6

Cyber Defense as Environmental Protection—The Broader Potential Impact of Failed Defensive Counter Cyber Operations

JAN KALLBERG

ROSEMARY A. BURK

Contents

Introduction

Key in the critique of the likelihood of cyber conflict has been the assumption that cyber does not lead to long-term and irrevocable effects; therefore it cannot be fought as a war. This might be true if cyber attacks are constrained to specific functions of a computer system or set of client computers; however, a failed cyberdefense can have wider effects than discussed in earlier debates of potential consequences and risks. The environmental aspect of cyberdefense has not drawn attention as a national security matter. We all, as people, react to threats to our living space and natural environment. Jeopardizing the environment, unintended or intended, has historically led to the immediate injection of fear and strong reactions in the population. Even unanticipated accidents with environmental impact have triggered strong moves in the public sentiment toward fear, panic, anger against government, and challenges to public authority.

One such example is the Three Mile Island (Pennsylvania) accident that created significant public turbulence and fear—an incident that still has a profound impact on how we envision nuclear power. For a covert state actor that seeks to cripple our society, embarrass the political leadership, and project to the world that we cannot defend ourselves, environmental damages are inviting. An attack on the environment feels for the general public more close and scary than a dozen servers malfunctioning in a server park. We are all dependent on clean drinking water and non-toxic air. Cyber attacks on these fundamentals for life could create panic and desperation in the general public, even if the reacting citizens were not directly affected.

Adversarial nations pursue covertly, or later as open hostile acts in a cyber conflict, the ability to create significant damage and disruption as noted by the President of the United States in "Sustaining US global leadership: priorities for 21st century defense":

> Both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland.[1]

The U.S. Secretary of Defense Leon Panetta delivered in his speech on October 12, 2012 a clear assessment of the risk for these attacks:

> These attacks mark a significant escalation of the cyber threat and they have renewed concerns about still more destructive scenarios that could unfold. For example, we know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country.
>
> We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking

> to create advanced tools to attack these systems and cause panic and destruction and even the loss of life.[2]

Even if the nation's leadership has identified the risk, expressed concern, and started to allocate resources to improve national cyberdefense, the likelihood of a cyberwar is considered by some scholars as marginal. One of the leading arguments against the likelihood for future cyberwar has been the absence of long-term damage.[3] This argument is based on a marginalization of cyber attacks as intermittent disruptions of client computers built on crude and unsophisticated distributed malign software that create temporal havoc.[4] These attacks are portrayed to be anecdotal disruptions of minor importance, maybe not even noticed by the target. The perception of damage is limited to the attacked computer networks, not the external environment that relies on these networks. The wider and holistic outlook on cyber, beyond the computer networks, is embedded in the concerns aired by Secretary of Defense Leon Panetta, originating from the assessment made by the president.

In this chapter we present a tangible argument for the long-term damage cyberwar can inflict on a targeted society beyond the actual destruction of a defending computer network. When a computer system, such as an industrial control system, fails, it is a component of a larger system. A failure in the larger system can create long-term environmental consequences. The environmental damage is a consequence of a lost cyberwar and failed national cyberdefense.

The last decade's intense study of cyber security with a focus on networks and network security has left the environmental risk posed by cyber-controlled networks unaddressed.[5] Cyber security tends to be narrowly focused on information assurance and the network conduit. The focus on cyber security has included providing for restoration of information systems by incorporating detection, protective, and reactive capabilities. From the information security's early inception in the 1980s to today's secured environments, we have become skilled in our ability to secure and harden information systems. The fluid, even soon-automated, battlefield of cyber operations is a novelty. An automated attack can discover and exploit a multitude of vulnerabilities, and by doing so being able to attack a specific utility at many locations at the same time. Instead of focusing on hardening systems, cyber defense has to go beyond the actual computer system and see what is impacted by the computer system and the effects that can occur.

The Concept of Cyberwar

Cyberwar, as any war, is a conflict between state actors in the pursuit of seeking a policy change in the other party. Therefore, cyberwar has to been seen first from a strategic viewpoint and second from lower levels of abstraction. A central part in all conflict is the fear of consequences—the actual repercussions of opposition to a will that seek to subdue. The reason why nuclear weapons are feared is because the weapons have validated and visualized devastating effects. Cyber weapons will need to show damage; otherwise the threat or deterrence with cyber weapons evaporates. In earlier studies of cyberwar, the key focus included technical or military temporal capacity disruptions and resilience through ability to operate in a degraded environment. The potential ability to destroy opposing systems through digital lethality has only recently been introduced.[6] In these scenarios, the factual long-term damage is limited. For an adversary who seeks to impact U.S. policy, current vulnerabilities in our industrial control systems are an inviting opportunity because of the possibility of tangible damage. Industrial control systems are viable targets mainly by several second-tier effects such as societal impact factors—fear, uncertainty, and public pressure on political leadership if environmental damage occurs.

