The Journal on Terrorism and Security Analysis

SPRING 2017 | 12th EDITION

CONTRIBUTORS

Joseph Abrenio
Marc Barnett
Christopher Folk
joel gridley
Andrew Foote
Neil Noronha

SATSA
Student Association on Terrorism & Security Analysis

The Journal on Terrorism and Security Analysis

12th Edition (Spring 2017)

Syracuse University

Syracuse, New York 13244

Contents

Message from the Editor-in-Chief

The Journal on Terrorism and Security Analysis (JTSA) has now reached its 12th edition! We are very thankful to our authors this year for meeting short deadlines and producing top quality work for us to publish.

We would like to thank the Institute of National Security and Counterterrorism (INSCT) for the continued support in publishing this journal, which we could not do without.

We are grateful for our wonderful editing staff that worked hard through our short deadlines and helped to ensure the journal would be completed on time. A special thanks to Brittani Howell and Kyle Tucker for going above and beyond their duties to make this journal a success.

We feel that with the topic of cybersecurity this year we published some exciting and interesting pieces that will add greatly to the field of national security.

We hope you enjoy the journal!

Sincerely,

Blake Vierra
Editor-in-Chief

Cyber Security and the Grid: We'll Leave the Lights on for You (If We Can)

Joseph Abrenio, joel gridley, and Christopher Folk

Overview

The U.S. power grid plays a vital role in the nation's health and welfare. The U.S. relies upon a consistent and continuous supply of electrical power to fuel transportation, power its industries, and sustain its healthcare system. Yet, this critical asset is often taken for granted, even though just a minor disruption of the vast network of our power grids could have devastating impacts. The loss of power—in even a small, isolated area—can leave homes without heating or cooling, interrupt local businesses, and down traffic control devices. A regional or national disruption could bring commerce and manufacturing operations to a halt, or even worse, disable critical care and surgical facilities. The ripple effects could mean catastrophic economic loss or loss-of-life. Furthermore, the short-term and long-term national security implications that would arise from an attack on our critical infrastructure would be significant.

The goal of this white paper is to provide a deeper understanding of the role of the grid in our critical infrastructure paradigm; the current grid regulatory scheme; and the technical and non-technical cyber threats facing the grid, including legal liability for operators.

As an introduction, we provide an overview of critical infrastructure and specifically, the power grid, as well as technical and non-technical issues facing the grid. Next, we offer an overview of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards that provide a regulatory framework. Finally, we address best practices, risk mitigation, risk transfer methods, and security risk assessments in the context of operations, IT operations, and compliance.

I. Critical Infrastructure

The electric grid is one of the most complex and critical components of infrastructure because so many other sectors are dependent upon it for their own continued operations. With the transition from mechanical devices to digital remote and control functions to manage the grid, the risks presented by bad actors have dramatically increased. Furthermore, the risks to critical infrastructure and cyber events in general have received widespread media attention in recent years. While it is beneficial to shed light on the problems, many media outlets have been quick to jump to conclusions and provide poorly-vetted accounts of cyber intrusions, which can do more harm than good by sensationalizing such news and ultimately lead to industry and consumer fatigue or even disbelief. Consider the December 2016 report, which stated that a Vermont utility was hacked and reportedly had signs related to Grizzly Steppe.[1] While this was widely reported, it was quickly revealed that the Vermont grid had not actually been infiltrated, the device in question was never connected to the grid networks, and the origin was not likely Russia[2] Consequently, security professionals must be vigilant and ensure that they properly investigate and understand the situations that may be encountered.

A. Power Grid Overview

The first local grid began operating in 1882, suppling a small group of customers in Manhattan with low-voltage electricity using direct current connections.[3] At the end of the 19th century, the industry largely adopted the use of alternating current (AC), which enabled electricity to be transmitted across far greater distances. This technolog-

---

1 Warner Todd Huston, *Washington Post's Fake News of Russian Vermont Power Plant Hack*, Breitbart News (Dec. 31, 2016), http://www.breitbart.com/big-government/2016/12/31/washington-posts-fake-news-russian-vermont-power-plant-hack/.

2 *Id.*

3 JS, *How Electricity Grew Up? A Brief History of the Electrical Grid . . .*, Power2Switch (Oct. 25, 2012), https://power2switch.com/blog/how-electricity-grew-up-a-brief-history-of-the-electrical-grid (The Pearl Street Station in Manhattan provided service to 85 customers, powering approximately 400 lamps).

ical advancement sparked a period of utility consolidation, and by the turn of the 20th century, approximately 4,000 distinct and isolated electric utilities distributed electricity to their geographic localities.[4] This was further bolstered by the industrialization effort in a post-World War II era. Ultimately, 2,000 electric distribution utilities were grouped into three "sectional" grids that supply power to 48 states: (1) The Eastern Interconnection (typically includes those states east of the Rockies); (2) the Western Interconnection (which reaches from the Rocky Mountain states to the Pacific Ocean; and (3) the Texas interconnected system (which, as the name implies, includes Texas).[5] These sectional grids continue to exist today.

II. What is SCADA?

Like all industries, the power industry looked to new technologies to increase efficiency and profitability by coordinating and optimizing power transmission between and amongst interconnected grids. [6] Grid operators employed industrial control systems (ICS), and specifically, supervisory control and data acquisition (SCADA) systems, for greater energy transmission.[7] SCADA is essentially a combination of hardware and software that allows complex control and monitoring of physical industrial equipment.

While often associated with utilities, every industry leverages SCADA. In fact, the term SCADA is a generic category which implies the system from which control and monitoring is achieved. For example, car manufacturers use SCADA systems to control the machinery involved in the manufacturing process.[8] Similarly, a dam operator

---

4 *Electricity Explained: How Electricity is Delivered to Consumers*, U.S. Energy Info. Admin., http://www.eia.gov/energy_in_brief/article/power_grid.cfm (last visited Nov. 22, 2016); *The Electricity Grid: A History*, Burn an Energy J., http://burnanenergyjournal.com/the-electricity-grid-a-history/ (last visited Dec. 27, 2016).

5 *Id.*

6 Tamilman Vijayapriya & Dwarkadas Pralhadas Kothari, *Smart Grid: An Overview*, Sci. Res. (June 7, 2011), http://file.scirp.org/pdf/SGRE20110400016_22126588.pdf.

7 *Id.*

8 Zenon for Automotive, CopaData (last visited Feb. 8, 2017), https://www.copadata.com/en/process-control-system/automotive/.

uses a SCADA system to measure the amount of water flow through a dam's controlled spillway, while pharmaceutical companies utilize SCADA systems to control mechanized sorting machines and conveyors in the automated packaging of drugs for delivery to distribution centers.[9]

However, the specific uses of SCADA systems are industry-driven. While certain principles, architecture, and terminology remain standard, specialization or customization from industry to industry is required. The use of ICS and SCADA was a large driver in the evolution from an analog to a digital grid, referred to as the Smart Grid.

A. Evolution of the Smart Grid

The power grid's network of mechanical, analog controls was highly inefficient in the transmission and distribution (T&D) of energy because each mechanical component introduced resistance. Multiplied over hundreds or thousands of devices, the cumulative resistance was significant. Experts estimate that traditional, non-digital controls limited the grid to approximately 60 percent of overall transmission capabilities.[10] The mechanically-controlled, analog grid was a collection of moving parts that was doomed to fail over time due to thermal breakdown or mechanical component failures.[11]

In response, grid operators began designing and implementing electronic controls and devices using solid-state superconductors, which increased electricity transmission and distribution. Just as critical, these new technologies allowed for remote control, monitoring, and modification, thereby decreasing maintenance time and further increasing utility profits.

---

9 Frank R. Spellman, Dam Sector Protection and Homeland Security (Bernan Press, 2017).

10 U.S. Dep't of Energy, Enabling Modernization of the Electric Power System: Technology Assessments (2015), https://energy.gov/sites/prod/files/2015/09/f26/QTR2015-3F-Transmission-and-Distribution_1.pdf.

11 *Id.*

As a direct result of electronic devices—and supported by the design, development, and deployment of the Internet of Things (IoT)—the modern Smart Grid was born. The Smart Grid is now capable of interacting through even basic household appliances through their embedded technologies. However, this Internet gateway possesses unintended threats, as these IoT devices are particularly susceptible to power issues.[12] Nonetheless, as our electrical infrastructure continues to age, and various components are approaching their useful end-of-life (EOL), the movement to the Smart Grid (with monitoring, analysis, control, and communication capabilities) is essential to providing reliable and consistent power transmission in the face of ever-growing needs.

For instance, one of the key Smart Grid components is demand side management, which maximizes load balancing and minimizes cascading failures.[13] Demand side management enables grid connections to distributed generation power (wind turbines, photovoltaic (solar) arrays) and fosters grid energy storage, wherein stored power is used to offset high demand periods and prevent rolling outages.

Additional Smart Grid functions include:[14]

- Efficient transmission of electricity;
- Re-generation and restoration of services in a post-power disturbance scenario;
- Demand and load balancing; and
- The integration of renewable energy sources.

The economic benefits from these new functionalities are lower operational and management costs. In addition, grid operators can leverage large-scale power production and provide more consumer-driven power production, again benefitting the economic bottom line.

---

12 *What is Smart Grid and Why is it Important?*, Nat'l Electrical Manufacturers Ass'n, https://www.nema.org/Policy/Energy/Smartgrid/Pages/What-Is-Smart-Grid.aspx (last visited Nov. 23, 2016).

13 *Id.*

14 *What is the Smart Grid?*, SmartGrid.Gov, https://www.smartgrid.gov/the_smart_grid/smart_grid.html (last visited Nov. 23, 2016).

B. Critical Infrastructure Threats

Following the domestic terrorism event in Oklahoma City in 1995, Attorney General Janet Reno urged President Clinton to create a commission to examine U.S. vulnerability to attacks at "key facilities."[15] Consequently, President Clinton formed the Presidential Commission on Critical Infrastructure Protection (PCCIP).[16] General Robert Marsh (USAF Ret.),[17] was appointed as its Chairman. The PCCIP developed the term "critical infrastructure" to designate key U.S. facilities, and formed the "Marsh Commission" to investigate and report on threats to the nation's critical infrastructure.[18]

In 1997, the Marsh commission delivered a report (the "Marsh Report") that focused on the Internet, underscoring the fact that the country's most important functions were often routed through the Internet, and any disruption of the Internet could cause widespread outages or damage to our critical infrastructure.[19] The Marsh Report urged a coordinated effort to protect the U.S. against the prospect of nation-states creating "information war" offensive units.[20]

However, the Marsh Report warned that much of the burden would fall upon the private sector, as it owned the bulk of the critical infrastructures.[21] The Marsh Report further warned that these industries would likely be reticent to invite government regulation in their industries under the guise of cyber security.[22]

---

15 Richard A. Clarke, Cyber War: The Next Threat to National Security and What to do About it 105 (2010).

16 *Id.*

17 *Id.* at 106.

18 *Id.*

19 *Id.*

20 Clarke, *supra* note 15.

21 *Id.*

22 *Id.*

C. The Wake-Up Calls: 1999 and 2003

A cyber threat to critical infrastructure was realized on June 11, 1999, when a gasoline pipeline in Washington State burst and began spilling fuel into a nearby creek.[23] The gasoline ignited, killing three people and causing extensive damage to a nearby water-treatment plant.[24]

A subsequent investigation by the U.S. National Transportation Safety Board (NTSB) determined that the root cause of this event was a software failure within the SCADA system.[25] Although there was no indication in the report that the incident was related to any malicious activity, the fact that a software failure in a SCADA system could result in palpable, physical damage underscored the fact that cyber security was a legitimate concern.[26]

In 2003, a computer malware worm named "Slammer" infiltrated and consumed computing power within power grid SCADA systems, causing the controls to become less responsive.[27] Consequently, when a tree fell in Ohio and caused a surge, the SCADA systems could not successfully prevent a cascading power loss affecting eight states and more than 50 million people.[28] This single event demonstrated that a targeted cyber-attack on the power grid coupled with a physical attack could have devastating effects.

---

23 *Id.* at 97.

24 *Id.*

25 CLARKE, *supra* note 15, at 97.

26 This is an inference made by the author since the report did not point to malicious intent but rather a failure in a SCADA system from which physical damage resulted.

27 Paul Ducklin, *Memories of the Slammer Worm: Ten Years Later*, NAKED SEC. (Jan. 27, 2013), https://nakedsecurity.sophos.com/2013/01/27/memories-of-the-slammer-worm/.

28 CLARKE, *supra* note 15, at 99.

D. The Threat Becomes Real: Cyber-Attacks on Power Grids and Critical Infrastructure

As recently as December 17, 2016, a cyber-attack directed at the Ukraine power grid left homes without power for over an hour.[29] This was reminiscent of a similar attack that occurred in December 2015, when a cyber-attack against the Ukraine power grid resulted in a loss of power for more than 225,000 citizens.[30] According to the Department of Homeland Security (DHS), this event marked the first successful cyber-attack to take a power grid offline.[31] Fortunately, the latest incident in 2016 was short-term in duration and had a narrow reach. With temperatures ranging from 15 to 30 degrees Fahrenheit, if the outage lasted longer, and occurred over a broader geographical swath, people could have died.[32]

In the summer of 2013, Iranian hackers infiltrated the control systems of a dam near New York City.[33] While this attack resulted in no known damage, the fact that the hackers were able to penetrate and gain access to these control systems was remarkable.[34] Even more concerning, experts report that Iranian attackers targeting other criti

---

29 John Leyden, *Energy Firm Points to Hackers after Kiev Power Outage*, REGISTER, http://www.theregister.co.uk/2016/12/21/ukraine_electricity_outage/ (last visited Dec. 27, 2016).

30 *Id.*

31 Dustin Volz, *U.S. Government Concludes Cyberattack caused Ukraine Power Outage*, REUTERS, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K (last visited Nov. 23, 2016) (The attacks on the Ukraine were purportedly initiated from remote cyber intrusions into three regional electrical power distribution companies where ICS systems were targeted and exploited).

32 Leyden, *supra* note 29.

33 *Schumer: Iranian Cyber-Attack on New York Dam was "Shot Across the Bow"*, TOWER (Mar. 15, 2016, 8:09 AM), http://www.thetower.org/2090-schumer-iranian-cyber-attack-on-new-york-dam-was-shot-across-the-bow/.

34 *Id.*

cal infrastructure have successfully exfiltrated highly sensitive data such as mission-critical power plant blueprints.[35]

A rising concern for U.S. officials is the combination of a kinetic and cyber-attack in a multi-phasic approach to trigger an actual invasion. For instance, Russia's alleged pre-emptive distributed denial-of-service (DDoS) attack against Georgia was used to disrupt the country's communication networks prior to the Russian army invasion.[36] This cyber event was powered with a kinetic conventional attack in the form of a physical invasion, which made for a highly-effective belligerent action.[37] The one critical distinction between Georgia and the U.S. in this instance is that Georgia was not as reliant upon technology. The cyber-attack perpetrated against Georgia caused little damage other than the loss of website accessibility—all other communication methods remained online.[38] Were such an attack directed at the U.S., the effects could be far more severe and wide-ranging, as the U.S. is much more dependent on Internet communications.

The well-known Stuxnet computer worm—reportedly designed to infiltrate Iran's Nuclear centrifuge program—is another example of a cyber incident with implications in the physical realm. The Stuxnet attack targeted command and control software and caused the centrifuges to essentially self-destruct, while also disrupting monitoring capabilities so everything appeared to be running normally.[39] This event was significant, as it was reportedly the first actual deployment of a cyber-physical attack that crossed the two realms, causing damage within each.

---

35 *Id.*

36 John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. Times (Aug. 12, 2008), http://www.nytimes.com/ 2008/08/13/technology/13cyber.html?_r=0.

37 *Id.*

38 *Id.*

39 Bipartisan Policy Ctr., Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat (2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/ Cybersecurity%20Electric%20Grid%20BPC.pdf.

Using the lessons learned from these events, the National Research Council (NRC) delivered a report in 2012 in which it concluded that a coordinated terrorist attack directed at the power grid could result in a wide-scale blackout that would persist for weeks or perhaps months.[40] The NRC also theorized that if a combined kinetic and cyber-attack were coordinated and timed to transpire during periods of prolonged cold weather, the effect could be catastrophic.[41] Aside from the obvious economic losses, an attack of this scale could also result in thousands or hundreds of thousands of deaths due to extended exposure to extreme cold temperatures.[42]

E. Technical Cybersecurity Issues Facing the Grid

i. Esoteric Nature of SCADA systems

For the reasons discussed above, power grid SCADA systems are extremely unique and specialized. Moreover, the applications and processes that manage and direct telemetry and control communications of each SCADA system are proprietary software and are specific to the vendor which produces it. Because vendors are often responsible for designing these specialized SCADA systems, the IT Operations staff ultimately operating them may lack a comprehensive understanding of their own SCADA environment, as they are often based on proprietary software.

Even when installed on typical operating systems such as Unix or Windows, the operating system itself can behave in unfamiliar ways. What would be considered standard IT procedures in any other environment (such as routine OS updates or password changes) may prove disruptive in a specialized and proprietary SCADA environment.

---

40 Nat'l Acad. of Sci., Terrorism and the Electric Power Delivery System (2012), https://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system.

41 *Id.*

42 *Id.*

ii. Corporate Move to "Cloud" Environments

A recent trend, both among corporations and the vendors they employ, is moving infrastructure and services to the "cloud." Even sensitive services, such as security patches (CIP-007R2), or anti-virus software and signature updates (CIP-007R3), (which many responsible entities are dependent upon for maintaining compliance and a secure SCADA environment) are moving, or have already moved to the cloud.[43]

In addition to services such as weather forecasts and Outage Management Systems (OMS) directly interacting with the SCADA environment, responsible entity corporate networks are becoming increasingly dependent upon cloud-provided services, applications, and storage, and are inextricably exposed to data leakage risks.[44]

iii. Cost of Commitment, Lack of Interoperability

Choosing a SCADA system vendor is a massive commitment in time and capital expense. Furthermore, a utility is often locked into a vendor for many years as these systems have virtually no interoperability with any other equipment, other than custom interoperability designed and implemented in the initial SCADA solution.[45] Because of this lack of interoperability, if any equipment or software bundled in the solution is found to be unable to conform to compliance requirements or security best practices, there is usually very little to no opportunity to replace the equipment or software with

---

43 Kevin Parker, *SCADA Remains Relevant for Industrial Automation*, CONTROL ENGINEERING (Dec. 7, 2016), http://www.controleng.com/single-article/scada-remains-relevant-for-industrial-automation/5e5c4f48da a67663752ffe385047ab4a.html.

