow its activities with CERT-UK through "due diligence" and the utilization of public–private partnerships. The clear message that is being conveyed is that nation-state-based law applies in cyberspace.[106] This is based on the Budapest Convention on Cyber Crime (2011) and European Union laws.[107] Still, whether prosecutions in jurisdictions, many of which view these issues differently than liberal democracies, are possible or viable is a real problem. If the case of Gary McKinnon, a U.K. citizen who hacked into the U.S. Department of Defense and whom the United Kingdom refused to extradite to the United States after a decade-long legal case, is a litmus test it is even a problem area for even the closest of allies.[108]

An attack on public utilities or financial services could have far more profound social, financial, and political consequences than any cyber crime yet reported. This is already recognized by the European Union, which finalized the Network and Information Security Directive in July 2016 to require CNI owner-operators to adopt "measures to ensure a high common level of network and information security across the Union."[109] The effect

---

[104]"Prospectus Introducing the National Cyber Security Centre" (May 2016), 2. Accessed at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf, 18 October 2016.

[105]Ibid.

[106]Chatham House Conference, "Cyber Security Building Resilience Reducing Risk," Chatham House, London, 19–20 May 2014. As this conference was conducted under Chatham House Rules, individual speakers are not allowed to be identified.

[107]Council of Europe, "Details of Treaty No. 185, Convention on Cybercrime," accessed at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, 16 July 2014 and Council of Europe, "Action Against Cybercrime," accessed at http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp, 16 July 2014. See also Michael A. Vatis, "The Council of Europe Convention on Cybercrime," Proceedings of a Workshop on "Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy," accessed at http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf, 16 July 2014.

[108]"Profile: Gary McKinnon," BBC News, 14 December 2012, accessed at http://www.bbc.co.uk/news/uk-19946902, 18 July 2014.

[109]European Commission, "The Directive on security of network and information systems (NIS Directive)", 28 July 2016, accessed at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, 18 October 2016. Further details on U.K. cybersecurity practices can be found in Kristan Stoddart, "UK Cyber Security and Critical National Infrastructure Protection," *International Affairs* 92 (September 2016): 1079–1105.

of Britain's terms of exit from the European Union following its June 2016 referendum might mean its nonadoption, even though this is in the United Kingdom's interest.

## CYBER ESPIONAGE AND CYBER WAR: DIPLOMACY, THE INTELLIGENCE COMMUNITY, AND MILITARY

The reasons for attacks on CNI remain multifarious, but Verizon's 2014 Data Breach Investigations Report lists among them the long-standing problem posed by espionage.[110] This encompasses espionage from states as well as from private companies. The national interest remains dominant in conceptualizing cyber threats, but as we all swim in the same information ocean, this does not deal sufficiently with organized crime, which spans national jurisdictions (including those outside the European Union or North America), or with building trust between states and state organizations.

Under these conditions, it is important to raise awareness of the potential threat all states face. This also encompasses highly protected military systems and assets, many of which are profoundly dependent on ICT and increasingly rely on global positioning systems to perform to their best.[111] As John Arquilla, the originator of the concept of cyber war,[112] has argued, "this new way of war-possibly quite potent on the battlefield, but [is] also able to strike at others' homelands without the need to defeat their military forces first."[113] The United States and the United Kingdom, together with their allies in NATO, see offensive cyber operations at the operational/tactical and strategic levels as part of military planning and declared cyber to be a fifth domain of warfare at NATO's meeting in Warsaw in July 2016.[114] As James A. Lewis highlights, "cyber operations are increasingly embedded

[110]Verizon Data Breach Investigations Report, 2014, accessed at http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf, 17 July 2015.

[111]Remarks made under Chatham House Rules at the NATO Intelligence Fusion Centre, RAF Molesworth, 2–5 November 2015. For a conceptual discussion of military thinking on these issues drawing on the prisoner's dilemma, see Martin Libicki, "The Nature of Strategic Instability in Cyberspace," *Brown Journal of World Affairs* 18 (Fall/Winter 2011): 71–79.

[112]John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12 (Spring 1993): 141–165.

[113]John Arquilla, "The Computer Mouse That Roared: Cyberwar in the Twenty-First Century," *Brown Journal of World Affairs* 18 (Fall/Winter 2011): 39–48. This is under active scrutiny. See, for example, NATO's Tallinn Process, exemplified by the *Tallinn Manual.* Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013). See also the proceedings of NATO's excellent CyCon conferences (International Conference on Cyber Conflict), accessed at https://ccdcoe.org/cycon/past-cycon-conferences.html, 15 February 2016. On the attribution problem from a state-based perspective, see Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *Brown Journal of World Affairs* 18 (Fall/Winter 2011): 57–70.

