VOLUME 3 ◆ NUMBER 1 SPRING 2018

THE CYBER DEFENSE REVIEW

ARMY CYBER INSTITUTE ◆ WEST POINT

Countering the Cyber Threat

Shawn Henry
Dr. Aaron F. Brantly

ABSTRACT

The current path to national cybersecurity hides a fatal design flaw. Resident within the current national approach is the assumption that we can continue business as usual with limited sharing between the public and the private sector, the creation of information sharing and analysis centers, the National Cybersecurity and Communications Integration Center, and a range of ad hoc local, state and federal organizations each addressing a slice of a complex and highly interconnected environment. The result is a lack of integrated coordination, continued hacks, and a public increasingly weary of all things cyber. We are approaching the current challenge as if we are living in August of 2001, ignorant and oblivious to the tragedies just over the horizon. All the while the private sector treats each incident in isolation, highly focused on their slice of a broader digital ecosystem.

In the aftermath of the 9/11 attacks, Congress, the executive agencies and departments, and the judicial system in coordination with the will of the American people moved swiftly on legislation and strategies to address a complex asymmetric threat. While many of these new pieces of legislation failed in the courts, the unity of effort and the subsequent cooperative environment across all levels of government, and with the private sector, have arguably altered the national security posture and environment within the United States. Most of these changes have created a safer and more resilient domestic environment that has largely been spared the ravages of foreign-inspired terrorism. While not perfect, the current approaches adapted through years of learning, information sharing, and practice have safeguarded the homeland in an increasingly dangerous world. Lessons from the last 16 years of countering terrorism (CT) should serve as a roadmap for developing a robust, whole-of-society approach to safeguarding the homeland against the threats emanating from cyberspace looming beyond view.

Shawn Henry is the President of CrowdStrike Services and CSO and a retired executive assistant director of the FBI. Henry, who served in three FBI field offices and at the bureau's headquarters, is credited with boosting the FBI's computer crime and cybersecurity investigative capabilities. He oversaw computer crime investigations spanning the globe, including denial-of-service attacks, bank and corporate breaches, and state-intrusions. He posted FBI cyber experts in police agencies around the world, including the Netherlands, Romania, Ukraine and Estonia. He has appeared on "60 Minutes," "CBS Evening News," "Good Morning America," "The Today Show," "Dateline," "Rock Center with Brian Williams" and C-SPAN. He has been interviewed by Forbes, BusinessWeek, The Wall Street Journal, the Associated Press and USA Today.

Henry earned a Bachelor's degree in Business Administration from Hofstra University and a Master's degree in Criminal Justice Administration from Virginia Commonwealth University.

As we move to address the complex cyber environment with nearly one hundred percent Internet saturation,[1] 20 billion internet-enabled devices,[2] and a world controlled by industrial control systems (ICS), big data,[3] machine learning[4] and more we must ask ourselves what lessons can we draw from the CT community? We argue for a concerted national effort at every level of government and within the private sector. Below, we outline the fundamental challenges facing the United States and Western Democracies and provide a measured approach for advancing a coordinated effort to safeguard the underpinnings of modern society.

The Evolving Complexity Problem

It is a bit hard to fathom just how far we have progressed in the 25 years since Congress passed the Scientific and Advanced-Technology Act, 42 U.S.C. § 1862(g) when NSFNET was permitted to interconnect and support access to non-educational networks. Although most trace the history of the Internet back to Donald Davies' or Paul Baran's conceptualization of packet switched networks or perhaps to Vint Cerf or Robert Khan who devised TCP/IP, the Internet became truly global when legal barriers to interconnection began to fall away first in 1992, and then again as the restrictions on cryptography began to dissipate between 1992 and 2000 allowing for secure transactions to occur. In 1994, just over 11% of Americans were connected to the Internet, 23 years later more than 87% are connected.

The number of connected devices per American has also grown rapidly as individuals have purchased everything from personal computers to tablets and phones. As the citizenry have increasingly connected to the Internet so to have the businesses, utilities, and governments upon whom they depend daily for commerce, healthcare, banking, education, electricity, entertainment and so much more. What

Dr. Aaron F. Brantly is Assistant Professor of Political Science, Virginia Polytechnic and State University and Cyber Policy Fellow at the Army Cyber Institute and Cyber Fellow at the Combatting Terrorism Center at the United States Military Academy. He holds a Ph.D. in Political Science from the University of Georgia and a Master's of Public Policy from American University.

