INFRAGARD

JOURNAL

Winter 2020 - Issue 3, Volume 1

Critical Infrastructure & the Emerging Market for Domestic Terrorism

Maggie O'Connell[1]

Abstract:

This paper examines the modern threat landscape to critical infrastructure in the context of the existing legal framework for domestic terrorism. The United States has developed a conceptual understanding of terrorism perpetrated by foreign individuals and groups, but homegrown actors, many of whom have no clear ties to violent jihad, are increasingly prevalent, sophisticated, and misunderstood. Domestic terrorists are capitalizing on emerging, lesser known attack vectors, including insider access, cybersecurity breaches, and drones. This burgeoning market for terrorism requires a more holistic legal and regulatory approach to ensure our nation's critical infrastructure asset owners and operators are empowered to defend against these threats, and that federal investigative and prosecutorial bodies can effectively respond.

Keywords: Domestic terrorism, critical infrastructure

CRITICAL INFRASTRUCTURE ASSET OWNERS and operators are no strangers to the threat landscape in which their facilities reside.[2] Companies invest millions of dollars annually to secure their fencelines, patch their cybersecurity vulnerabilities, and develop protocols and procedures to comply with regulations seeking to mitigate and prevent terrorist activity. The safety and security of facility operations, personnel, and the surrounding communities are the goals of these investments, and critical infrastructure companies cannot afford to shortchange in any of these areas. Nevertheless, the threat landscape often evolves so quickly that the legislative and regulatory frameworks fall vastly behind the curve. The nation becomes the victim of a divisive political climate, a lack of understanding, and a general distrust for big corporations. What remains is a door wide open to nefarious actors and emerging threats, the vast majority of which are not yet completely understood nor accounted for in the law.

Although guns, guards, and gates are still the first lines of defense along a fenceline, they can provide a false sense of security. In February 2016, two airport employees in Somalia facilitated the transfer of a sophisticated bomb built into a laptop through airport security, where it was carried onto plane and detonated (Kriel and Cruickshank, 2016). Malware stormed the Ukrainian industrial control systems (ICSs) in 2015, 2016, and again in 2017, the latter effectively shutting down the government and key critical functions, including the radiation monitoring system at the Chernobyl nuclear power plant (Greenberg, 2018). In September 2019, a series of drone attacks at Saudi Aramco oil processing facilities in Abqaiq and Khurais in eastern Saudi

[1] Regulatory Affairs Specialist, American Fuel & Petrochemical Manufacturers Association, moconnell@afpm.org 1800 M Street NW, Suite 900 North, Washington, D.C. 20036

[2] The Department of Homeland Security (DHS) Cyber and Infrastructure Security Agency (CISA) outlines "16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (DHS 2019a).

Arabia forced the country to shut down half of its oil production capacity, to the tune of 5.7 million barrels per day (Li, 2019). This attack was a major blow to both the country and the global markets. Meanwhile, extremist environmental justice activists are turning pipeline valves, potentially causing harmful spills, injuries, and catastrophic explosions that could cripple the very communities they seek to protect (Williams, 2016).

Although some of these examples did not occur in the United States by homegrown actors, they all could have, and these are real cases of activities that skirt existing U.S. laws and regulations intended to safeguard critical infrastructure from domestic terrorist activity. Currently, U.S. critical infrastructure owners and operators have little-to-no recourse when it comes to such threats. The nation must understand that homegrown violent extremists (HVEs) are capable of carrying out attacks previously perpetrated by foreign-born terrorists. A reactive approach to terrorism does little to thwart the threat, and near misses can very quickly turn into hits without the proper statutes in place to give relevant authorities the license to enhance their pre-attack intelligence gathering and investigative efforts. There must be accountability in the legal and regulatory framework to investigate and prosecute those persons who tamper with, attack, and threaten any critical infrastructure operation in the United States.

Understanding Domestic Terrorism

The concept of domestic terrorism in the United States is complex. Domestic terrorist activities are often understood as mass shootings at soft targets and crowded places, and certainly qualify as terrorism. However, this only represents one aspect. As the lead agency for investigating terrorist activity, the Federal Bureau of Investigation (FBI) classifies domestic terrorism as U.S. persons who commit criminal acts based on their "political, religious, social, racial, or environmental" ideologies, rather than for monetary purposes (FBI, 2019). This definition illuminates an important component of domestic terrorism that is often understated in the context of threat analysis: a criminal act does not need to result in mass casualties to be investigated as an act of terrorism. From a prosecutorial standpoint, the Department of Justice (DOJ) views domestic terrorism as activities that:

(A) involve acts *dangerous to human life* that are a violation of the criminal laws of the United States or *of any State*;
(B) appear to be intended –
  (i) to intimidate or coerce a *civilian population*;
  (ii) to influence the policy of *a government* by intimidation or coercion; *or*
  (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; *and*
(C) *occur primarily* within the territorial jurisdiction of the United States [emphasis added] (18 U.S. Code § 2331.5)

Given this broad definition, there is no single crime of "domestic terrorism." Gaps exist in the federal statute and are ripe for exploitation, particularly via emerging threats. Although a person or group involved in a targeted attack will not escape prosecution, the charge may not fall under the *federal* terrorism statute. State criminal laws offer some avenues for penalizing terrorist activity, but punishments vary greatly state-to-state.

Chapter 113B of Title 18 of the U.S. Code remains the federal statutory guide for terrorism, but the crimes described therein are somewhat limited to foreign terrorism in that many require a

transnational or foreign element in the fact pattern. Although a few can apply to domestic terrorist activity – most notably through an interstate commerce element – the language in these statutes do not effectively capture emerging threats. They cover the use of traditional explosives or assume that lone actors and small, very loosely coalesced groups cannot easily rise to the level of active terrorists. In today's threat landscape, such assumptions create an environment in which terrorists can use emerging technologies and techniques to maximize devastation with limited effort and at minimal cost.

Emerging Threats

Over the last several decades, domestic terrorists have targeted critical infrastructure to advance political or social justice agendas. However, some maintain that domestic terrorists lack the organizational capacity and technical wherewithal to accomplish any meaningful attack on critical infrastructure (Riedman, 2017). This argument is myopic. Although it is true that the number of successful attacks against critical infrastructure in the United States is historically small, it is not prudent to rest on our laurels with respect to the nation's critical functions.[3] A successful attack need not be from a formally organized group. In fact, the FBI notes that current threat actors are typically "autonomous and lone offenders, and small cells pose the greatest threat" (McGarrity and Brzozowski, 2019). Evolution and access to technologies, open markets, and the dark web make homegrown terrorists just as organized as the international groups traditionally associated with terrorist activity. Earlier this year, Assistant Director of the Counterterrorism Division at FBI, Michael McGarrity, noted domestic terrorism is "on the rise" (Levine, 2019). Indeed, three factors actively contribute to the growth and evolution of this threat landscape according to the FBI: the internet, use of social media, and HVEs.[4]

In 2018, the FBI investigated 50 reported incidents, threats, or suspicious activity at pipelines alone (McGarrity and Brzozowski, 2019). In that same year, the FBI investigated 87 reported threats to refineries (McGarrity and Brzozowski, 2019). These are real, credible threats. In fact, on September 19, 2019, a federal grand jury returned an indictment charging two women with knowingly and willfully damaging and attempting to damage the Dakota Access Pipeline, causing "a significant interruption and impairment of a function of an energy facility" (DOJ, 2019a). The women made no secret of their efforts to sabotage the pipeline to advance a political agenda, by burning exposed valve sites and attempting to pierce portions of empty pipeline with torches (Schiano, 2019). These acts are dangerous to human life, in violation of the laws of the country and state, and are intended to influence the policy of the government. However, there is no mention of domestic terrorism in the indictment because the federal terrorism statute does not account for these types of attacks. Prosecutors must instead rely on other criminal laws to charge offenders - most of which carry far more lenient sentences.

Although these women operated as part of a larger extremist environmental justice movement, lone or small cell insider threats are another increasingly significant concern in the security space. Apart from a disgruntled employee carrying out a devastating, mass casualty attack on facility property, insider threats can take the form of economic espionage, cyber hacks, and –

[3]"Critical functions" is a term used by DHS CISA, and is defined as: "The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (DHS, 2019b).

[4] Currently, the FBI is investigating suspected HVEs in every state and view HVEs as a primary terrorism threat in the U.S. The FBI defines an HVE, in part, as someone who "receive[s] no individualized direction from terrorist groups" (FBI, 2019).

for these purposes – actions that cause or can cause catastrophic physical damage to facility assets and systems. In December 2013, a former avionics technician entered a secure gate at the Wichita airport using a valid employee access card and attempted to detonate a car bomb. He later pled guilty to one count of use of a weapon of mass destruction – a federal terrorism charge – only because his well-documented ties to violent jihad very clearly revealed a transnational element in the fact pattern of the case (DOJ, 2015).

Now imagine the following scenario: the largest refinery in the United States at Port Arthur, TX undertakes a turnaround to repair a major process unit. In these instances, the regular permanent staff of approximately 1,450 might double to include contractors, temporary help, and outsourcers. A turnaround is a major security risk in and of itself. The regulatory framework exists to help mitigate these risks through certain measures within the Department of Homeland Security's (DHS) Chemical Facility Antiterrorism Standards (CFATS) and the Transportation Safety Administration's (TSA) Transportation Worker Identification Card (TWIC) system, but there are significant flaws in both of these programs.[5] Even so, one contractor with a hidden political agenda whose background check failed to detect any terrorist affiliations or criminal history, with authorized temporary access to a refinery or chemical facility's operational technology (OT) could, with relative ease, facilitate a devastating event that does not involve an explosive device like a car bomb. Such a situation may seem unrealistic, but it is not. Although asset owners and operators do their best in good faith to comply with regulations to manage these security and safety risks, the sheer volume of employees in large turnaround-type situations creates a statistical advantage for the lone assailant. Nonetheless, depending upon the type of attack, such as disabling OT controls to cause a noxious chemical leak versus use of an improvised explosive device, the crime itself may not be prosecuted under federal terrorism laws.

As illustrated, just one person can cause an incident at a critical infrastructure facility, and this is particularly true for cyberattacks. The Department of Energy (DOE) and DHS are actively conducting outreach to educate stakeholders on the ramifications of cyber intrusions on physical security and safety. It is well known that hackers can steal sensitive data with relative ease (Yahoo, 2013 and 2014; Target, 2013; Marriot, 2018; Facebook, 2019; Capital One, 2019; Ecuador, 2019, among others), and remarkably, these reported data breach incidents are occurring with increasing frequency. In addition to sensitive data, a hacker can also access and manipulate ICSs in the United States. A couple of young computer scientists readily demonstrated this by hacking into a 2014 Jeep from more than 10 miles away and remotely taking over the controls (Greenberg, 2015). Certainly, a nuanced hacker with targeted phishing campaigns to a facility's third party suppliers knows how to capitalize on that access to open gates, shut valves, and bridge both the information technology (IT) and OT systems so it becomes possible not to recognize that an attack is occurring until an explosion happens.