44 *Integrated Distribution Management on a Cloud*, CAPGEMINI, https://www.br.capgemini.com %2Fresource-file-access%2Fresource%2Fpdf%2Fintegrated_distribution_management_system _on_a_cloud.pdf& usg=AFQjCNHRjT8-nj6LYI_iihy71Zin_zgORw&sig2=O8jw416dOlsDPL-pHEIUfw (last visited Feb. 8, 2017).

45 SCADA solutions are generally custom-tailored to specific environments and uses. Thus, an entity that implements a SCADA solution can customize it and enable interfaces when it is implemented. Post-implementation, an entity would either need to rely on in-house expertise or use vendor resources to enable interoperability with other products.

alternatives. As a result, there is no easy upgrade when SCADA solutions become outdated. A utility is forced to develop a completely new architecture, purchase new equipment, and conduct new training for the IT Operations Staff.

iv. Undocumented "Features" in SCADA Environments

IT Operations Staff are often forced to rely upon the documentation provided by SCADA vendors to understand the operational behaviors and requirements of the environment. Unfortunately, not all behaviors and requirements are explicit, and sometimes they are only implied. Thus, IT Operations Staff who may be unfamiliar with the SCADA application, device, or process may miss or misinterpret signals.

Because SCADA solutions are proprietary products, there are few, if any, additional resources besides the vendor to turn for more documentation, explanation, or instructions. Adding to this is the sensitive nature of SCADA solutions in the utility industry. Although you can typically find all sorts of online resources regarding managing firewalls, databases, and servers, it's difficult to find such information when it comes to SCADA solutions. The "security through obscurity" paradigm typically applied in SCADA environments often produces unintended results, as operators and staff do not share critical threat information from one utility to another.

v. Updates Delayed by Shortcomings in SCADA Software

During the lifecycle of any computing environment, security patches and operational updates are common and expected. However, vendors are routinely slow in producing timely SCADA security software patching, leaving SCADA systems dangerously vulnerable to even know cyber weaknesses. These vulnerabilities are routinely cited in vulnerability assessments, often including warnings of unapplied security patches and existing Technologically Feasibility Exceptions (TFE).

vi. Infiltration of "Internet of Things" (IoT)

Before the IoT became common, mundane equipment such as uninterrupted power supplies (UPS), heating ventilation and air conditioning (HVAC), closed circuit television cameras (CCTV), and other devices common in regulating the physical data center environment were not a security concern as they were typically not network-capable. Now, manufacturers are incorporating network connectivity in almost all appliances, including refrigerators, toasters, ovens, microwaves, and coffee makers. Not surprisingly, these appliances, once introduced into even non-secure areas such as a control center breakroom, could pose a threat to the utility network. Therefore, continuous passive monitoring for unknown devices on ESP networks may help to identify their presence.

F. Non-Technical Cyber Security Issues Facing the Grid

i. Vendor Responsibility and Accountability

The role and importance of a SCADA vendor cannot be overstated. The level of service and responsiveness of technical support from the vendor should be considered with just as much weight as the capabilities of the architecture itself. Along with support considerations, vendors should also be examined for how robust and effective their internal controls are, and how they handle customer data, specifically NERC CIP protected information about BES Cyber Assets.

Vendors are not independently accountable to NERC, but are required to comply with NERC CIP. This includes conducting background checks and controlling access to any NERC CIP sensitive information they may have.

While vendors can provide expertise on the SCADA systems, they are not necessarily experts on NERC CIP requirements. Furthermore, each customer can have very different positions regarding some of the more ambiguous requirements. As

a result, NERC CIP compliance is a very difficult issue and is often a moving target for what is required for one customer (based on policy), and what is required for another. It is therefore up to the responsible entity to ensure that vendors, who commonly hold the keys to their crown jewels, are taking that responsibility seriously by using strong internal controls, even when they're not actively connected inside the responsible entity's Electronic Security Perimeter (ESP).

An example of this scenario occurred in 2015, when a vendor went on-site to a customer to apply updates to a SCADA database.[46] Her escort discovered that she had all the customer's system accounts and passwords written down in a ragged spiral-bound notebook she had carried with her.[47] Upon further inspection, the customer also discovered that other sensitive information, such as host names paired with IP addresses and operating systems, was also in the notebook.[48] These notes were likely kept with the goal to improve the vendor's customer support (and for the sake of convenience), but this was a possible violation that needed to be self-reported to the Regional Enforcement Entity. Regular dialogue between the vendor and the customer, along with a review of internal control assessments, could have prevented the possible violation.

Language should be considered in service contracts to address the risks that vendors represent. There is a lot of trust placed in them to handle sensitive information, and there is an expectation to protect that data with appropriate technical and procedural controls—with built-in oversight and perhaps even possible sanctions by the customer.

ii. Legacy "If It's Not Broken, Don't Fix it" Mentality

The utility industry's unspoken *de facto* position has historically been, "if something isn't broken, don't meddle with it" for the fundamental reason that functioning mechanical

46 The above scenario transpired while the co-author, Joel Gridley, was performing a site-visit at an unnamed client.

47 *Id.*

48 *Id.*

equipment had no need to be disturbed, and if it were disturbed, it would often result in unintended consequences. Today, the technologically sophisticated Smart Grid requires nearly constant maintenance to ensure reliable operation. Regular updates and emergency security patches are a common occurrence. Far too many dispatchers and operators cringe at the thought of tinkering with a grid that appears to be humming along. While historically a sound strategy, failing or refusing to update the modern Smart Grid ensures that it will quickly become outdated or vulnerable to malicious or inadvertent disruption.

iii. Positions Based on Ease of Meeting Compliance

Throughout the NERC CIP standards there are requirements with language that reads, "Identifies, assesses, and corrects . . ." (IAC).[49] Many of these IAC requirements include general guidance on topics the policy or process is required to address, but give room for the responsible entity to include more refined details surrounding those processes. For example, CIP-006R2.1 requires an IAC documented visitor control program to "*Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.*"[50] This may provide the utility with a basic framework to develop a program, but it lacks specificity regarding how many visitors a single escort can bring into the environment per trip or while logged in (as required by CIP-006R2.2), for example, or whether the escort is required to accompany the visitor during brief trips outside the physical security perimeter (such as bathroom breaks). Many NERC CIP standards leave these additional details up to the individual responsible entity. As a result, utilities may be unknowingly creating a standard that they are held to in the future by the NERC regulators.

---

49 *Transition Program FAQs*, North American Electric Reliabilty Corp., http://www.nerc.com/pa/CI/Pages/Transition-Program-FAQs.aspx (last visited Feb. 8, 2017) [hereinafter Transition Program].

50 *CIP-006-6 Cyber Security: Physcial Security of BES Cyber Systems*, North American Electric Reliability Corp., http://www.nerc.com%2Fpa%2FStand%2FPrjct2014XXCrtclInfraPrtctnVr5Rvns%2FCIP-006-6_CLEAN_06022014.pdf (last visited Feb. 8, 2017).

There are two scenarios in which responsible entities can get into trouble. One causes compliance issues, and the other causes security issues. The first occurs when well-intentioned managers create utopian policies: requirements that are extremely conservative and demanding, but completely infeasible to follow for lack of staff, technology, or process. Often, such policies result in the utility answering uncomfortable questions from regulators.

The second instance is not so easy to discover, as the policies developed will satisfy the letter of the requirements, but fall shy of following security best practices. Merely having check boxes for the existence of the policy and evidence the policy is followed may result in the appropriateness of the policy itself being overlooked.

Similarly, ambiguous terminology such as *custom software* from CIP-010R1.1 which requires a corporate legal position, or doctrine as to how the responsible entity defines the ambiguous term (and therefore audited against the position) can also fall into the two traps mentioned above.[51] In the example given, a comprehensive and all-encompassing definition will quickly become onerous and cumbersome for compliance purposes, but a definition with strict limitations on what is included can expose the environment to risk.

Introduced in NERC CIP v5 is the concept of "Transient Devices" and allowance of "Removable Media" in CIP-010R4.[52] These can be easily abused for the sake of convenience while complying with the letter of the requirement, but careful consideration must be made to ensure that security best practices are maintained.

---

51 *CIP-010 Cyber Security: Configuration Change Management and Vulnerability Assessments*, North American Electric Reliability Corp., http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-2&title=Cyber%20Security%20-%20Configuration%20Change%20Management%20and%20Vulnerability %20Assessments (last visited Feb. 8, 2017) [hereinafter Configuration].

52 *Id.*

iv. Compliance Staff Lacking Technical Skills

Compliance staff oversee and manage all aspects of compliance, including supervising and managing the gathering of evidence, composing Reliability Standard Audit Worksheets (RSAWs), and submitting TFEs and self-reports. However, they do not always have a technical background and often rely heavily upon the IT Operations staff for terminology, evidence gathering, and mitigation suggestions. Much of the information collected from the IT Operations staff must be taken at face value, since the compliance staff may not have the technological expertise to challenge or question the information.

Because of the additional expense of clearing other corporate resources with technical expertise who would be able to review the provided information with objectivity, this option is often not leveraged. An objective eye with technical expertise is required to preserve true separation of duties. Therefore, there is yet another opportunity for things to be missed either intentionally or unintentionally with no system of checks and balances in place.

v. Critical Infrastructure Regulations

Pursuant to the Energy Policy Act of 2005, the power industry is regulated by mandatory cyber security standards.[53] These regulations fall within the jurisdiction of the Federal Energy Regulatory Commission ("FERC").[54] The cyber security standards are developed by the North American Electric Reliability Corporation ("NERC").[55] NERC is a not-for-profit international regulatory authority that covers the continental United States, Canada, and the northern portion of Baja California, Mexico.[56] NERC relies on industry experts and government representatives at both the state and federal level to formulate its

53 Energy Policy Act of 2005, Pub. L. No. 109-58.

54 *Frequently Asked Questions About Cybersecurity and the Electric Power Industry*, Edison Electric Inst., http://www.eei.org/issuesandpolicy/cybersecurity/documents/cybersecurity_faq.pdf (last visited Nov. 23, 2016) [hereinafter EEI].

55 Transition Program, *supra* note 49.

56 EEI, *supra* note 54.

cyber security guidelines.[57] Once developed, they must be authorized by Congress, then reviewed and approved by FERC.[58] The reliability standards that govern the three interconnected power grid systems were developed by the electric power industry, and then approved by FERC to ensure interoperability and coordinated electrical systems.[59]

NERC standards are only applied to utilities that fall within the definition of Bulk Electric System (BES).[60] Currently, the definition for BES includes all transmission elements operated at 100 kilovolts (kV) or higher, as well as real or reactive power connected at 100kV or higher.[61] NERC CIP 002-5.1, however, defines a BES as including Distribution Providers that own facilities, systems, and equipment that is: (1) an under frequency load shedding (UFLS), or (2) an under voltage load shedding (UVLS) program that is subject to NERC/Regional Reliability Standards, or (3) performs automatic load shedding under a common control system of 300MW or more (without human intervention).[62]

This raises an issue, as NERC's CIP regulations and FERC's reliability mandates will not apply to facilities below these thresholds. Thus, attackers could potentially

57 *Id.*

58 *Id.*

59 *Id.*

60 *Id.*

61 FERC Order No. 693, FERC Stats. & Regs. 31,242 Mandatory Reliability Standards for the Bulk-Power, 693 Fed. Energy Reg. Comm. ORD. § 4.2 (Mar. 17, 2007).

62 *CIP-002-5.1 Cyber Security: BES Cyber System Categorization*, North American Electric Reliability Corp., http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-002-5.1&title=Cyber%20Security %20%E2%80%94%20BES%20Cyber%20System%20 Categorization&jurisdiction=null (last visited Dec. 29, 2016) [hereinafter BES Cyber].

use these non-covered entities as backdoor access points for cyber intrusions.[63] Additionally, BES systems are further classified as either high impact or medium impact.[64]

For BES, FERC has approved eleven critical infrastructure protection CIP standards, which are focused specifically on cyber security. Additionally, in February 2013, President Obama issued executive order (EO) 13636: Improving Critical Infrastructure Cyber Security, along with a Presidential Policy Directive (PPD) 21. Specifically, EO 13636 calls for the following[65]:

- Developing a technology-agnostic cyber security framework;
- Promoting and incentivizing the adoption of cyber security practices;
- Increasing cyber threat information sharing;
- Leveraging privacy and civil liberties protections within any initiative to secure critical infrastructure; and
- Exploring the use of pre-existing regulations to promote cyber security.

Whereas, PPD-21 advocates for:[66]

- Developing situational awareness to address physical and cyber elements of infrastructure in real-time;
- Analyzing and understanding the potential cascading consequences that might arise from infrastructure failures;
- Evaluating and improving the partnership between the private and public sector;
- Evaluating and updating the National Infrastructure Protection Plan; and
- Developing a comprehensive research and development plan.

---

63 Consider, for instance, data breaches such as the Target data breach wherein 45 million card numbers were exfiltrated by attacking Target's databases through an unsecured backchannel built to allow their HVAC supplier to remotely access monitor and control on-site systems. Here too, in an interconnected framework it is feasible that an attacker could target (no pun intended) smaller, non-BES entities that are not NERC CIP compliant and use that to elevate privileges and access BES entities. Meagan Clark, *Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer*, Int'l Bus. Times (May 5, 2014), http://www.ibtimes.com/ timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

64 BES Cyber, *supra* note 62 (High Impact and Medium Impact are defined in CIP 002-5.1).

65 *EO 13636 and PPD-21*, Dep't Homeland Sec., https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf (last visited Nov. 23, 2016).

66 *Id.*

The current NERC CIP regulations include the following:[67]

- CIP 002-5.1: Cyber Security - BES Cyber Systems
- CIP 003-6: Cyber Security - Security Management Controls Categorization
- CIP 004-6: Cyber Security - Personnel & Training
- CIP 005-5: Cyber Security - Electronic Security Perimeter(s)
- CIP 006-6: Cyber Security - Physical Security of BES Cyber Systems
- CIP 007-6: Cyber Security - Security System Management
- CIP 008-5: Cyber Security - Incident Reporting and Response Planning
- CIP 009-6: Cyber Security - Recovery Plans for BES Cyber Systems
- CIP 010-2: Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP 011-2: Cyber Security - Information Protection Standard
- CIP 014-2 Physical Security[68]

For this white paper, we focus on the following NERC CIP guidelines:

CIP 005: The establishment of electronic security perimeter conclaves within a corporate environment are exceedingly difficult to implement and maintain under ideal conditions. This should, however, be taken in the context of the President's Cybersecurity Commission report released in November 2016, which stated that enterprise electronic security perimeters are outdated, outmoded, and ineffective. This is an interesting regulation which is increasingly dynamic.

CIP 007: This regulation includes the bulk of the operational implications of daily cyber security tactics that an entity will need to perform. A lot of "the what," "the when," and "the where," is described and this information is critical for IT operations.

CIP 008: From an operational perspective, this piece is critical. From a liability and legal exposure perspective, the creation, adoption of, and adherence to this CIP is essential.

---

67 *CIP Standards: Subject to Enforcement*, North American Electric Reliability Corp., http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (last visited Dec. 15, 2016).

68 While NERC lists this as "subject to enforcement" this CIP has not yet been adopted and is pending. *Id.*

While this is a proactive regulation implemented to manage a post-incident reactionary response, here the focus is going to be on the legal side.

CIP 009: This is the IT operational analogue to the legal issues and reporting requirements under CIP 008. This would generally be an aspect or even the driving force behind a comprehensive disaster recovery plan. As with any DR plan, creation and implementation are largely prophylactic unless applied within actual testing scenarios.

CIP 010: Within this regulation, the potential for ongoing and daily impacts to IT operations is significant. The policies and procedures must be developed and fully implemented across the organization. While the human element is often regarded as the weakest link, the use of systems and software that are not patched to address known vulnerabilities is certainly near the top of that same list.

Because of the CIP cyber security standards and those dictated by EO 13636 and PPD-21, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) was created and has been used to share threat information between the public industry and private sector entities.[69]

vi. Critical Infrastructure: Legal Implications

Depending on "the how, and the where" from which an attack is initiated, and depending on who the attacker is, there are varying cyber security implications.[70] Likewise, in the realm of the power grid, the legal implications are quite different from those which a typical company or industry may encounter. In the power industry, while PII certainly exists and is collected and stored, the richer targets are the operations them

69 Joseph S. Abrenio, *Illuminating Issues of Grid Cybersecurity*, U.S. Cybersecurity Mag., http://www.uscybersecurity.net/united-states-cybersecurity-magazine/fall-2016/mobile/index.html#p=Cover (last visited Feb. 7, 2017).

70 Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attack that Target and Degrade the Grid*, 40 Wm. Mitchell L. Rev. 647 (2014).

selves and the continuous flow of electricity. Thus, it is less likely that a BES will need to focus on data breaches and breach notification laws; and instead will need to focus on the legal implications they may face in the case of a cyber-event that results in loss of power.[71] Furthermore, in this industry, it is far more likely that a cyber-event could have material impacts on quality of life. There is a potential for loss-of-life circumstances that would be the natural result of a sustained power loss situation in either extreme hot or cold weather conditions.

Additionally, the mere fact that the power grid is included within critical infrastructure underscores the national security implications inherent in continuous and reliable power transmission. Therefore, this industry differs significantly from the retail or entertainment industries where a cyber-event could be a nuisance, and could affect large numbers of individuals in a financial sense, but is unlikely to have even a tangential relation to national security.

Consequently, it is increasingly likely that a targeted attack against the grid would result in ongoing and after-action coordination with state and federal authorities versus a purely private sector response. Considering the greater potential for a national response to a grid cyber-event, the onus is even higher for a complete and thorough analysis of the operations to provide a high level of confidence as to the timing of any breach, and as much metadata as possible to ensure accurate event tracing.

vii. Risk Mitigation

To mitigate risk, many areas can and should be addressed. A prominent area of focus needs to be compliance with NERC CIP policies. Grid utilities that operate below the designated BES thresholds should consider adopting all or at least portions of the NERC CIP regulations to demonstrate compliance and reduce overall liability. Obviously, any utility designated with BES status should and must comply with both the

71 *Id.* at 756-57.

spirit and the letter of the NERC CIP policies. Consequently, if risk mitigation is a primary motivator, then any BES should strongly consider conducting a third-party vendor assessment of any non-BES utility that has interconnections with the power grid. This is merely one piece in a much larger mosaic that paints a picture of cyber security.

G. Best Practices

Whereas the regulatory framework provided by NERC/FERC provides basic guidance, the framework should be viewed merely as the minimum baseline and aspirational in nature. Given the ever-changing technology landscape, cyber threats are dynamic. Entities must meet the baseline defenses while moving towards higher levels of cyber security to forestall any issues. Resilience and security are long-term goals which do not comport themselves to rigid, static guidelines. Rather, the operators in this space must remain vigilant to develop, maintain, continuously expand, and adapt their cyber security practices.[72]

H. Human Assets and Resources

System Operators and Dispatchers are those professionals tasked with management, operation, and reliability of the BES.[73] System Operators and Dispatchers are certified and credentialed through NERC, which maintains those credentials and modifies training and testing requirements as needed.[74] After becoming certified as a System Operator or Dispatcher, the credential must be maintained through continuous education and training.[75] Additionally, each Regional Transmission Organization (RTO) requires certification of Operators and Dispatchers for both Transmission facilities and

---

72 Abrenio, *supra* note 69.

73 *System Operator Certification*, North American Reliability Corp., http://www.nerc.com/ pa/Train/SysOpCert/Pages/default.aspx (last visited Feb 8, 2017).