Dr. Brantly has worked on issues related to cybersecurity from multiple angles including, human rights and development, intelligence and national security and military cybersecurity. His interests span the political science and computer science divide. He is currently working on a year-long project on cyber deterrence funded by OSD Minerva R-Def. For further information, please visit www.afterwestphalia.org.

once was a network of academics and researchers has spread to touch every aspect of life.[5] Our credit card purchases are monitored based on amount, location, time of day, and frequency for fraud analysis, our power grids balance the load for entire swaths of the nation, our financial markets shift trades around the world in new patterns based on algorithms designed to derive profits from hundredths of a percent change in value. We are conditioned to think of each of these things, these experiences within our daily lives as discrete events, discrete systems, but the reality is far different. We are rapidly advancing towards what William Gibson, the progenitor of the term Cyberspace referred to in fictional terms as a "consensual hallucination."

This modern connected environment is on a trajectory that will only lead to the increasing proliferation of Internet connected devices and general interconnectivity of nearly every aspect of every individual's daily existence. Because each of the systems within this evolving ecosystem is managed by a different company, government, or individual, each addresses the problems at their level of interaction or occasionally within their sector. The efforts to share information more broadly have been met by distrust of government, legal, financial and business concerns and an onslaught of attacks that overwhelm all but the most well-funded information security operations at major corporations or in the Department of Defense.[6] The cybersecurity challenge is multifaceted and decentralized with criminal and state actors spread around the globe.[7] A distributed cyber network structure is in many ways similar to the evolving nature of networked terrorism.[8] While the volume and spread of nodes within the cyber context are likely more voluminous, the reach and scope of terrorism into state and criminal networks[9] is not significantly different than the spread of cybercrime, cyber espionage and cyberattack capabilities across a range of actors.

On September 12, 2001, the problem of transnational terrorism loomed large, and the capacity of international partners, federal, state, local authorities, financial institutions, and a variety of organizations to deal with a complex problem was virtually non-existent. [10] Beyond recognizing the problem of terrorism, it was abundantly clear that actors across all levels and within multiple sectors needed to learn to communicate, plan, organize, and react to problems in near real-time. The military, the intelligence community, law enforcement and first responders needed to develop both endogenous capacity and the ability communicate, strategize and rapidly respond to events. These skill-sets and the technical tools to make them viable were not in existence in September 2001. Yet, today a network of fusion centers, building on the lessons of 9/11, Hurricane Katrina and other significant events have learned to contain and manage crises. The problems posed by cyber threats are unique, in that the technical capacity to respond at both the scale and speed necessary requires many of the same structural and human capital developments to be addressed at a wide range of levels and across a multitude of institutions. In this way, terrorism provides a roadmap for technical and human development to address the cyber challenge now facing the United States.

Solving the cyber problem by planning for it

Responding to a problem in real-time requires utilizing the tools available. Yet, because the cyber problem is evolving and changing as more and more devices come online, it is better to flip the equation. Assuming a 9/11 scale event against the United States in the future, what tools would the US government, state and local authorities need, what resources could be made available to not one, or two, but dozens of industries simultaneously? What communicative and technical capacity is required at every level, and within each organization to contain a considerable crisis?

First, to advance cybersecurity, there needs to be a consensus across the public and private sector. Consensus must occur both within the United States, and internationally within the community of nations. Great strides have been made to achieve international consensus through the United Nations Group of Governmental Experts (UNGGE). [11] The U.S. Department of State has been instrumental in pushing forward key normative issues within the broader international community. Moreover, NATO member countries are slowly moving towards consensus on the urgent need to address cybersecurity. [12] NATO member countries have also begun to incorporate critical infrastructures into the discussion on the future of cybersecurity through the NATO Industry Cyber Partnership. [13] Other key initiatives include the Budapest Convention on Cybercrime which advances a consensus related to criminal activities within cyberspace. Each of these steps at the international level fosters increased understanding and in the case of NATO communications—how to address significant cyber events.

The United States made strides at the federal level under the Obama administration to create information sharing and analysis organizations, strengthen information and analysis centers [14] and manage the federal response to significant cyber incidents under PPD41. [15] Many of these coordination and management improvements have advanced a more robust and unified domestic approach to national cybersecurity in tandem with advances in military cybersecurity development that began in the mid-2000s and began to rapidly increase in speed in 2010 with the creation of U.S. Cyber Command. Yet, despite sweeping organizational changes, cybersecurity within the Federal government remains both complicated [16] and poorly implemented with continued significant intrusions into government networks. [17]

Below the federal level, most states and larger cities are only now just beginning to develop internal cybersecurity capabilities, while most counties and local municipalities have long been woefully ill-equipped to deal with a cyber domain that is quickly facilitating and encompassing larger portions of their information management procedures and constituent services delivery. [18] Many of the issues that plague the Federal government are more pronounced at the state and local level, namely human capital and coordination between actors.