Cyberattacks are such a powerful tool that they are increasingly used as part of the United States' military strategy (Schneider, 2019). Still, given that the U.S. is inextricably tied to the global communications infrastructure, the nation's own vulnerabilities are countless. In the critical infrastructure world, companies work tirelessly to uncover and correct these vulnerabilities before they are exploited. Even so, cybersecurity cannot really be guarded by prescriptive regulations

[5] Chief among these concerns is the failure of distinct government agencies to understand these regulatory programs and their risks. For example, a 2019 Department of Justice Office of Inspector General Report noted that 214 terrorist watchlisted individuals applied for a TWIC through FBI between 2006-2017, and some were issued. The TWIC is required by law for unescorted access to secure areas on ports and docks, which many critical infrastructure facilities have on site (DOJ, 2019b, 10).

because innovation is stifled and adaptation in response to new attack vectors is limited. Technologies spread quickly. Within the last 40 years, the world shifted from mainframes to desktops to laptops to mobile devices, then the cloud, and now the "Internet of Things" (Danzig, 2014, 2018). Terrorists, domestic and foreign, exploit these rapid advancements. Acting Director of National Intelligence (DNI) Joseph Maguire recently called attention to this very issue, observing that: "At one point in time, you had to be a sovereign nation to have this kind of technology, but with the proliferation of technology and with the global economy, much of it is now easy to acquire and simple to use" (Cruickshank and Dodwell, 2019, 2011).

Not only is cyberterrorism challenging to attribute, but it is not defined anywhere in the federal criminal code. This is a recognized problem, both for purposes of understanding what constitutes cyberterrorism and for prosecuting offenders. Acting DNI Director Maguire continues, "[Terrorists] use the internet and encryption to a great extent. They understand technology. We are a technological nation, and we have to make sure we understand the problem set and not be reactive but be anticipatory to what they're going to do" (Cruickshank and Dodwell, 2019, 12). As cyberattacks continue to increase and become more sophisticated, safeguarding against cyberterrorism is no longer exclusively a matter of ensuring that private industry is equipped with the appropriate tools to mitigate the risks. The government must assure its citizens, as well as the owners and operators of critical infrastructure assets, that those who perpetrate cyberterrorism are held accountable.

One final emerging threat to critical infrastructure that is increasingly worrisome is drones. The potential safety hazards and security threats presented by errant or malicious unmanned aircraft systems (UAS) activity and the evolving tactics used by hostile operators are provoking a growing number of efforts by public and private sector entities to address these risks. Not only can drones drop explosives and hazardous substances, but they can also be equipped with weapons, conduct unauthorized surveillance, aid hackers in overcoming physical barriers, and act as kamikaze agents for nefarious actors.

The potential for UAS activity to inhibit or halt operations at critical infrastructure facilities is known, as evidenced by recent disruptions to operations at Gatwick Airport in the United Kingdom (December, 2018), Newark Liberty International Airport (January, 2019), and most recently the attacks on Saudi Arabian oil and natural gas infrastructure (September, 2019). At the root of the challenges with UAS activity is the absence of a meaningful regulatory and legal framework.[6] While a catastrophic act performed by a drone could potentially warrant a terrorism charge against the operator, critical infrastructure owners and operators are severely restricted in their ability to defend against these emerging technologies, creating an enormous security and safety risk for assets and personnel.

Although the majority of documented incidents stem from the group of UAS operators categorized as "careless or clueless," there are operators with potential criminal intent. Like the regulatory hurdles that limit response to the careless and clueless, the current legal framework also poses significant challenges for authorities' response to criminal operators. Indeed, there are

[6] Remote Identity (ID), like a license plate on your vehicles, is a foundational regulation needed for technological solutions to work and the basis for other important rulemakings. Unfortunately, the regulation has been delayed multiple times by the United States Federal Aviation Administration (FAA), and was recently relayed to the White House's Office of Information and Regulatory Affairs (OIRA) for interagency review. Providing the critical infrastructure community, law enforcement, and government with a key tool that can identify and distinguish authorized UAS from those that may pose a safety or security threat greatly advances their ability to respond to and prevent potentially hazardous situations.

numerous provisions in Title 18 that preclude critical infrastructure owners from engaging in UAS detection and mitigation activities including the Wiretap Act (18 U.S.C. §2511), the Pen Register Act (18 U.S.C. §2511), and the Aircraft Sabotage Act (18 U.S.C. §32), just to name a few. Despite the clear proliferation of advanced technology and the increased risk that errant UAS present to critical infrastructure and their surrounding communities, a regulatory and funding framework that empowers local authorities to respond to threats by UAS is lacking. Only four federal agencies have the authority to engage in counter-UAS (C-UAS) actions in the United States,[7] and this authority does not allow for continual C-UAS coverage at critical infrastructure facilities. The absence of C-UAS coverage creates a security gap and leaves the critical infrastructure community in the difficult position of balancing a potential threat with the reality of limited funds and authority to effectively respond.

Recognizing these gaps, Congress provided FAA the statutory framework to allow certain facilities to apply for designation as a UAS no-fly zone. Section 2209 of the FAA Extension, Safety, and Security Act of 2016 (FESSA) directs the Secretary of Transportation to establish a process to allow critical infrastructure owners and operators to petition the FAA Administrator to prohibit or restrict the operation of an unmanned aircraft near a fixed site facility.[8] This provision is invaluable for critical infrastructure operators seeking to ensure that rogue UAS are not flying above or near their facilities. However, as of October 2019, FAA has yet to initiate the rulemaking for establishing this process.

A Path Forward

In the wake of recent mass shootings, Congress renewed its call to examine how the United States can better contend with domestic terrorism before violent acts occur. Notably, two recent draft bills proposed by Sen. Martha McSally (R-AZ) and Rep. Adam Schiff (D-CA) would create a crime of domestic terrorism modeled after the current statutory definition, and would criminalize providing material support and resources to those knowingly carrying out these acts (McQuade, 2019). Also of significance, both bills include attempt and conspiracy provisions that embolden federal authorities to intervene before an attack occurs (McQuade, 2019). Nonetheless, civil rights groups say expanding the label of domestic terrorism in the federal statute violates the First Amendment in many cases and is a prime example of federal overreach. Proponents of legislation argue that a statute can be carefully crafted to protect civil liberties and yet still give federal authorities the tools necessary to investigate and prevent terrorism from within the borders.

These proposed bills envision a more globalized threat landscape in line with today's realities. A domestic terrorism law does not need to be a violation of fundamental freedoms: there is no call for the creation of a "domestic terror organizations" list or for peaceful protestors to be arrested. In fact, both bills specifically cite acts of domestic terrorism as "violent acts" and attacks that inflict damage to property that could result in "serious bodily injury" (McQuade, 2019). The intent of domestic terrorism legislation is not to prosecute sign-wielding activists or subdue a fiery political debate, but rather to provide federal authorities with the tools necessary to proactively address a domestic terrorism event that was not yet envisioned when Title 18 was enacted.

[7] These four agencies are the Department of Justice, Department of Defense, Department of Homeland Security, and the Federal Bureau of Investigation.

[8] Appropriate applicants include operators and proprietors of critical infrastructure, such as energy production, transmission, and distribution facilities and equipment, oil refineries and chemical facilities, amusement parks, and other locations that warrant such restrictions. In making such determinations, the FAA Administrator is to consider aviation safety, protection of persons and property on the ground, national security, and homeland security issues.

The creation of a meaningful domestic terrorism statute would empower federal agencies to act swiftly in promulgating regulations that support security for our national critical functions. It would bolster private sector efforts to protect critical infrastructure assets. Perhaps most significantly, a domestic terrorism label would have the important narrative effect of signaling the gravity of these crimes and of delegitimizing political violence. First Amendment concerns can and should be respected; these are not mutually exclusive positions, and the U.S. Constitution will always be the bedrock of the laws of the country. No matter how we get there, the United States can no longer afford to disregard the security risks of the 21st century.

References

Congressional Research Service. "Public Mass Shootings in the United States: Selected Implications for Federal Public Health and Safety Policy." Updated April 16, 2013. https://crsreports.congress.gov/product/pdf/R/R43004.

Cruickshank, Paul and Brian Dodwell. 2019. "A View from the CT Foxhole: Joseph Maguire, Acting Director of National Intelligence." *CTC Sentinel* 12, no. 8 (September 2019): 8-13. https://ctc.usma.edu/view-ct-foxhole-joseph-maguire-acting-director-national-intelligence/.

Danzig, Richard J. "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies." Center for New American Security, July 2014. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf?mtime=20161010215746.

Department of Homeland Security. 2019a. "Critical Infrastructure Sectors." Accessed October 11, 2019. https://www.dhs.gov/cisa/critical-infrastructure-sectors.

Department of Homeland Security. 2019b. "National Critical Functions Overview" Accessed October 8, 2019. https://www.dhs.gov/cisa/national-critical-functions-overview.

Department of Justice. 2015. "Kansas Man Pleads Guilty in Plot to Explode Car Bomb at Airport." Office of Public Affairs, June 5, 2015. https://www.justice.gov/opa/pr/kansas-man-pleads-guilty-plot-explode-car-bomb-airport.

Department of Justice. 2019a. "Two Women Charged with Offenses Related to Pipeline Attacks." U.S. Attorney's Office for the Southern District of Iowa, October 2, 2019. https://www.justice.gov/usao-sdia/pr/two-women-charged-offenses-related-pipeline-attacks.

Department of Justice. 2019b. "Audit of the Federal Bureau of Investigation's Management of Maritime Terrorism Threats." March 2019. https://oig.justice.gov/reports/2019/a1918.pdf.

Federal Bureau of Investigation. 2019. "Terrorism." Accessed October 2, 2019. https://www.fbi.gov/investigate/terrorism.

Greenberg, Andy. 2015. "Hackers Remotely Kill a Jeep on the Highway – With Me in It." *Wired*, July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Kriel, Robyn and Paul Cruickshank. 2016. "Source: 'Sophisticated' laptop bomb on Somali plane got through X-ray machine." *CNN*, February 12, 2016.

https://www.cnn.com/2016/02/11/africa/somalia-plane-bomb/index.html.

Levine, Mike. 2019. "7 key questions about the threat of domestic terrorism in America." *ABC News*, August 6, 2019. https://abcnews.go.com/Politics/key-questions-threat-domestic-terrorism-america/story?id=64811291.

Li, Yun. 2019. "Saudi oil production cut by 50% after drones attack crude facilities." *CNBC*, September 24, 2019. https://www.cnbc.com/2019/09/14/saudi-arabia-is-shutting-down-half-of-its-oil-production-after-drone-attack-wsj-says.html.

McGarrity, Michael and Thomas Brzozowski. "The 2019 Threat Landscape to the Fuel and Petrochemical Supply Chains." Presentation, 2019 AFPM Security Conference, Austin, TX, May 1, 2019.

McQuade, Barbara. 2019. "Proposed Bills Would Help Combat Domestic Terrorism." *Lawfare*, August 20, 2019. https://www.lawfareblog.com/proposed-bills-would-help-combat-domestic-terrorism.

Riedman, David. 2017. "The Cold War on Terrorism: Reevaluating Critical Infrastructure Facilities as Targets for Terrorist Attacks." *Homeland Security Affairs* 13, Article 3 (June 2017). https://www.hsaj.org/articles/13976.

Schiano, Chris. 2019. "Two Indicted for Sabotaging Dakota Access Pipeline." *Unicorn Riot*, October 2, 2019. https://unicornriot.ninja/2019/two-women-indicted-for-sabotaging-dakota-access-pipeline-construction/.

