Student Name

Dr. Rick White

CS 4950 Homeland and Cyber Security

The 2015 Ukraine Blackout: Implications for Cyber Homeland Security in the U.S

The concept that the immaterial domain of cyber can influence the material world has always only been a theoretical possibility subject to the whims of imaginative fictions. However, recent events, beginning with the 2010 Stuxnet attack, have illuminated the reality of cyber attack's capability to affect the real world. The implications of this realization are severe, especially when considering the impacts on key national infrastructures. One of the largest concerns is the scenario where the US electric grid is attacked. While, at this time, an attack on the US electric grid is mere speculative concern, the all too real potentialities and consequences were demonstrated "On 23 December 2015, [when] a synchronized and coordinated cyber-attack compromised…Ukrainian regional electric power distribution companies" (Liang et. all). By studying the avenues of attack, current situation, and future implications, and comparing them to the current situations and potential impacts in America, specifically regarding the protection of key critical infrastructures such as the power grid, one can come up with scenarios to prevent and protect from similar attacks or plans of action to respond and recover given the eventuality of an attack.

According to Trivellato and Murphy, the 2015 Ukraine blackout can be broken down into three sections: malware, denial of service (DDoS), and the physical opening of substation breakers. The malware component was a BlackEnergy based trojan called KillDisc which allowed attackers access to the Supervisory Control and Data Acquisition (SCADA) systems of

several Ukrainian energy providers to rewrite the memory allocated for the master boot record, effectively ruining any attempt of a software reboot of the system. While hijacking the SCADA system, the attackers flooded the call center to prevent customer reports of the problem to reach the energy suppliers. Between the two, this allowed the attackers means to enter the SCADA systems from the outside to physically open the substation breakers, effectively cutting power for several hours in Ukraine. The breakers had to be manually closed, and Ukraine remains in a state of heightened threat level for fear of remnants of the first attack and threats of future ones (Trivellato and Murphy). Carlsson and Gustavsson credit to the Russian hacking group *Sandworm*, which has been known to utilize BlackEnergy and KillDisk software in the past. The theory that the Russians are behind the attacks is supported by the political climate between Russia and Ukraine since the downfall of the Soviet Union and by the fact that that there have been further Russian backed attacks on key Ukrainian cyber based infrastructures through 2016 and 2017 (Carlsson and Gustavsson).

Current events have shown that the impact of the 2015 Blackout and further attacks have been more psychological than physically damaging. Arguably, the true importance of the persistent cyber fire from Russia from the perspective of the Ukrainians is the understanding that they are unwilling participants in a form of hybrid warfare (Plėta, Karasov, and Jakštas). In response to the unexpectedly powerful and persistant threat, the Ukrainian government is attempting to place implicit understandings of cyberattacks on key national infrastructure into their legislations. The hope is that decisions "regarding the provision of cybersecurity of [Critical Infrastructure(CI)] is directly proportional to the level of effectiveness of the response to cyber threats, their timely detection, prevention and localization in the case of cyberattacks on CI" (Plėta, Karasov, and Jakštas). This would be done by legally enforcing security measures on

identified critical infrastructures and, in the case of an uncaught attack, identify which group is responsible for recovery efforts. This is a good step towards the protection of the nation of Ukraine, but, as Plėta, Karasov, and Jakštas conclude, it is important that further steps are taken to protect Ukraine, not just on the national level, but the international level.

The future for Ukraine undoubtedly contains more cyberattack on critical infrastructures. It is better, faster, and cheaper than accumulating and risking physical resources to target the same objective. This fact is not only applicable to Ukraine, but to any national power utilizing computer systems to control key pieces of their infrastructure that has cyber capable adversaries. In fact, one of the current beliefs among cyber security professionals is that Ukraine has become a live testing ground of cyber weapons in preparation for attack on other developed countries. (Carlsson and Gustavsson). This means that the software and hardware exploits seen in the Ukrainian theatre has the potential to be prevalent in attacks on other nations. One of the future steps for both Ukraine and other cyber capable nations such as the US should be to enforce regulatory standards on the software architectures being used in CIs. Khan et all suggest architecture changes to prevent against Black Energy attacks on synchrophasor based systems through exploitations in connected systems, especially related to systems directly connected to the US electric grid such as the nascent Smart Grid. These suggestions refer to the implementation of black/white IP lists, event monitoring, implementing end to end encryption, eliminating remote accesses to Phasor Measurement Units (PMUs), and protocol specific strategies that monitor and report suspicious network traffic. Beyond these preventative measures, it is essential to develop strategies and resources given the eventuality of a successful cyberattack on key infrastructure taking out not just one, but multiple CIs in concert.

The topic of the 2015 Ukraine Blackout and the continuous cyberwarfare that followed is important to analyze in the context of its implications, especially when considering its effect on homeland and cybersecurity in the US. The successful 2015 attack should carry the same worldwide awakening to the destructive potential of cyber as the 1995 Tokyo Subway attacks did in introducing the capabilities of non-nation-state actors to inflict cataclysmic harm. In both the case of the 2015 Ukraine Blackout and the case of the 1995 Tokyo Subway attacks, the impact in terms of disasters was relatively small. However, 1995 was a harbinger of the event 6 years later, September 11th, 2001. To prevent the vicious cycle of history, rather than breathing a sigh of relief that the attack happened to someone else, the world needs to take 2015 as a warning shot for the eventuality of catastrophic simultaneous attack via cyber on key national infrastructures. At this point, it is important to note that cybersecurity is not being blatantly ignored, especially in the US and, now, Ukraine. However, the question that should be asked is this: are the prevention measures and responsive protocols being put into place enough to safeguard a nation from a truly cataclysmic concerted attack? The purpose behind choosing this topic for research is an effort to respond to that question. It is essential that the history and current research becomes readily available, to any individual pursuing a career in a technological field so that those individuals can shape the future of security and disaster response. While this is an exceedingly obvious fact for those pursuing education in cyber security, from the standpoint of software and systems engineers, and even mechanical and aerospace engineers, it is important to emphasize that security is something built from the ground up, in all aspects of a system, especially including system-human interactions and the unhappy edge use-cases. Wrapping secure networks and protocols around secure software and hardware leads to inherently more secure products. Furthermore, knowing that these inherently secure products are

still fallible to attacks and redundant capabilities and manual overrides are necessary for disaster reducibility is essential to understand. At this time, the only theoretical concept related to cyber that belongs in fiction is the idea of a truly infallible, unbreakable system design.

Works Cited

Carlsson, Anders, Gustavsson, Rune. "The Art of War in the Cyber World," *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 42-44. doi: 10.1109/INFOCOMMST.2017.8246345

Khan, R., Maynard, P., McLaughlin, K., Laverty, D., & Sezer, S. (2016). "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid".*4th International Symposium for ICS & SCADA Cyber Security Research* 2016 (pp. 53-63). BCS. DOI: 10.14236/ewic/ICS2016.7.

Trivellato, Daniel, Murphy, Dennis. "Lights out! Who's next?". *Security Matters*. February 2016. URL: tranzilla.ru/media/uploads/profile/1437/6281/a5c9/d62d/a8c8/3bfa/7a10/c7cb/b3fe/3758/939f/f494/c56b/2ef6/9b12/e978/whitepaperukraineen.pdf.

Plėta, T., Karasov, S., Jakštas, T. 2018. "The Means to Secure Critical Energy Infrastructure in the Context of Hybrid Warfare: The Case of Ukraine", *Journal of Security and Sustainability Issues* 7(3): 569–579. http://doi.org/10.9770/jssi.2018.7.3(16)x.