Whereas in the aftermath of 9/11 there was a rapid movement across all levels of government to train and equip state and local authorities to manage significant terrorist crises, the same urgency is lacking in response to reoccurring cyber incidents. The scale and frequency of damage caused by cyberattacks against federal, state and local entities is substantial. Recent years provide a plethora of events in which courts, local governments, or mass-transit systems have been substantially impacted by cyberattacks. [19] While the recognition of the enormity of the problem is slowly being realized, the speed with which state and local actors are addressing these issues leaves millions of individuals, and thousands of firms and governments vulnerable.

Outside of government, private sector problems associated with cybersecurity are extensive but stratified across thousands of industries, sizes and types of firms, each with differing levels of capacity to address an ever more complicated threat environment. Although terrorism affected businesses and their operational plans, not all businesses and firms were necessarily affected by terrorism to the same extent that each company is vulnerable to cyberattacks. Specific industries such as aviation, banking, and utilities among others were directly affected and required to implement new security measures, monitoring of accounts and take other precautions; generally, the threat environment was more constrained than it is presently in cyberspace. By contrast, the impact of cyberattacks on one industry can rapidly cascade and affect other industries, most recently demonstrated by the NotPetya and WannaCry attacks of 2017. [20]

Cybersecurity is currently fragmented. Each actor acts mainly alone or with limited connections to other entities within their industry and varying government interactions. It is imperative that we continue to build consensus around the problems associated with cybersecurity at every level. It is only when there is a universal recognition of the cyber challenge that as a nation we can focus our efforts on the second and third critical tasks that must occur to foster cybersecurity nationally.

Upon the development of consensus, the second facet of addressing the cybersecurity problem is the creation of a tightly interwoven information and communications network that provides rapidly declassified and anonymized threat indicators to halt the spread of malware, quickly detects emerging attacks, and enables attribution. The third undertaking is the sustained development of the human capital necessary to develop, understand, and respond to these threat indicators. These indicators are early warnings of imminent events. Presently, the classification of data, legal, financial or other concerns regarding the dissemination of information delay the development and transmission of this information, complicating the responses of corporations and governments across all ecosystems. Businesses and government agencies should be incentivized to engage in information sharing with assurances that the data being provided will not end up classified or used to adversely affect their firm or government as long as gross negligence or criminal acts did not occur. Trust within an ever-expanding, and resilient information and communications network for cybersecurity is of critical importance and should be incentivized at every level of government and across the private sector. Upon receipt of threat indicators, it is imperative that each entity has the necessary minimum qualified personnel to address the threat to their firm and prevent its spread to other companies within its ecosystem.

Fourth, building on information sharing networks and trained personnel is a need to develop robust public-private, cross-firm, and cross-industry liaison networks. Such networks would serve to minimize localized thinking in threat response and help firms and governments act more broadly by understanding cross-firm-sector-government challenges. By understanding these challenges and addressing how defensive or offensive actions in one industry affects others, the intent is to create a network that responds through a unified effort that minimizes systemic problems and their impact not only within a single firm but across entire sectors. Liaisons have been beneficial to the post-9/11 counter-terrorism efforts and would most certainly be of benefit to addressing cybersecurity challenges. [21]

Fifth, cybersecurity is a team sport. It is not isolated to one company, one sector, or one type of government but crosses boundaries between and amongst them. Shifting the focus from a one-off company or government protection to a more holistic team-based approach will increase the aggregate resilience of the nation. Likewise, while the short-term

costs incurred in developing the structures and processes above are likely to be high, the efficiency gains and savings through the avoidance or minimization of risk are expected to result in net benefits. Where firms or governments are too small to adequately provide protection independently, they would benefit from liaison relationships and cybersecurity coordination with larger firms within the same or similar industries. The larger firms or governments might not see an immediate benefit to providing support to smaller entities, but in providing support to less capable allies, they defend their networks against potential vectors of attack.