[114]Remarks made during presentations at the 8th International Conference on Cyber Conflict, Tallinn, Estonia, 1–3 June 2016.

into military operations . . . Offensive cyber capabilities will shape the battlefields of the future."[115]

They are also shaping present-day conflicts and concepts of new forms of hybrid conflicts and warfare that utilize multiple attack surfaces beyond hard military-backed power and the conventional use of force.[116] Military forces and the power projection they provide depend on the civilian infrastructure they are tasked to defend. This includes the information infrastructure embodied by the Internet, which can house any Internet-facing military networks. Compromise of these systems and networks has the capacity to degrade, disrupt, or even cripple military interventions and the command and control on which they depend before, during, or after deployment. In addition, the intelligence and information on which they depend can also be compromised from the outside through external hacking or from trusted insiders run by foreign intelligence agencies. As Lewis argues, this can "disrupt data and services, sow confusion, damage networks and computers (including software and computers embedded in weapons systems) [and] machinery. Offensive cyber operations would strike military, government and perhaps civilian targets such as critical infrastructure in the opponent homeland used to support war efforts."[117]

Combatting these ubiquitous threats to civilian and military infrastructure and assets requires "building blocks" at the diplomatic level to establish "red lines" and rules for state behavior in cyberspace. This is an issue publicly raised by Richard Ledgett, deputy director of the NSA, in an October 2015 interview that he gave to the BBC.[118] That same month, the director general of MI5, Andrew Parker, argued that the threat from terrorism is at its greatest level in his 32 years in the service, providing good reasons to increase international state collaboration.[119] This call for increasing state-

[115]James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence" (Tallinn Paper 8, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2015), 3, accessed at https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf, 7 June 2016. For more on the issues of military uses of cyber capabilities, see the excellent series of articles available from NATO's Cooperative Cyber Defence Centre of Excellence, accessed at https://ccdcoe.org/publication-library.html, 7 June 2016.
[116]Michael Kofman and Matthew Rojansky, "A Closer look at Russia's 'Hybrid War'" (Kennan Cable 7, Woodrow Wilson International Center for Scholars, Washington, DC, April 2015), accessed at https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf, 7 June 2016. See also N. Pissanidis, H. Rõigas, and M. Veenenddaal, eds., *Cyber Power 2016 8th International Conference on Cyber Conflict* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016).
[117]Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence," 4.
[118]Gordon Corera, "NSA Warns of Growing Danger of Cyber-Attack by Nation States," BBC News, 27 October 2015, accessed at http://www.bbc.co.uk/news/world-us-canada-34641382, 28 October 2015.
[119]"MI5 Boss Wants 'Mature Debate' on Surveillance Powers," BBC News, 29 October 2015, accessed at http://www.bbc.co.uk/news/uk-34663929, 30 October 2015.

based collaboration was incorporated into the 2015 SDSR, with responsible state-based behavior in cyberspace championed by the "London Cyber Process," which also paid heed to the challenges facing the current international economic and political order.[120] For the United Kingdom, increased transparency, trust, and cooperation are also important for trade relations, as Britain is a global financial hub.[121] This encompasses the series of £30 billion agreements that Britain has entered into with China (which includes deals on the United Kingdom's next-generation civil nuclear power plants), so that these do not provide gateways into strategic influence over computer-controlled U.K. CNI.[122] With China and Russia's intelligence agencies both accused of mapping electrical grids in the United States and installing software traps that could be used to damage or disrupt CNI, there has to be some concern despite Chinese assurances.[123]

The use of The Onion Router and proxy servers only compounds problems for intelligence agencies and police in the United States, United Kingdom, and elsewhere in terms of identification/attribution and prosecution, as does the growing use of encryption by major technology companies.[124] Indeed, the use of end-to-end encryption might well mean that the surveillance activities of the intelligence community will become much more difficult in eavesdropping on electronic communications.[125]

The encryption debate was brought into sharp public focus during the first half of 2016 by the dispute between the FBI and Apple over unlocking or hacking the iPhone of Syed Rizwan Farook, the Islamic State–inspired terrorist who, along with his wife Tashfeen Malik, killed 14 people and wounded 22 others during an attack in San Bernardino, California, in

---

[120]Prime Minister's Office, *National Security Strategy and Strategic Defence and Security Review 2015*, 20, 41.

[121]Ibid., 17.

[122]"Hammond Rejects Security Fears over China Investment," BBC News, 20 October 2015, accessed at http://www.bbc.co.uk/news/uk-politics-34582673, 24 October 2015. See also Carrie Grace, "Hinkley Point: Theresa May's China calculus", BBC News, 31 July 2016, accessed at http://www.bbc.co.uk/news/world-36937511, 18 October 2016.

[123]Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, 8 April 2009, accessed at http://www.wsj.com/articles/SB123914805204099085, 24 October 2015 and Kamal Ahmed, "China Admits—Our Reputation Is on the Line over Nuclear Security," BBC News, 21 October 2015, accessed at http://www.bbc.co.uk/news/business-34595677, 24 October 2015. See also "UK/China Cyber Security Deal: National Security Attacks Still OK, It Seems," *The Register*, 22 October 2015, accessed at http://www.theregister.co.uk/2015/10/22/uk_china_cyber_security_agreement_ip/, 29 December 2015.

[124]See, for example, Joe Miller, "Google and Apple to Introduce Default Encryption," BBC News, 19 September 2014, accessed at http://www.bbc.co.uk/news/technology-29276955, 31 March 2015 and "Tor Project Makes Efforts to Debug Dark Web," BBC News, 23 July 2014, accessed at http://www.bbc.co.uk/news/technology-28447023, 31 March 2015.

