Journal of Socialomics

White, J Socialomics 2017, 6:2
DOI: 10.4172/2167-0358.1000201

Commentary OMICS International

Homeland Security and Cybersecurity

Richard White*

Department of Computer Science, University of Colorado, Colorado Springs, CO, USA

***Corresponding author:** Richard White, Department of Computer Science, University of Colorado, Colorado Springs, CO, USA, Tel: 7193603805; E-mail: rwhite2@uccs.edu

Rec Date: Feb 10th, 2017; **Acc Date:** Feb 23rd, 2017; **Pub Date:** Mar 01st, 2017

Commentary

Cybersecurity is essential to critical infrastructure protection, which is essential to homeland security, which is about safeguarding the United States from domestic catastrophic destruction. A coordinated cyber-attack on critical infrastructure could result in the worst catastrophe in US history. Three scenarios give rise for concern:

- Undermining the US Federal Reserve
- Causing two or more nuclear plants to simultaneously meltdown
- Shutting down the North American Electric Grid. None of these would be easy, but none of them would be impossible, and the consequences would be catastrophic.

The possibility that US critical infrastructure could become vulnerable to cyber-attack was first raised in a 1997 report by the Presidential Commission on Critical Infrastructure Protection [1]. Chartered following the 1995 Tokyo Subway Attacks, the Commission found US infrastructure physically sound, but expressed concern that Industrial Control Systems were becoming increasingly reliant on Internet technology, and could become susceptible to cyber-attack. In response, President Clinton issued Presidential Decision Directive #63 in May 1998 ordering critical infrastructure protection from both physical and cyber-attack [2]. PDD-63 became the framework for protecting the nation's critical infrastructure following 9/11, which itself was an attack on US transportation infrastructure. The 2002 Homeland Security Act made critical infrastructure protection and cybersecurity core missions of the new Department of Homeland Security [3].

Critical infrastructure protection and cybersecurity are the responsibility of the DHS National Protection and Programs Directorate. The NPPD Office of Infrastructure Protection works in voluntary cooperation with infrastructure owners and operators under the auspices of the National Infrastructure Protection Plan [4] to reduce infrastructure vulnerability through a continuous improvement program called the Risk Management Framework. OIP also maintains the National Infrastructure Coordinating Centre to maintain watch over the nation's infrastructure and coordinate Federal support should it become necessary. Likewise, the NPPD Office of Cybersecurity and Communications maintains watch over US cyber infrastructure from the National Cybersecurity and Communications Integration Centre. If it spots trouble, the NCCIC can call on two cyber emergency response teams: US-CERT and ICS-CERT. If requested, the ICS-CERT can deploy teams to assist owners/operators as needed. The fact of the matter, though, is that DHS response assets are few, and their ability to contains and solve problems limited. As with all infrastructure under its protection, DHS has little direct authority over any of it. Direct authority for protecting cyber assets resides with system owners and operators. The 1984 Counterfeit Access Device and Computer Fraud and Abuse Act makes it a crime to access a computer without permission from the owner/operator.

A 1986 amendment made it a further crime to distribute malicious code, traffic passwords, or conduct denial of service attacks [5]. Cyber-attack, according to the National Research Council is any "deliberate action to alter, disrupt, degrade or computer systems or networks or the information and or programs resident in or transiting these systems or networks" [6]. Cybersecurity is defined by DHS as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against the damage, unauthorized use or modification, or exploitation" [7]. In theory, cybersecurity is easy. All you must do is ensure confidentiality, integrity, and availability of a computer and its data. Confidentiality ensures that the system and data are not accessed by an unauthorized agent. Integrity ensures that the system and data are not corrupted by an unauthorized agent. Availability ensures that the system and data are always accessible when needed. These seemingly simple goals, though, are impossible to attain because computers are inherently stupid and fragile.