Schneider, Jacquelyn. 2019. "Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran?" *The Washington Post*, October 1, 2019. https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/.

Williams, Nia. 2016. "Activists disrupt key Canada-U.S. oil pipelines." *Reuters*, October 11, 2016. https://www.reuters.com/article/us-usa-canada-pipelines/activists-disrupt-key-canada-u-s-oil-pipelines-idUSKCN12B26O.

Drone Emergency Response: A Planning System for Critical Infrastructure

Bill Edwards[9]

Abstract:

This study considers the infrastructure effects of drone attacks. After reviewing the methods and risks of drone attacks, this article proposes a planning system to protect critical infrastructure. Public events are also considered as an extension of this methodology.

Keywords: *Drone emergency response, infrastructure security, coordinated drone attacks*

THE KINGDOM OF SAUDI ARABIA AWOKE on September 14, 2019, to the alarming news that its largest oil-producing facilities had been attacked and were quickly downgraded to 50% operational capability. The world watched as an estimated 5% of the world's oil capacity burned (Safi and Wearden, 2019). These attacks, in addition to being a tragedy, were also an enormous wake-up call regarding the use of drones and drone swarms in attacks on critical infrastructure. It sends a message that the use of unmanned aerial vehicles (UAVs) and current drone technologies represents a severe threat that governments and security professionals should take seriously.

Those responsible for the attack are only doing what a determined enemy always does in a protracted conflict against another military power—using whatever tools possible to give them parity. The use of inexpensive drone technology accomplishes this. The technological evolution of drones and a drone's use of highly sophisticated state-of-the-art functions, including autonomous flight, proximity sensing, geo-location, and extended attack distances, means creative planning and counter-drone solutions are needed for immediate deployment and execution.

Additionally, UAVs can operate from extended distances, carry larger payloads, and in some instances fly in elevations that easily allow for "under the radar" realities. Furthermore, proximity sensing and global positioning sensors allow for swarm tactics to take shape as they did in this reported combined missile and UAV (drone) attack.

The technologies associated with this type of strike and the use of drone platforms will only continue to evolve. Therefore, understanding the nature of the threat landscape is vital to preparing for and executing a Drone Threat and Vulnerability Risk Assessment (DVRA) and a Drone Emergency Response Plan (DERP). These two processes represent the focus of this article.

[9] Bill Edwards is an Associate Principal of protective design and security at Thornton Tomasetti and can be reached at BEdwards@thorntontomasetti.com. He is responsible for planning, coordinating, resourcing and building operational/technical security services across a range of project types. Bill and his team are experts in counter-terrorism, counter-theft, cybersecurity, electronic security, and physical security and provide customized solutions to protect clients' critical assets and investments.

1. DVRA and DERP

DVRA and DERP are processes and methods that give security professionals at the planning and operations levels a way to view the threat and develop proper reactions when an event occurs. They also provide a methodology to combine a proactive and predictive posture to any security situation. It is important to note that combined human and technological solutions are needed to ensure that a comprehensive, layered and integrated approach is taken to mitigate risk and limit the physical harm and damage to people and facilities.

The DVRA is the foundation and consists of a detailed threat analysis, UAV and commercial drone capability review, identification of critical assets, vulnerabilities of those assets and risk mitigation recommendations and measures that could be implanted to "buy down the risk." This includes an understanding of UAV and commercial drone capabilities, layered zones of interest, a defense in depth mindset, mutual aid agreements and partnerships, and knowledge of applicable laws and regulations that support a comprehensive plan. Additionally, a thorough understanding of critical assets is necessary to achieve a targeted use of resources in situations where drones are a threat, but only one of many, in a complex security environment. Lastly, the ability to employ technology to detect, monitor, interdict and even destroy must be considered important courses of action depending on the Special Event Assessment Rating (SEAR) level in the U.S. or its equivalent outside of the U.S.

The DERP should at a minimum address the following key elements from a framework perspective:

1. *Identify the area you will defend.* Assess the site and the surrounding area and identify critical assets. Essentially, this is where you set physical boundaries in depth around the Restricted Area that is intended to be protected. At a minimum, there should be a detection zone, a no-fly zone, and a restricted area. In order to accomplish this, a clear understanding of approach routes and most likely flight patterns is needed. Additionally, RF or a combination of RF and Radar sensors can provide the standoff needed for detection and proactive response.

2. *Form response teams and identify their functions and reporting procedures.* Define response team expectations during an event. This is initially an organizational task that helps to provide an operational response. Response teams assist in the overall security plan during events. They are trained to understand the necessary action to take when a threat arises. An example may be as simple as executing shelter-in-place instructions to event participants or helping to provide orderly evacuation on designated routes. Response teams help large venues secure space in manageable increments. This also applies to drone detection, as response teams can have designated areas to observe that help with providing early warning. If organized, trained and exercised on a regular basis, response teams are a security force multiplier across a myriad of events.

3. *Identify laws and regulations that limit the effect of the plan.* Current laws with regard to drone detection and monitoring in the U.S. are still maturing and do not allow for disrupting a drone's flight unless it is determined a threat over critical infrastructure or Department of Defense facilities. As the commercial drone market continues to expand and grow, it is important for security professionals to understand their limits of response. Additionally, as cybersecurity concerns grow with drone usage, a general

understanding of the recently published European GDPR (2018) and California's CCPA (2020) should be considered with any drone response plan as it pertains to data and personal privacy (Umhoefer and Shpiro, 2019).

4. *Identify zones of interest and influence, and develop a listening and observation post (LP/OP) array for deployment.* Essentially, this is an added layer of defense with regard to the DERP. As mentioned previously, a layered approach to drone detection includes the use of RF and Radar technologies, but it is also important to think in terms of physical audio and optical posts connected via dedicated communications that allow for real-time reporting as an additional measure of proactive planning and response. LP/OP's are an effective way to extend the perimeter of the restricted/protected space during an event.

5. *Develop reporting standards and templates, such as the technological package to be deployed and operations center standard operating procedures.* This is an important step within the DERP. Synchronizing reporting templates, communication packages, and security operation center (SOC) actions is critical for emergency response planning and action. Typically, simplifying how a report is formatted and sent to the SOC is the first step. Publishing a Size, Activity, Location and Time (SALT) report is an ideal way to extend the drone perimeter and is easily communicated to the SOC for a response. It is also important to clearly determine how communications are set-up and executed. Ideally, as technology advances, security directors should have their own private LTE network that goes beyond the facility's WiFi architecture. This would allow for stability in the secure communications network and would negate using the system that is used by staff and guests during events. Redundancy with regard to communications is also key and establishing a Primary, Alternate, Contingency and Emergency (PACE) communication standard is a critical function for the overall security posture. Additionally, InfraGard members, at the time of writing, have access to GETS (Government Emergency Telecommunications Service) and Wireless Priority Service (WPS).

6. *Formulate individual munitions, biohazard, chemical response plans and organize quick reaction forces, communications plans, medical and HAZMAT response planning.* These plans are appendices to the DERP. Simply stated, each area should have its own emphasis and tie directly into the overarching plan. The keys to successful appendices are external support, points of contact and consistent training with local first responders. Additionally, understanding federal support in these areas is essential. Local exercises should be conducted quarterly and annually with federal entities. The Center for Disease Control (CDC) provides a simple template as an example of how to tailor to the DERP (Center for Disease Control, 2020).

7. *Develop evacuation plans.* Identify ingress and egress routes by both land and air, and develop lockdown and shelter in place procedures. Emergency response planning should include triggers for potential evacuation or shelter-in-place decisions. In the case of a kinetic drone threat, security directors will need to establish when to evacuate and when to shelter-in-place. As we saw with the attacks during the Paris soccer match

between France and Germany the situation was nebulous as players, fans and staff were confused about what to do (Borden, 2015). This scenario is all too common in large-scale public events. In the event of a drone threat in the US, such as the one in the Bay Area during NFL games, leaflets dropped from a drone could easily have been ordnance or a chemical (The Seattle Times, 2017). Preparing security personnel and staff on these actions is another important step with regard to DERP development.

8. *Stock emergency supplies, such as water, food and medical.* Specifically, stock emergency supplies for a shelter-in-place event that may require a large crowd to remain in a place for an extended period of time.

9. *Coordinate with local public support agencies and emergency services.* Coordination with relevant government agencies should be a standard within all steps for DERP where applicable. Leveraging external support outside of the venue or facility is a smart way to extend the security program's effectiveness and depth.

10. *Consider cyber implications and protect crucial data and information.* Cybersecurity assessments are an important subset of the DVRA and should be considered as a standard for identifying vulnerabilities to critical assets. The IoT is a major contributing factor to all of the functions of modern facilities in particular life systems (power, water, and HVAC) that are of critical importance to secure (CDW, 2019).

11. *Establish business continuity options/plans and form mutual aid agreements for support.* The DVRA and DERP provide solid foundations for the development of business continuity plans (BCP). How a business maintains functional capability after an event is critical to its survival. BCP along with mutual aid agreements help to keep a business viable. A subset of BCP is continuity of operations (COOP) actions such as training and exercises for off-site relocation to maintain the business's momentum.

Security professionals need to better understand these threats and have the capability to advise the public. Kinetic attacks using drones are only the beginning. In the near future, complex cyber attacks will emerge from these platforms and critical data will be freely exploitable in everyday life. Combing kinetic and cyber attacks will present a formidable challenge that requires inventive security solutions. The increase in these types of attacks based on successful events such as the recent attacks in Saudi Arabia will promulgate further among nefarious groups and individuals. The growth of these types of scenarios will be very similar to what we've already seen with hostile vehicle attacks and active shooter events.

Simply put, drone attacks are another way for terrorists to grab the media's attention and send a message that no one is safe. Drone technology should be taken very seriously and approached in a manner similar to how the world has reacted to vulnerabilities in the cyber domain. There is no way around this. Drones and their use as weapons of disruption and destruction are here to stay.

References

Safi, M. and G. Wearden, "Everything you need to know about the Saudi Arabia oil attacks", *The Guardian*, September 16, 2019, https://www.theguardian.com/world/2019/sep/16/saudi-arabia-oil-attacks-everything-you-need-to-know.

Umhoefer, Carol and Shpiro, Tracy, "CCPA vs. GDPR: the same only different", DLA Piper, April 11, 2019, https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/

CDC, "Emergency Action Plan (Template), Center for Disease Control, Accessed on January 4, 2020, https://www.cdc.gov/niosh/docs/2004-101/emrgact/emrgact.pdf

Borden, Sam, "As Paris Attacks Unfolded, Players and Fans at Soccer Stadium Remained Unaware", The New York Times, November 14, 2015, https://www.nytimes.com/2015/11/15/world/europe/stade-de-france-paris-soccer.html

The Seattle Times, "Leaflets dropped over NFL games revive concerns about drones", The Seattle Times, November 27, 2017, https://www.seattletimes.com/nation-world/drone-pilot-arrested-for-dropping-leaflets-over-nfl-games/.