[125]See, for example, Conor Friedersdorf, "How Dangerous Is End-to-End Encryption?," *The Atlantic,* 14 July 2015, accessed at http://www.theatlantic.com/politics/archive/2015/07/nsa-encryption-ungoverned-spaces/398423/, 16 February 2016.

December 2015. Apple has cooperated with government agencies in the past, including the NSA's PRISM program, but as technology journalist Kim Zetter notes, "the government wants a way to access data on gadgets, even when those devices use secure encryption to keep it private."[126] This has implications beyond Apple and the FBI. As Zetter adds, "If the FBI is successful in forcing Apple to comply with its request, it would also set a precedent for other countries to follow and ask Apple to provide their authorities with the same software tool."[127] This means that authoritarian states can apply the same arguments as the FBI but for political dissidents as well as terrorists. If Apple and other technology providers that offer end-to-end encryption resist, they could be denied access to that market. This could make life difficult for them and their customers. In this particular case, Apple resisted the FBI's request, forcing the FBI to pay around $1 million to a third party to unlock Farook's iPhone.[128]

At the same time, the FBI's rationale is relatively straightforward. FBI director James B. Comey has already outlined the fear that law enforcement (as well as the intelligence community) in the United States could be "going dark"—a problem also recognized by Europol.[129] This means that they are unable to access encrypted devices and encrypted communications despite having the legal and constitutional authority to do so.[130] This valid argument could also be made by nonliberal democratic states and regimes that do not hold the same views of free speech as the United States.

Within this framework, part of the rationale of the PRISM mass surveillance program can be discerned.[131] It can also be found in the U.K. National Security Strategy and in the MoD's 2013 "Cyber Primer," which is a useful guideline for the United States and its allies in NATO. That document states,

---

[126]Kim Zetter, "Apple's FBI Battle Is Complicated. Here's What's Really Going On," Wired, 18 February 2016, accessed at https://www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/, 29 May 2016.
[127]Ibid.
[128]Mark Hosenball, "FBI Paid under $1 Million to Unlock San Bernardino iPhone: Sources," Reuters, 4 May 2016, accessed at http://www.reuters.com/article/us-apple-encryption-idUSKCN0XQ032, 29 May 2016.
[129]"Europol Chief Warns on Computer Encryption," BBC News, 29 march 2015, accessed at http://www.bbc.co.uk/news/technology-32087919, 29 May 2016.
[130]Amy Hess, Executive Assistant Director, Science and Technology Branch, Federal Bureau of Investigation, statement before the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigation, 19 April 2016, accessed at https://www.fbi.gov/news/testimony/deciphering-the-debate-over-encryption, 29 May 2016.
[131]Luke Harding, *The Snowden Files The Inside Story of the World's Most Wanted Man* (London: Guardian Books, 2014), 155–169, 314–315, 323–328; and Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the Surveillance State* (London: Hamish Hamilton, 2014).

> When observing changes in cyberspace, timescales vary from days or months to milliseconds. Individuals and groups operating in cyberspace leave digital trails but these can be disguised, thus making accurate identification, geo-location and attribution difficult. While there are no international treaties specifically governing cyber activity, cyber operations must be conducted in accordance with existing domestic law. The international law that applies to military cyber operations will depend on whether an armed conflict is in existence, be it an international armed conflict or a non-international armed conflict. Where there is no armed conflict, military cyber activities are governed by domestic and international law applicable in peacetime.[132]

International law includes the Law of Armed Conflict (LOAC), which adds both context and complexity to conflict in cyberspace. As the Second Edition of the "Cyber Primer" published in 2016 argues:

> Armed attack is not defined in international law, but it is generally accepted that it must be an act of armed force of sufficient gravity, having regard to its scale and effects. A cyber operation may constitute an armed attack if its method, gravity and intensity of force is such that its effects are equivalent to those achieved by a kinetic attack which would reach the level of an armed attack . . . The inherent right of individual and collective self-defence is customary international law and is also recognised by Article 51 of the United Nations Charter. An armed attack or imminent armed attack triggers the right of self-defence or anticipatory self-defence. Any response under self-defence must be necessary and proportionate . . . Cyber operations conducted during an armed conflict to which the UK is a party, and which are related to that conflict, are governed by the existing rules of the Law of Armed Conflict (LOAC) including the prohibition on perfidy (inviting the confidence of an adversary as to protection under the LOAC) and principles of neutrality.[133]

In addition, the implications of the law of self-defense turn on three practical issues: attribution; the speed with which an attack can be conducted, which greatly reduces the ability to respond to an imminent attack; and the difficulty of determining intent, even if actions are provable and actors identifiable.[134]

---

[132]Ministry of Defence, "Cyber Primer," December 2013, 1-23/1-26, accessed at http://www.securethecyber.uk/wp-content/uploads/2015/10/20140716_DCDC_Cyber_Primer_Internet_Secured-VERSION-TO-BE-USED.pdf, 18 October 2016. A new of the "Cyber Primer" has since been published. "Cyber Primer" Second Edition", July 2016. Accessed at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf, 18 October 2016. The relevant passages relating to timescales and international law can be found on 12-14, 26-27.