Cybersecurity is complex, and the structures and processes articulated in this section are oversimplifications. The process by which the nation responded to the threat of terrorism provides a pathway for developing the reforms necessary to address the cybersecurity problem. Through consensus, planning, and coordination, the United States can begin to take the independent actions of diverse groups and provide a unity of effort to advance cooperative security. This more effective and efficient environment is a foundational step necessary to create a safer and more resilient nation better able to address the cybersecurity problems of the present and into our future.

NOTES

1. http://www.internetworldstats.com/america.htm#us.

2. Amy Nordrum, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated." *IEEE Spectrum,* August, 2016.

3. Paul Burkhardt, "An Overview of Big Data." *The Next Wave* 20 (4): 2014, 1–47. https://www.nsa.gov/research/tnw/tnw204/article1.shtml; 2014. "Big Data: Seizing Opportunities, Preserving Values." Executive Office of the President.

4. "Big Data: a Report on Algorithmic Systems, Opportunity, and Civil Rights." Executive Office of the President, 2016.

5. Aaron F. Brantly, *The Decision to Attack: Military and Intelligence Decision-making.* University of Georgia Press, 2016.

6. Andrew Nolan, "Cybersecurity and Information Sharing: Legal Challenges and Solutions." 7 ed. Washington: Congressional Research Service, 2015; Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing." *Military and Strategic Affairs* 6 (3), 2014; Steven P. Wittenberg, "When to Disclose Data Breaches Under Federal Securities Laws," *Illinois Business Law Journal,* October; 2016, "2016 Financial Industry Cybersecurity Report." *https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf.*

7. United States Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity and Security Technologies, *Emerging Cyber Threats to the United States.* 114th Cong. 2nd sess. Washington: GPO. 2016; (Statement of Frank J. Cilluffo Director, Center for Cyber & Homeland Security at George Washington University).

8. Marc Sageman, *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press, 2011.

9. Scott Helfstein and John Solomon, "Risky Business: The Global Threat Network and the Politics of Contraband." Combating Terrorism Center at West Point, 2014.

10. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report,* Government Printing Office: 2004, 16-419.

11. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." A/70/174. New York: U.N., General Assembly, 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

12. http://www.nato.int/cps/en/natohq/topics_78170.htm.

13. http://www.nicp.nato.int.

14. Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing, https://www.gpo.gov/fdsys/pkg/DCPD-201500098/pdf/DCPD-201500098.pdf.

15. Presidential Policy Directive 41 -- United States Cyber Incident Coordination https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

16. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, Gao.Gov.* Washington, 2013; Richard Bejtlich, "What Are the Prospects for the Cyber Threat Intelligence Integration Center?," Brookings, Washington: February 19, 2015. https://www.brookings.edu/blog/techtank/2015/02/19/what-are-the-prospects-for-the-cyber-threat-intelligence-integration-center/.

17. *Federal Information Security Modernization Act of 2014: Annual Report to Congress Fiscal Year 2016,* Whitehouse.Gov, Washington, 2017.

18. Jim E. Crouch and Larry K. McKee Jr.,"Cybersecurity at the State and Municipality Levels: Where Do We Stand?." National Security Cyberspace Institute, February 25, 2011, http://www.nsci-va.org/WhitePapers/2011-02-25-State-Municipality%20Cybersecurity-NSCI-Crouch-McKee.pdf; Richard Clarke and Karen Jackson, "Commonwealth of Virginia Cyber Security Comission First Report, August 2015: 'Threats and Opportunities'," Commonwealth of Virginia.

19. James Scott and Drew Spaniel, "ICIT Ransomware Report." Institute for Critical Infrastructure Technology, 2016; Jack Stewart, "SF'S Transit Hack Could've Been Way Worse—and Cities Need to Get Ready," *Wired.com.* November 28, 2016, https://www.wired.com/2016/11/sfs-transit-hack-couldve-way-worse-cities-must-prepare/.

NOTES

20. Karan Sood and Shaun Hurley, "NotPetya Ransomware Attack Technical Analysis: a Triple Threat: File Encryption, MFT Encryption, Credential Theft," *Crowdstrike.com,* June 29, 2017, https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/; Adam McNeil, "How Did the WannaCry Ransomworm Spread? - Malwarebytes Labs." *Blog.Malwarebytes.com.* May 30, 2017, https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/.

21. Daniel Byman, "Intelligence Liaison and Counterterrorism: A Quick Primer." *Lawfare.* May 16, 2017, https://www.lawfareblog.com/intelligence-liaison-and-counterterrorism-quick-primer.