74 *Id.*

75 *Id.*

Generation facilities.[76] Because of this disciplined approach, Operators and Dispatchers are equipped with the basic knowledge required to perform their roles.

IT System Administrators are professionals within the computing industry responsible for maintenance and administration of cyber assets, which support the BES. In contrast to the credential requirements of the Operations staff, the IT Operations staff have no NERC or RTO sponsored certifications.[77] Even those requirements articulated in CIP-004 have no formal curriculum allowing regulated utilities to develop their own individual training which can take the form of anything from an email, reading course handouts, live classes, or navigating through a multi-media online seminar.[78] Testing of the curriculum is also optional.[79]

There are computer and security industry certifications such as the CISSP and GIAC, which regulated entities can require of their IT System Administrators but are not required by NERC.[80] It seems to be an oversight to require NERC and RTO regulated credentials for the System Operators and Dispatchers to protect critical assets, but to have no such requirements for the IT System Administrators who have system-level access to critical cyber assets which support, manage, or monitor those same critical assets.

While System Operators and Dispatchers have expertise in BES, and IT System Administrators have expertise in computers, applications, and routing protocols, the esoteric nature of individual SCADA systems leave both groups sometimes wholly dependent upon the SCADA vendor for expertise. In daily operations, this is not an issue, since most SCADA vendors provide excellent support and responsive service.

---

76 *Id.*

77 *CIP-004-6 Cyber Security: Personnel & Training*, North American Reliabilty Corp., http://www.nerc. com/pa/Stand/Prjct2014XXCrtclInfraPrtctnVr5Rvns/CIP-004-6_CLEAN_06022014.pdf, (last visited Feb. 8, 2017).

78 *Id.*

79 *Id.*

80 *Id.*

However, vendors are not always included in all projects within the ESP. This exclusion can sometimes lead to unintended disruption.

Vendors have become a popular attack vector for intrusions in many industries, and SCADA vendors—given their requirement for remote access into systems within the ESP to provide support—are an attractive target of malicious actors. Unfortunately, the security practices claimed by a SCADA vendor are typically not verified by their utility customers beyond what they need to satisfy CIP-004 for personnel risk assessments. While NERC CIP is indeed on the forefront of compliance requirements which make sense, it falls far short of the Federal Financial Institutions Examination Council's (FFIEC) requirements for examinations of Technology Service Providers (TSP). Because NERC does not require it, it is left up to each regulated entity to decide how much due diligence it will perform, and at what intervals to ensure they are not put at risk by allowing remote interactive access into the ESP by the SCADA vendor.

I. Conducting Assessments

Vulnerability Assessments (VAs) required by NERC CIP-010 R3.1 is not necessarily the security industry's definition of a vulnerability assessment. "Active" VAs in CIP-010 R3.2 and R3.3 adhere more to the security industry definition. Per Reliability First, a Regional Entity with delegated enforcement authority from NERC, the minimum requirements for a vulnerability assessment are:

- Network and access point discovery;
- Port and service identification;
- Review of default accounts, passwords, and network management community strings; and
- Wireless access point review.[81]

81 Rhonda Bramer, Frank Kapuscinski, & Scott Pelfrey, *CIP-010 CIP V5 Worksh*op, Reliability First, https://rfirst.org/compliance/Documents/RF%20CIPv5%20Workshop%20CIP-010.pdf (last visited Dec. 27, 2016).

In the "Guidelines and Technical Basis" section of CIP-010 for Requirement R3, these minimum requirements are further explained:[82]

Paper Vulnerability Assessment:

1. Network Discovery: A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification: A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review: A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review: Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery: Use of active discovery tools to discover active devices and identify communication paths to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification: Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning: Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning: Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within range of the wireless scanning tool.

One should note, there are no mention of authentication certificates, public/private keys, or shared secret keys. As best practice, consider taking inventory of these authentication types in use, and incorporate them into your password management program and processes. To prevent Protected Cyber Assets ("PCAs") from becoming Electronic Access Control or Monitoring Systems ("EACMS"), limit use of authentication certificates from PCAs to other BES cyber assets, as this would indicate the PCA controls access

82 Configuration, *supra* note 51.

to the remote BES cyber asset it is connecting to, and could arguably be considered an EACMS with all the accompanying requirements.

Another best practice is during the vulnerability scanning, and network port and service identification phases of active vulnerability assessments, to confirm validity of the information documented for each cyber asset for CIP-007R2.3 and CIP-010R1.1. Much of this information can be used as evidence to satisfy related requirements. Unless the BES Cyber Assets are highly unstable, it is recommended to perform the active vulnerability assessments whenever possible. The process is generally more streamlined, with standard output, and as seen above, much more comprehensive to support a secure computing environment.

i. Addressing Legal Liability

Given the fact that the application of cyber security standards to the grid is a relatively new development, there is little case law directly on point that deals with utility company liability in cases where the NERC CIP standards were not fully adhered to when a breach or outage occurred. The Federal District Court in *Waldon v. Ariz. Pub. Svc. Co*. held that non-utility customers lacked standing to initiate a case, and specifically held that while NERC standards created a duty between the government and utility suppliers, no similar duty was created with utility customers.[83] According to the American Public Power Association (APPA), negligence claims arising from a failure to prevent against cyber-attacks could expose electric utilities to liability.[84] Furthermore, APPA asserts that while states have considered legislation that would limit utilities' liabil

83 642 F. App'x 667, 669 (9th Cir. 2016).

84 *In Support of Appropriate Liability Protection for Electric Utilities Related to Cyber Attacks*, Am. Pub. Power Ass'n (June 17, 2014), https://www.publicpower.org/files/PDFs/Resolution%2014-08%20--%20Liability%20Protection%20for%20Utilities%20Related%20to%20Cyber%20Attacks%20--%20FINAL.pdf.

ity for cyber-attacks, there are currently no federal or state statutes in place that provide immunity from liability merely for adhering to cyber security standards.[85]

However, there are several cases in which enforcement actions were taken, penalties were assessed, and remediation procedures and processes were recommended. Of course, by their very nature, these violations occur within critical infrastructure. Consequently, some portions or identifying characteristics are removed from the public versions of these orders and stipulations.

For instance, in one case where an entity had failed to comply with portions of CIP-002-3, CIP-005-3s, CIP-006-3c, and CIP-007-3a the Unidentified Registered Entity (URE) was assessed a penalty of $250,000.[86] In another case, a URE was determined to have violated 19 CIP standards, with the root cause being the URE's failure to create and utilize a comprehensive change management plan which resulted in a lack of independent inspections of new substations to identify Critical Cyber Assets (CCAs), EACMs, and Physical Access Control Systems (PACS).[87] In this case, the URE was assessed a penalty of $1,125,000 as the nature of the risk was deemed to be serious.[88]

While there are potential FERC penalties that may be enforced with respect to liability due to outages, it is difficult to litigate against a utility, as a claimant would have to establish a basis for negligence. When dealing with risk of harm or loss of life, the

---

85 *Id.*

86 *NERC Full Notice of Penalty regarding Unidentified Registered Entity*, North American Electric Reliability Corp. (Oct. 31, 2016), http://www.nerc.com/pa/comp/CE/Enforcement%20Actions% 20DL/Public_FinalFiled _NOP_NOC-2492.pdf (In this case, all of these violations were noted during a self-reporting and self-certification process which the URE undertook. In each case the potential risk was deemed as moderate.).

87 *NERC Full Notice of Penalty regarding Unidentified Registered Entity*, North American Electric Reliability Corp. (Oct. 31, 2016), http://www.nerc.com/pa/comp/CE/Enforcement%20Actions% 20DL/Public_FinalFiled_NOP_NOC-2450.pdf.

88 *Id.* (Note: while the opinion referenced CCAs, in CIP V5 this terminology was updated to reflect BES Cyber Asset. The use of the term CCA was included merely because that was the exact verbiage utilized within the FERC opinion.).

calculus results in a lower burden for the claimant (essentially when the claim involves risk of harm or actual harm/death the claimant's case is more straightforward, and more likely to survive a dismissal motion in a pre-discovery context). For a cause of action to survive a motion for dismissal, the plaintiff must demonstrate standing to sue which requires actual injury.[89]

Therefore, even though it would be a difficult task for an end-user, consumer, or business customer of a utility to demonstrate standing, there are multiple instances of penalties, fines, and process modifications imposed by FERC on entities that violate the NERC CIP policies. Even where the names and details remain confidential, the impact on the entity through ongoing monitoring and compliance checks in addition to any financial penalties should give pause to investors considering their options within this industry. Furthermore, were an entity to be sanctioned by FERC, that sanction could also be used against them should a case or controversy arise and should standing be properly asserted.

There are two basic tests to prove standing, the first is a Constitutional test which requires the following: (1) the plaintiff must allege that they have suffered or imminently will suffer an injury; (2) the plaintiff must allege that the injury is fairly traceable to the defendant's conduct; (3) the plaintiff must allege that a favorable decision by the court would redress the injury.[90] The second basic test is referred to as the "prudential" test and states: (1) a party may only assert their own rights and not the rights of others; (2) a plaintiff may not sue merely as a class of taxpayers asserting the rights of the entire class; (3) a claim may only be raised if it is within the zone of interests protected by the statute in question.[91] Finally, it is possible to assert associational standing, whereby an association may show standing to sue on behalf of its members.[92] This too, imposes a three-part test: (1) the

89 *Supra* note 83.

90 Ne. Fla. Contractors v. Jacksonville, 508 U.S. 656, 663-64 (1993).

91 Lujan v. Defs. of Wildlife, 504 U.S. 555, 576-78 (1992).

92 Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 343 (1977).

members must otherwise have standing to use on their own; (2) the interests being sought are germane to the organization's purpose; and (3) neither the claim asserted nor the relief requested requires the participation in the lawsuit of the individual members.[93]

It is easy to see how difficult it would be to sue an entity for a power outage or a voltage line fluctuation that arose as the result of a cyber-incident. Therefore, it is far more likely that an entity would face sanctions from the FERC than redress from a court of law. However, under NERC CIP 008, the responsible entity must develop and maintain a cyber security incident response plan and must have processes and procedures in place to identify, classify, and respond to cyber security incidents.[94] Within the classification, a responsible entity must determine whether an event is either reportable or non-reportable. In the case of reportable events, the ES-ISAC must be notified within one hour of the cyber event.[95]

ii. Risk Transference

It has often been said that no one wants to pay for insurance when things are going well but as soon as things go awry everyone wishes they had insurance. The world of cyber security is no different with major data breaches hitting the headlines. The costs of downtime to utilities both in a purely economic sense in addition to the potential for loss of life, is a very real concern. While we would argue that cyber security insurance is a "should have" for any utility, for the BST entities with no other option, cyber security insurance is a "must-have."

In addition to understanding cyber security issues and taking steps to address them, utilities should prepare for a cyber security incident by procuring insurance

---

93 *Id.*

94 *CIP-008-5 Cyber Security: Incident Reporting and Response Planning*, North American Electric Reliability Corp. (July 9, 2014), http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-008-5&title=Cyber%20Security%20-%20Incident%20Reporting%20and%20Response%20Planning&jurisdiction=null.

95 *Id.* (One hour refers to a preliminary notification which is often informal (online, via phone) and submitted within one hour of determining that a reportable cyber event occurred.).

policies to attain coverage for anticipated events. Utilities need to take a best practices approach when evaluating a cyber security policy and managing compliance overall.

With respect to insurance policies, it is important to note the two main types of policies: (1) first-party policies—which cover losses directly incurred by the policyholder and (2) third-party policies—which cover a policyholder's liability to third-parties.[96] Under the first-party policy, a grid utility could have coverage that would include unplanned shutdowns or outages as such might occur in a cyber-attack.[97] Typically the deductibles for such a policy would be expressed in terms of time (e.g. insurer pays in excess of D days; or H hours, etc.). However, most insurance policies require physical damage so in the case of a cyber-attack that causes operational issues with the Smart Grid, it may prove difficult to establish that actual physical damage occurred and thus the insurer may not be required to compensate. Thus, policyholders must carefully review their policies to ensure that software and device issues are not excluded. Otherwise a pure cyber-attack with no kinetic component could result in huge losses to a utility which would not be covered under their insurance policy. The same could happen with respect to third-party coverage. Given the fact that an attack on the grid could potentially result in physical damage to persons, grid entities must review their policies to verify that they have either general commercial or cyber coverage that includes both physical and non-physical losses.[98] Otherwise, they could expose themselves to significant risk if they fail to account for both potential types of loss.

---

96 Erin L. Webb, *The Internet of Things: Cybersecurity, Insurance, and the National Power Grid*, 30 Nat. Resources & Env't 35 (2016).

97 *Id.*

98 *Id.*

Conclusion

We live in a connected world where critical infrastructure in general and the power grid specifically play vital roles. Without a consistent and reliable supply of electrical power throughout North America, nearly every aspect of everyday life would be negatively impacted. In the event of a long-term outage (more than a couple of days) that covers a wide area, the economic impacts would be staggering. Were such an outage to occur during either cold or heat temperature extremes, the loss of life could number in the tens or hundreds of thousands. These are very real and very dire implications that will arise should the power grid suffer an outage.

This paper discussed some of the implications of a power outage and looked directly at the cyber security implications for the grid utilities. Furthermore, it outlined how utilities can bolster their cyber security and mitigate some of the risks that they face. No one would deny the importance of the power grid within a critical infrastructure paradigm. Following the widespread media coverage of high profile cyber-incidents (the Sony Hack, the Stuxnet Virus, the OPM data breach) no one is denying the fact that cyber-attacks are occurring all around us. Consequently, security through obscurity is a fools' errand. Grid utility companies must face the reality within which they now operate; cyber-attacks are ongoing, and any industry within the critical infrastructure framework is going to be an attractive target for a myriad of reasons.

As we outlined, following the NERC CIP guidelines is a very good first step towards addressing cyber security needs and issues. However, that in and of itself is not enough. Grid utility companies must embrace the stark new reality and consider the implications of everything they do within all the areas in which they operate. The costs of baking-in cyber security in a technical sense to their ICS and SCADA systems must be balanced against the potential costs that a widespread outage could inflict both financial loss as and legal liability.

Grid utility companies must move towards greater cyber security hygiene. This includes both technical and non-technical issues facing the grid as well as the human element which is often the weakest-link in any cybersecurity initiative. The cost of doing nothing is too great. In an uncertain legal world, mere compliance with NERC CIP guidelines may also be insufficient to avoid legal liability. Therefore, companies should take a proactive approach to ensure that cyber security is not an afterthought or a check-mark on a framework. Cyber security must be an integral part of each and every project, and considered within every aspect of the grid utility operations

Transactions Costs, the Dark Web, and Drug Trafficking: From Corner to Computer

Marc Barnett

Introduction

The rise of technology has a transformative power for a variety of social and market issues, revolutionizing prior norms and behavior. Just as technological change altered market mechanisms for licit markets, technology, similarly, alters mechanisms for illicit markets. In regards to these illicit markets, technology galvanized drastic change in the drug market particularly for a variety of reasons. Most notably, technology lowered transaction costs significantly, allowing market participants to feel secure in their economic property rights on the online marketplace. In contrast, the transaction costs to traditional market engagement—that is, in person—stayed relatively stagnant. This incentivized certain market participants with the proper technological infrastructure and know-how to opt out of the traditional drug market and participate in the online marketplace for drugs. The development and proliferation of the Tor browser and Bitcoins represent the major technological developments that spurred the transition of one specific market segment to the online market. Solidarity, reputation, and shared philosophy that developed between buyers and sellers on sites, particularly Silkroad, further encouraged the shift.

This paper seeks to firstly elucidate and elaborate the shift of drug market participants to online marketplaces, providing sufficient background to place the issue into context. Next, the paper highlights three factors that sufficiently lowered transaction costs to spur migration from the traditional market to a new market. Technological development played a role in two of the three factors, in order to shift market participants, while the third factor is a social mechanism. In the fourth section of the paper, I consider several potential solutions developed by law enforcement and the private sector to drive

participants out of the online drug market by threatening anonymity. Finally, the paper offers a feasibility analysis of the proposed solutions, ending with a brief projection on the future of online drug markets.

I. A Rising Problem: Trends in the Drug Trade

According to the World Drug Report, drug consumption trends around the world have been increasing, coupled with changing drug consumption patterns and behaviors.[1] The report as well as other experts in law enforcement and customs at a conference this summer in Strasbourg frequently point to the dark web as a major catalyst for not only the increase, but also changing consumption patterns.[2] The dark web acts as a connector and facilitator for the globalization of drugs, increasing availability of drugs formerly considered regional.[3] Furthermore, the seeming consequence-free purchasing of drugs online widens the market and makes it more likely that these "irregular" market participants become "regular" participants.[4] Finally, the rise of online markets on the dark web shifted production, particularly of "made" drugs, such as ecstasy, LSD, and methamphetamine away from traditional manufacturing locations (Netherlands, Bulgaria) into Southeast Asia, as the dark web allows producers to bridge physical locations between production and consumption.[5]

---

1 *See* Barbara Tasch, *The Darknet Might be Changing Drug Smuggling Routes*, Bus. Insider (June 26, 2015, 11:53 AM), http://www.businessinsider.com/the-dark-net-might-be-changing-drug-smuggling routes-2015-6?IR=T.

2 *Id.*

3 *See Shedding Light on the Dark Web*, Economist (July 16, 2016), http://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete.

4 *See* Andy Greenberg, *A Heroin Dealer Tells the Silk Road Jury What it was Like to Sell Drugs Online*, Wired (Jan. 28, 2015, 7:06 PM), https://www.wired.com/2015/01/silk-road-heroin-dealer-testifies/.

5 *Combating Illicit Trafficking in Drugs: 30th Annual Meeting of the Airports Group*, Council of Eur. (June 19, 2015).