Computers are stupid because they are incapable of making value judgments regarding their actions and will perform as directed even if the consequences are catastrophic. Computers are also fragile because with any useful piece of software you don't know what you've got and have no way of finding out. According to a 2014 study, the two primary methods of cyber-attack are phishing and exploitation [8]. Phishing is a social engineering technique designed to fraudulently obtain names and passwords from authorized users. Exploitation takes advantage of software flaws to obtain access to a computer or its data. Quite simply, there is no cure for cyber-attack, nor does any present itself for the foreseeable future.

The nation's infrastructure is indeed vulnerable as predicted by the 1997 presidential report. To demonstrate the point, in 2007 the Department of Homeland Security and Department of Energy conducted Project Aurora whereby they issued commands over the Internet causing a baseline electricity generator to self-destruct [9]. In December 2016, the threat to electricity grids became more than a theoretical concern when Ukraine's capital Kiev was plunged into darkness from cyber-attack [10]. Moreover, the 2010 STUXNET attack against Iranian nuclear centrifuges proved that you don't have to be connected to the Internet to succumb to cyber-attack [11].

While there may not be a cure for cyber-attack, that does not mean our infrastructure must remain vulnerable to its threat. Changing technology, both evolutionary and revolutionary, may render critical infrastructure immune to the effects of cyber-attack. Microgrids are one such example. They partition the electricity grid into smaller segments incorporating their own generating and storage capacity, making it much harder for a local outage to cascade into a regional or

national one [12]. Passive safety features on nuclear reactors can make them less susceptible to attack. Several proposals, including the GE Economic Simplified Boiling Water Reactor, are fail-safe designs that will automatically shut down in the event of malfunction, either accidental or deliberate [13]. and in a March 2017 speech, Federal Reserve Governor Jerome Powell touted the potential use of blockchain technology to secure Federal Reserve transaction the same as they do bitcoin [14].

Ultimately, new and improved infrastructure technologies offer hope of escaping the cyber threat. In the meantime, cybersecurity remains essential to critical infrastructure protection, which is essential to homeland security, which is about safeguarding the United States from domestic catastrophic destruction.

References

1. President's Commission on Critical Infrastructure Protection (1997) Critical foundations: Protecting America's Infrastructure. Washington, DC: The White House.
2. The White House (1998) PDD-63, critical infrastructure protection. Washington, DC: The White House, pp: 63.
3. United States Congress (2002) Homeland Security Act of 2002. Washington, DC: United States Congress, pp: 107-296.
4. United States Department of Homeland Security (2013) National infrastructure protection plan. partnering for critical infrastructure. Security and Resilience. Washington, DC: United States Department of Homeland Security.
5. United States Congress (1986) Computer fraud and abuse act. Washington, DC: Government Printing Office.
6. National Research Council (2009) Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities. Washington, DC: Computer Science and Telecommunications Board.
7. United States Department of Homeland Security (2017) Explore terms: A glossary of common cybersecurity terminology. National initiative for cybersecurity careers and studies. United States Department of Homeland Security.
8. Centre for Strategic and International Studies (2014) Net Losses: Estimating the global cost of cybercrime. Santa Clara, CA: McAfee, Intel Security.
9. North American Electric Reliability Corporation (2010) High-Impact, Low-Frequency Event Risk to the North American Bulk Power System. Atlanta, GA: North American Electric Reliability Corporation.
10. Reuters (2017) Ukraine's power outage was a cyber attack: Ukrenergo. Technology News. [http://www.reuters.com/article/us-ukraine-cyberattack-energy-idUSKBN1521BA]. Accessed on: March 31, 2017.
11. Kerr PK, Rollins J, Theohary CA (2010) The stuxnet computer worm: harbinger of an emerging warfare capability. Washington, DC: Congressional research service. R41524.
12. Centre for the Study of the Presidency and Congress (2014) Securing the U.S. Electrical Grid. Washington, DC: Centre for the study of the presidency and congress.
13. Ragheb M (2015) Inherently Safe Reactors Designs.
14. United States Federal Reserve (2017) Board of governors of the federal reserve system speech by governor Jerome H. Powell: Innovation, technology, and the payments system. United States Federal Reserve.