[133]"Cyber Primer Second Edition", July 2016, 13.

[134]These operations are governed by four principles; military necessity, distinction, proportionality, and humanity. "Cyber Primer Second Edition", July 2016, 13-14.

The "attribution problem" leads to difficulties when it is a "nation-state like attack."[135] The attribution problem is well recognized already; many escape judicial proceedings, and it is quite likely that private sector intrusions lay undetected or reported. Whether acts such as an attack on the ICS of CNI committed by cyber "guns for hire" through the "Dark Web" can be deterred or prosecuted is a major problem. In this way, both state and nonstate actors such as al Qaeda or the Islamic State can have a force multiplier effect and become "David" to "Goliath."[136] That the Islamic State and other hostile terrorist groups, as well as nation-states, could attack CNI was part of the reason the SDSR increased the budgets for the security and intelligence agencies. In a speech at GCHQ in November 2015, George Osborne stated,

> ISIL are already using the internet for hideous propaganda purposes; for radicalisation, for operational planning too. They have not been able to use it to kill people yet by attacking our infrastructure through cyber attack. They do not yet have that capability. But we know they want it, and are doing their best to build it. So when we talk about tackling ISIL, that means tackling their cyber threat as well as the threat of their guns, bombs and knives. It is one of the many cyber threats we are working to defeat.[137]

Osborne also cautioned,

> If the lights go out, the banks stop working, the hospitals stop functioning or government itself can no longer operate, the impact on society could be catastrophic. So government has a responsibility towards these sectors, and the companies in those sectors have a responsibility to ensure their own resilience. Any new regulation will need to be carefully done—light enough and supple enough that it can keep up with the threat, so it encourages growth and innovation rather than suffocates it.[138]

Alex Dewdney, the director of cybersecurity at the CESG, noted a potential shift in U.K. policy, becoming "more interventionist and active in how it takes on some of these [cybersecurity] challenges—still with

---

[135]See, for example, Rid, "Cyber War Will Not Take Place."
[136]See, for example, Myriam Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology and Politics* 4 (April 2008): 19–36; David J. Betz and Tim Stevens, *Cyberspace and the State Towards a Strategy for Cyber-Power* (Abingdon: Routledge/International Institute for Strategic Studies, 2011), 134–139; Jason Rivera, "Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk," in M. Maybaum, A.-M. Osula, and L. Lindström, eds., *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), 7–24.
[137]"Chancellor's Speech to GCHQ on Cyber Security."
[138]Ibid.

industry, but doing more than providing threat information and expecting companies to deal with it."[139] This is to be welcomed, and it is a path the U.S. government should think about. Intervention and regulation, however, present a difficult balancing act, one that other states are grappling with.

## CYBERSECURITY, CNI, AND THE RULE OF LAW

Estonia, as one of the leading nations in cybersecurity practices, having been subject to a concerted attack in 2007,[140] founded a Department of Critical Infrastructure Protection. This is designed to defend both public and private networks through a centralized approach.

> [It] conducts risk assessments, collects information on critical infrastructure, and proposes defensive measures to counter cyber threats. Projects include mapping critical infrastructure and designing contingency plans for large-scale cyberattack. Estonia's focus is now shifting towards the protection of intellectual property in order to preserve economic assets and advantages over the long term. To protect both critical and economic infrastructure, Estonia is building partnerships between the public and private sectors.[141]

Germany and the Netherlands, meanwhile, are also bringing academics into government decision making on CNI cybersecurity, as well as having private sector representation.[142]

There are two areas of difficulty for governments in mounting the activities outlined earlier or deepening those activities, as in the case of Estonia. First, a wholly defensive approach to cybersecurity is unlikely to be anything other than reactive and will place them on the back foot. It is known, partly through the Snowden revelations over PRISM, that both the NSA and GCHQ have offensive cyber capabilities against both state and nonstate actors. As of June 2016, it is suspected that there are 29 states with offensive cyber capabilities; 16 of them are declared.[143] What is far from clear is where the balance lies between cyber defense and cyber offense especially when this includes intelligence gathering and espionage practices, as well as surveillance and reconnaissance by cyber means. These

---

[139]Warwick Ashford, "National Cyber Security Centre to Be UK Authority on Information Security," *Computer Weekly,* 21 March 2016, accessed at http://www.computerweekly.com/news/4500279563/National-Cyber-Security-Centre-to-be-UK-authority-on-information-security, 9 June 2016.
[140]Andreas Schmidt, "The Estonian Cyberattacks," in Healey, ed., *A Fierce Domain,* 174–193.
[141]Lewis and Neuneck, *The Cyber Index.*
[142]Ibid., 19. The strategies of many other states are discussed in this valuable document.
[143]Remarks made during presentations at the 8th International Conference on Cyber Conflict, Tallinn, Estonia, 1–3 June 2016.

