Old Dominion University

Can America Protect Critical Infastructure From Cyber-Terrorism?

Timothy Klein

IDS300W

Dr. Pete Baker

December 14th, 2022

Can America Protect Critical Infastructure From Cyber-Terrorism?

Computerized systems are the backbone of which modern civilization is built and operated upon. These systems operate in a separate dimension of time where in one second thousands, if not millions of signals are received, analyzed, and actions taken. Since these complex systems operate with such high capability it allows for the technologically advanced modern society in America today. However, computer technology is a tool and like any tool has the propensity to be used for both constructive and destructive purposes. Given the importance and necessity of computerized infrastructure it also creates a direct target for cyber terrorism. While conventional terrorism focusses on physical targets, cyber terrorism employs malicious computer techology rather than just pure force (Gross, M. 2017). The more critical a system, the larger a target it is for cyber terrorism. This being the case, the fields of energy, telecommunications, healthcare, and manufacturing are most often targeted to cause as much disruption as possible. Even a single breach can potentially affect millions of people causing psychological harm or possibly even physical peril as people are shut off from services needed to survive.

Protecting critical infrastructure remains a key priority as a matter of national security. Yet how to provide such protection is a work in progress. Since technology is constantly being developed it means the field of cybersecurity must be adaptive at the core as new exploitation methods or friendly securities technology are being implemented daily. Also while infrastructure has always been a component of civilization the computerization of it is relatively new meaning the only historical examples lie in recent history while the consequences are still being played out in the current era. Educational literacy on the subject of cybersecurity and safe cyber practices must become a priority within academia as the breakneck pace of technological

advancement demands immediate action to provide for the defensive needs of today. By combining workable knowledge within the field of actual protection, cybersecurity, studying how the course of politics shapes the future of technology , and observing the economic impacts which a potential successful cyber attack could cause, it can be determined whether it is possible for these systems to be safeguarded against exploitation.

To understand prevention of cyber terrorism it is necessary to first understand why and how it occurs in the first place. In World War II there were massive military operations conducted on both the Axis and Allied sides in the conflict which aimed to destroy what was considered critical infrastructure necessary for the country's ability to wage war. In current times the same types of infrastructure are attacked remotely in a completely different manner “it is important to understand the unique dimensions of the cyber space. Since the cyber space environment is not limited by any conventional boundaries or borders, clandestine cyber attacks can be carried from thousands of miles away at unbelievable speeds”(Albahar, M. 2019). Attacks can be launched from anywhere in the world making it far simpler to access the potential target. It also no longer takes entire armies or groups of highly trained special forces to damage the critical lines in a country, all it takes is a laptop and an internet connection. The threshold for what is needed to commit an act of cyber terrorism has become dramatically low allowing for near constant attacks to be made against defensive systems, searching for exploits to gain access and/or control. The math unfortunately works in the favor of cyber crime, low cost, small chance of location detection due to VPNs(Virtual Private Network), minimal training for attackers needed, and the possibility of destruction on an incredible scale. All the factors fall into line which make cyber terrorism a pragmatic method for bad actors. The benefits of applied technology are massive but come with a heavy compromise “the tradeoff comes in the form of

the increasing vulnerability of major installations to such attacks."(Albahar, M. 2019). The sheer scale of cyber attack potential reveals the reason such strong moves are needed in order to prevent cyber terrorism. As a society it is known to value physical assets and their protection like pipelines, nuclear power facilities, and data centers yet public awareness is not on the most vulnerable yet accessible part of the system, its cyber security.

While in order to conduct cyber attacks the bar of entry is very low the defensive side needs much more nuance "Real-world cyber security problems have technical, organizational, diplomatic, strategic, economic aspects."(Gheorghe 2017). Cyber defense is far from a one-act-show, it takes a coordinated team of professionals from many fields in order to correctly execute an effective defense plan. It must be viewed from multiple perspectives as the knowledge needed to act and the results of either success or failure impact so many. Politically the actions taken can have severe implications as cyber attacks, if traced back to its perpetrator, can be considered acts of war and retaliated against. Many times cybersecurity will be viewed through an economic lens. The two fields have many similar problems and thus are consistently merged as those with economic backgrounds find themselves in cyber security doing risk analysis (Gheorghe. 2017). This combined approach is known as "Economic Intelligence" as the need for the cross-disciplinary capabilities is enough where a merged field is developing.