Attacking industrial control systems in pursuit of environmental damage is an act of war. As long as attribution is unsolved and there is no punitive mechanism in place, the prohibitions against such acts in international law are at the attacker's discretion to recognize. If the adversary is skilled, it is more likely the attribution investigation will end with a set of spoofed, innocent actors whose digital identities have been exploited in the attack rather than attribution to the real perpetrator. A strong suspicion would impact interstate relations, but full attribution and traceability are needed to create a case for reprisal and retaliation. Today, there are limited options to enforce accountability for cyber attacks through international law, if any. The threat posed by the adversarial nations' pursuit to hijack industrial control systems in covert cyber operations becomes real when there are no risks for the attacking party. The scenario becomes more complex if a state actor gathers information about cyber vulnerabilities in the networks of a targeted organization or other nation and then outsources the attack to a criminal or terrorist network. This innovative *modus operandi* creates numerous obstacles and considerations for the targeted country. States can pay to get things done. If necessary, a covertly operating state can pay criminal networks cash, drugs, weapons, or any currency to act as a proxy. Terrorist organizations can finance their operations through cyber operational "entrepreneurship" instead of engaging in other forms of financing far riskier for detection such as drug dealing and credit card fraud. The covert warfare in cyberspace resembles in many cases the covert operations in the Cold War. The targeted country, or organization, could assume where the attack is coming from, but attribution is not strong enough for retribution.

Environmental Effects of Cyberwar

If an adversary can create major irreversible environmental damage to the United States through cyber attacks on industrial control systems, or even pre-conflict establish control over numerous systems, it would defuse U.S. policy options. The threat and risk have to be considered, and it would give a minor power a force multiplying effect in a direct conflict with the United States.

The barrage of cyber attacks on the nation's infrastructure in the last decade is a major concern for the federal government.[7] These attacks have been extended to include SCADA (supervisory control and data acquisition) systems which are a subset of industrial control systems. SCADA systems control the processes in our industry, energy sector, transportation, lights, and signals, and are the backbone in the technical structure of our society. SCADA systems can remain viable for decades, depending on the processes and machinery these systems control. However, SCADA systems often lack capacity or are difficult to upgrade to meet contemporary cyber security challenges. Many of these systems were never intended or designed to be connected to any other computer, let alone linked to a global information network as the Internet conduit. The range of vulnerabilities has increased dramatically as embedded software in electro-mechanical machinery has become a standard feature. These programmable controllers in industry and utility companies have limited cyber security features. The hardening and increased protection of American SCADA systems is likely to take decades; the majority of SCADA systems are not upgraded once installed or need additional computer hardware to be secured. The defense of these systems is defense in depth, where the corporations and municipalities are parties as well as the Department of Defense in conjunction with other federal agencies. The most able components in these defensive layers reside within the federal sphere. The question is that if cyberdefense fails, what could happen? The environmental ramifications have not received appropriate attention in comparison to the potential threat.

Hydroelectric Dams and Reservoirs

As an example, a cascading effect of failing dams in a larger watershed would have significant environmental impact. Hydroelectric dams and reservoirs are controlled using different forms of computer networks, either cable or wireless, and the control networks are connected to the Internet. A breach in the cyberdefenses for the electric utility company leads all the way down to the logic controllers that instruct the electric machinery to open the floodgates. Many hydroelectric dams and reservoirs are designed as a chain of dams in a major watershed to create an even flow of water that is utilized to generate energy. A cyber attack on several upstream dams would release water that increases pressure on downstream dams. With rapidly diminishing storage capacity, downstream dams risk being breached by the oncoming water. Eventually, it can turn to a cascading effect through the river system which could result in a catastrophic flood event. The traditional cyber security way to frame the problem is the loss of function and disruption in electricity generation, overlooking the potential environmental effect of an inland tsunami. This is especially troublesome in areas where the population and the industries are dense along a river; for example, Pennsylvania, West Virginia, and other areas with cities built around historic mills. If the cyber attack occurs during a hurricane[8] when the dams are already stressed, any rapid increase in water level that adds to the hurricane can trigger cascading dam collapses. This could lead to a catastrophic loss of lives and property and a corresponding loss of hydroelectric capacity.