Silkroad represents the first and most enduring example of online drug bazaars on the dark web, marketing themselves as the "Amazon" of drugs.[6] Started in 2011 by Ross Ulbricht, username the "Dread Pirate Roberts" from the cult hit "The Princess Bride," the FBI arrested Ulbricht and seized the dark web site in 2013.[7] Authorities estimate that in the two years that Silkroad operated, the site sold over 200 million dollars of merchandise, mostly illicit drugs.[8] Though the FBI seized the site and arrested founder, Ross Ulbricht, similar sites appeared and proliferated, including Silkroad 2.0, Agora, and Evolution.[9] The rise of these online sites allow non-traditional market participants, professionals who dose recreationally, to participate in the drug market with low threat of violence and access to a much higher quality of drug.[10] The major fear of law enforcement and drug trafficking experts centers on dark web sites, not replacing traditional markets, but, rather, augmenting these markets by attracting non-traditional, infrequent users that over time transition into frequent users. In regards to this niche market, technology sufficiently lowered transaction costs to allow these non-traditional participants to fully participate regardless of location or prior connections.[11]

---

6 Nina Burleigh, *The Rise and Fall of Silk Road, the Dark Web's Amazon*, Newsweek (Feb. 19, 2015, 6:52 AM), http://www.newsweek.com/2015/02/27/silk-road-hell-307732.html.

7 *Id.*; Nina Burleigh, *Key Moments in the Life of Silk Road Creator Ross Ulbricht*, Newsweek (Feb. 19, 2015, 6:50 AM), http://www.newsweek.com/key-moments-life-silk-road-creator-ross-ulbricht-307815; Joshua
Brustein, *Silk Road's Dread Pirate Roberts vs. The Princess Bride's*, Bloomberg (Oct. 3, 2013, 1:45 PM), https://www.bloomberg.com/news/articles/2013-10-03/silk-roads-dread-pirate-roberts-vs-dot-the princess- brides.

8 David Kushner, *The Darknet: Is the Government Destroying 'The Wild West of the Internet'?*, Newsweek
(Nov. 8, 2015, 3:03 PM), http://www.newsweek.com/darknet-government-destroying-wild-west-internet-391511.

9 Cyrus Farivar, *After Silk Road Takedowns, Dark Web Drug Sites Still Thriving*, ARSTechnica (Dec. 19, 2014, 9:10 AM), https://arstechnica.com/business/2014/12/after-two-silk-road-takedowns-dark-web-drug-sites-still-thriving/.

10 Steven Nelson, *Silk Road's Vision Still Thrives*, U.S. News & World Report (Feb. 5, 2015, 5:05 PM), http://www.usnews.com/news/articles/2015/02/05/silk-roads-vision-thrives-in-deep-web.

11 Marie Claire Van Hout & Tim Bingham, '*Surfing the Silk Road*': *A Study of Users' Experiences*, Int'l J. of Drug Pol'y, 526 (2013), https://www.gwern.net/docs/sr/2013-van-hout-2.pdf.

II. Lowered Transaction Costs

A. Tor

Anonymity on the online drug market facilitated by two contemporary technologies immensely lowered the transaction costs, causing a specific portion of the traditional market to enter the online marketplace. First and foremost, the creation, evolution, and dissemination of the Tor browser represents the most significant technological development. The U.S. Naval Research Laboratory created the Tor (The Onion Router) browser in the 1990's in order to protect important information, including the identity of agents in the field.[12] The browser encrypts information end-to-end, while routing through a series of "volunteer servers" that hide the original IP address through layers, allowing anonymity as well as secrecy.[13] The Tor browser, anonymous and secret, facilitates multiple users for a variety of different reasons in several different spheres, some licit and some illicit. [14]

Online drug marketplaces, such as Silkroad, exploit the anonymity of Tor utilizing its "hidden service" features.[15] These marketplaces compose part of the infamous dark web, a portion of the web that can only be reached through the anonymizing features of Tor and have specific, non-searchable, web addresses, ending in .onion.[16] The end-to-end encryption on these sites protect the administrators, vendors, and buyers from law enforcement.[17] The encryption features of Tor have proven incredibly difficult

12 L. Christopher Skufca, *The Pros and Cons of Using Tor*, Camden Civ. Rts. Project (Jan. 8, 2016), https://camdencivilrightsproject.com/2016/01/08/the-pros-and-cons-of-using-tor/.

13 Joe Uchill, *Servers of Anonymous Browsing Network Tor Designed to Hack Sites*, Hill (July 6, 2016, 12:00 PM EDT), http://thehill.com/policy/cybersecurity/286656-many-servers-of-anonymous-browsing-network-tor-designed-to-hack-sites.

14 *See* Danny Bradbury, *Unveiling the Dark Web*, Network Sec., Apr. 2014, at 14.

15 *Create Hidden Service in Tor like Silk Road or Darknet*, Blackmoreops.com (Aug. 19, 2015), https://www.blackmoreops.com/2015/08/19/create-hidden-service-in-tor-like-silk-road-or-darknet/.

16 Bradbury, *supra* note 14, at 14.

17 *Id.* at 15.

for law enforcement to penetrate.[18] Most success against cybercriminals and cyber-traffickers, such as Operation Onymous, exposed and arrested culprits on the dark web resulted from human error rather than a technological breakthrough by even the most sophisticated agencies (FBI, NSA, Europol).[19] This provides users with incredible assurance as to the safety of the technology, if not necessarily the site administrators. With the security of Tor consistently reported and validated in the media, buyers and sellers feel secure and protected in their anonymity and secrecy while operating online.[20] This security helps to delineate economic property rights from government interference, intervention, and seizure. The Tor browser, ensuring safety from a technological standpoint, lowers transaction costs of operating online.[21] The two remaining factors to be considered, crypto-currency and reputation, will further lower the transaction costs of shifting to online drug marketplaces, allowing a sector of the traditional drug market to successfully change markets.

B. Crypto-Currencies

Crypto-currency is a technical term for a type of currency that preserves anonymity online.[22] Crypto-currency is different from virtual, or e-currency, in two main respects. Unlike e-currency, crypto-currencies preserve anonymity and have value in the real world, i.e., they have an exchange rate.[23] Bitcoin is the most famous of these

---

18 Sarah Volpenhein, *Dark Web Poses Challenges for Law Enforcement*, Gov't Tech. (Aug. 10,2015), http://www.govtech.com/internet/Dark-Web-Poses-Challenges-for-Law-Enforcement.html.

19 *See* Cath Everett, *Should the Dark Web be Taken Out?*, Network Sec., Mar. 2015, at 12.

20 *See* Steven Nelson, *Buying Drugs Online Remains Easy, 2 Years After FBI Killed Silk Road*, U.S. New (Oct. 2, 2015, 3:12 PM), http://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road.

21 Cara Bloom, *Silk Road: Anonymous Deep Web Marketplace*, Apr. 2013, at 5, http://www.carabloom.com/papers/silkroad.pdf.

22 Joshua Davis, *The Crypto-Currency*, New Yorker (Oct. 10, 2011), http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency.

23 Carter Graydon, *What is Cryptocurrency?*, Cryptocoin News (Sept. 16, 2014), https://www.cryptocoinsnews.com/cryptocurrency/.

crypto-currencies, and the one utilized by the infamous Silkroad; however, other crypto-currencies, such as the recently defunct Liberty Reserve, exist and can be utilized on both traditional web and the dark web sites for illicit or licit purposes.[24] The foundation of Bitcoin resembles Tor in that Bitcoin was developed to preserve anonymity in the general sense, not necessarily for neither "bad" agents to exploit.[25] Online drug markets utilize these anonymous crypto-currencies to facilitate a feeling of ease and security, incentivizing use and lowering transactions costs by increasing security. [26]

C. Social Factors

A variety of additional reasons further galvanized movement to dark web online drug marketplaces. The escrow system, made popular by Ross Ulbricht on the original Silkroad, minimizes risk for buyers who may be otherwise cheated by the vendor.[27] Based on the Silkroad model, similar sites now hold money from buyers while the buyers wait for their drugs to arrive in the mail.[28] Once the drug arrives, the empowered buyer finalizes the transaction and the vendor receives payment (after the website takes commission).[29] Several online drug markets also include a complaint mechanism arbitrated by site administrators.[30] The online safeguards couple with the reputation of ven

---

24 *See* Jake Halpern, *Bank of the Underworld*, Atlantic (May 2015), https://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/.

25 *See* Justin Brecese, *Money from Nothing: The Socioeconomic Implications of "Cyber-Currencies"*, ASA Instit. For Risk & Innovation, 2013, at 2-3, http://anniesearle.com/web-services/Documents/ResearchNotes/ASA_Research_Note_MoneyFromNothing-TheSocioeconomicImplicationsofCyber-currencies_August2013.pdf.

26 *See* Bloom, *supra* note 21, at 2.

27 *Id.* at 5-6. *See also* Chris McCandless, *Scam Prevention and Finalizing Early*, Deep Dot Web (Oct. 30, 2015), https://www.deepdotweb.com/2015/10/30/scam-prevention-and-finalizing-early/.

28 *See, e.g.*, *Silk Road and the Other Dark Web Markets*, Silk Road Drugs, https://silkroaddrugs.org/silk-road-and-the-other-dark-web-markets/.

29 McCandless, *supra* note 27.

30 Bloom, *supra* note 21, at 8-11.

dors to further overcome and solve the problem of trust.[31] Similar to eBay or Amazon, buyers review and leave feedback under the seller's profile, providing a percentage of "satisfied customers."[32] Additionally, as with Reddit, buyers, sellers, and administrators have "Karma," which can be positive or negative to further instill confidence in buyers and lower transaction costs.[33] Finally, both buyers and sellers must trust the administrators of the site, as the site administrators could steal the money in escrow anonymously and then shut down the site.[34] Market participants must also trust the security apparatus provided by the administrators of the site, and if this trust does not exist, participants will be hesitant to join the market exchange. Libertarian philosophy, propagated by site administrators and shared by a majority of buyers and sellers, helps to bind the marketplace together through trust.[35] This shared mindset of a majority of participants and stakeholders in the market alleviate risks inherent to an anonymous market, and creates a sense of community on the site with shared norms, rules, and procedures. The creation of these formal and informal norms and rules drastically lower transaction costs and allow market exchanges to take place. [36]

D. Necessary and Sufficient

When considered together, these three factors lower transaction costs sufficiently to allow market participation. Lower transaction costs on online drug platforms signify a better definition of property rights and more complete and more accessible in-

---

31 *Id.* at 8-9. *See also the Amazons of the Dark Net*, Economist (Nov. 1, 2014), http://www.economist.com/news/international/21629417-business-thriving-anonymous-internet-despite-efforts-law-enforcers.

32 Bloom, *supra* note 21, at 9.

33 *Id.* at 12.

34 Rita Zajácz, *Silk Road: The Market Beyond the Reach of the State*, Info. Soc'y, Feb. 2017, at 27. *See also* Carrie Kirby, *Scams, Hacks and Poor Management: Life After Silk Road*, CoinDesk (Apr. 27, 2014, 13:11 GMT), http://www.coindesk.com/scams-hacks-poor-management-life-silk-road/.

35 *See* Zajácz, *supra* note 34, at 25-26.

36 *See* Hout & Bingham, *supra* note 11, at 528.

formation that together limit cheating.[37] The establishment and delineation of economic property rights in the case of an illicit market represent the utmost importance due to the fact that legal property rights do not exist.[38] Whereas Tor and Bitcoin lower transaction costs of entering an illegal market in terms of protection from authorities, these factors also facilitate cheating within the marketplace. Cheating within the market by the vendor can take two forms: delivery of a subpar product or failure to deliver any product at all.[39] The typical set-up of the online marketplace designs "contracts" to be paid by the weight of the drug in grams, meaning that the quality of the drug will be "relinquished to the public domain."[40] However, the reputation of the vendor, assuming a repeated game, acts to limit the extent that the quality of the drug is relinquished to the public domain. Secondly, the escrow system solves the delineation of property rights dilemma by acting as an intermediary while the transaction occurs, verifying that the buyer received the order before delivering the funds to the seller.[41]

However, just as technological advances help to protect property rights from the state, the technology represents a prohibitively costly barrier for some desiring to enter the market.[42] The technological expertise required to participate in the online drug marketplace prohibits entrance save only for a select few. In order to enter the market, a potential buyer must have access to a computer, have a bank account, sufficient monetary

---

37 Douglas W. Allen, Economic Principles: Seven Ideas for Thinking ... About Almost Anything (4th ed. 2011).

38 Yoram Barzel, Economic Analysis of Property Rights (1997).

39 *See* James Martin, *Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket'*, Criminology & Crim. Just., 2014, at 359, http://journals.sagepub.com/doi/pdf/10.1177/1748895813505234.

40 *Id.*

41 Allen, *supra* note 37.

42 *See How Can You Buy Illegal Drugs Online?*, Economist (Aug. 25, 2013), http://www.economist.com/blogs/economist-explains/2013/08/economist-explains-11; Silk Road for Dummies, http://silkroadfordummies.blogspot.com/ (last visited Feb. 8, 2017) [hereinafter Silk Road].

means, and technical expertise.[43] The bank account and accompanying expertise to obtain Bitcoins, or another crypto-currency, highlights the most restrictive and selective conditions.[44] Secondly, the technical expertise to download and properly exploit the Tor browser for the purchase of drugs sufficiently limits potential participants as well. [45] Though the computer clause may also seem, at first glance, sufficiently prohibitive, public libraries and internet cafés provide access to a larger portion of potential buyers. However, those in extreme and concentrated poverty may still not have proper access to either a public library or an internet café. The market barriers underline why the online drug market has only attracted a "niche" sector of the traditional drug market, though as knowledge of Bitcoin and Tor continue to proliferate the participants may increase in the future. [46]

III. Lessons Learned: Possible Solutions

Law enforcement agencies have enjoyed several prominent successes battling these online drug markets, most notably Silkroad, Silkroad 2.0, and Agora.[47] Government agencies, such as the FBI and the NSA, devote more and more resources to tackling and taming the dark web, especially as terrorist groups, such as ISIS and Al Qaeda, exploit the anonymity offered by the Tor browser.[48] International cooperation, such as

---

43 Silk Road, *supra* note 42.

44 Brecese, *supra* note 25.

45 *See* Hout & Bingham, *supra* note 11, at 526.

46 *Id.* at 528.

47 *See* Jeff Stone, *Silk Road's Demise Spawns Agora, A Popular New Online Drug Marketplace*, Int'l Bus. Times (Sept. 10, 2014, 2:24 PM), http://www.ibtimes.com/silk-roads-demise-spawns-agora-popular-new-online-drug-marketplace-1684550; Andy Greenberg, *Agora, the Dark Web's Biggest Drug Market, is Going Offline*, Wired (Aug. 26, 2015, 11:45 AM), https://www.wired.com/2015/08/agora-dark-webs-biggest-drug-market-going-offline/.

48 *See, e.g.*, Natasha Bertrand, *ISIS is Taking Full Advantage of the Darkest Corners of the Internet*, Bus. Insider (July 11, 2015, 11:26 AM), http://www.businessinsider.com/isis-is-using-the-dark-web-2015-7; Barton Gellman, Craig Timberg & Steven Rich, *Secret NSA documents show campaign against Tor encrypted network*, Wash. Post (Oct. 4, 2013), https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html?utm_term=.1e5c3881f976.

Operation Shrouded Horizon and Operation Onymous, spurred further success against major drug trafficking sites on the dark web, arresting dozen of suspects and seizing various sites.[49] As criminals continue to perverse and distort the original purpose of The Onion Router, incentives for government agencies and private software companies to break Tor's security system and de-anonymize the dark web persist and increase. [50]

Private software security companies, most notably Hacking Team, develop and market software designed to exploit vulnerabilities in the Tor network in order to reveal user identities as well as server locations.[51] Leaked communications from the Milan based Hacking Team show an FBI official inquiring about the effectiveness of the firm's software and tools in fighting anonymity granted by the Tor browser.[52] In addition to Hacking Team, Defense Advanced Research Project Agency ("DARPA") has also made strides in fighting dark web criminals.[53] DARPA created Memex, a dark web search engine able to crawl these "anonymous sites," which led to success against ISIS recruiting sites in the dark web, as well as against human trafficking sites and online drug marketplaces.[54] Agora, one of the largest drug marketplaces after the Silkroad 2.0 seizure, recently shut down due to security concerns, centering on de-anonymizing attacks by

---

49 Andy Greenberg, *Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains*, WIRED (Nov. 11, 2014, 6:00 AM), https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/; *Alastair Stevenson, These are the 3 scariest alleged Darkode hackers arrested during the FBI's 'Operation Shrouded Horizon'*, BUS. INSIDER (July 16, 2015, 10:20 AM), http://www.businessinsider.com/darkode-suspects-include-an-ex-fireeye-intern-and-alleged-botnet-masters-2015-7.

50 Kushner, *supra* note 8.

51 Jeff Stone, *Hacking Team Tried to Break Tor Anonymity Network; Spy Company Joins Tor's Long List of Enemies*, INT'L BUS. TIMES (July 13, 2015, 2:39 PM), http://www.ibtimes.com/hacking-team-tried-break-tor-anonymity-network-spy-company-joins-tors-long-list-2006135.

52 Kushner, *supra* note 8.

53 JC Torres, *DARPA's "Dark Web" Revealing Memex Tool is also Pretty Scary*, SLASH GEAR (Feb. 17, 2015), https://www.slashgear.com/darpas-dark-web-revealing-memex-tool-is-also-pretty-scary-17369396/.

54 *See* Pierluigi Paganini, *The ISIS Advances in the DeepWeb Among Bitcoin and Darknets*, SEC. AFFAIRS (May 22, 2015), http://securityaffairs.co/wordpress/36961/intelligence/isis-in-the-deepweb.html.

the U.S. government against the site.[55] Recent successes by law enforcement agencies blunted potential growth on dark web drug marketplaces. However, steady migration to these sites from the traditional drug market occurred despite these successes.

IV. The Dark Web: Enduring Drug Bazaar

Despite major operational successes and so-called "breakthroughs" by law enforcement agencies tackling dark web traffickers, sustained and comprehensive success seems unlikely. Operational successes, such as Operation Onymous and Operation Shrouded Horizon, reflect traditional police work, rather than technical breakthroughs necessary to systemically fight the dark web.[56] The inter-agency operation that seized the original Silkroad site and arrested founder Ross Ulbricht mobilized teams of agents and lasted over a year.[57] Subsequent operations involved numerous agencies and agents, relying on a complex, intertwined mix of traditional policing techniques coupled with innovative cyber approaches. Claims of success by private software firms exhibit a marketing ploy rather than the truth, and the dark web search engine, Memex, developed by DARPA, can only crawl through sites that are not behind a "paywall," or password protected, limiting the overall utility of such a tool. The race to de-anonymize the dark web continues, regardless of prior claims.

In light of the limited success of law enforcement agencies fighting the dark web, a newer and more decentralized drug marketplace developed and the decentralized nature of the marketplace further ties the hands of law enforcement with limited resources. After the government seizures of three prominent dark web marketplaces (Silkroad and Silkroad 2.0, Agora), several other sites collectively filled the market gap.[58] Without a

---

55 Kushner, *supra* note 8.

56 *See Global Action Against Dark Markets on Tor Network*, Europol (Nov. 7, 2014), https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network.