When the computerization of infrastructure operations began it was typically reliant on PCSs (Process Control Systems) and SCADA (Supervisory Control and Data Acquisition) which controlled everything from essential manufacturing to generating electricity at power plants (Gheorghe 2017). These were systems which would typically be air gapped from outside connection and their Human Machine Interface (HMIs) were guarded as those would allow operation of the system. While generally safe from outside attacks over the Internet the trade off

was that these systems had an exploit in their main control systems (Oliveira, D. 2010). As development has continued there has been a shift to Commercial-Off-The-Shelf (COTS) hardware which is run by mainstream operating systems which unlike SCADA systems connect to other industry networks allowing for them to communicate with each other (Gheorghe 2017). This allows for extremely fluid communication between a great variety of infrastructure systems but creates a large network to be able to attack and exploit. When infrastructure systems are connected the current approach blends the different sectors together until they are almost one united system rather than many separate ones. Given the large nature of both the scale of system networks and the range of areas to be attacked, cybersecurity teams are constantly creating patches to their portions of the system to defend against new exploits which are ever evolving in nature. Economically this approach yields great benefits as it is the basis for the globalization of commerce and industry. Even though the method continually raises the stakes on the potentially catastrophic outcome the results are deemed worth it. There has been significant development put into cybersecurity as a long term investment to the prevention of future threats. Politically there seems to be a gamblers approach to the current interconnected system of infrastructure. It is necessary for the expansion of the economy but should an act of cyber terrorism occur under the watch of a politician or their party they could be held responsible for not enforcing greater cybersecurity measures since it is the essential duty of the government to protect United States infrastructure.

The current era of cybersecurity and specifically what the potential threat to physical infrastructure is was defined in 2010 when the Stuxnet virus was discovered. Stuxnet was a malware which is largely believed to have been developed by American and Israeli intelligence services in order to disrupt Iran's nuclear development program. Specifically within that program

Stuxnet targeted the centrifuges which spin incredibly fast to process Uranium-238 to Uranium-235 which is the specific element used in nuclear bombs (Farwell, J. 2011). Stuxnet was designed to infiltrate an air-gapped network which means a network which is completely separate from the internet and other local connections. This malware was designed to spread from machine to machine extremely easily and once launched it was hands off from there. Stuxnet infected its way through the uranium enrichment laboratory's network until it found the control code to the motors for the centrifuges and simply had the voltage change erratically causing the centrifuge to over spin and sometimes underspin causing major damage to the centrifuges which set Iran's nuclear program back an estimated 2 years (Farwell, J. 2011). Once Stuxnet was discovered the world began to realize that a virtual malicious code had the ability to cause destruction and disruption even within a network which was designed against such threats. It showcased the fact that while a computerized system can yield the benefits of something as complex as nuclear fission the systems are inherently exploitable despite major precautions. Politically Stuxnet seemed to achieve only more hostile relations from Iran towards America and Israel. It set a precedent which would be difficult to take back. While the attack was not aimed at causing any harm to individuals it showed the ability to strike at an adversary virtually to operate within the gray zone of conflict. Showcasing the vulnerabilities of physical infrastructure also created an even larger target as global attention was brought to Stuxnet and what future malware may be capable of. While cyber attacks are not a matter of If but of When the specific target of cyber terrorist groups is debated amoung industry professionals "Clarke, a former national security advisor to the U.S. government states that if under any circumstances a terrorist organization decides to launch a cyber attack against the United States it will most probably be an intent-based attack directed towards the financial institutions and any damage to infrastructure