are areas in which conceptual arguments of deterrence add value.[144] This is not a straightforward calculation and is further exacerbated by the speed, range, sophistication, and diversity of attacks. This means that the range of passive and active measures not only has to contend with Stuxnet-type attacks at the highest (state-based) level but also lower-level threats. Second, is there a point at which a cyberattack will lead to a kinetic (military) response? Under current international law, cyberattacks would have to lead to violent "real-world" deeds before a kinetic (military) response could be contemplated.[145] Furthermore, as Jaak Aaviksoo, the Estonian defense minister, asked after the Russian cyberattacks on Estonia,

> Do we have a proper legal code that defines the cyber attacks in detail—where does cyber crime stop and terrorism or war begin? Should NATO, for example, safeguard and defend not only its communications and information systems but also some national critical physical infrastructures? And what to make of collective defense in case of cyber war against one of the allies?[146]

Although this line of reasoning helped initiate the *Tallinn Manual,* this set of issues remains unresolved. They remain viable, difficult, and complex issues for NATO and national governments.[147]

Both common law and international law need to be reformed, and new or updated legislation is needed against these threats and general agreement established on enforceable rules, norms, and values and respect for national laws (and how national laws apply in cyberspace).[148] Without renewing these legal frameworks, technology will run far ahead and will do so rapidly. In this vein, a number of former policymakers have called for an international treaty under the United Nations to mitigate or penalize cyberattacks by nation-states or individuals and groups within states.[149]

---

[144]Libicki, "The Nature of Strategic Instability in Cyberspace," 71–79.

[145]This point is emphasized in Rid, *Cyber War Will Not Take Place,* 11–34.

[146]"Defence Minister Jaak Aaviksoo: CYBER DEFENSE—THE UNNOTICED THIRD WORLD WAR," 8 May 2008 accessed at http://www.kaitseministeerium.ee/en/news/defence-minister-jaak-aaviksoo-cyber-defense-unnoticed-third-world-war, 118 October 2016.

[147]Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Some of the issues that the expert legal group encountered in drafting the *Tallinn Manual* are discussed in Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?," *Stanford Law & Policy Review* 25 (2014): 269–300. A cyber "code of conduct" was proposed by China and Russia to the United Nations General Assembly in 2011 see Timothy Farnsworth, "China and Russia Submit Cyber Proposal," *Arms Control Today,* 2 November 2011, accessed at https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal, 20

[148]Lewis and Neuneck, *The Cyber Index.*

[149]See, for example, Clarke and Knake, *Cyber War,* 220–228, 235–242, 268–269; and Omand, *Securing the State,* 11, 66–72, 80–84.

Currently, preparations against potential cyberattacks continue to be conducted in what remains a largely anarchic environment.

A concerted attack on one sector of CNI, such as the economy, is likely to produce unanticipated and unpredictable cascade effects to others sectors.[150] Awareness of the range of threats, and of the increasing capability of nonstate actors to harm nation-states, is being provided by a variety of intelligence agencies, including those in the United States and the United Kingdom.[151] With these practical and jurisdictional issues in mind, the protection of CNI and SCADA systems are, arguably, issues that can be tackled through means and methods that can only be realistically achieved through cooperation between nation-states and national governments.

PRISM showed that a wholly top-down/central-government-driven approach is likely to be resisted by private industry and individual citizens or prove ineffective with mass surveillance seen as the antithesis of the Internet and our increasing levels of hyperconnectivity. With around 80 percent of national cyber infrastructure privately owned and operated, does this instead make private industry responsible or liable for national protection?[152] It is also worth pondering our scale of dependency and potential vulnerability as individual consumers of new technologies, as well as how that dependency will increase with "smart technologies" in the home and the drive toward more efficient "smart cities" and "smart grids."[153]

A wholly bottom-up approach to cybersecurity is also likely to prove unsatisfactory for national governments, which, after all, have a mandate to govern and protect us as citizens. First, most CNI might be housed exclusively in the host nation, but a percentage will be transnational. This means that for logistical, legislative, jurisdictional, and legal purposes, a dialogue with partners/stakeholders is essential. Second, a significant number of companies in the various sectors that enable and police CNI are not based in the United States or the United Kingdom or are foreign owned. However, private industry is resistant to increased regulation,

---

[150]Chatham House Conference, "Cyber Security Building Resilience Reducing Risk." See also Chris Keeling, "Waking Shark II: Desktop Cyber Exercise: Report to Participants," 12 November 2013, accessed at http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf, 20 July 2014.

[151]U.K. practices have been alluded to earlier. U.S. examples include those provided in the National Intelligence Council report "Global Trends 2030: Alternative Worlds," accessed at http://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf, 20 July 2014.

[152]Chatham House Conference, "Cyber Security Building Resilience Reducing Risk."

[153]See, for example, European Innovation Partnership on Smart Cities and Communities, accessed at http://eu-smartcities.eu/, 23 July 2014 and Jane Wakefield, "Tomorrow's Cities: Do You Want to Live in a Smart City?," BBC News, 19 August 2013, accessed at http://www.bbc.co.uk/news/technology-22538561, 23 July 2014.

which is seen to impinge on the running of their business.[154] For central government, increased regulation might prove difficult to implement and successfully manage, and it is also likely to be costly—especially during a period of continued financial austerity.