CDW, "What is the Internet of Things (IoT)", Tech Tips, January 24, 2019, https://www.cdw.com/content/cdw/en/articles/networking/2019/01/24/what-is-the-internet-of-things.html

Deception, Lies, and Manipulation in Cyberspace: Critical Thinking as a Cognitive Hacking Countermeasure

Dr. Cecile S. Jackson[10]

Abstract:

Fallacious or misleading information disseminated using technology to deceive, exploit, and manipulate psychological weaknesses, perceptions, and decision-making is identified as disinformation. The exponential growth of the internet and the immense wilderness of information impacts human judgment, perception, and cognitive ability to discern the credible from incredible. The purpose of this literature review is to explore critical thinking as a counter to cognitive hacking and provide a conceptual analysis of fallacy and fallacious appeals as underpinnings to disinformation. The results of this literature review suggest that with bias suspension and awareness of fallacy and fallacious appeals, critical thinking is a viable solution to recognize disinformation. Also, future research may involve qualitative and quantitative studies on disinformation and the impacts on societal reality, decision-making, and the existence of truth.

Keywords: *Cognitive hacking, critical thinking, decision-making, disinformation, fallacious appeals, fallacy, truth*

THE COGNITIVE EFFECTS OF DISINFORMATION are existential societal threats. Since antiquity, deceptive and coercive tactics have influenced individual opinions and ideas. However, aided by the borderless and mass-connectedness of cyberspace, disinformation is propagandized to manipulate the cognitive processes of society on a large-scale. The exponential growth of the internet and immense wilderness of information has created a challenge likened to cognitive hacking where judgment, perception, and reasoning are exploited through psychological vulnerabilities. Because humans are poor judges of dishonesty and trickery[11], the cognitive ability to discern accuracy in information propagation is a global social concern.

Disinformation, in the context of this article, is fallacious information circulated using the internet to intentionally deceive, exploit, and manipulate psychological weaknesses, perceptions, and decisions. Rapid propagandizing distorts truth and blurs the lines between fact and fiction, where society is increasingly misinformed. The consequences of repeated exposure to disinformation result in altered perceptions and distorted beliefs - leaving accurate discernment an individual responsibility. However, while fiction is subjective, fact must remain objective and free of emotional connotations; thus, supporting critical thinking as a disinformation counter and viable solution to cognitive hacking. Therefore, the purpose of this paper is twofold: First, to discuss critical thinking as a counter to disinformation and cognitive hacking. Secondly, to provide a conceptual analysis of fallacy and fallacious appeals as underpinnings to disinformation.

[10] Independent scholar, Computer Scientist, Leadership Consultant, Public Speaker, cecile.s.jackson@gmail.com, 1910 Navarre Road #5409, Navarre, FL 32566

[11] Charles F. Bond Jr and Bella M. Depaulo, "Accuracy of Deception Judgments," *Personality and Social Psychology Review* 10, no. 3 (2006).

Critical Thinking and Disinformation

Disinformation distorts the perception of truth, and critical thinking is a conceivable and practical counter. The human mind creates a personal view of the world conjured through emotions, thoughts, and feelings that exert influence over reasoning, decision-making, and behavior. Repetitive exposure to disinformation impacts cognitive processes and hampers clarity in perception and judgment. More so, critical thinking acts as a firewall that filters disinformation and allows clarified perception, judgment, and decision-making.

When in search of truth, awareness of emotional impacts on perception is requisite to critical thinking. Interestingly, a societal baseline for truth goes unestablished but aligns with Kuhn's argument that truth is based on the constraints of culture and individual perceptions[12]. The validity of information draws on preconceived existences of genuineness used as a compass toward truth. However, when perception is loosely footed on biases, critical thinking is flawed; thus, weakening suppositions and increasing influences of disinformation. The presence of cognitive weaknesses, i.e., biases, supports rationalizations of inconsistent fusions of formal and informal fallacies. As a result, fallacy is justified while behaviors and decisions change to ease cognitive dissonance, which is antagonist to critical thinking.

Defining Critical Thinking

Over 2,400 years ago, the Socratic Method was developed based on Socrates' questioning philosophy. Through scrutiny, reasoning, and analysis, the Socratic dialogue prompted problem-solving elucidation through the decomposition of cognitive thought to encourage one to think.[13] Socrates recognized the necessity of clarified and lucid critical thought. However, extant and seminal literature lacks a universal definition of critical thinking which prompted scholars in various fields to attempt an overarching description, as follows:

- "reasonable, reflective thinking that is focused on deciding what to believe."[14]
- "incarnation of beliefs about the human process of coming to know and judge something."[15]
- "examines assumptions, discerns hidden values, evaluates evidence, and assesses conclusions" and stresses the awareness of fallacies in thinking.[16]
- "the systematic evaluation or formulation of beliefs, or statements, by rational standards. Critical thinking is systematic because it involves distinct procedures and methods...and it operates according to rational standards in that beliefs are judged by how well they are supported by reasons." [17]

---

[12] Barry Barnes, Scientific Knowledge and Sociological Theory, (Routledge, 2013), https://doi.org/10.4324/9780203706541.

[13] James C. Overholser, "Elements of the Socratic Method: I. Systematic Questioning," *Psychotherapy: Theory, Research, Practice, Training* 30, no. 1 (1993).

[14] R. Ennis, "A Taxonomy of Critical Thinking Abilities and Dispositions," *Teaching Thinking Skills: Theory and Practice* (1987), 10.

[15] Rosemarie Rizzo Parse, "Critical Thinking: What Is It?," *Nursing Science Quarterly* 9, no. 4 (1996), 10.1177/089431849600900401, 139.

[16] David G. Myers and C. Nathan Dewall, Exploring Psychology (New York: Worth, 2007), xv.

[17] L. Vaughn, *The Power of Critical Thinking: Effective Reasoning About Ordinary and Extraordinary Claims*, (Oxford: Oxford University Press, 2005), 4.

Similarities thread through each meaning and root the concepts of discernment, belief, and thinking. Therefore, in the context of this article, the definition of critical thinking offered by Scriven and Paul is accepted:

> *The intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action. In its exemplary form, it is based on universal intellectual values that transcend subject matter divisions: clarity, accuracy, precision, consistency, relevance, sound evidence, good reasons, depth, breadth, and fairness.*[18]

The denotation touches multiple aspects of clarified thinking through objectivity and highlights the complexity of analyzing and questioning the validity of information by thinking conscientiously, viewing data holistically, questioning loosely-connected facts, and looking beyond constraints to reach accuracy and credibility. Viewing information from various perspectives, in parallel, and from the edge aligns with an inquisitive, open-minded, and well-informed critical thinker. Additionally, objective reasoning, suspension of biases, and abating insinuations of personal innuendoes are essential critical thinking qualities. Critical thinkers encompass an intellectual aptitude and the ability to take "one's thinking apart systematically…analyze each part, assess it for quality,"[19] and minimize flawed inferences that are inherently biased. The disposition of unbiased reasoning is a foundational criterion when seeking truth. For example, to circumvent creep of undisciplined or irrational suppositions, Norris and Ennis stress an ability to "reason from [disagreed] starting points…without letting the disagreement interfere with…reasoning."[20] Critical thinking should, at some point, result in a sound conclusion or judgment; however, where judging should occur in the overall cognitive process is heavily debated.

Judgment in Critical Thinking

Judgment is deductive reasoning of significant facts from various premises; nevertheless, deliberation ensues if judgment should occur during or after critical thinking analysis. Many researchers argue against the inclusion of judgment during the critical thought process.[21;22;23;24] Dewey proposes critical thinking eliminate all aspects of judgment to gain clarity free of personal bias which provisions holistic acceptance of newly discovered knowledge before a final

---

[18] M. Scriven and R. Paul, "Defining Critical Thinking," accessed 01 December 2019 https://www.criticalthinking.org/pages/defining-critical-thinking/766, para. 2.

[19] Linda Elder and Richard Paul, "Critical Thinking: Distinguishing between Inferences and Assumptions," *Journal of Developmental Education* 25, no. 3 (2002), http://www.ncde.appstate.edu, para, 1.

[20] Stephen P. Norris and Robert H. Ennis, *Evaluating Critical Thinking. The Practitioners' Guide to Teaching Thinking Series* (Tulsa, OK: Midwest Publications, 1989, 12).

[21] John Dewey, *How We Think*, (New York: D.C. Heath & Co., 1909), https://www.gutenberg.org/files/37423/37423-h/37423-h.htm.

[22] Richard Feldman, "Deep Disagreement, Rational Resolutions, and Critical Thinking," *Informal Logic* 25, no. 1 (2005), http://amr.uwindsor.ca/ojs/leddy/index.php/informal_logic/article/viewArticle/1041.

[23] Gary R. Kirby and Jeffery R. Goodpaster, *Thinking*, 4th ed. (New Jersey: Pearson Prentice Hall, 2007).

[24] M. Miller, *The Book and the Right: The Roots of America's Greatness* (Maitland, FL: Xulon Press, 2010).

determination. Similarly, Feldman supports the suspension of judging in successful critical thinking, and Miller argues the abeyance of personal virtues to avoid incriminating judgment because even the most highly intelligent are subject to immorality. Lastly, Kirby and Goodpaster caution the inclusion of judging due to potential bias creep; specifically, when there is a personal vested stake.

Contrastingly, Facione identifies critical thinking as a "purposeful, self-regulatory judgment that results in interpretation, analysis, evaluation, and inference, as well as an explanation of the evidential, conceptual, methodological, criteriological, or contextual considerations upon which that judgment is based."[25] Additionally, several researchers support the inclusion of judging with an expertise caveat.[26;27;28;29] Bailin and Willingham posit when a critical thinker is well versed in the subject matter, judgment is acceptable – a concept supported by Lipman. However, mindfulness of appealing to credibility, along with the argument of Feldman, raises concerns of experienced individuals succumbing to corruption when discerning fallacy and fallacious appeals.[30]

Fallacy

In *De Sophistici Elenchi*, Aristotle denotes fallacy as a refutation - "…a deduction whose conclusion contradicts the statement that was previously made by the interlocutor"[31] Fogelin and Duggan characterize fallacy as "our most general term for criticizing any general procedure used for the fixation of beliefs that has an unacceptably high tendency to generate false or unfounded beliefs, relative to that method of fixing beliefs."[32] Fallacies are defects in reasonings, whether intentional or unintentional, and fictitious underpinnings used to persuade opinions, undermine truth and desecrate rules that govern argument. The façades transcend boundaries of economic stature, historical backgrounds, and religious preferences, as society is naïvely subject to fallacious arguments, particularly when defending taboo topics such as religion, abortion, politics, and sexuality. Therefore, constraint, discipline, and impartiality are requisites for critical thought to prevail.

The delusional beauty of fallacy permits dishonesty to appear more factual than truth. In Mein Kampf, Adolf Hitler declares, "In this, they proceeded on the sound principle that the magnitude of a lie always contains a certain factor of credibility, since the great masses of the people…in view of the primitive simplicity of their minds, they more easily fall a victim to a big lie than to a little one."[33]

---

[25] Peter A. Facione, "*Critical Thinking: A Statement of Expert Consensus for Purposes of Educational Assessment and Instruction. Research Findings and Recommendations*," (1990), http://files.eric.ed.gov/fulltext/ED315423.pdf, 3.

[26] Sharon Bailin, "Critical and Creative Thinking," *Informal Logic* 9, no. 1 (1987).

[27] ———, "Critical Thinking and Science Education," *Science & Education* 11, no. 4 (2002).

[28] Matthew Lipman, "Critical Thinking-What Can It Be?," *Educational Leadership* 46, no. 1 (1988), http://www.journal.viterbo.edu.