or loss of people's lives will be secondary events"(Albahar, M. 2019). However this is in direct contrast to developments of malware specifically designed to harm individuals. The Central Scientific Research Institute of Chemistry and Mechanics in Moscow created a destructive piece of malware called the Triton or Trisis which was used against a chemical plant in Saudi Arabia. Thankfully the would be cyber terrorists tripped an internal software safeguard while attempting to hack into the system but when the safeguard was alerted the whole plant shut down (Nakashima, E. 2020). The outcome would have been terrible as the intended effect was to have the plant go critical and cause an explosion which may have killed dozens at least. While this was not an attack against the United States directly, iterations of that malware have since been found attempting to exploit domestic infrastructure. Politically the development of the Triton malware was significant as it represented a direct, premeditated attack against the United States and its allies from Russia. Many times attacks from one nation state against another are conducted by use of proxies but the blatant nature of Russia crafting the malware for use against Western powers raised both tensions and the stakes of cyber conflict. Economically the Triton attack "resulted in tens of millions of dollars in lost production" (Nakashima, E. 2020). Considering the attack was not fully realized the potential for economic impact was much higher.

While predictions of which specific areas may be focused for an attack the reality is a major exploit into critical infrastructure systems may result in damage which impacts not just the financial sector but also the population's ability to access systems necessary for survival. Due to the interconnected nature of infrastructure no attack outcome would be confined to one specific field. To use the 2017 cyber attack on the Saudi chemical plant as an example, should the attack have been successful, the state of politics, lives of those in proximity, and the economy would have been disrupted in major fashion. When it comes to cyber terrorism the impact can be

difficult to fully calculate as the scope of consequences encompasses such a wide range. Due to the complexity of infrastructure networks each exploit must be analyzed as it is discovered and handled with immediacy. However this leaves a system which survives on a series of patch work solutions rather than any form of comprehensive protection. It is not due to inadequate performance of the multidisciplinary teams which protect these networks but the reality of the constantly evolving world of cyber operations. Technology is designed and implemented faster than the collective understanding of its long term effects. Economically technological progress is far too valuable to hold back and study so it is used with immediacy. Politically it is tied in with economic motivations but with the added layer of competition between countries and the protective need to stay ahead.

Infrastructure as it expands and modernizes becomes an ever larger target for cyber terrorism to exploit. The interconnection of the computerized systems which run the essential processes needed for stability within the country also means there will always be an alluring target for cyber terrorist to exploit. Given how simple the logistics are to attack infrastructure and how accessible they are with the Internet the networks which operate the crucial systems relied upon by millions are on near constant assault. The methods, techniques, and technology used in this cyber offensive are always changing, looking for new exploits in the armor of the cybersecurity defenses. The United States cannot provide absolute protection against cyber terrorism due to the near countless attempts being made to penetrate those protected networks. Eventually attacks get through and cause damage until the exploit can be patched and the vulnerability studied. By keeping an adaptable outlook and keeping a pulse on the economic and political structures which govern the direction cybersecurity takes, the infrastructure of today is protected to the best of the country's ability to provide it and developing the hope of more

comprehensive solutions in the future. It is impossible to know where the next threat will occur so the process must be one of continued education, learning from each situation to ensure the protection of the foundations of societal operation. With technology as the constant tool of progress it will ever come with the dual potential for disaster.

References

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics, 25*(4), 993-1006. https://doi.org/10.1007/s11948-016-9864-0

Farwell, J., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival (London), 53*(1), 23-40.

Gheorghe, Tatar, Gokce, Gheorghe, Adrian V., Tatar, Unal, Gokce, Yasir, & ProQuest. (2017). *Strategic cyber defense. A multidisciplinary perspective.* (NATO science for peace and security series. Sub-series D, Information and communication security ; ol. 48). Amsterdam, Netherlands: IOS Press B.V.

Gross, M., Canetti, D., & Vashdi, D. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity (Oxford), 3*(1), 49-58.

Lonsdale, D. (2020). The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios. *Journal of Military Ethics, 19*(1), 20-39.

Nakashima, E. (2020). U.S. sanctions Russian lab that built what experts say is potentially the world's deadliest hacking tool. *The Washington Post*, p. The Washington post, 2020.

Oliveira, D. (2010). Cyber-terrorism & critical energy infrastructure vulnerability to cyber-attacks. *Environmental & Energy Law & Policy Journal, 5*(2), 519.

Yaokumah, W. (2020). Predicting and Explaining Cyber Ethics with Ethical Theories. *International Journal of Cyber Warfare and Terrorism, 10*(2), 46-63.