57 Burleigh, *supra* note 6.

58 Nelson, *supra* note 10.

major site controlling the majority of the traffic, law enforcement resources must diffuse to a greater range, effectively limiting future success. As most of the sites utilize the traditional Silkroad template, the seizure of one site by law enforcement does not drastically alter the aggregate market as buyers shift to a familiar site with similar rules and norms. Recent law enforcement efforts have certainly threatened the security, and therefore raised transaction costs, of the administrators. However, the net effect for buyers and sellers has been limited, as their security has remained stagnant without a major technological breakthrough exploiting the core aspects of the Tor browser. Therefore, the "cat and mouse" game between market participants and law enforcement remains relatively stable as the basic "balance of power" remains with the buyers and sellers.[59] The current development of a decentralized model on dark web marketplaces signifies a more sustainable model than unipolar system exemplified by the once-dominant Silkroad, and further migration from traditional drug markets to online marketplaces will continue as further technical expertise proliferates around the world.[60]

Conclusion

Law enforcement and government agencies exhaustively work towards decoding and de-anonymizing the dark web, while the same technology proliferates to more and potential market participants. The "cat and mouse" game will continue into the future as traditional drug market participants incrementally migrate to the online marketplace. The lack of one major site, such as Silkroad, makes the overall drug marketplace more sustainable, as there are several redundancies built into the system if law enforcement seizes one site. Without a major technological breakthrough against Tor or Bitcoin by law enforcement, drug trafficking on the dark web will endure. Market participants feel secure and protected by the technology, Tor and Bitcoin, and the marketplace site

59 Kushner, supra note 8.

60 Nelson, supra note 10.

design delineates property rights adequately for sufficiently low transaction costs. Taken together, the technology and site design allow entrance into the market place by a niche, technologically savvy, market sector. The phenomenon of dark web drug trafficking will persist for the immediate future despite the best intentions of law enforcement, but as political will increases to tame the dark web, the long-term survival of the phenomenon may be in doubt.

Cybersecurity and the Protection of the PII: A Survey of Issues That Will Impact CIOs

Andrew Foote

Overview

We live and work in a global community that has only been dreamt of by past generations. Although this dream can be a benefit, it can also be a hindrance to society. In particular, the use of the Internet and cloud computing has posed some interesting challenges for policy makers and businesses. The primary issue is that of safeguarding privacy. Taking a closer look, privacy has many aspects. The first is safeguarding an individual's right and expectation to privacy. The second is safeguarding an institution's privacy. Finally, there is the level of privacy that is expected by the force of custom in our society.

For years, cyber experts knew the truth about the vulnerable nature of the Internet, while business leaders and society chose to ignore the facts. With Edward Snowden's exodus to the East came a revelation about the pervasive reality of cyber espionage and how it impacts governments, corporations and the individual. While many of the lessons Mr. Snowden exposed to us are still being digested, they are far from being understood by the private sector. Companies still have substandard policies and technology in place to prevent surreptitious attempts of collecting data. CIO.com published an article stating that a survey of 882 IT professionals had reported "one in five organizations (21%) suffered a security breach involving a mobile device sometime in the past, primarily due to connections to malicious Wi-Fi hotspots and malware."[1] The article goes on to state "37% of organizations were not even sure whether mobile devices had been involved in security breaches in the past."[2] The underlying issue is that privacy

1 Matt Hamblen, *One-fifth of IT Pros Say their Companies had Mobile Data Breach*, CIO.COM (Mar. 29, 2016), http://www.cio.com/article/3049217/mobile/one-fifth-of-it-pros-say-their-companies-had-mobile-data-breach.html.

2 *Id.*

protection, be it policy or law, has not kept up with the leaps and bounds of the IT sector. It is also widely known that many of the U.S. trade partners actively engage in corporate and economic espionage.[3]

There is also the culture of the *Hacker Ethic* that "reflects an open and free approach to using and exploring computers."[4] Chief Information Officer's ("CIO") are faced with this non-aligned threat that uses asymmetric approaches to retrieve data. The nature of this type of attacker is very hard to predict since their agenda and motivation is more whimsical than others. They typically are not affiliated with any nation state and owe allegiance to the mythology of a free and open society. This threat is unpredictable in nature and hard to defend against since pre-event indicators are as hard to define as they would be with a state sponsored hack.

This paper will explore some of the policy and legal issues surrounding privacy in the cyber domain and offer some of the best practices for CIOs.

I. The Challenge

A. CIOs must maintain a balance between fiduciary responsibilities and ROI.

Protecting IT assets for a company is complex and goes far beyond the application of a gadget or software. The Cyber Threat Intelligence Integration Center (CTIIC), an organization within the Office of the Director of National Intelligence (ODNI or DNI), views the protection of IT and cyber as part of an intelligence effort.[5] The National Counterintelligence Security Center ("NCSC") is tasked along with other agencies, to ensure that the United States cyber infrastructure is as secure as possible.[6] The poten-

---

3 *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* (Jul., 1995) https://fas.org/sgp/othergov/indust.html.

4 Orin S. Kerr, Computer Crime Law 11 (3d ed. 2012).

5 *Who We Are*, Off. Dir. Nat'l Intelligence, https://www.dni.gov/index.php/about/organization/ctiic-who-we-are (last visited Feb. 8, 2017).

6 *What We Do*, Off. Dir. Nat'l Intelligence, https://www.dni.gov/index.php/about/organization/ ctiic-what-we-do?highlight=WyJjeWJlciJd (last visited Feb. 7, 2017).

tial for data breaches is high and persistent.[7] Yet, the challenge that the U.S. government faces is a lack of coordination between corporations, the government (federal, state and local), and laws that can safeguard cyber domains.[8]

The private sector is extremely vulnerable. According to NCSC, "the private sector alone lacks the resources and expertise to thwart foreign efforts to steal critical American know-how. This is in large part because counterintelligence is not a typical corporate function, even for well-trained and well-staffed security professionals."[9] The threat is real, constant and sophisticated. In 2011, James Dyson, the inventor of the Dyson vacuum cleaner, warned that Chinese students were stealing trade secrets from universities in the United Kingdom.[10] He also noted that these same students were implanting malware on computer systems before returning to China.[11] Trade partners are always trying to gain a comparative advantage; sometimes, it is through less than direct methods. When industry is coupled with national interest, the available assets to gain such an advantage increases significantly. The People's Liberation Army (PLA) influences many of the critical industrial sectors in China.[12] CIOs who are attempting to secure their cyber domains face a formidable enemy, a well-organized, and trained hacking force. China is not the only nation that has this level of capability. North Korea and

---

7 Memorandum from Michael E. Horowitz, Inspector Gen., on Top Mgmt and Performance Challenges Facing the Justice Dep't to the Attorney Gen. and the Deputy Attorney Gen. (Nov. 10, 2016) https://oig.justice.gov/challenges/2016.pdf.

8 *Id.*

9 *Top Issues: Economic Espionage*, Nat'l Counterintelligence Sec. Ctr., https://www.ncsc.gov/issues/economic/index.html (last visited Feb. 7, 2017).

10 Robert Watts & Jack Grimston, *Chinese Students Steal Secrets: Inventor James Dyson*, Australian (Mar. 27, 2011) http://www.theaustralian.com.au/news/world/chinese-students-steal-secrets-inventor-james-dyson/news-story/f00bfeed83e79a6db52a4eb67fae94a7.

11 *Id.*

12 *See* Swaran Singh, *Rise and Fall of the PLA's Business Empire: Implications for China Civil-Military Relations*, https://www.idsa-india.org/an-may9-4.html.

Russia also employ state sponsored computer intrusion, and the list goes well beyond those three nations.[13]

CIOs have a tough challenge. In the private sector, a culture of profit is prevalent and often runs in direct conflict to counterintelligence (CI) best practices. Business schools teach outsourcing to nations that are hostile to U.S. interests and hungry to develop their comparative advantage. The problem is partly based in a conventional wisdom that espionage only targets military or similar secrets. Why would an intelligence service or foreign corporation want to know about emerging technology? But in truth, CIOs have little idea about the targeting requirements of foreign intelligence services (FIS). The other problem is that the U.S. is not capable of producing high-end technology completely made in the U.S.[14] The reliance on foreign made components is nearly inescapable. The door is wide open for malware and other forms of collection and disruption to be implanted without the knowledge of the consumer. Sometimes, it may not even be a FIS directing the altering of software. In 2015, Lenovo found itself involved in a class action lawsuit over the preloading of Superfish adware.[15] Essentially, this is spyware that was designed to be undetectable, and nearly impossible to remove.[16] It was able to track in real time the computer habits of the users.[17] Lenovo admitted that they "messed up."[18]

---

13 Patryk Pawlak & Gergana Petkova, *State-sponsored Hackers: Hybrid Armies?* European Union Institute for Security Studies (Jan., 2015),.http://www.iss.europa.eu/uploads/media/Alert_5_cyber___hacktors_.pdf.

14 *Made In China*, The Economist (Mar. 14, 2015), http://www.economist.com/news/leaders/21646204-asias-dominance-manufacturing-will-endure-will-make-development-harder-others-made

15 Lance Whitney, *Lenovo Hit by Lawsuit Over Superfish Adware*, CNET (Feb. 24, 2015), https://www.cnet.com/news/lenovo-hit-by-lawsuit-over-superfish-adware/.

16 *Id.*

17 Alan Henry, *Everyone's Trying to Track What You Do on the Web: Here's How to Stop Them*, LifeHacker (Feb. 22, 2012) http://lifehacker.com/5887140/everyones-trying-to-track-what-you-do-on-the-web-heres-how-to-stop-them.

18 Agam Shah, *Lenovo Slapped with Lawsuit over Dangerous Superfish Adware*, PC World (Feb. 23, 2015), http://www.pcworld.com/article/2887392/lenovo-hit-with-lawsuit-over-superfish-snafu.html.

American business culture is different than any other. While companies in other nations are partnered with various government agencies, effectively making them state-influenced businesses, the U.S. has the opposite. The separation between the government and corporations is not only cultural but also preferred. This schism has a critical vulnerability—the perception that the government is an enforcer as opposed to partner and valued stakeholder.[19] While this perception pervades, there will always be a lack of congruence in sharing of information and development. CIOs are also the first line of defense in protecting trade secrets.[20] Given the over-reliance on technology and the potential for distributed access from virtually any device, accessing trade secrets has become relatively easy.[21] With new technology relying more on Bluetooth technology, which uses an unencrypted signal, the stealing trade secrets will become even simpler.[22]

II. Legal

Businesses are becoming more regulated. This trend is not only in the U.S., but globally. Cyber is an essential aspect in all industries, just as the typewriter was. It is everywhere and the presence is growing. Laws and policies are in place, but there lacks coordination between Federal, State and Local (FSL) authorities.[23] There has been a legislative vacuum from the Federal government that has been filled by States and many municipalities.[24] In some instances, these laws contradict each other. While in theory,

---

19 John T. Chambers, *Vulnerability Disclosure Framework*, National Infrastructure Advisory Council (Jan. 13, 2004), https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf.

20 Bill Mariano, *Managing Confidential Data: The Best Defense*, CFO (April 8, 2013), http://ww2.cfo.com/fraud/2013/04/managing-confidential-data-the-best-defense/.

21 Charlee Vorakulpipat, *A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives*, Hindawi (2017), https://www.hindawi.com/journals/scn/2017/2057260/.

22 *Economic Espionage: 'Company Man' Campaign*, FBI (July 23, 2015), https://www.fbi.gov/news/stories/economic-espionage.

23 *Coordinating Drug Policy at the State and Federal Laws*, Rand (1997), http://www.rand.org/pubs/research_briefs/RB6005/index1.html.

24 *Id.*

the USG is supposed to provide unifying guidance, the politics and lack of understanding of the nature of the threat has weakened the FSL troika. Regardless of a specific cyber law that covers privacy, there are also other legal avenues that should be mentioned. Negligence is something that can be used by an injured party. Vendor fraud is also another tool within a prosecutor's tool kit. It is the duty of the CIO to have a sophisticated level of *working knowledge* in order to protect themselves and the stakeholders from breaking the law.

One of the paramount tools that any threat prevention effort has is the sharing of actionable information in a timely manner. To do this in a way that is efficient and reliable, the USG has enacted into law the Cyber Security Act 2015 (CSA).[25] This law makes sharing of cyber threat information between the U.S. government and corporations possible.[26] The CSA became law in December 2015.[27] Time will tell if this law is useful or not, but it is too early to tell.Cyber privacy has become a growing topic of concern for all. After the terrorist attacks of 911, the Patriot Act provided what some critics have felt as a broad-brush authorization to collect the data of people and companies in the name of national security.[28] Nearly 15 years later, the sentiment on privacy has swung to the other direction. Privacy is seen as a sacred and unalienable right. The recent terrorist attack in San Bernardino and the industry reluctance to unlock an alleged terrorist's iPhone show just how far the pendulum has swung.[29] A Federal Court ordered that Apple must provide the encryption keys to unlock the phone and also to

---

25 Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat 2242 (2015).

26 *Cyber Security Legislation Watch*, Cybersecurity Nexus, http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx (last visited Feb. 7, 2017).

27 Cybersecurity Act of 2015, *supra* note 25.

28 *See* Charles Doyle, Cong. Research Serv., RL31377, The USA PATRIOT Act: A Legal Analysis (2002).

29 Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. Times (Feb. 17, 2016) https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

view the iCloud backup.[30] Apple decided to defy the court order, stating that they were protecting the privacy of everyone, thus avoiding the slippery slope of state sponsored surveillance.[31]The recent Apple/FBI situation has seen the use of one of the oldest laws in the U.S., the All Writs Act. This law gives courts the ability under extraordinary circumstance to compel cooperation with regards to surveillance.[32] In *United States v. New York Telephone Co.*, the Court permitted pen/traps before the enactment of the Pen Register Act, using the All Writs Act to successfully gain valuable information from New York Telephone Co.[33] This company has drawn an interesting line in the sand. Apple is showing governments that IT companies are powerful and capable of dictating terms in the face of court orders.[34] Effectively, CIOs will have to understand the business operations of an entire enterprise, have a high degree of IT familiarization but also understand legal and political nuances. Stratfor has suggested that IT companies are becoming supranational entities.[35]

Computer fraud is also covered under 18 USC Section 1030 *et seq.*[36] These systems are especially vulnerable to people who want to manipulate the performance or the data of a computer system that could be essential to the operations of a company. A recent case out the U.S. District Court for the Middle District of Pennsylvania demon-

---

30 *Id.*

31 *Id.*

32 Amy Davidson *The Dangerous All Writs Act Precedent in the Apple Encryption Case*, New Yorker (Feb. 19, 2016) http://www.newyorker.com/news/amy-davidson/a-dangerous-all-writ-precedent-in-the-apple-case.

33 *See* 434 U.S. 159 (1977); Eric Limer, *Most Useful Podcast Ever: Why Is the FBI Using a 227-Year-Old Law Against Apple?*, Popular Mechanics (Feb. 24, 2016), http://www.popularmechanics.com/ technology/a19483/what-is-the-all-writs-act-of-1789-the-225-year-old-law-the-fbi-is-using-on-apple/.

34 *Id.*

35 Matthew Bey, *The Tech Revolution Comes of Age*, Stratfor (Mar. 29, 2016), https://www.stratfor.com/weekly/tech-revolution-comes-age.

36 *See* 18 U.S.C. § 1030 (2012).

strates how a disgruntled employee later gained access to his former employer's computer network.[37] The former employee was fired and wanted to retrieve what he felt was his intellectual property.[38] In the process of going through files on a restricted network, it is alleged that he also deleted some log files.[39] The former employee also attempted to extort money from his former employer.[40] Here, not only was there an illegal access of a computer network, and altering of files, but also an attempt for the Defendant to gain financially from those actions.[41] The Defendant was also charged with a violation of the Hobbs Act (extortion).[42]

The case above shows just how vulnerable companies and organizations are to the actions of a lone actor. The Defendant had knowledge and ability to enter a computer network. Should an organization essentially change the locks every time an employee is let go? And how much would that cost?

CIOs will face a tough situation when seeking guidance from the Federal government if they are looking for the passage of cyber laws designed to protect PII. Technology is advancing faster than the lawmakers can keep up. Politics also inhibits the furthering of sufficient laws that would protect PII and also enable a CIO to act in a fiduciary manner. While the business model of Apple is on face value one that amongst other things protects your privacy in the face of *Big Brother*, it also sets forth a corporate precedent. Apple is implying that they mistrust the government and that their products are trustworthy. This cultural paradigm could pose significant problems for CIOs who are trying to walk the fine line between fiduciary responsibilities and corporate compliance.

---

37 United States v. Prugar, No. 1:12-cr-0267, 2015 WL 5602886, at *1 (M.D. Pa. 2015).

38 *Id.*

39 *Id.*

40 *Id.*

41 *Id.*

42 *Prugar*, 2015 WL 5602886, at *1.

In the absence of law, policies can put into place and strategies designed to protect PII and cyber domains. The up-front expense is often regarded as costly. But the return on investment ("ROI") is high if the data is secured successfully. What laws are in place are often dated. They do a good job of applying a utilitarian approach to law enforcement. Yet, in the ever-changing arena of the cyber landscape, will laws that preempt such costs and ability for an organization to operate efficiently and in some situations at a profit be more effective?

III. Economic Espionage

Economic espionage is very common. It is essentially the theft of trade secrets.[43] The Economic Espionage Act of 1996 was passed with the hopes of punishing and deterring the misuse of this information.[44] A trade secret under this statute has a broad definition. It encompasses virtually all forms of business transactional information, patents, methods, etc.[45] Additionally, the copying of source code is also covered under the EEA.[46]

CIOs are faced with protecting the trade secrets of an organization. The wealth of knowledge is in many situations immense. Couple that with a growing interconnectedness and a desire to trade risks for profits—a perfect storm is always possible. At the rate of development current IT implementation is going, there is a serious risk that companies will become even more vulnerable. Uses of the cloud for storage pose risks as well. The degree of security afforded by having a hard copy of a trade secret and storing a hard drive in a secure location is hard to match.

Economic espionage does not have to be initiated by a state actor. It can also be done between companies. This opens up the possibility where companies seeking a competitive advantage could initiate a data breach operation to gain trade secrets.

---

43 *See* Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839 (2012).

44 *Id.*

45 18 U.S.C. § 1839.

46 *Id.*

IV. Wiretap Act

Companies registered within the U.S. also face the onus of being subject to the laws of the land. At some point they may find themselves subject to a Foreign Intelligence Surveillance Act ("FISA") request or a similar law that falls under the criminal code. CIOs have to be aware of the impact and the appropriate organizational response. The Wiretap Act is a good example of such a law.