This view of public–private partnerships and how they should function is rooted in a much wider, and embedded, issue concerning government intervention and regulation of the free market and private industry. This neoliberal model has been a part of U.S. and U.K. government thinking since the 1980s through policies promoting economic deregulation.[155] These included CNI such as telecommunications,[156] public transport, and utilities such as gas and electricity. Notwithstanding, at a conference on cybersecurity organized by the United Nations Institute for Disarmament Research in late 2011, it was pointed out that "every actor—cyber-terrorists, criminals, militaries, as well as civil society and the private sector—is operating in the same environment, with the same tools, domains, and targets."[157] Efforts beyond a "whole-of-nation" response are needed in cybersecurity.

Increased regulation and legislation stand against free market neoliberal ideals through which state intervention in private industry is minimized. It is also likely to be resisted by the private sector, which desire self-regulation in different forms. Having said this, it was apparent during the financial crisis that begun in 2008 that central government intervention (with cross-party support) in the private sector will happen when in it is the national interest. The financial crisis also brought to light for some that they were not fit to police themselves.[158] Moreover, both communist and totalitarian states continue to exist, but there is also a "third way" typified by the likes of Russia and China. They do not adhere to the liberal democratic model, and this poses challenges in terms of international cooperation and the rule of law.[159]

---

[154]Chatham House Conference, "Cyber Security Building Resilience Reducing Risk."

[155]On the neoliberal model pioneered at this time, see David Harvey, *A Brief History of Neoliberalism* (Oxford: Oxford University Press, 2007).

[156]There already exists the International Telecommunications Union run by the United Nations, but its mandate is unclear and no one agrees who is, or should be, in charge. For its work and role, see http://www.itu.int/en/about/Pages/default.aspx, accessed 20 July 2014.

[157]International Conference on "Challenges in Cybersecurity, Risks, Strategies, and Confidence-Building," Institute for Peace Research and Security Policy, University of Hamburg, 13–14 December 2011, accessed at http://www.unidir.org/files/medias/pdfs/conference-report-eng-0-373.pdf, 19 July 2011.

[158]See, for example, Ralph Haas and Iman Lelyveld, "Multinational Banks and the Global Financial Crisis: Weathering the Perfect Storm?," *Journal of Money, Credit and Banking* 46 (2014): 333–364.

[159]On cyber crime, see Misha Glenny, *DarkMarket: Cyberthieves, Cybercops and You* (London: Bodley Head, 2011); and Glenny, *DarkMarket How Hackers Became the New Mafia* (London: Random House, 2011). See also Cabinet Office, "Cyber Security Guidance for Business," 5 September 2012, accessed at https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility, 2 July 2014.

These complex (and successful) actors have stolen intellectual property, taken commercially sensitive data, accessed government and defense-related information, disrupted government and industry services, and exploited information security weaknesses through the targeting of partners, subsidiaries, and supply chains both domestically and abroad. These threats arrive in several guises, varying in magnitude and tempo, and might be basic or sophisticated. These threats often emanate from individuals and groups that are well organized and "based in hard-to-reach jurisdictions."[160] They can also be (or are simultaneously) from industrial competitors and foreign intelligence services or simply hackers or hacktivists who draw on political or ideological rationales.[161] Moreover, the complexity of attacks has seen exponential growth: "What was considered a sophisticated cyber attack only a year ago might now be incorporated into a downloadable and easy to deploy internet application, requiring little or no expertise to use."[162]

## CAN WE "LIVE FREE" WHILE AVOIDING DYING HARD?

Although reporting of cyber threats is encouraged alongside government cyber awareness campaigns, companies in the private sector could still be sleepwalking into difficulties regarding their cybersecurity. This might not be the "Cybergeddon" or "Live Free or Die Hard" scenario from which it will be difficult to recover. Still, it would be unwise to rule this out—especially in any future state-based conflict involving major developed states such as the United States and China.

Stuxnet aside, there have already been cyberattacks conducted by Russia against the former Soviet republics of Estonia in 2007 and Georgia in 2008—the latter of which involved military action alongside sustained cyberattacks. There was also the 2014 attack on the German steel mill and the cyberattack on Ukraine's power grid in 2015. While these do not represent scenarios of "cyber doom," these are shots across the bow of those like Sean Lawson who remain skeptical of the threats we face.[163] They contribute to rising international insecurity, increasing regulatory pressures, and calls for norm building.

---

[160]Cabinet Office, "Cyber Security Guidance for Business."

[161]On "hacktivism," see Jonathan Diamond, "Early Patriotic Hacking," in Healey, ed., *A Fierce Domain,* 136–151.

[162]Cabinet Office, "Cyber Security Guidance for Business."

[163]Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10 (January 2013): 86–103; and Sean T. Lawson, Sara K. Yeo, Haoran Yu, and Ethan Greene, "The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate," in Pissanidis, Rõigas, and Veenenddaal, eds., *Cyber Power 2016,* 65–80.