[29] Daniel T. Willingham, "Critical Thinking: Why Is It So Hard to Teach?," *Arts Education Policy Review* 109, no. 4 (2008), http://insight.bostonbeyond.org/wp-content/uploads/2017/05/Willingham-2007-1.pdf.

[30] Feldman, "Deep Disagreement, Rational Resolutions, and Critical Thinking".

[31] Annamaria Schiaparelli, "Aristotle on the Fallacies of Combination and Division in Sophistici Elenchi 4," Article, *History & Philosophy of Logic* 24, no. 2 (2003), http://dx.doi.org/10.1080/0144534031000096145, 111.

[32] Robert J. Fogelin and Timothy J. Duggan, "Fallacies," *Argumentation* 1, no. 3 (1987).

[33] Adolf Hitler, "Causes of the Collapse," in *Mein Kampf* (New York: Mariner, 1998).

To the same degree, George Orwell asserted:

> *And if all others accepted the lie which the Party imposed — if all records told the same tale — then the lie passed into history and became truth. "Who controls the past…controls the future: who controls the present controls the past." And yet the past, though of its nature alterable, never had been altered. Whatever was true now was true from everlasting to everlasting. It was quite simple. All that was needed was an unending series of victories over your own memory. "Reality control."*[34]

Humans are prone to profound psychological denials when lies are deeply engrained in personal convictions. When beliefs are challenged, desires to avoid cognitive dissonance are driven by self-deception, justification, and rationalization to substantiate perceptions, opinions, and biases. As a result, decisions and perceptions filtered through justified beliefs increase the appeal of fallacies. Consequently, when bias supports an erroneous end state, the directive to seek justice is difficult to attain. Fallacious appeals are deceptive influences inaccurately supported by authority, logic, and emotion. Exercising epoche in crucial thinking is obligatory to bracket and suspend biases. Furthermore, detecting fallacy in disinformation is difficult, and doing so requires an understanding of formal and informal arguments.

Formal fallacies are defective in argument form; whereas, informal fallacies are defective in argument content which may result in defective argument form. The list of fallacy types is numerous; therefore, this article will briefly address only informal fallacies, specifically, appeal to authority, circular reasoning, and red herring, which relates to the Aristotelian Triad of ethos, logos, and pathos, respectively. Additionally, informal fallacies are arguments that seem irrefutable and superficially sound, used to persuade ideas and opinions, and validity realizes conflict between premise and conclusion. Furthermore, unlike formal fallacies, informal arguments are flawed in reasoning rather than in logic.

Ad Verecundium (Appeal to Authority)

Pseudo authority, false authority, or *Argumentum Ad Verecundium*, is an argument of ethos that appeals to credibility and provincial authority. Appeal to authority results in flawed reasonings which provisions acceptance of a claim based on information presented by an inexpert. Appeal to authority blurs the lines between facts and opinions under the guise of reputation characterized as experience. *Ad Verecundium* is a conclusion supported upon the expertise premise, see Table 1.

[34] George Orwell, 1984 (World Public Library Association, 2017), http://117.211.153.211:8001/jspui/bitstream/123456789/467/1/1984.pdf, 14.

Table 1

Appeal to Authority Example

Argument	Statement
P1	A claims that P true
P2	A claims to be an expert on P
C	Therefore, P is true

Note. A is seemingly an expert on the subject of P and claims P is true; therefore, P is true. A = expert; P = premises; C = conclusion.

Accepting inexpert claims as truth influences the belief of erred reasoning, which limits adept authority to accept a claim as legitimate. The *Tongue and Quill* notes, "false authority is a fallacy tied to accepting facts based on the opinion of an unqualified authority. [Society] is chock-full of people who, because of their position or authority in one field, are quoted on subjects in other fields for which they have limited or no expertise."[35] To err is human and even experts are subject to culpabilities; therefore, cautious acceptance of expert opinions is crucial in deductive reasoning. Discernment lies in careful analysis of reasonableness versus emotions when weighing the evidence to conclude the premises with certainty.

Petitio Principii (Circular Reasoning)

Circular reasoning, begging-the-question, Catch-22, or *Petitio Principii*, is an argument of logos that renders the premises as the conclusion. *Petitio Principii* doubles back and is technically valid but fails to include an additional premise or reasoning for the conclusion, see Figure 1.

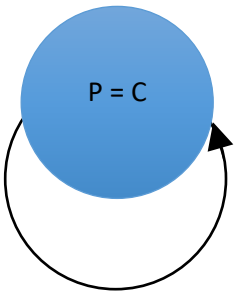

Figure 1. A depiction of circular reasoning. The premise is also the conclusion. (1) P is claimed as true. (2) Therefore, P is true.

The argumentum supports disinformation on actual or closely related proposals as a foundation of reasoning. A commonly used example advocated by Hahn, Oaksford, and Corner is "God exists

[35] Air Force Handbook (AFH) 33-337, Communications and Information Tongue and Quill, 27 July 2016, https://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afh33-337/afh33-337.pdf, 49

because the Bible says so and the Bible is the word of God"[36]; therefore, God must exist. The argument of circular reasoning formulates a logical premise of evidence that the Bible is the word of God because the conclusion supports that God exists because the Bible says so. The argumentation of *Petitio Principii* is unjustifiable independent of the conclusion and represents a single premise that equates to an identical deduction. Discernment of circular reasoning involves identifying a separate reason for a conclusion that is outside of the premises.

Ignoratio Elenchi (Red Herring)

Irrelevant conclusion, Red Herring, or *Ignoratio Elenchi*, an argument of pathos[37] that influences by distracting attention from the issue at hand by appealing to emotions or introducing irrelevant information. Arguing valid but immaterial viewpoints to evoke feelings or divert attention toward an unrelated subject is the foundational premise of red herring, see Figure 2.

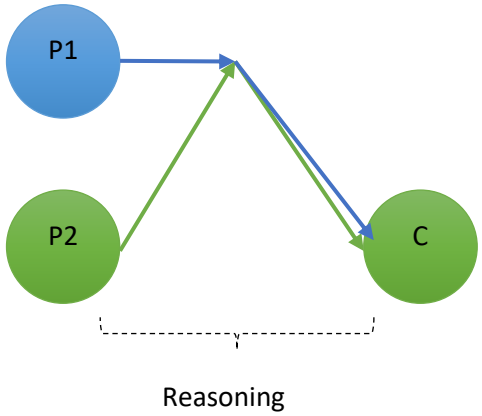

Figure 2. A depiction of red herring. A secondary argument (P2) is introduced and diverts reasoning away from the primary argument (P1), which results in an unrelated conclusion. (1) Topic P1 is under discussion. (2) Topic P2 is introduced as related to topic P1. (3) Topic P1 is abandoned. (4) Topic P2 is under discussion. (5) A flawed conclusion is regarded as true.

The red herring fallacy is a diversion tactic to manipulate and distract attention from the topic of discussion. Furthermore, all fallacies are persuasive strategies to manipulate an argument regardless of the truth.[38] Leeriness of ethos, logos, and pathos within the exhaustive list of fallacious reasonings is crucial to disinformation identification and critical thinking processes.

Conclusion

Truth rests at the conjunction of information technology and human cognition. Distinguishing fact from fiction may become more difficult as disinformation is continuously

[36] Ulrike Hahn, Mike Oaksford, and Adam Corner, "Circular Arguments, Begging the Question, and the Formalization of Argument Strength," *Proceedings of AMKLC'05, International Symposium on Adaptive Models of Knowledge, Language and Cognition* (Espoo, Finland2005), http://www.cis.hut.fi/AKRR05/papers/amklc05hahn.pdf, para. 6.
[37] Elliot D. Cohen, *Critical Thinking Unleashed* (Landham, MD: Rowman & Littlefield, 2009).
[38] Antoine C. Braet, "Ethos, Pathos and Logos in Aristotle's Rhetoric: A Re-Examination," *Argumentation* 6, no. 3 (1992).

circulated across the internet. As a counter, where information exists, so should critical thinking; however, the societal seed has yet to root. The quality of critical thinking is flawed and subject to biases and presuppositions. Regardless, the failure or inability of society to decipher disinformation has morphed fallacy into an indistinguishable pseudo-truth. A significant issue supervenes in that the cognitive process of critical thought must be exercised beyond a few – the majority must recognize the presence of disinformation.

Does truth really exist if hidden inside the minds of a small percentage of critical thinkers? According to Kierkegarrd, "truth always rests with the minority…because truth is generally formed by those who really have an opinion, while the strength of a majority is illusory, formed by the gangs who have no opinion."[39] However, this researcher concluded that because the internet has distracted society and obscured truth in such a significant manner, conviction is deemed to rest in the number of social media likes and followers. Unfortunately, new truth, i.e. fake truth, pseudo truth, resides in the mainstream and definition is formed through repeated information exposure and manipulation of cognitive thought, which impacts discernment of fact from fiction. Therefore, a single individual who questions information is powerless when standing alone against the amalgamation of material that manipulates truth and clouds the judgment of society.

Nonetheless, although truth will remain truth, societal populism must interrogate the validity of propagandized information for authentic truth to prevail. Moving critical thought a step further, just as technology is taught in grade schools, so should critical thinking curricula to root seeds of creative thought and bias suspension for truth to remain victorious amid the perplexing wilderness of data. Future research may include (1) critical thinking as a learned societal skill; (2) the willingness of society to employ critical thinking versus easing cognitive dissonance, and (3) the impacts of disinformation on tradition – passing fallacy through the generations.

References

Air Force Handbook (AFH) 33-337, *Communications and Information Tongue and Quill*, 27 July 2016.

Bailin, Sharon. "Critical and Creative Thinking." *Informal Logic* 9, no. 1 (1987): 23-30.

Bailin, Sharon. "Critical Thinking and Science Education." *Science & Education* 11, no. 4 (2002): 361-375.

Barnes, Barry. *Scientific Knowledge and Sociological Theory*. Routledge, 2013. https://doi.org/10.4324/9780203706541.

Bond Jr, Charles F., and Bella M. DePaulo. "Accuracy of Deception Judgments." *Personality and Social Psychology Review* 10, no. 3 (2006): 214-234.

Braet, Antoine C. "Ethos, Pathos and Logos in Aristotle's Rhetoric: A Re-Examination." *Argumentation* 6, no. 3 (1992): 307-320. doi:http://dx.doi.org/10.1007/BF00154696.

Cohen, Elliot D. *Critical Thinking Unleashed.* Landham, MD: Rowman & Littlefield, 2009.

Dewey, John. *How We Think*. New York: D.C. Heath & Co., 1909. https://www.gutenberg.org/files/37423/37423-h/37423-h.htm.

Elder, Linda, and Richard Paul. "Critical Thinking: Distinguishing Between Inferences and Assumptions." *Journal of Developmental Education* 25, no. 3 (2002): 34. http://www.ncde.appstate.edu, para, 1.

[39] Søren Kierkegaard. *The Diary of Søren Kierkegaard.* Ed. Peter Rhode. (New York: Citadel Press, 1960). No. 128 (1850).

Ennis, R. "A Taxonomy of Critical Thinking Abilities and Dispositions." *Teaching Thinking Skills: Theory and Practice* (1987): 9-26. 10.

Facione, Peter A. "*Critical Thinking: A Statement of Expert Consensus for Purposes of Educational Assessment and Instruction. Research Findings and Recommendations*." (1990). http://files.eric.ed.gov/fulltext/ED315423.pdf, 3.