The Wiretap Act permits law enforcement to *intercept* communications by a third party.[47] The communications must be *prospective* and not *retrospective*.[48] This is not a data mining expedition. With regard to things such as emails waiting in an inbox, the issue of prospective vs. retrospective gets blurred. Data collection devices, such as keystroke loggers put in place by an authorized law enforcement agency, tend to use this law.[49] If the nature of the target and the scope of the investigation go on to include national security matters, FISA is adopted, which is broader in scope but has similar intentions.[50] Given the nature of the interconnectedness of business and the international nature of commerce CIOs will likely face both of these laws, and must be in compliance. "The authority to issue these national security letters (NSL) is comparable to the authority to issue administrative subpoenas." [51] Yet, unlike a subpoena that requires a judge to order, the NSL requires a "reasonable, articulable suspicion that the specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation for such terrorism."[52]

---

47 18 U.S.C. §§ 2510-2522 (2012).

48 *See* Christopher R. Brennan, Note, *Katz Cradle: Holding on to Fourth Amendment Parity in an Age of Evolving Electronic Communication*, 53 Wm. & Mary L. Rev. 1797, 1811-1812 (2012).

49 *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 45 (2004).

50 *Id.* at 79.

51 Charles Doyle, Cong. Research Serv., RL33320, National Security Letters in Foreign Intelligence Investigations: Legal background (2015).

52 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over

If a company is developing technology that is of interest to another government, they could become the target of Federal Intelligence Surveillance (FIS) activity. They may employ various computer intrusion techniques that are used by FIS. This would be enough for the FBI to draft a NSL. CIOs also should be aware that if they have a client in a foreign country and the work their company does onsite (in that foreign nation) is brought back to the U.S., they could also fall under the Wiretap Act and possibly FISA, depending upon the nature of the investigation.

V. Areas of Vulnerability

Examining some of the areas of vulnerability will help give context to the challenges that are faced. This section will look at cloud computing, culture, and insider threat.

A. Cloud Computing

In addition to a legal framework (or lack thereof) that could provide guidance, there are also other domains that are vulnerable. Cloud computing is extremely vulnerable to penetration and hacking. The reason is twofold. First, the cloud in itself is vulnerable due to inadequate software that is needed to protect it.[53] Second, policies that would ensure a lower risk of penetration are also seldom in place or enforced since "ultimately, organizations are responsible for protecting their own data in the cloud."[54]

The attractiveness for businesses to adopt a cloud platform is high. Many see the benefits and discard the risks. Nevertheless, the liabilities that companies face when there is a breach are severe. The loss of data combined with the loss of capital could be catastrophic to a company. As the shift to using cloud computing over data centers in

---

Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

53 Patrick Nelson, *Most CMS-run Websites Have Obsolete Software and Are Vulnerable to Attack*, Network World (May 26, 2016) http://www.networkworld.com/article/3074908/security/most-cms-run-websites-have-obsolete-software-and-are-vulnerable-to-attack.html.

54 Fahmida Y. Rashid, *The Dirty Dozen: 12 Cloud Security Threats*, InfoWorld (Mar. 11, 2016) http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html.

creases, hackers too are shifting their efforts. If the institutions are in the financial sector or the medical sector, specific laws will be enacted to seek justice for the injured parties. While negligence is still a viable legal route for the injured, class action lawsuits take time. If PII is not protected by use of effective cyber policies and procedures backed by encryption a company will be at risk.

The security of the cloud is evolving. Ensuring that appropriate risk mitigation strategies are in place is essential. A lot of this will have to do with the surrounding laws that are in place and can be levied against a company for a breach. Many of these laws differ in scope and effectiveness depending on jurisdiction.

The attractiveness of the cloud offers something unique. It offers an on-demand IT suite. This is different than capacity building that was seen with data centers. The cloud is also accessible anywhere. Cloud Service Providers (CSP) are numerous and offer various levels of encryption. The U.S. government has a policy initiative to modernize their IT infrastructure called "Cloud First."[55] It utilizes "NIST cloud reference architecture" as the prevailing guidance.[56] Given the severity of the OPM breach, it would appear that the USG is using a policy structure with the goal of preventing the next big breach. CIOs in the private sector could benefit from this approach and adopt the best practices from NIST.

The type of person who typically engages in disruptive covert activities is often broken down into two categories. An agent who is working for another organization could go undercover with the intention to disrupt a company's activities. Or it could be a person who has a moral crisis and covertly subverts their organization's efforts. Edward

---

55 CIO Council et al., Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service 1 (2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

56 *Id.*

Snowden is a good example of a man who had a moral crisis and seemingly acted on his own according to his understanding of his moral azimuth.

Personal hardships are always a difficult one. It is one of the key profile elements in detecting fraud. Hardships can occur without warning and make people desperate and prone to manipulation. A person going through such a situation could be enticed to steal data and sell it to offset a problem in their lives.

These three elements are part of a perfect storm that enables the insider threat. The nature of these elements is covert in many ways, which is why they are hard to detect. Often it isn't until the act of acquiring data is done that the activity comes to light. Then the damage is in many cases beyond containment.

There are some ways that this threat can be mitigated. The first is to ensure your employees are happy. If they are happy with their job and believe they have a future, then it is more unlikely they will want to disrupt that future. The second way is to screen them before they enter as employees and see if they are capable of telling the truth. Understanding their financial health is critical. But also paying them a wage that can help them overcome any financial hardship is important.

Limiting access to sensitive information is a third strategy. There should be a need to know information. Databases should not be a library card for access to sensitive data. Additionally, an audit function within the software should be able to track employee's activities on company computers.

VI. Culture

All too often the culture around the protecting of PII in the cyber domain is at odds with the corporate culture. This schism causes organizational friction that will make the implementation and change of the culture difficult if not impossible. Yet, one thing CIOs have going for them is that the specter of cyber breaches is growing. This is

a burning platform that is hard to ignore in American companies. CIOs in the Federal government are already aware of the regulatory constraints that are designed to protect PII. Laws also prescribe the way in which data is supposed to be kept for recordkeeping purposes. Guidance can be found in the Freedom of Information Act (FOIA), and the Federal Records Act (FRA) are somewhat clear on how IT infrastructure is to be set up.[57] The private sector does not have such clear-cut guidance. The driving force should be predominantly long term profit, as in the public arena where the driving force is more of a justification of tax allocation and expenditure. Both drivers pose unique challenges for a CIO that ultimately has to satisfy the stakeholders' expectations. There is an implied expectation in the private sector that they can self-govern as well and even better than the government.

VII. Insider Threat

The insider threat is one of the hardest to understand and anticipate. The insider threat is often a trusted employee. They have access to information, passed all the screening hurdles and by all accounts are vetted. So what makes a seemingly model employee turn into a person who is able to inflict massive amounts of damage to an organization? Some things to consider are psychological balance, previous allegiances, and personal hardships.

Psychological balance is one that is tricky to assess. Due to discrimination laws it is hard to justify testing and evaluation. In an article written by Dr. Brickfeild for George Mason's National Security Law Journal, he posits that Snowden would have been detected if he went through a routine psychological evaluation.[58] This is something that happens regularly in the Intelligence Community for employees but not contractors.[59]

---

57 *See* 5 U.S.C. § 552 (2016); *See* Federal Records Act of 1950, 64 Stat. 583.

58 *See* Francis Brickfeild, *Improving Scrutiny of Applicants for Top Secret/SCI Clearances by Adding Psychological Assessments*, 2 Nat'l Sec. L. J. 252-54, 288, 299 (2014).

59 *Id.* at 264.

Nor does it usually happen in the private sector. The American's with Disabilities Act (ADA) offers a degree of protection against screening for employment suitability. While members of the Executive Branch often have to follow different rules or are asked to waive various protections under the law, due to the nature of the legal tropes that govern the branch, this is not so for the vast majority of the private sector workforce.

The ADA provides guidance on how a medical office within a hiring process can use the results of psychological screening. However, the restrictions do not extend to the placement of a psychologist in a HR office.[60] This would demonstrate a departure from the paradigm suggested in the ADA. A test can be used to determine if a person is capable of honesty. The Equal Employment Opportunity Commission (EEOC) tends to view tests that look to diagnose mental illness as medical exams.[61] This would counter the nature of the ADA, as a test to derive a candidate's ability to be truthful is not strictly a medical test, since it is not looking to determine if there is a mental illness present.[62]

The ADA does provide some guidance for medical examinations once a person becomes an employee. Under the rubric of medical examinations that are designed to see if the employee is capable of doing their job, a psychological examination could be carried out. While elements within the Executive Branch are willing and used to submitting to such invasive measures, it is questionable if the private sector would. Such measures would most likely be met with vigorous opposition. Enforcing this as a best practice would also be tough for CIOs due to cultural traditions within the private sector that view the office as a glorified tech shop. This is far from where the CIO has to be to ensure that cyber security is effective.

---

60 *Id.* at 264-65.

61 *Id.* at 265.

62 *Id.*

VIII. So We Have the Data, Now What???

Hackers who have successfully breached a system and now have the data will be able to sell it. But what worth is all this data to someone? Information peddling and collection is often referred to as the second oldest profession. The recent OPM breach, which exposed sensitive PII of federal employees' past and present, can be used by FIS to target and blackmail.[63] To another extent, the potential for identity theft by organized crime is high.

If the data is of patented or technical nature it could be used to impact any competitive advantage that a company may have. This in turn could affect stock prices and the livelihoods of stakeholders. Economic espionage is prevalent. The Department of Justice recently indicted five Chinese hackers who are members of the Peoples Liberation Army (PLA) with industrial espionage against "U.S. nuclear power, metals and solar products industries."[64] Former Attorney General Eric Holder commented on this case by positing:

> The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global market place should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market.[65]

---

63 *See* Kim Zetter & Andy Greenberg, *Why The OPM Breach Is Such a Security and Privacy Debacle*, Wired (Jun. 11, 2015) https://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.

64 *U.S. Charges Five Chinese Military Hackers for Cyber Espionage*, U.S. Dep't Just. (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

65 *Id.*

His statement highlights the demand for information from commercial sources. When considering how many nations are working very hard to keep up to pace in the market place, the potential for cyber breaches increases. But trade secrets are not the only target. PII is very useful to understanding how organizations work and also help with understanding what an organization is working on by reviewing the credentials of the workforce.

IX. Best Practices

A partial list of best practices/key judgments for a CIO to consider in regards to understanding the cyber domain and privacy is derived from the current situations that are facing our global workplace. The best practices will be grouped into three main categories: objective oriented, workload, and process.

A. Objective Orientated

CIOs should work with their legal teams and develop a high level of working knowledge. This is to say that laws are evolving and regulation is increasing. The Federal State and Local (FSL) troika is lagging with regards to cyber and privacy. Yet, there are legal concepts in place such as negligence and fraud that can be applied in the event of a data breach. If a CIO is working in the medical industry, HIPPA will have guidelines in place. Conversely, if a CIO is not in such a well thought out industry, they run the risk of not having sufficient guidance that is ready and applicable.

Many policy and technical aspects were touched on in this paper. What they show for a CIO is that the ability for privacy in the cyber domain is hard to achieve. The problem is so pervasive that it has become a national security risk. CIOs will face sophisticated attempts at breaches that are designed and implemented by FIS's. They will also face problems with internal cultural perspectives that will prevent best of practice standards to be implemented. The urge to make a profit over security is a cultural bias

that prevents a ROI over the long term. CIOs have to be able to set forth a risk sensitive culture that is receptive to the threats facing the cyber domain.

Beyond hacking and other external threats CIOs will face the issue of the insider threat. Similar to creating a risk sensitive culture this issue deserves individual attention. The power a single person can do to a large organization is impressive. CIOs must put forth policy in conjunction with human resources that protect organizations against the insider threat. These policies may enforce the restriction of data, disable USB ports or have thumb drives that can be remotely deactivated. Additionally, the use of ethical hackers to test systems on a regular basis is also required. But this is only the tip of the iceberg. The creation of a cyber incident response center and team are essential along with policy to ensure that breaches are mitigated before they become catastrophic.

CIOs must be aware of how foreign nations are seeking a dominant position in the market place. Being able to adopt a global view of business seems to be a natural progression in an increasingly connected global market.

B. Workload

The use of metrics to monitor the workload will ensure that PII is adequately protected through workforce requirements. This will ensure that the right resources are in place and that there is never a shortage of resources or personnel when needed to handle a surge.

C. Process

An independent third party should do audits of cyber capabilities and counter-measures. This will ensure a level of bias reduction while the health of the system is being evaluated.

X. Culture of Risk Management

Risk management has long had a nebulous working definition. Looking at the root, it is essentially managing risk, but how is that done well? The *tone at the top* often

dictates a lot of how risk aversion is expressed. Being on the verge of redundancy, the risk of ignoring a risk can be detrimental to an organization. This section will be more anecdotal in nature, as any in-depth analysis would require a separate paper.

From a workforce standpoint, there are two types of people who spread a culture through an organization. Type 1 are those who are in an organization for a limited time. It is a means to punching a ticket or a stepping-stone. The implication is that the person doesn't identify fully with the company. A pitfall is that the impact on the company as a whole is temporary. Any problems can be swept under the carpet and left for the next person to deal with. Seeing their employer more as an entity and something that is going to be reflecting upon their character is often not the case.

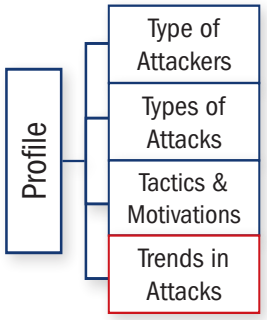
Type 2 are those who see themselves as part of the culture. They essentially drank the Kool-Aid and take responsibility for the company as is proportionate to their station. Regardless of how long they are at their company, they seldom look at themselves as an employee but instead as a member of an organization. This long view adaptation is more inclined to view risk as something that has to be dealt with rather than being swept under the carpet.

Of course with any archetype there are holes in the model. But as an ideal, the two types illustrate the point that some people working in organizations come and go looking to self-propel their careers. While others take a long view and look to establish their careers in the identity of an organization.

Organizations often like to appear impervious utilizing a fortress mentality. Any cracks in the defenses are seen as a problem. But how those cracks are dealt with is also seen as either an opportunity or a problem. Looking at the job of a CIO, they are in a position to identify the weak points and can then organizationally change to adjust to the threat. Cyber is perhaps one of the easiest modes to defend against. Relatively, it just takes the attitude of an organization coupled with technology to effect a change. If the

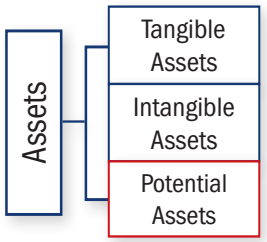
will demonstrates a decisive commitment to constant adaptation, any gray swans can be averted or at worse managed.

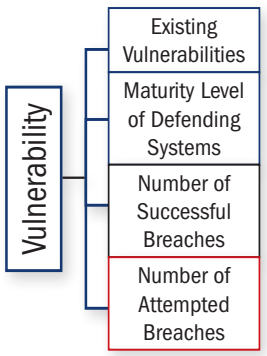
Indicators of an organization that is taking the long view are seen in a robust risk management program that views risk as an opportunity to lose valuable data and capability. Often when a risk is found, be-it conceptually or as something more tangible it is identified and dealt with. The lessons of why it is there are learned and make the organization stronger as a whole.



A. Cyber VaR

A recent article from Deloitte draws similarities between the financial services industry and cyber security.[66] Both deal with risks and both, if in a state of failure, will see ripples compounded across their respective areas.[67] Another nexus between the two is that of using modeling to identify hidden risks across a complex system. The value at risk (VaR) is a routine calculation and concept to comprehend the risk of loss to a financial endeavor. Though this predictive model has limits and can only, under ideal circumstances, predict a loss or the risk of a loss. The Cyber VaR (outlined in the graphic) goes further in that is has with the input of the World Economic Forum identified three macro compo-





66 J.R. Reagan et al., *Quantifying Risk: What Can Cyber Risk Management Learn From the Financial Services Industry?*, Deloitte Rev. (July 25, 2016), https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/quantifying-risk-lessons-from-financial-services-industry.html.

67 World Econ. Forum, Partnering for Cyber Resilience Towards the Quantification of Cyber Threats (2015), http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf

nents with various micro components.[68] These components comprise the areas of concern and attempt to create a paradigm that will allow organizations to apply best practices. The addition of three red sub-components signifies an addition that the World Economic Forum did not originally include. The intention is that the Cyber VaR not be inflexible in application like the VaR. The cyber realm is too fluid and too adaptive to have any real value added by systems of governance that are not at least as flexible in application.

B. Cyber VaR Components

While both Deloitte and World Economic Forum have a different order than the graphic depicts, it is by no accident that profiling takes a dominant role in the graphic above versus vulnerability. Switching the primary focus offers a more offensive measure to preparing and understanding how to protect against surreptitious cyber intrusions. All too often, cyber countermeasure is designed to counter a threat. What if organizations employed an anti-measure that is offensive in nature? Knowing and analyzing the threat before it becomes unmanageable would give a degree of running room for an organization to devise an appropriate strategy that, in turn, would be utilized as a tactic. It is also important to understand that companies do not utilize offensive cyber tactics as a best practice.

i. Profile

Cataloguing the types of attacks and techniques, tactics and procedures of the attacker are crucial to understanding the vulnerability of a potential IT infrastructure. Types of attackers range from state sponsors, criminals, industrial espionage, and enthusiastic amateurs.[69] The types of attacks are the usual pantheons. But how they are employed and evolve through complex systems is the hallmark of the capability and sophistication of the threat that CIOs face. The addition of trends in attacks would be very useful in understanding the potential for an attack or the type. Analysis of the

68 *Id.*

69 *Id.*

trends would be able to pull together the other components and make the key findings actionable.

ii. Assets

The tangible assets of an organization are best seen in the physical mechanics or a process. That is to say if a company is in manufacturing, then their machinery could be at risk. Or, if the organization is a utility, then a power generation facility could be vulnerable. Intangible assets are often understood to be: reputation, institutional knowledge or some other paradigm that forms the capability and identity of an organization. When the Office of Personnel Management (OPM) was hacked, it could be said that many intangible assets were compromised. The reputation of OPM was tarnished as well as institutional knowledge made obsolete.

iii. Vulnerability

An audit of existing vulnerabilities would create an accurate picture of the health of IT infrastructure. The age of existing systems is also critical to understand. Cyber evolves continually. What worked yesterday may not work today. Constant upgrades can become costly and hard to justify if attacks are either infrequent or within tolerable rates of loss. The number of successful breaches is also a critical metric. It shows two things. The first is that an organization can detect an intrusion. The second is that an organization can plan to deter future attacks.

The final component is the number of attempted breaches. Understanding the failures of hackers is as important as understanding the event after the fact. This would also call for the essential planning and budgeting needed to prevent potential cyber intrusions. Once the existing vulnerabilities are understood and a plan (on paper at the least) is in place, justification for upgrades can be pitched.

iv. We Only Know What We Know

Cyber VaR is not the end all be all. The World Economic Forum noted that the process requires a great deal of historical data.[70] Often this is not possible.[71] A mitigation technique is to use a Monte Carlo model to detect the probability of an event happening.[72] This model has worked well in other industries to give decision makers an idea of the potential of an occurrence. Additionally, near real-time sharing of information is essential. This would have to go beyond the enterprise and include the cooperation of governments and other organizations both private and public.