There have been several proposals for cybersecurity norms. Some come from governments, beginning with the *Tallinn Manual* and including the Budapest Convention on Cybercrime and the London Cyber Process. Some are from nongovernmental organizations and some from industry leaders such as Microsoft.[164] This includes norms not to attack infrastructure during peacetime and CERTs not to be used for offensive action, with an emphasis on self-restraint based on international law. On the threat intelligence side, industry leaders such as Microsoft and Google are cooperating with the United States and United Kingdom. Industry has also tried to guide governance by proposing a G20 + ICT 20 forum derived from the G20 economic group to drive a dialogue on cybersecurity norms between leading states and industry leaders. This requires adherence to these norms and holding violators accountable. The evolution of computer forensics means that attribution is now seen as an opportunity for norm compliance and less of an obstacle. With many technical improvements now made on attribution, this could be a real game changer.[165] Nevertheless, we are in the middle of a cyber arms race, and if improved organizing principles cannot be established, then a "Wild Wild West"–style anarchy within the World Wide Web might prevail for the foreseeable future. The international experts group at the United Nations has been a help in progressing the discussion of state-based norms but, it is not the only avenue.[166]

Instead of "Cybergeddon," there might instead be lower-level attacks to disrupt elements of CNI such as utilities or transport. However, given the globalized and interconnected nature of national economies, it might not be that an attack of this nature will affect only the target state, sector, or company. A spillover or cascade effect cannot be ruled out. This is particularly true in terms of the economic and energy sectors. An illustration of the problem that companies face in these sectors can be found in a 2014 BBC report that power companies are being refused insurance against cyberattacks because they are not seen to be doing enough to

[164]See, for example, Microsoft, "International Cybersecurity Norms Reducing Conflict in an Internet-Dependent World," 2015, accessed at http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf, 12 October 2016.

[165]Remarks made during presentations at the 8th International Conference on Cyber Conflict, Tallinn, Estonia, 1–3 June 2016.

[166]NATO Cooperative Cyber Defence Centre of Excellence, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," 31 August 2015, accessed at https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html, 6 June 2016.

protect their systems and assets (with demand for this type of insurance increasing).[167]

The size and complexity of the problem being faced is perhaps indicated by the assessments of ICT specialists for insurers that cybersecurity was inadequate. Laila Khudari, an insurance underwriter at the Kiln Syndicate, which offers coverage via Lloyd's of London, told the BBC, "In the last year or so we have seen a huge increase in demand from energy and utility companies."[168] Prior to this rise in demand, insurance brokerages would offer insurance against data breaches involving the theft of customer data. Now, however, "the same firms were seeking multi-million pound policies to help them rebuild if their computers and power-generation networks were damaged in a cyber-attack." But, Khudari added, "We would not want insurance to be a substitute for security."[169] That private sector cybersecurity is unlikely to be underwritten by the insurance industry, especially if security is found to be insufficient, should sound warning bells. This is especially the case if this involves CNI and has national security implications.

Mike Assante, who was heavily involved in setting cybersecurity standards for the North American electric power industry, has claimed that power generators and distributors are now struggling with the size and complexity of the networks they manage. For cost and logistical reasons, companies see benefits in remotely operating their systems, but this also opens up attack vectors. Moreover, highly trained ICT specialists are at a premium, and there are simply not enough to cope with demand. If these problems are to be taken seriously, more investment is needed to meet this demand, and companies need to recognize the scale of the problems they are facing. It appears that the private sector in the United States is further down the road toward providing for the cyber protection of CNI, but practices are inconsistent.[170]

Many ICT specialists are already well aware of the types of attack vectors that even unsophisticated websites and search engines can generate. Alastair O'Neill of the Insecurety computer security research collective and

---

[167]Mark Ward, "Energy Firm Cyber-Defence Is 'Too Weak', Insurers Say," BBC News, 27 February 2014, accessed at http://www.bbc.co.uk/news/technology-26358042, 15 July 2014.
[168]Ibid.
[169]Ibid.
[170]"Michael Assante Holds Forth on Cybersecurity Leadership," *Smart Grid Security Blog*, 1 August 2012, accessed at http://smartgridsecurity.blogspot.co.uk/2012/08/michael-assante-holds-forth-on.html, 15 July 2014. The full record of the interview can be accessed at http://asmarterplanet.com/blog/2012/08/18457.html, 15 July 2014. See also U.S. Department of Energy, "Energy Department Develops Tool with Industry to Help Utilities Strengthen Their Cybersecurity Capabilities," news release, 28 June 2012, accessed at http://energy.gov/articles/energy-department-develops-tool-industry-help-utilities-strengthen-their-cybersecurity, 3 March 2015.

others have discovered from the Internet "public control interfaces for heating systems, geo-thermal energy plants, building control systems and manufacturing plants … treatment systems, power plants and traffic control systems."[171] The International Cyber Security Protection Alliance is one nongovernmental organization that seeks to provide a private sector–financed hub that highlights these kinds of dangers.[172] Another is the U.S.-based Internet Security Alliance, which offers guidelines for corporate cybersecurity and public–private engagement with input from a number of large multisector corporations.[173] One of the important issues that business has to address is how risk is identified.[174] One of these areas of risk remains the "insider threat." The insider threat remains a problem for all businesses, as it does for government organizations despite security vetting procedures.[175]

## CONCLUSION

There are still major areas of uncertainty that lay ahead, including the precise role of the state in cyber defense/security and regulation. Cybercrime is one area for state-based collaboration, but this in itself is contested because it encompasses not only nonstate hackers and criminals but also "patriotic hackers" and states themselves or their intelligence agencies. It is also the case that civilian cyberattackers will target the weakest links in the chain or in an organization—as will hostile nation-states—the so-called low-hanging fruit, which is easier to pick.