Feldman, Richard. "Deep Disagreement, Rational Resolutions, and Critical Thinking." *Informal Logic* 25, no. 1 (2005): 13-23.

Fogelin, Robert J., and Timothy J. Duggan. "Fallacies." *Argumentation* 1, no. 3 (1987): 255-262. doi:http://dx.doi.org/10.1007/BF00136777, 256.

Hahn, Ulrike, Mike Oaksford, and Adam Corner. "Circular Arguments, Begging the Question, and the Formalization of Argument Strength." In *Proceedings of AMKLC'05, International Symposium on Adaptive Models of Knowledge, Language and Cognition* Espoo, Finland: 2005. http://www.cis.hut.fi/AKRR05/papers/amklc05hahn.pdf, para. 6.

Hitler, Adolf. "Causes of the Collapse." Translated by James Murphy. Chap. X In *Mein Kampf*. New York: Mariner, 1998.

Kierkegaard, Søren. *The Diary of Søren Kierkegaard.* Ed. Peter Rhode. New York: Citadel Press, 1960.

Kirby, Gary R., and Jeffery R. Goodpaster. *Thinking.* 4th ed. New Jersey: Pearson Prentice Hall, 2007.

Lipman, Matthew. "Critical Thinking-What Can It Be?" *Educational Leadership* 46, no. 1 (1988): 38-43. http://www.journal.viterbo.edu.

Miller, M. *The Book and the Right: The Roots of America's Greatness* Maitland, FL: Xulon Press, 2010.

Myers, David G., and C. Nathan Dewall. *Exploring Psychology* New York: Worth, 2007. xv.

Norris, Stephen P., and Robert H. Ennis. *Evaluating Critical Thinking. The Practitioners' Guide to Teaching Thinking Series.* Tulsa, OK: Midwest Publications, 1989, 12.

Orwell, George. *1984* World Public Library Association, 2017. http://117.211.153.211:8001/jspui/bitstream/123456789/467/1/1984.pdf, 14.

Overholser, James C. "Elements of the Socratic Method: I. Systematic Questioning." *Psychotherapy: Theory, Research, Practice, Training* 30, no. 1 (Spr 1993): 67-74.

Parse, Rosemarie Rizzo. "Critical Thinking: What Is It?" *Nursing Science Quarterly* 9, no. 4 (1996): 139. 10.1177/089431849600900401, 139.

Schiaparelli, Annamaria. "Aristotle on the Fallacies of Combination and Division in Sophistici Elenchi 4." Article, *History & Philosophy of Logic* 24, no. 2 (2003). http://dx.doi.org/10.1080/0144534031000096145, 111.

Scriven, M., and R. Paul. "Defining Critical Thinking." accessed 01 December 2019 https://www.criticalthinking.org/pages/defining-critical-thinking/766, para. 2.

Vaughn, L. *The Power of Critical Thinking: Effective Reasoning About Ordinary and Extraordinary Claims*. Oxford: Oxford University Press, 2005. 4.

Willingham, Daniel T. "Critical Thinking: Why Is It So Hard to Teach?" *Arts Education Policy Review* 109, no. 4 (2008): 21-32.

Cyber-Security Vulnerabilities: Domestic Lessons from Attacks on Foreign Critical Infrastructure

Anthony Moreno

Dr. Petter Lovaas[40]

Abstract:

Technology, and its increasing integration in today's world, have created new threat vectors that were previously unheard of. Although this technology integration streamlines efficiencies and improves communication, its usage can have grave consequences when not properly secured or hardened against cyberattacks. This can be especially true when considering our nation's critical infrastructure systems. Critical infrastructure systems and networks support a vast array of related services that help shape our modern society. Power grids, hospitals, and educational institutions are just some examples of critical infrastructures. Examination of past cyberattacks on foreign critical infrastructure systems will help identify lessons learned and be used to recommend defense in depth approaches and solutions to this challenge.

Keywords: *Cyber security, critical infrastructure*

PRESIDENTIAL POLICY DIRECTIVE (PPD) 21 WAS written to promote the safety and security for the United States' critical infrastructure.[41] Protecting critical infrastructure is increasingly difficult as malicious actors continually pose a threat. In the modern age, nearly all industries and government services now incorporate mission and business critical devices that connect and interact with various public networks. As a society we have come to especially rely on various critical infrastructures that utilize these shared computer networks. Critical infrastructures are formally defined as "the basic facilities, services, and installations needed for the functioning of a community or society".[42]

All United States critical infrastructure sectors currently employ controls over networks for their operation. Supervisory Control and Data Acquisition (SCADA), Internet of Things (IoT) monitors, and other

[40] Department of Computer Information Sciences (CIS), Niagara University, 5795 Lewiston Rd, New York 14109. amoreno@mail.niagara.edu (Moreno) and plovaas@niagara.edu (Lovaas).

[41] Interagency Security Committee, "Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper," February 2015, https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf.

[42] Wendy Steele, Karen Hussey, and Stephen Dovers, "What's Critical about Critical Infrastructure?," *Urban Policy and Research* 35, no. 1 (2017): 74-86, DOI: 10.1080/08111146.2017.1282857.

internet-connected computer systems are all used to ensure smooth and efficient operations of their various functions. Countless SCADA systems are deployed worldwide and are used to provide a means to identify and rebound from system faults and other mechanical failures.[43] The IoT, on the other hand, is not limited to industrial controls, but rather is a general term for various embedded technology devices "and their logical representations [within our] information systems".[44] Frequently these same monitors, systems, and networks, are not sufficiently hardened against cyber threats.

With the internet now connecting numerous countries and malicious actors alike (often without clear attribution), cyberattacks can have a significant impact on political and governmental institutions. Our study is qualitative in nature and explores at depth our nation's critical infrastructures, past successful cyberattacks, and the current steps being taken to harden critical infrastructure networks and computer systems. We conclude by identifying and designing a holistic method for critical infrastructure protection, utilizing a defense in depth approach.

1) Literature Review:

Defining Critical Infrastructures:

Critical infrastructures are responsible for providing the required services and functions that modern life and society have come to rely and depend on. In the United States specifically, the Department of Homeland Security defines 16 critical infrastructure sectors that include a wide range of different industries.[45] Although not an exhaustive list, these industries include the chemical sector, the energy sector, the food and agriculture sector, and the government facilities sector.[46] The importance of each critical sector cannot be understated. The Department of Homeland Security explains that each sector is "so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, [and] national public health [and] safety".[47]

Many of the industries that compose critical infrastructure systems require the constant observation of a myriad of controllers and devices "to ensure [their] proper [and continuous] operation".[48] Operational requirements have transformed critical infrastructure systems "into complex networks that support communication between a central control unit and multiple remote units".[49] These remote units often are not computers, but rather an IoT or SCADA device.

---

[43] A. Nicholson et al., "SCADA security in the light of Cyber-Warfare," *Computers & Security,* 31, no. 4 (2012): 418-436, https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2012.02.009.

[44] Daniel Minoli, *Building the Internet of Things with IPv6 and MIPv6 : The Evolving World of M2M Communications*, (Somerset: John Wiley & Sons, Incorporated, 2013), 2, https://ebook central.proquest.com/lib/niagara-ebooks/reader.action?docID=1216195&ppg=21.

[45] "Critical Infrastructure Sectors," accessed March 30, 2019, https://www.dhs.gov/critical-infrastructure-sectors.

[46] Ibid.

[47] Ibid.

[48] Vinay Igure, Sean Laughter, and Ronald Williams, "Security issues in SCADA networks," *Computers & Security,* 25 no. 7 (2006): 498-506, https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2006.03.001.

[49] Ibid.

Defining SCADA:

Although IoT devices are primarily found in consumer-based products and homes, SCADA controllers are especially prevalent in the implementation and operation of large Industrial Control System (ICS) devices and processes. In order to provide improved central control and monitoring over great distances, SCADA controllers and the networks they reside on are commonly placed on publicly connected networks.[50] However, the improved communication allotted with connecting SCADA networks to the public internet comes with risks.

Although the improved [and increased] connectivity can aide in the optimization of various manufacturing and distribution processes, it can also expose the safety-critical industrial network to the vast amount of cyber threats found on the global internet today.[51] Concerned with these same shortcomings, a group of researchers in 2012 tested SCADA and ICS devices and networks.[52] In a distressing conclusion, they found significant cyber vulnerabilities in numerous "top industrial control systems… used in critical infrastructure and manufacturing facilities" across the U.S.[53]

The researchers uncovered a "lack of authentication and encryption, and weak password storage" among the SCADA and ICS devices investigated.[54] Alarmingly, the researchers divulged they were able to acquire their access without significant effort.[55] Most concerning was the discovery that allowed the researchers "to interfere with specific critical processes… [including] the opening and closing of valves".[56] The identified vulnerabilities, combined with the large scope and breadth of critical infrastructures, provide evidence that a far-reaching, inclusive, and defense in depth strategy will be required to adequately strengthen overall cyber security.

2) Findings/Discussion:

With the current increase and varying types of cyberattacks, SCADA controllers and their associated networks must be safeguarded and secured. For example, suppose that the researchers in the above-mentioned 2012 study were instead malicious actors that had gained access to a nuclear power generation facility.[57] Remotely turning off critical control valves could have resulted in a catastrophic event that would have put many innocent lives at grave risk.[58] Although this example is only a hypothetical scenario, past cyberattacks have proven that critical infrastructures and their integrated controllers are vulnerable and susceptible to cyber threats.

[50] Nicholson et al., "SCADA security in the light of Cyber-Warfare."
[51] Nicholson et al., "SCADA security in the light of Cyber-Warfare."
[52] Kim Zetter, "Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software," last modified January 19, 2012, https://www.wired.com/2012/01/scada-exploits/.
[53] Ibid.
[54] Zetter, "Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software."
[55] Ibid.
[56] Ibid.
[57] Ibid.
[58] Ibid.