E. Closing the Loop

This paper puts a heavy emphasis on law due to the growing level of regulations (laws) that are being imposed upon companies. The cyber domain is growing faster than expected. It will be the third technical revolution behind the ability to navigate deep-sea passages to enable commerce, and the industrial revolution.[73] While IT companies are beginning to test the waters with a special relationship with governments, they have a dominant position. They are on the cutting edge of computing ability. This is something no nation has. Coupled with immense fortunes to fuel R&D, CIOs will play a growing role in policy development. Another theme is the prevalence of state sponsored hacking. Cyber warfare is becoming more prevalent and industry is the prime target. CIOs have now become participants in a war that has a hard to define front line.

American business is culturally different from that of the rest of the world. There is a seemingly tangible dividing line between the Government and the Corporation. While regulations grow over business, there still is segregation between the two that is seen as sacred. The rest of the world however, enjoys partnerships between their gov-

70 World Econ. Forum, supra note 67, at 15.

71 Id.

72 Id.

73 See Bey, supra note 35.

ernments and businesses. This opens up resources to businesses that are not available to American companies. Some of these resources are access to Foreign Intelligence capabilities with regards to the acquiring of trade secrets. While there are many treaties that form alliances between the U.S. and other nations for national security and defense, similar protections do not exist in the private sector.

As noted by the DNI's National Counterintelligence and Security Center, the private sector is ill prepared for counterintelligence work.[74] But that is precisely what they must become proficient in to do well in a market place that is dependent upon the international nature of business. The role of the CIO is expanding from providing computers and software to safeguarding the integrity of business systems from hackers and thieves.

74 *Who We Are*, *supra* note 5.

Combating International Cybercrime: A Counter-Threat Finance Initiative to Fight Terrorism

Neil Noronha

PART I: Cybercrime—A National Security Threat

P1: Cybercrime is increasing because of higher profitability and the difficulty behind the attribution and prosecution of its perpetrators

Cybercrime has existed since the creation and expansion of cyberspace, and, just as defining cyberspace is an on-going process, what characterizes cybercrime is still up for debate. Symantec Corporation, the creator of Norton Anti-Virus products, defines cybercrime as "any crime that is committed using a computer network or hardware device."[1] From this broad definition, this paper will strictly focus on cybercrime that immediately impacts, but does not significantly disrupt, retail and financial services sectors.

In this subset of cybercrime, criminals orchestrate computer network exploitations (CNEs) to illegally steal information or data of any individual, company, or government for direct financial gain. Cybercrime in the retail sector, such as account takeovers, third party payment processor breaches, ATM skimming and point of sale schemes, and mobile banking exploitation, involves the CNE of a person's online shopping or banking accounts for unauthorized purchases of retail products or withdrawal of money. Cybercrime within the financial services sector is a CNE, such as supply chain infiltration, insider access theft, and securities and market trading exploitation, that allows cybercriminals to exploit trading accounts or exchanges for financial gain. Similar to that in the retail sector, this CNE only affects the parties targeted, as real-time trading environments are generally not compromised. However, cybercrime within the financial services sector is far more complex and reflects the constantly evolving financial system,

1 *What is Cybercrime?*, Norton, https://us.norton.com/cybercrime-definition/ (last visited Feb. 6, 2016).

in which new web-based trading products are created every few years.[2] For example, criminals profit from fraudulent binary options web sites by inducing unsophisticated online investors into depositing money into fake trading accounts and then either denying victims access to their accounts or proactively ensuring trading losses.[3]

Given its multiple forms and high returns, cybercrime not surprisingly has grown over the last few years. In June 2014, the Center for Strategic and International Studies in partnership with MacAfee published a report assessing the economic impact of cybercrime. Accordingly, they estimated that the likely annual cost to the global economy from cybercrime is more than $400 billion, with a range from $375-575 billion.[4] According to a study conducted by the threat intelligence consultancy firm, Risk Based Security, there were 4,149 incidents reported exposing 4.2 billion records through December 31, 2016.[5] While less than the 4,326 reported in 2015, the incidents in 2016 affected more people, with 822 million people exposed in 2015.[6] Moreover, risks to engaging in cybercrime are low because identifying the criminals responsible for CNEs is very difficult. Criminals are able to hide behind the massive number of users and relatively anonymous nature of the cyber domain. In 2015, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 288,012 complaints from victims residing within the United States.[7] Out of the 288,012 complaints, 3,644

---

2 Gordon M. Snow, Assistant Dir., Cyber Div., Statement Before the House Financial Service Committee (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

3 *See* Sec. & Exch. Comm'n, Office of Inv'r Educ. & Advocacy, Investor Alert: Binary Options and Fraud (2013), https://www.sec.gov/investor/alerts/ia_binary.pdf.

4 Ctr. for Strategic & Int'l Studies, Net Losses: Estimating the Global Cost of Cybercrime 2 (2014), https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [hereinafter CSIS].

5 Risk Based Sec., Data Breach QuickView Report: 2016 Data Breach Trends - Year in Review 3 (2017), https://pages.riskbasedsecurity.com/2016-ye-breach-quickview.

6 *Id.*

7 Internet Crime Complaint Ctr., 2015 Internet Crime Report 4 (2015), https://pdf.ic3.gov/2015_IC3Report.pdf.

complaints provided 165 referrals to eight FBI Cyber Task Forces, which opened up 39 investigations.[8] Given these numbers, getting caught by law enforcement for cybercrime is anecdotal and unlikely. Not surprisingly, the IC3 last reported the number of convictions resulting from these complaints in 2010. In that year, there were only six convictions out of the 42,808 complaints that the FBI and law enforcement deemed significant to prepare cases; thus, there was one jailed cybercriminal for approximately every 7,135 complaints.[9] To note, each of the statistics presented are likely associated with different definitions of cybercrime. While the data varies and is mostly incomplete in this area, the trend is clear. Cybercrime is a growing illicit business for criminals because of its profitability and the difficulty of attribution. So who commits cybercrimes, then? Since cybercrime began, lone wolf criminals, who look for huge, short-term financial gains, have been the majority of the perpetrators. Yet, the growth of the industry has drawn the interests of other larger-scale, illicit non-state actors.

P2: Cybercrime is becoming a TOC discipline

Despite the dominance of lone hackers, cybercrime is becoming more organized, with groups of hackers, separated vastly by geographic distances, joining together to increase the number and reach of CNEs. As ex-Director of the Federal Bureau of Investigation, Robert Mueller said, "Organized crime in cyber space offers a higher profit with a lower probability of being identified and prosecuted."[10] To understand how TOC groups incorporate cybercrime into their funding streams, look no further than to Russia, where organized cybercriminals are the gold standard bearers of the activity. Group-IB, the Russian cybercrime investigation company, found that Russian-speaking cyber

8 *Id.* at 9.

9 Internet Crime Complaint Ctr., 2010 Internet Crime Report 5 (2010), https://pdf.ic3.gov/2010_IC3Report.pdf.

10 Robert S. Mueller, III, Dir., Fed. Bureau Investigation, Statement Before the Senate Judiciary Committee (May 16, 2012), https://archives.fbi.gov/archives/news/testimony/oversight-of-the-federal-bureau-of-investigation-4.

criminals apparently raked in roughly 36% of the global cybercrime market (according to their estimates, $4.5 billion out of the total $12.5 billion) in 2011.[11] Of the Russian TOC groups engaged in cybercrime, none was as infamous as was the Russian Business Network (RBN), which conducted CNEs and sold their services as well as hacking tools and software to those who were less technologically savvy.[12] While pressure from the U.S. and Russian law enforcement eventually shut down the original RBN, offshoots of the group still conduct this illicit business, working from servers in several countries around the world.[13] This problem is not confined to just lone hackers coming together to start their own group. Traditional TOC drug-traffickers employ cybercriminals to facilitate their business operations and provide operational security.[14]

While there is only confirmation of Eastern European mafias conducting cybercrime activities, the lucrative nature of cybercrime offers an attractive, yet relatively low risk, option for other TOC groups to increase profits.[15] Thus, non-cyber TOC groups will most likely start developing offensive cyber capabilities. Cybercrime's integration into the TOC discipline is like that of drug trafficking, extortion, and piracy. TOC groups use it solely as a financial end. However, there are others who see cybercrime's economic benefit as a means to fulfilling a larger, less financially-driven goal.

---

11 Group IB, State and Trends of the Russian Digital Crime Market 6 (2011), http://www.group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

12 *Russian Computer Hackers Are a Global Threat*, Newsweek (Dec. 9, 2009), http://www.newsweek.com /russian- computer-hackers-are-global-threat-75837.

13 *Id.*

14 Tom Bateman, *Police Warning After Drug Traffickers' Cyber-attack*, BBC News (Oct. 16, 2013), http://www.bbc.com/news/world-europe-24539417.

15 Steven Chabinsky, Deputy Assistant Dir., Cyber Div., The Cyber Threat: Who's Doing What to Whom?, Address at GovSec/FOSE Conference (Mar. 23, 2010), https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom.

P3: Cybercrime can be a conduit for furthering the "crime-terror nexus" among TOC groups and terrorist organizations

Besides TOC groups, terrorist organizations would value the benefits of cybercrime, particularly as a funding stream to finance their operations, which focus on furthering their political or religious goals. At this time though, major terrorist organizations do not possess their own offensive capabilities to conduct CNEs for cybercrime.[16] Rather, they, such as the Islamic State of Iraq and Syria, use cyberspace for propaganda, intelligence gathering, communications, and fund-raising purposes.[17] For cybercrime to be a significant part of terrorist financing, major terrorist organizations would either have to develop the offensive cyber capabilities themselves or contract the work out to professionals willing to, either by financial or ideological motivations, help. Since the former is a capital-intensive investment, requiring time and money, the latter, which requires only money, is more feasible. However, how would terrorist organizations recruit cybercriminals?

Known as the crime-terror nexus, the convergence in activity between profit-motivated TOC groups and politically-motivated terrorists has been a growing, on-going phenomenon over the last two decades.[18] Through either shared tactics and methods, or short-term or long-term, transaction-based services-for-hire, terrorists and criminals engage in strategic partnerships to shore up financial or operational gaps in their capabilities so that they are more poised to meet their respective goals.[19] Thus, given the abundant cybercriminal networks, terrorist organizations can contract out cybercrime capabilities as

---

16 Nigel Webb & Sarah Tomalewicz, *Small Crimes Can Lead to Big Consequences: Raising Awareness of Cybercrimes and Links to Terrorism*, FTI Consulting (Apr. 11, 2016), http://www.uksecurityexpo.com/_media/PDFs/FTI_Cyber_Crime_Report.pdf.

17 Steven P. Bucci, *The Confluence of Cyber Crime and Terrorism*, Heritage Found. (June 12, 2009), http://www.heritage.org/research/lecture/the-confluence-of-cyber-crime-and-terrorism; Joseph Marks, *ISIL Aims to Launch Cyberattacks on U.S.*, Politico (Dec. 29, 2015), http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179.

18 *See* Dr. Shelley Louise, Dirty Entanglements: Corruption, Crime, and Terrorism (2014).

19 Sam Mullins, *Parallels Between Crime and Terrorism: A Social Psychological Perspective*, 32 Stud. Conflict & Terrorism 811 (2009).

a service, with financial compensation provided. At the same time, the crime-terror nexus does have its limitations. Common disincentives for such collaboration include increased and unwanted attention from authorities, risk of infiltration, and compromise of internal security.[20] However, given the difficulty of identifying and prosecuting cybercriminals, cybercrime can mitigate these concerns and thus proliferate the partnerships between terrorist organizations and TOC groups. Given the inevitability of terrorist organizations to develop indirect capabilities to conduct cybercrime, is it possible to anticipate who will be their future targets? If so, the USG could train and equip these potential victims now so that they will be able to protect themselves from future attacks.

Currently, most cybercriminals target financial infrastructures of wealthier countries, which have higher national incomes and have more retail businesses and financial services conducted over web-based platforms.[21] At the same time, cybersecurity is becoming more prioritized as a national security threat in the developed world.[22] Thus, conducting cybercrime against developed countries becomes more difficult and the corresponding returns start to shrink.

P4: Cybercriminals will target more financial infrastructures in the developing world

Over the last few years, developing countries have undertaken significant progress in developing new technologies to meet consumer demands, especially with regard to access to information.[23] In fact, according to the International Telecommunications Union (ITU), the United Nations' specialized agency for information and

---

20 John Rollins, International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress 5 (2010).

21 CSIS, *supra* note 4; *World Cyber Threat Map*, Clear Point, https://www.threat-cloud.com/ThreatPortal/#/map (last visited Feb. 6, 2017); *IPViking*, Norse Corp., http://map.norsecorp.com/#/ (last visited Feb. 6, 2017).

22 *Fact Sheet: The 2016 G-20 Summit in Hangzhou, China*, White House (Sept. 5, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/fact-sheet-2016-g-20-summit-hangzhou-china.

23 Guillermo Esteve & Angel Machin, *Devices to Access Internet in Developing Countries*, Vodafone Grp. 1 (May 12, 2007), http://www2007.org/workshops/paper_106.pdf.

communication technology, 2.5 billion of the world's 3.5 billion Internet users are from the developing world.[24] With growing connectivity and the transformation of traditional business into e-commerce, low-income countries will face the same cybersecurity challenges that are plaguing developed nations today.[25] However, terrorist organizations and TOC groups that have adapted to the sophisticated cybersecurity measures of the developed world will have more knowledge about cyberspace than the private sector or governments of developing countries will. For example, ITU in 2014 developed a global cybersecurity index to rank the cybersecurity capabilities of nation states.[26]

These results exemplified the weak cybersecurity capabilities of developing nations.[27] Specifically, in sub-Saharan Africa, only three out of the forty-four countries received an index high enough to qualify for intermediary-level cybersecurity readiness.[28] On a scale of 0 (worst possible readiness) to 1 (the benchmark), sub-Saharan African countries scored, on average, a 0.1611 with a median of 0.0882.[29] Not surprisingly, cybercriminals are increasingly engaging in cybercrime activities in Africa that use botnets, remote access Trojans, and banking/finance-related malware because of the continent's increased

---

24 *ICT Facts and Figures 2016*, Int'l Telecomms. Union 4 (2016), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf.

25 *See* Dr. Marco Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, Int'l Telecomms. Union (2011), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf.

26 *Global Cybersecurity Index: Conceptual Framework*, Int'l Telecomms. Union, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf (last visited Feb. 6, 2017).

27 *Id.*

28 *Global Cybersecurity Index: Africa Ranking*, Int'l Telecomms. Union, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_2014_Results_for_Africa_Region.pdf (last visited Feb. 6, 2017).

29 *Id.*

Internet availability at lower costs, a rapidly growing Internet user base, and a dearth of cybercrime laws on the continent.[30]

Ultimately, the difference in understanding how cyberspace operates will provide terrorist organizations and TOC groups an advantage, for which they can exploit. In fact, cybersecurity professionals already witness such a shift with the increasing exploitation of mobile platforms, the preferred source for connectivity in the developing world.[31] Moreover, with no common cybersecurity standards, such measures are weaker among low-income countries because businesses see cybersecurity as a cost and not an added value. Companies must weigh how much risk they are willing to accept against potential cybercrimes versus how much they are willing to spend to reduce that risk. If companies are unaware of their losses to cybercrime or underestimate their vulnerability, they will underestimate the risk and choose to not spend. In addition, even if a cybercrime is committed, there are few recourse mechanisms for consumers to hold companies, who can bribe corrupt government officials, accountable. Thus, cybercriminals will probably diversify their cybercrime strategies to include CNEs against financial institutions within the developing world.

Assessment: Terrorist organizations, with the help of individual cybercriminals and TOC groups, will increasingly use cybercrime, targeted against retail and financial sectors in the developing world, as a terrorist financing mechanism over the next five years

While the premises logically build upon one another to support this assertion, there is already anecdotal evidence validating the claim that terrorist organizations use

---

30 *See* Loucif Kharouni, Africa: A New Safe Harbor for Cybercriminals? (2013), www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf; *See* Eric Tamarkin, The AU's Cybercrime Response: A Positive Start, But Substantial Challenges Ahead (2015), https://issafrica.org/research/policy-brief/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead.

31 CSIS, *supra* note 4; 21 Symantec, Internet Security Threat Report 10 (2016), https://www.symantec.com/content/dam/ symantec/docs/reports/istr-21-2016en.pdf?aid=elq_&om_sem_kw=elq_16908641&om_ext_cid=biz_email_ elq_&elqTrackId=3f9e79f4cbf14b9a9d39e52f9e438f5f&elqaid=2902&elqat=2.

cybercrime generally to finance their terrorist operations. For example, Imam Samudra, an Indonesian terrorist convicted for the 2002 Bali nightclub bombings, wrote in 2004 about the use of credit card fraud and carding as a means to fund terrorist activities in his 280-page autobiography.[32] More directly, Younes Tsouli, Waseem Mughal, and Tariq Al-Daour, three British men convicted in 2007 for inciting murder via the internet under the United Kingdom's Terrorism Act of 2000, also pled guilty to conspiracy to defraud banks and credit card companies.[33] Specifically, they used roughly 37,000 stolen credit card numbers obtained through phishing scams to make more than $3.5 million in fraudulent charges in order to purchase equipment, prepaid cell phones, airline tickets, and other items to support jihad field operations.[34] As validation to P3, the terrorists obtained some stolen data through contacts with Russian-based criminal gangs, providing a concrete example of the crime-terror nexus around cybercrime.[35]

Using this example, Michael Jacobson, a senior fellow in The Washington Institute's Stein Program on Counterterrorism and Intelligence, warns of the serious counterterrorism vulnerabilities the internet creates as terrorists can relocate to other jurisdictions that are less vigilant about monitoring and countering this type of illicit activity (cybercrime).[36] Thus, it is not inconceivable to image a situation where the Pakistani-based terrorist organization Lashkar-e-Taiba works with a Ukrainian cybercrime ring to prey on customers and retail businesses in Guatemala in order to finance a terrorist operation within India. The important question now is how does the USG organize and resource itself to stop this situation from becoming a reality.

---

32 Rita M. Glavin, Acting Assistant Attorney Gen., Criminal Div., Dept. of Justice, Do the Payment Card Industry Data Standards Reduce Cybercrime?, Hearing Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology (Mar. 31, 2009), https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm.

33 *Id.*

34 *Id.*

35 *Id.*

36 Michael Jacobson, *Terrorist Financing on the Internet*, CTC Sentinel Vol 2. Issue 6 (2009), https://www.ctc.usma.edu/posts/terrorist-financing-on-the-internet.