Moreover, a World Economic Forum and McKinsey & Company report on risk and resilience led those organizations to conclude that risks for the private sector are growing faster than the ability to act.[176] This is set within a context in which there are currently 70 billion cyber events a month. Of these, 250,000 attacks are noteworthy, with 60 to 70 of them meriting considered attention. The volume of attacks is too large to deal with without sufficient infrastructure and investment in key

[171]Mark Ward, "How to Hack a Nation's Infrastructure," BBC News, 20 May 2013, accessed at http://www.bbc.co.uk/news/technology-22524274, 15 July 2014.
[172]International Cyber Security Protection Alliance, accessed at https://www.icspa.org/, 15 July 2014.
[173]Internet Security Alliance, accessed at http://www.isalliance.org/isa-publications/, 19 July 2014.
[174]"Cyber Security 2014," accessed at http://www.corporatelivewire.com/round-tables.html?id=cyber-security-2014, 20 July 2014.
[175]Tom Groenfeldt, "Insiders Pose a Serious Threat to Corporate Information," *Forbes,* 8 May 2014, accessed at http://www.forbes.com/sites/tomgroenfeldt/2014/05/08/insiders-pose-a-serious-threat-to-corporate-information/, 20 July 2014.
[176]David Chinn, James Kaplan, and Allen Weinberg, "Risk and Responsibility in a Hyperconnected World: Implications for Enterprises," January 2014, accessed at http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises, 20 July 2014.

personnel.[177] However, this is not enough by itself. Greater public awareness is needed as well as greater corporate awareness and the need to grapple with the "ownership" issue. It is not enough to believe this is "somebody else's problem." It remains the case that "[t]he potential for damage, both economic and reputational, from complacency over matters of cyber dependency and vulnerability is too high to be ignored by even the largest multinationals."[178] A concerted response to attacks on CNI could require a joint response from multiple organizations or national governments, all of which would have different practices and structures.

In addition, the ever-increasing development of ICT capabilities and technologies means that the pace of change and integration grows daily, and increased risk can accompany this. The United States and United Kingdom could set positive examples by fostering an environment of collective protection and mutual self-help. This is an activity that central government can both facilitate and coordinate at a regional level without needing to micromanage. This should allow for improved dialogue, risk management, reporting, and response. However, what currently appears to exist is "a disparate patchwork of knowledge, capabilities, processes and attitudes . . . and lack the skills or knowledge to identify and mitigate the harm caused by a wide variety of emerging threats in cyberspace, and this is compounded by their systemic dependency on other vulnerable actors in the environment."[179] Cyberspace is neither completely anarchic nor completely ordered. The shape of the order that can be imposed for the needs of national governments, global governance, while meeting the demands of private industry and civil society, will require diplomacy, compromise, and coordinated efforts.[180] As Kello argues, "the cyber revolution is influencing the tendencies of anarchic international politics."[181] This will continue without sincere efforts from the international community writ large.

These are not issues that can be tackled by the United States or United Kingdom alone or by national governments singlehandedly. Rather, these issues invite collective action from a bottom-up and top-down approach by central governments and the United Nations through the Internet Governance Forum. This requires the pivotal involvement of private industry and

---

[177]Chatham House Conference, "Cyber Security Building Resilience Reducing Risk."
[178]Cornish et al., *Cyber Security and the UK's Critical National Infrastructure,* viii.
[179]Ibid., 27.
[180]This line of reasoning borrows from those of Hedley Bull, *The Anarchical Society,* 4th ed. (Basingstoke: Palgrave Macmillan, 2012) and the English School. See also Paul Cornish, "Governing Cyberspace through Constructive Ambiguity," *Survival* 57 (June/July 2015): 153–176.
[181]Kello, "The Meaning of the Cyber Revolution," 38–39.

growing awareness from civil society. Protecting SCADA and ICS as part of CNI is, as should be readily apparent, in the national interest. It is also in the supranational and global interest. A more informed discourse between private industry and central governments, in partnership with civil society, could help make us wiser before rather than after the event in a world that is ever more dependent on ICT. Should the worst happen, call for John McClane.**

**The authors would like to thank the peer reviewers of this article and the editorial board of *Political Science Quarterly* for this reviewing process. This work is funded and supported by the SCADA-CSL programme of Airbus Group Endevr Wales, a joint research funding initiative between Airbus Group and the Welsh Government.