One such successful cyberattack that targeted a specific type of SCADA controller is the 2010 Stuxnet virus cyberattack.[59] In total, it was found to have impacted more than 60,000 computers in countries ranging from China, the United Kingdom, and even to the United States.[60] However, the Stuxnet virus particularly targeted the country of Iran.[61] More specifically, the virus was found to target Iranian centrifuges that were being used to refine nuclear fuels for power production.[62]

In this case, the virus was able to infect the centrifuges and controllers that were offline and not connected to the public Internet.[63] Further, the malicious code used USB thumb drives as the intermediary to gain and establish control of the offline centrifuges.[64] Once the Stuxnet virus had successfully infiltrated the appropriate computer and centrifuge control system or SCADA device, the "Stuxnet worm [then exploited the] Siemens' default password to access Windows operating systems that ran the WinCC and PCS 7 [control] programs".[65]

After the virus had successfully compromised the centrifuge controllers, it then "alternate[d] the frequency of the electrical current that powered the centrifuges".[66] As a result, the centrifuges would then "switch back and forth between high and low speeds".[67] This oscillation "at intervals for which the machines were not designed" rendered the ability to process nuclear fuel inert and physically destroyed the centrifuges themselves.[68] The basic process and steps are outlined in the graphic shown in Figure 1[69]:

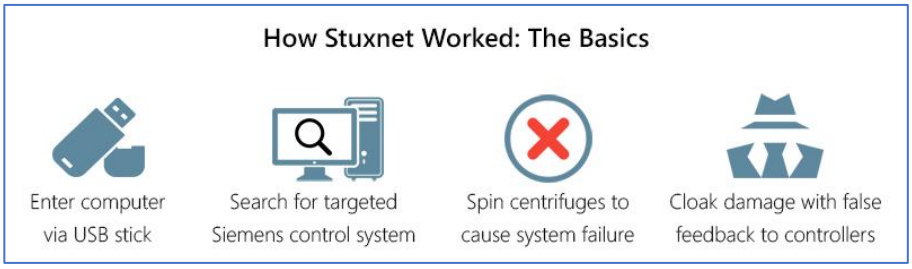

Figure 1

[59] Steve Murphy, "The State of Cybersecurity in the Water/Wastewater Market," *InfraGard Journal*, Volume 1, https://www.infragardnational.org/wp-content/uploads/2019/05/The-State-of-Cybersecurity-in-the-WaterWastewater-Market.pdf.
[60] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, 53 no.1 (2011): 23-40, https://doi-org.ezproxy.niagara.edu/10.1080/00396338.2011.555586.
[61] Murphy, "The State of Cybersecurity in the Water/Wastewater Market."
[62] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."
[63] Ibid.
[64] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."
[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Ibid.
[69] Matt Puskala, "Industrial Security: 4 Ways to Keep Your Factory Safe from Cyber Attacks," September 23, 2016, https://www.dmcinfo.com/latest-thinking/blog/id/9293/industrial-security-4-ways-to-keep-your-factory-safe-from-cyberattacks.

Although an official statement, acknowledgement, or motive of the attack remains elusive, many countries and researchers alike question if the nuclear fuel sought by Iran was in fact being created for power production.[70] Experts speculate that Iran was using the centrifuges with the intention of creating weapons grade nuclear compounds in their unsanctioned pursuit of nuclear weapons.[71] Regardless of the motive or origin, the Stuxnet virus significantly hindered the nuclear program Iran was attempting to develop without any loss of life.[72]

A similar analysis of the Stuxnet attack is warranted in order to determine if the United States own centrifuges and similar systems are vulnerable to a comparable type of an attack. In fact, the U.S. National Nuclear Security Administration (NNSA) in October 2018 announced the desire to expand "domestic uranium-enrichment capabilities".[73] Given the desire to increase the production of the United States' own nuclear fuel supplies, it will be especially important to ensure the ICS and SCADA devices used to moderate these processes are adequately protected.

Although SCADA and other industrial controls themselves can be comprised, the computer networks on which they reside and the users that operate them are also at risk. For example, the Ukrainian power grid was shuttered during a cyberattack in 2015, not necessarily by vulnerabilities in the SCADA and ICS devices themselves, but rather the computer systems and networks to which they were connected.[74] This cyberattack against Ukraine's critical infrastructure power grid ultimately resulted in power outages that affected at least 225,000 people.[75]

The groundwork for the attack was initiated by attackers who were able to successfully employ a form of social engineering.[76] A phishing email containing a malicious Excel attachment executed BlackEnergy malware onto the power company's computer and SCADA control network.[77] When it was time to commence the attack, "the hacker used the preinstalled malware to remotely take control of the HMI [human-machine interface]" for the SCADA controllers.[78] The hacker then switched off switchgears available to them through the interface.[79] The hackers were also perceptive enough to include additional code preventing the user from regaining access to networks and SCADA devices, prolonging the recovery.[80] Although the resulting power outage was relatively short, the control systems took much

---

[70] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."
[71] Ibid.
[72] Ibid.
[73] Frank N. von Hippel and Sharon K. Weiner, "No Rush to Enrich: Alternatives for Providing Uranium for U.S. National Security Needs," July/August 2019, https://www.armscontrol.org/act/2019-07/features/rush-enrich-alternatives-providing-uranium-us-national-security-needs#bio.
[74] Patrice Bock et al, "Ukrainian power grids cyberattack," *InTech Magazine*, March/April 2017, https://www.isa.org/intech/20170406/.
[75] Tom Leithauser, "Ukraine grid attack sparks inquiry about U.S. power grid cybersecurity," *Cybersecurity Policy Report*, August 1, 2016, http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A460465703/ITOF?u=nysl_we_niagarau&sid=ITOF&xid=d17e0252.
[76] Ibid.
[77] Ibid.
[78] Bock et al, "Ukrainian power grids cyberattack."
[79] Ibid.
[80] Ibid.

longer to repair.[81] In fact, more than two months after the attack, the control centers [were] still not fully operational.[82]

In the winter of 2016, Ukraine suffered another crippling cyberattack against their power grid.[83] This time new malware known as Industroyer was unleashed and "shut down the power grid.. [of] Kiev, [the capital of] Ukraine".[84] Industroyer proved to be a substantial evolution from BlackEnergy, in that it was the first malware capable of compromising power grids automatically.[85] With many critical infrastructure sectors relying on electricity, a similar successful attack on the United States power grid would be devastating. A threat actor, according to a Congressional report, would only need to disable or disrupt nine power substations across the United States to cause a 'coast-to-coast blackout.[86]

3) Recommendations/Improvements:

The Stuxnet virus and cyberattacks on Ukraine's power grid demonstrate that the threats faced by our current critical infrastructure systems are vast, ever changing, and should serve as a call to action for the United States. In response, some have suggested that steps be taken to return older, non-computerized technologies to service.[87] For instance, legislation that would aim to protect the U.S. electric grid from hackers by studying ways to reincorporate older technologies into control systems was recently introduced in the United States Senate.[88]

Senate Bill S.174 – Securing Energy Infrastructure Act was placed on the Senate Legislative Calendar for further review and discussion on August 16, 2019.[89] Although not yet passed, the Bill outlines the new proposed strategy of the United States power grid operations: to increase the "use [of] analog and manual technology to isolate… important control systems".[90] To achieve this goal, "key devices like computer-connected operating systems that are vulnerable to cyberattacks [would be replaced] with

[81] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," last modified March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[82] Ibid.
[83] Robert Lipovsky, "Seven years after Stuxnet: Industrial systems security once again in the spotlight," last modified June 16, 2017, https://www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/
[84] Ibid.
[85] Ibid.
[86] J.M. Porup, "Why America is not prepared for a Stuxnet-like cyberattack on the energy grid," last modified January 28, 2019, https://www.csoonline.com/article/3336061/why-america-is-not-prepared-for-a-stuxnet-like-cyber-attack-on-the-energy-grid.html.
[87] Tom Leithauser, "Bill would study use of older tech to thwart power grid cyberattacks," *Cybersecurity Policy Report*, June 13, 2016, http://go.galegroup.com.ezproxy.niagara.edu/ps/i.do?p=ITOF&sw=w&u=nysl_we_niagarau&v=2.1&it=r&id=GALE%7CA456351445&sid=summon&asid=90a09485caed686de0b0bf677605aaf5.
[88] Ibid.
[89] "S.174 - Securing Energy Infrastructure Act," accessed October 19, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/174/text.
[90] Kate O'Flaherty, "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks," last modified June 3, 2019, https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#d6a07d3191d5.

analog and human-operated systems".[91] If the bill passes, the United States power grid would increasingly become disconnected and its component devices would no longer have internet access.[92]

Proponents for this model argue the greater "manual operations offer more control and lower risk" for defending against cyberattacks.[93] Further, the manual control ability was credited as a significant factor in Ukraine's power grid cyberattack recovery in 2015.[94] In contrast, our view is that this model may prove counter-intuitive in the long term. Manual controls reintroduce greater probability of human error, which could ultimately impact the safety and efficiency at which our nation's power grid currently operates.[95] To better combat such a wide and complex challenge, while still utilizing the advantages of technology devices, we recommend the adoption of a defense in depth approach.

A defense in depth scheme can be used to manage risk with diverse defensive strategies.[96] In other words, layering cyber defense controls and techniques is required. One layer to this approach should focus on better user training. In the case of the Stuxnet virus and the BlackEnergy cyberattack, the first line of the failed defense were the operators that introduced the exploits onto the networks and controllers. User-orientated phishing training campaigns can teach users of what to look for in malicious emails and attachments.[97] Promising studies indicate that phishing training helps users identify phishing emails".[98] Additionally, training users of the dangers associated with unknown USB devices should be incorporated, as infected USBs are often an overlooked threat.[99]

Another layer in the defense in depth approach is operational, i.e., ensuring firmware and other security patches are applied and up-to-date on all systems and controllers. Planning for system and controller security maintenance will need to be added to other routine mechanical maintenance tasks already in place today. Such operations should occur regardless of whether or not the specific controller is connected to the internet.

An additional area for improvement is the standardization of cyber-security technology in SCADA controllers and networks. One concept under development would interject anti-virus protection onto the SCADA controllers themselves.[100] For example, partnerships like the one between Intel Security's McAfee

---

[91] Leithauser, "Bill would study use of older tech to thwart power grid cyberattacks."
[92] O'Flaherty, "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks."
[93] Ibid.
[94] Ibid.
[95] Ibid.
[96] Sean Barnum, Michael Gegick, and C.C. Michael, "Defense in Depth," last modified September 13, 2005, https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth.
[97] Olga Zielinska et al., "One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 58, no. 1 (September 2014): 1466–70, https://doi-org.ezproxy.niagara.edu/10.1177/1541931214581306.
[98] Ibid.
[99] "Wombat security announces mobile-responsive, 508 compliant modules to increase training flexibility and accessibility for end users," *PR Newswire*, September 13, 2016, https://ezproxy.niagara.edu/login?url=https://search-proquest-com.ezproxy.niagara.edu/docview/1818653125?accountid=28213.
[100] "Honeywell and Intel Security collaborates to secure critical infrastructure and Industrial Internet of Things," *Telecom Tiger*, June 27, 2015, http://bi.galegroup.com.ezproxy.niagara.edu/essentials/article/GALE%7CA419572982?u=nysl_we_niagarau&sid=summon.

and Honeywell Industrial Cyber Security Solutions seek to provide "enhanced security software [onboard SCADA devices in order to protect]… control systems from malware and misuse".[101]

Further standardizations could require that the default password be changed when setting up an industrial controller or SCADA device.[102] In regards to IoT devices, the State of California is preparing to enforce similar policies through legislation "mandating [IOT] device manufacturers… create a unique password for each device… or require the user to create one when they interact with the device for the first time".[103] Despite the relatively straightforward approach to implement many of these suggestions, there is currently a lack of central legislation to drive the adoption of such changes.