PART II: USG Current Response to International Cybercrime

Given that President Trump's tenure in office has only just begun, this section will examine USG efforts under President Obama, who recognized the seriousness of cybercrime and the urgent need to fight it internationally.[37] Also, given that the Trump Administration has not yet released specific details on its approach to combat international cybercrime, this section is set in the present and assumes that USG efforts under President Obama are still continuing.

The USG's approach to combating international cybercrime focuses on law enforcement, extending both collaboration and the rule of law with foreign governments.[38] Specifically, the USG participates fully in international cybercrime policy development, harmonizes cybercrime laws internationally by expanding accession to the Council of Europe Convention on Cybercrime ("CEC"), focuses cybercrime laws on combating illegal activities not restricting access to the Internet, and denies terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.[39] For instance, the United States joined the Netherlands in 2015 in founding the Global Forum on Cyber Expertise, a global platform for countries, international organizations, and the private sector to exchange best practices and expertise on cyber capacity building.[40] Within this forum, the United States, through the Department of State (DoS), promised to fund an expanded set of cyber capacity building initiatives, including Computer Security Incident Response Team (CSIRT) development projects,

---

37 *See International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, White House (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy _for_cyberspace.pdf.

38 *Id.*

39 *Id.*

40 *Global Forum on Cyber Expertise Launched During GCCS2015*, Nat'l Cyber Sec. Ctr. (Apr. 16, 2015), https://www.ncsc.nl/english/current-topics/news/global-forum-on-cyber-expertise-launched-during-gccs2015.html.

with the Council of Europe, the Organization of American States, the African Union Commission, and the United Nations Global Program on Cybercrime.[41]

Besides participation in international institutions and forums, the USG outreach on this issue includes training programs, extensive coordination, and information sharing with developed and regionally strategic nations. For example, the FBI created in September 2006 the Strategic Alliance Cyber Crime Working Group, which includes Australia, New Zealand, Canada, and the United Kingdom, to increase operational coordination on intrusion activity and cyber threat investigations related to organized crime.[42] Moreover, FBI agents are embedded full-time in the police agencies of Estonia, the Netherlands, Romania, Ukraine, and Colombia to assist with cyber investigations.[43] These cyber personnel have identified cyber organized crime groups targeting U.S. interests and supported other FBI investigations.[44] Through the Department of Justice (DoJ) International Criminal Investigative Training Assistance Program (ICITAP) and the DoS International Law Enforcement Academies (ILEAs), the United States has trained foreign law enforcement officers from more than 40 nations in cyber investigative techniques over the past two years.[45]

---

41 *See Department of State International Cyberspace Policy Strategy*, Dep't of State (2016), http://www.state.gov/documents/organization/255732.pdf; *Administration Cybersecurity Efforts 2015 Fact Sheet*, White House (Jul. 9, 2015), https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.

42 *Cyber Solidarity: Five Nations, One Mission*, FBI (Mar. 18, 2008), http://www.fbi.gov/news/stories/2008/march/cybergroup_031708.

43 *See* Snow, *supra* note 2.

44 *Id.*

45 *International Criminal Investigative Training Assistance Program*, Dep't of Just. (July 27, 2016), http://www.justice.gov/criminal/icitap/programs/eurasia.html (last visited Feb. 6, 2017); Christopher M. E. Painter, Coordinator for Cyber Issues, Dep't of State, International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms, Testimony Before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy (May 25, 2016), http://www.foreign.senate.gov/imo/media/doc/052516_Painter_Testimony.pdf.

Despite this concerted effort to combat international cybercrime, current responses are limited in scope geographically and functionally. For example, the CEC, the first international treaty seeking to address Internet and computer crime, has only Senegal, Sri Lanka, Mauritius, Panama, South Africa, and Dominican Republic as the only non-member countries in the developing world that have either signed or ratified the convention.[46] Given the future direction of cybercrime will include targeting of financial institutions in the developing world, the USG should get more Latin American and African countries as signatories to the CEC or to even their regional bodies' own frameworks. For example, while the African Union Commission adopted on July 27, 2014 the Convention on Cyber Security and Personal Data Protection, none of the fifty-four member states have ratified it so far.[47]

Moreover, not incorporating a counterterrorism perspective into this heavily-focused law enforcement strategy ensures that responses to international cybercrime are reactive, not proactive. The CEC's law enforcement framework operates in many cases on a time scale that is too long to protect victims of cyber attack from harm.[48] The CEC is no more effective in preventing cyber attacks than criminal law enforcement is in preventing conventional attacks. To be proactive, the United States needs to assist developing countries create cybersecurity capacities by working with their ministries of defense and finance and by selling or donating more USG-cleared cybersecurity equipment. Currently, these efforts are mostly bilateral, leaving many governments incapable

---

46 *Chart of Signatures and Ratifications of Treaty 185*, Council of Eur., http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures(last visited Feb. 6, 2017).

47 African Union, African Union Convention on Cyber Security and Personal Data Protection (2016), https://au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf (last visited Feb. 6, 2017).

48 William A. Owens et al., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 62 (2009).

of assisting in any cyber investigation or employing preventive and remedial actions that may be required beyond their territories.[49]

While the DoS and the DoJ have laid the groundwork for international cybersecurity engagement and development, the USG needs to incorporate other agencies, specifically the Department of Defense (DoD), and make this discipline part of the larger capacity-building partnership for counterterrorism. In 2011, the DoD publically released its strategy for how it would operate in cyberspace.[50] Under Strategic Initiative #4, the DoD will build "robust" relationships with U.S. "allies and international partners" to strengthen collective cybersecurity by "develop[ing] shared warning capabilities, engag[ing] in capacity building, and conduct[ing] joint training activities."[51] Viewing combating cybercrime as a CTF issue will make the USG's international cybersecurity efforts more proactive and effective as the military can leverage its resources and previous experiences in CTF. Namely, during the Iraq and Afghanistan Wars, the National Security Council directed USG agencies to create interagency CTF cells, blending military, law enforcement, intelligence, and diplomatic efforts to identify and disrupt adversaries' terrorist financing mechanisms. Through the CTF cells in Iraq and Afghanistan, the USG used a whole-of-government approach to degrade and disrupt terrorist organizations' financial networks, reducing their operational capabilities.[52] For example, DoD provided CTF cells with personnel, intelligence support, infrastructure, and guidance (strategic, operational, and tactical).[53] Consequently, having achieved success within this field, DoD in December 2008 formally integrated CTF into its warfighting doctrine and planning with Directive-Type Memorandum 08-034, which has

---

49 Abraham D. Sofaer et al., Cyber Security and International Agreements 197, 201 (2010).

50 *See* Dep't of Def., Department of Defense Strategy for Operating in Cyberspace (2011).

51 *Id.* at 9-10.

52 Dennis M. Lormel, *Combating Terrorist Financing at the Agency and Interagency Levels*, CTC Sentinel Vol 1. Issue 4, pg 5-7 (Mar. 15, 2008), https://www.ctc.usma.edu/posts/combating-terrorist-financing-at-the-agency-and-interagency-levels.

53 *Id.*

since been incorporated into DoD Directive 5205.14 (last amended on October 21, 2015) and subsequently cancelled.[54] Expanding this engagement and synced interagency focus on CTF, to include cybercrime, would give more momentum to USG efforts on international cybersecurity.

PART III: How to Improve USG International Counter-Cybercrime

Strategy

The USG, with coordinated support from its allies, should invest into capacity building with nations who have weak cybersecurity governance and are willing to cooperate. The following plan looks to leverage diplomatic efforts, military engagement, linkages among financial institutions, law enforcement partnerships, and connections with NGOs. In this way, synergizing individual efforts of USG agencies will create a more unified and comprehensive USG international counter-cybercrime strategy.

Plan: Create an international counter-cybercrime development and engagement task force at the combatant commands (COCOMs) that will work with host nations to develop whole-of-society cybersecurity strategy, provide cybersecurity resource support, and incorporate them into international discussions and forums.[55]

In line with DoD's Cyber Combat Mission Force Core, these interagency task forces, co-led by DoJ and DoD, would provide cybersecurity resources (personnel, training, equipment, and intelligence) to current cyber engagement cells at the appropriate COCOMs. DoS, the Department of Homeland Security (DHS), and the De

---

54 Gordon England, Deputy Sec'y, Directive-Type Memorandum (DTM) 08-034, DoD Counterthreat Finance (CTF) Policy (Dec. 2008), https://fas.org/irp//doddir/dod/dtm-08-034.pdf; William Lynn, III, Deputy Sec'y, DoD Counter Threat Finance (CTF) Policy, Department of Defense Directive No. 5205.14 (last amended Oct. 2015), http://www.dtic.mil/whs/directives/corres/pdf/520514p.pdf.

55 John D. Negroponte et al., Defending an Open, Global, Secure, and Resilient Internet 26 (2013).

partment of Treasury would play essential, but enabling, roles on the task force. These task forces would incorporate cybersecurity capabilities into current and future USG contingency planning. Having a task force at each COCOM syncs the needs of each geographic area of responsibility (AOR) with the USG International Strategy for Cyberspace. For example, the main cybersecurity concern of U.S. Pacific Command and U.S. European Command is probably Russian and Chinese thefts of intellectual property rights and intrusions into U.S. defense systems.[56] On the other hand, U.S. Southern Command (USSOUTHCOM), U.S. Africa Command, and U.S. Central Command are probably more concerned with cybercrime and the threat finance benefits it may accrue for TOC groups and terrorist organizations.[57] Finally, these task forces allow the USG to leverage the authorities of the aforementioned agencies—Title 18 for law enforcement, Title 22 for diplomatic efforts, Title 50 for intelligence activities, and Title 10 for military operations—and fight cybercrime in a holistic and comprehensive manner. Participating agencies can detail their own personnel to the task force, reducing personnel costs.

Given the current level of cybersecurity engagement and development between the United States and the developed world**,** this plan pertains more to working with developing countries. Each USG department and agency involved, based upon its spe

---

56 Admiral Harry B. Harris Jr., U.S. Navy Commander, U.S. Pacific Command, U.S. Pacific Command Posture, Statement Before the Senate Committee Armed Services (Feb. 23, 2016), http://www.armed-services.senate.gov/imo/media/doc/Harris_02-23-16.pdf?; General Philip M. Breedlove, U.S. Air Force General (Ret.), U.S. European Command, U.S. Forces Europe, Statement Before the Senate Armed Services Committee (Mar. 1, 2016), http://www.armed-services.senate.gov/imo/media/doc/Breedlove_03-01-16.pdf.

57 Admiral Kurt W. Tidd, U.S. Navy Commander, U.S. Southern Command, U.S. Southern Command Posture, Statement Before the Senate Armed Services Committee (Mar. 10, 2016), http://www.armed-services.senate.gov/imo/media/doc/Tidd_03-10-16.pdf.; General Lloyd J. Austin, U.S. Army Commander (Ret.), U.S. Central Command, U.S. Central Command Posture, Statement Before the Senate Armed Services Committee (Mar. 8, 2016), http://www.armed-services.senate.gov/imo/media/doc/Austin_03-08-16.pdf?; General David M. Rodriguez, U.S. Army Commander (Ret.), U.S. Africa Command, U.S. Africa Command Posture, Statement Before the Senate Armed Services Committee (Mar. 8, 2016), http://www.armed-services.senate.gov/imo/media/doc/Rodriguez_03-08-16.pdf.

cialized mission and capabilities, will work with a specific segment of society on cybersecurity development:

- DoD: Engage in military-to-military contact and training of civilian and defense authorities, conduct joint cyber exercises, share data on threats and remediation, and provide USG-cleared cybersecurity equipment, all of which should be in accordance with DoD Instructions and Directives (Leads: **Office of the Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, the Defense Security Cooperation Agency, Office of the Deputy Assistant Secretary of Defense for Cyber Policy, DoD Cyber Crime Center**).[58]
- DoS: Promote the signing and ratification of the CEC as the legal framework against cybersecurity, develop a common set of security practices and technology standards, and use private sector and NGOs to increase cybersecurity awareness in host nations and help solve cybercrime attacks (Leads: **Office of the Coordinator for Cyber Issues, Bureau of International Narcotics and Law Enforcement Affairs**).
- DoJ and DHS: Train foreign law enforcement agencies how to respond to cybercrime attacks, share up to law enforcement sensitive information on cybercriminals, and embed U.S. law enforcement personnel within foreign law enforcement agencies, vice versa (Leads: **FBI Cyber Directorate, ICITAP, DHS Office of Cyber Policy, Immigration and Customs Enforcement, U.S. Secret Service**).
- Department of Treasury: Work with financial institutions to improve internal cybersecurity measures, strengthen their relationships with domestic law enforcement agencies, and improve their technical expertise on the issue (Leads: **Office of Financial Institutions, Office of Terrorism and Financial Intelligence**).

After implementation, task forces will complete annual assessments, adjusting funding requirements as needed.

PART IV: Main Challenges to Proposed Plan

The following two questions represent the main challenges to the proposed plan:

Q1: How does this plan garner attention from senior leadership to devote resources?

58 *See* DEP'T OF DEF., DEPARTMENT OF DEFENSE INSTRUCTION 45-49 (2014).

The USG must prioritize its national security threats and the corresponding responses in a constrained budgetary environment. The danger cybercrime, as this paper defines, poses to the United States, writ large, is secondary, in that the money stolen can end up in the hands of terrorist organizations. Computer Network Attacks (CNAs) against critical U.S. infrastructure or defense systems can immediately threaten the United States. Thus, USG agencies are more willing to put in the time and resources necessary towards strengthening U.S. homeland defense than towards cybersecurity capacity-building internationally. However, this plan focuses on coordinating existing individual efforts by USG departments and agencies to fight cybercrime and physically centralizing them under a COCOM to deliver a more synchronized impact. For example, USSOUTHCOM is already "building cybersecurity and cyber defense capabilities with seven regional partners and working with Brazil, Peru, Colombia, and Chile to establish dedicated cyber defense commands or capabilities."[59] Additionally, the USG could outsource to reserve components of the U.S. military some of the manpower and technical support needed. Reservists with cybersecurity backgrounds could provide select remote services, such as testing hardware equipment, to the COCOMs for these capacity building activities.

Q2: With which developing countries would the United States partner?

Edward Snowden's 2013 revelations about the use of sensitive USG technology, specifically to collect intelligence on foreign leaders, impacted U.S. relations with other countries.[60] While the impacts from these disclosures may have lessened, some countries, especially those in the developing world, may still be hesitant when partnering with the United States regarding cybersecurity issues, fearing that U.S. intelligence agencies will target them. As a result, they may not want to share threat information from

59 Tidd, *supra* note 57.

60 Robert Nolan, *5 Undeniable Fallouts from the Edward Snowden Leaks*, U.S. News & World Rep. (Sept. 20, 2013), http://www.usnews.com/opinion/blogs/world-report/2013/09/20/brazil-russia-and-the-impact-of-edward-snowden-on-us-foreign-relations.

CNEs or CNAs, which would hamper the USG from assessing developing countries' capabilities and figuring how to address their cybersecurity gaps.[61] At the same time, the USG would only want to work with developing countries who are willing to develop the necessary legal frameworks to prosecute cybercrime and invest in the proper cybersecurity infrastructure.[62] These willing partners could then maintain whatever technical assistance or equipment the USG provided.

Thus, given the sensitivities behind data sharing and the commitment to cybersecurity required by developing countries, these tasks forces should focus on the most promising and U.S.-friendly countries within their respective AORs (i.e. U.S. Africa Command with Mauritius, U.S. Southern Command with Colombia) and strengthen those countries' cybersecurity capabilities so that they can export their successes throughout their regions. This approach towards building cybersecurity capacities of developing countries would mirror the outcomes of USG efforts to counter drug trafficking in Latin America. Here, the USG, through PLAN Colombia, has provided $10 billion since 1999 in training, equipment, and aid to combat drug trafficking in Colombia, whose government and military now advise, train, and offer material support to help their counterparts in Central and South American countries tackle this problem.[63] Additionally, the USG could work with the United Nations or other international organizations to broker cybersecurity partnerships. In general, developing countries would probably be more willingly to work on this issue with a country within their region or an unbiased and well-respected international institution than with the United States.

---

61 Lilly Pijnenburg Muller, Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities (2015), https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf.

62 *Id.*

63 Jim Wyss, *Plan Colombia: 15 Years Later Much has Changed, but Some Remains the Same*, Miami Herald News (Feb. 2, 2016), http://www.miamiherald.com/news/nation world/world/americas/colombia/article 58037878.html; Wesley Tomaselli, *Colombia's Security Export*, OZY Mag. (June 2014), http://www.ozy.com/fast-forward/colombias-security-export/31788.

PART V: Conclusion

Within the field of counterterrorism, the United States always needs to be one step ahead of terrorists. The USG shift towards CTF has adversely impacted terrorist organizations' operational capabilities. Over time though, terrorists have adapted and developed more convoluted ways of financing their operations. Shown by this paper, the USG once again has a crucial opportunity to be one step ahead of this adversary given that cyberspace is becoming more intertwined with daily activities and human interactions.

Contributors

Christopher Folk

Christopher Folk is a third-year student at Syracuse University College of Law. Christopher served in the Marine Corps, graduated from Cornell University with a B.S. in Applied Economics, attended Northeastern University's High-Tech MBA Program, received a M.S. in Computer Information Systems, and spent several years working in the high-tech field. Christopher externed with a cybersecurity firm after his first year at SUCOL.

Marc Barnett

Marc Barnett is an MAIR from the Maxwell School of Citizenship and Public Affairs and an MPP from the Hertie School of Governance. He is currently a researcher for Wikistrat in Washington, DC.

Andrew Foote

Andrew Foote has experience in national security policy as well as the private sector. He was an Intelligence Analyst with the FBI and later a Consultant at Deloitte Consulting's Federal Practice. He holds a Masters of Diplomacy and International Relations from Seton Hall and is currently pursuing his iMBA at the Whitman School of Management at Syracuse University.

Neil Noronha

Neil Noronha earned his B.S. in Foreign Service and M.A. in Security Studies from Georgetown University. From August 2014 to January 2017, he worked in the President Barack Obama Administration at the US Department of Defense and for the White House National Security Council staff.

Editor's Note

It came to our attention that a past issue of *JTSA* contained an article which had a portion not attributed to the author who wrote it. The article has been removed from the Journal's website. Our apologies to Dr. Peter Romaniuk, who was the author whose work was not attributed in a previous publication.

The Journal on Terrorism and Security Analysis

is sponsored by:

INSCT
INSTITUTE FOR NATIONAL SECURITY AND COUNTERTERRORISM SYRACUSE UNIVERSITY

SYRACUSE UNIVERSITY
Maxwell School
of Citizenship and Public Affairs

SYRACUSE UNIVERSITY
COLLEGE OF LAW