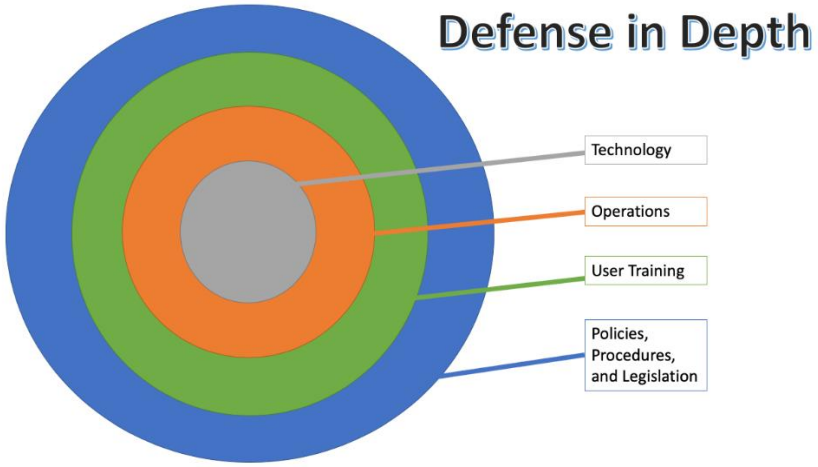

Figure 2

As evidenced in Figure 2[104], polices, procedures, and legislation will be a critical first layer to the proposed defense in depth approach. Future legislation requiring integrated cyber-security measures for SCADA and ICS devices should be explored and adopted. Moreover, legislation requiring cyber threat user training for all our nation's critical infrastructure industries should also be implemented. Without regulation, a comprehensive defense in depth approach will be next to impossible to implement. The popular belief that there is "sufficient financial and business incentives currently in place to encourage private firms to protect their own systems and networks," is an outdated mindset in our view.[105] A more

[101] Ibid.
[102] Andrii Degeler, "California bans default passwords on any internet-connected device," last modified October 5, 2018, https://www.engadget.com/2018/10/05/california-default-password-ban-information-privacy-connected-devices-bill/?ncid=txtlnkusaolp00000616.
[103] Ibid.
[104] Vishruta Rudresh, "Securing Industrial Control Systems: A Holistic Defense-In-Depth Approach," last modified April 16, 2018, https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/.
[105] Cath Everett, "Who is responsible for securing critical infrastructure?," *Computer Fraud & Security,* 2010 no. 10 (2010): 5-8, https://doi.org/10.1016/S1361-3723(10)70130-5.

hardline approach should be adopted as "governments have a responsibility to intervene in the[ir] national interest".[106]

Lastly, a final recommendation to improve the overall defense in depth strategy is to enhance current partnerships among the United States and its allies. Canada, arguably one of the United States' strongest and geographically closest allies, also shares some critical infrastructure networks and resources. Collaboration should continue to be built and fostered, to "deepen [the] cooperation between U.S. and Canadian cyber emergency response teams".[107] The 2010 Canada-United States Action Plan for Critical Infrastructure was created with exactly this goal in mind.[108]

The Action Plan lays out initiatives to promote cooperation in strengthening the security and resiliency of critical infrastructure for both nations.[109] The cooperation outlined by the plan will "provide for more robust private-sector information sharing and promote better 'public awareness' of the multifaceted cyber threat".[110] The United States and Canada, potentially along with other key allies, should also explore more offensive cyber capabilities as part of their defense in depth strategy to protect critical infrastructures. Trusted partner nations, such as those as part of the Five Eyes Alliance (United States, United Kingdom, Canada, Australia, and New Zealand), may also be considered to be included in such efforts.[111]

4) Conclusion:

Critical infrastructure systems will remain an important asset for the United States. Steps need to be taken to ensure they improve their information security posture to maintain protection from cyberattack and vulnerabilities. With critical infrastructures serving as the backbone of our nation's economy, security, and health, any interruption to their services provided can have dire consequences.[112] The threat faced by critical infrastructure systems is present and ongoing.

To further illustrate this point, Russia was recently discovered to be making attempts against United States critical infrastructure control systems.[113] As recently as March 15, 2018, the "Russian government [took] actions targeting U.S. Government entities".[114] The Russians in this case specifically

---

[106] Ibid.

[107] Scott Shackelford and Zachery Bohm, "Securing North American critical infrastructure: a comparative case study in cybersecurity regulation," *Canada-United States Law Journal*, (2016): 61+, http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A468334914/AONE?u=nysl_we_niagarau&sid=AONE&xid=9fa623da.

[108] Celia Louie, "U.S.-Canada Cybersecurity Cooperation," last modified September 8, 2017, https://jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/.

[109] Ibid.

[110] Shackelford and Bohm, "Securing North American critical infrastructure: a comparative case study in cybersecurity regulation."

[111] Louie, "U.S.-Canada Cybersecurity Cooperation."

[112] "What is Critical Infrastructure?"

[113] Bruce Sterling, "US-Cert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," last modified March 15, 2018, https://www.wired.com/beyond-the-beyond/2018/03/us-cert-russian-government-cyber-activity-targeting-energy-critical-infrastructure-sectors/.

[114] Ibid.

targeted "organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors".[115]

Perhaps most alarming is that the Russians targeted areas of weakness that had previously been identified as needing current improvement. The Russian threat actors, "targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks".[116] Additionally, the malicious actors "conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems" and SCADA devices.[117]

Although the Russian hackers in this case were discovered and stopped before any real damage could occur, it helps bring to light the very real and present threat our critical infrastructures face today. In adopting a defense in depth strategy that focuses on users, multi-national partnerships, operations, technology, policies, and legislation, the United States could significantly harden its current critical infrastructure control systems. The cyber security effort surrounding such systems will be required to evolve, match, and overcome any cyber threat of tomorrow.

References:

Barnum, Sean, Gegick, Michael, and Michael, C.C. "Defense in Depth." Last modified September 13, 2005. https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth

Bock, Patrice, Hauet, Jean-Pierre, Francoise, Romain, and Foley, Rober. "Ukrainian power grids cyberattack." *InTech Magazine*, March/April 2017. https://www.isa.org/intech/20170406/.

"Critical Infrastructure Sectors." Accessed March 30, 2019.

https://www.dhs.gov/critical-infrastructure-sectors.

Degeler, Andrii. "California bans default passwords on any internet-connected device." Last modified October 5, 2018. https://www.engadget.com/2018/10/05/california-default-password-ban-information-privacy-connected-devices-bill/?ncid=txtlnkusaolp00000616.

Everett, Cath. "Who is responsible for securing critical infrastructure?." *Computer Fraud & Security,* 2010 no. 10 (2010): 5-8. https://doi.org/10.1016/S1361-3723(10)70130-5.

Farwell, James and Rohozinski, Rafal. "Stuxnet and the Future of Cyber War." *Survival*, 53 no.1 (2011): 23-40. https://doi-org.ezproxy.niagara.edu/10.1080/00396338.2011.555586.

Hippel, Frank N. von and Weiner, Sharon K. "No Rush to Enrich: Alternatives for Providing Uranium for U.S. National Security Needs." *Arms Control Association*, July/August 2019. https://www.armscontrol.org/act/2019-07/features/rush-enrich-alternatives-providing-uranium-us-national-security-needs#bio.

"Honeywell and Intel Security collaborates to secure critical infrastructure and Industrial Internet

[115] Ibid.
[116] Sterling, "US-Cert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors."
[117] Ibid.

of Things." *Telecom Tiger,* June 27, 2015. http://bi.galegroup.com.ezproxy.niagara.edu/essentials/article/GALE%7CA419572982?u=nysl_we_niagarau&sid=summon.

Igure, Vinay, Laughter, Sean, and Williams, Ronald. "Security issues in SCADA networks." *Computers & Security,* 25 no. 7 (2006): 498-506. https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2006.03.001.

"InfraGard, Critical Infrastructure Sectors." Accessed October 19, 2019. https://www.infragard.org/Application/General/SectorList.

Interagency Security Committee. "Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper." February 2015. https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf

Leithauser, Tom. "Bill would study use of older tech to thwart power grid cyber Attacks." *Cybersecurity Policy Report*, June 13, 2016. http://go.galegroup.com.ezproxy.niagara.edu/ps/i.do?p=ITOF&sw=w&u=nysl_we_niagarau&v=2.1&it=r&id=GALE%7CA456351445&sid=summon&asid=90a09485caed686de0b0bf677605aaf5

Lipovsky, Robert. "Seven years after Stuxnet: Industrial systems security once again in the spotlight." Last modified, June 16, 2017. https://www.welivesecurity.com/2017/ 06/16/seven-years-stuxnet-industrial-systems-security-spotlight/.

---. "Ukraine grid attack sparks inquiry about U.S. power grid cybersecurity." *Cybersecurity Policy Report*, August 1, 2016. http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A460465703/ITOF?u=nysl_we_niagarau&sid=ITOF&xid=d17e0252

Louie, Celia. "U.S.-Canada Cybersecurity Cooperation." Last modified September 8, 2017. https://jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/.

Minoli, Daniel. *Building the Internet of Things with IPv6 and MIPv6 : The Evolving World of M2M Communications.* Somerset:John Wiley & Sons, Incorporated, 2013. https://ebookcentral.proquest.com/lib/niagara-ebooks/reader.action?docID=1216195&ppg=21.

Murphy, Steve. "The State of Cybersecurity in the Water/Wastewater Market." *InfraGard Journal*, Volume 1. https://www.infragardnational.org/wp-content/uploads/2019/05/The-State-of-Cybersecurity-in-the-WaterWastewater-Market.pdf

Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. "SCADA security in the light of Cyber-Warfare." *Computers & Security,* 31, no. 4 (2012): 418-436. https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2012.02.009.

O'Flaherty, Kate. "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks." Last modified June 3, 2019. https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#d6a07d3191d5.

Porup, J.M. "Why America is not prepared for a Stuxnet-like cyberattack on the energy grid."

Last modified January 28, 2019. https://www.csoonline.com/article/3336061/why-america-is-not-prepared-for-a-stuxnet-like-cyber-attack-on-the-energy-grid.html.

Puskala, Matt. "Industrial Security: 4 Ways to Keep Your Factory Safe from Cyber Attacks."

Last modified September 23, 2016. https://www.dmcinfo.com/latest-thinking/blog/id/9293/industrial-security-4-ways-to-keep-your-factory-safe-from-cyberattacks.

Rudresh, Vishruta. "Securing Industrial Control Systems: A Holistic Defense-In-Depth Approach." Last modified April 16, 2018. https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/.

"S.174 - Securing Energy Infrastructure Act." Accessed October 19, 2019.

https://www.congress.gov/bill/116th-congress/senate-bill/174/text.

Shackelford, Scott and Bohm, Zachery. "Securing North American critical infrastructure: a

comparative case study in cybersecurity regulation." *Canada-United States Law Journal*, (2016): 61+. http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A468334914/AONE?u=nysl_we_niagarau&sid=AONE&xid=9fa623da.

Sterling, Bruce. "US-Cert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." Last modified March 15, 2018. https://www.wired.com/beyond-the-beyond/2018/03/us-cert-russian-government-cyber-activity-targeting-energy-critical-infrastructure-sectors/.

"What is Critical Infrastructure?" Accessed March 30, 2019. https://www.dhs.gov/sites/default/files/publications/ip-fact-sheet-508.pdf.

"Wombat security announces mobile-responsive, 508 compliant modules to increase training flexibility and accessibility for end users." *PR Newswire*, September 13, 2016. https://ezproxy.niagara.edu/login?url=https://search-proquest-com.ezproxy.niagara.edu/docview/1818653125?accountid=28213.

Zetter, Kim. "Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software." Last modified January 19, 2012. https://www.wired.com/2012/01/scada-exploits/.

--- "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Last modified March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zielinska, Olga, Rucha Tembe, Kyung Wha Hong, Xi Ge, Emerson Murphy-Hill, and

Christopher B. Mayhorn. "One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* 58, no. 1 (September 2014): 1466–70. https://doi-org.ezproxy.niagara.edu/10.1177/1541931214581306.