The environmental effects would be dramatic and long term: freshwater resources would be contaminated, complete ecosystems destroyed, toxic agents released, and massive soil erosion. Populations of fishes could be decimated along with fisheries that rely upon them. The short-term and long-term effects would be substantial, and restoration efforts could be beyond the national financial reach. The environmental damage is then permanent.

U.S. Chemical Industry

Another example is the sizable U.S. chemical industry. Manufacturing plants and storage facilities store large quantities of industrial chemicals. The U.S. chemical industry produced chemical products to a value of $759 billion in 2011.[9] Over 96% of all manufactured products in the United States are relying on chemical input material. The United States produces 15% of the world's chemicals. In the United States, each year 847 million tons of chemicals are transported on railways, highways, and freight ships.[10] The transportation routes are adjacent or passing creeks, rivers, ground water aquifers, urban areas, and agricultural land. These chemical fluids can, once released, create contamination that requires long-term mitigation, restoration, and in some cases land subsidence equal to an EPA superfund site.[11] If Syria, or any other totalitarian adversarial developing nation, used chemical weapons against civilian Americans the response would have biblical proportions. An attack on the industrial control systems in our chemical industry could have a similar effect with limited risk of severe repercussions for the attacker. Chemicals can infiltrate to groundwater and make the water a health hazard, pollute the air, contaminate soil, and lead to land subsidence for housing, agriculture, and development. Damages such as those are irreversible—if the national cyberdefense fails.

Public Opinion and Sentiment

Environmental damages are tangible and highly visible—flooding, undrinkable water, mudslides, toxic air, and chemical spills directly affect the population and their surrounding environment. A failed computer server park does not drive media attention and becomes something for discussion in the general population, as a hundred thousand dead fishes floating down a river. The environmental impact is visible, connects with people on a visceral level that computers as of today has not reached, and generates a notion that the human core of existence is in jeopardy. Environmental damages trigger radical shifts in the public mind and general sentiment. For a minor state actor, such as an adversarial developing nation, these attacks can be done with marginal budget and resources and still create significant political turbulence and loss of confidence in the population of a major power. War, as mentioned, seeks to change policy and influence another nation to take steps that it earlier was unwilling to take. The panic that can follow environmental damages is a political force worth recognizing.

Loss of Legitimacy and Authority

Covert successful cyber attacks that lead to environmental impact are troublesome for the government, not only the damage but also the challenge to legitimacy, authority, and confidence in the government and political leadership. The citizens expect the state to protect them. The protection of the citizens is a part of the unwritten social contract between then citizens and the government. The federal government's ability to protect is taken for granted—it is assumed to be in place. If government fails to protect and safeguard the citizens, the legitimacy is challenged. Legitimacy concerns not who can lead but who can govern. A failure to protect is a failure to govern the nation, and legitimacy is eroded. Political scientist Dwight Waldo believed that we need faith in government; for government to have a strong legitimacy it has to project, deliver, and promise that life would be better for citizens. In a democracy, voters need a sense that they are represented, government works in their best interests, and government improves life for citizens and voters. In the "Administrative State,"[12] Waldo defined his vision of the "good life" as the best possible life for the population that can be achieved based on time, technology, and resources.[13] Authority is the ability to implement policy.

Environmental hazards that lead to loss of life and dramatic long-term loss of life quality for citizens trigger a demand for the government to act. If the population questions the government's ability to protect and safeguard, the government's legitimacy and authority will suffer. One example is the Three Mile Island accident that had an impact, even decades after the incident, on how citizens perceived the government's nuclear policies and ability to ensure that nuclear power was a safe energy source. Harold R. Denton, the director of the Office of Nuclear Reactor Regulation, was able to calm the public and reduce fear during the Three Mile Island accident.[14] During the duration of the events, Harold R. Denton was President Carter's personal representative at the site.[15] It was essential for President Carter to show and project ability to handle the incident and to restore confidence in the general public for the government's energy policies. Environmental risks tend to appeal not only to our general public's logic but also to emotions, foremost to the notion of uncertainty and fear. A population that fears the future has lost confidence in government.

The difference between the Three Mile Island incident and cyber attacks on our infrastructure creating environmental damage is that the Three Mile Island incident was local, solitary, and could be contained and understood. During the Three Mile Island incident, millions of Americans had a sincere fear for their life and future when faced with the possibility of a nuclear meltdown.

Cyber attacks on our national infrastructure cannot be predicted or contained, and these attacks can be massive if the exploit utilized for the attack is a vulnerability that many systems contain. The fear generated by the Three Mile Island incident could in retrospect have been marginal to the fear generated by a large-scale cyber attack on the national infrastructure.

Environmental Cyberdefense

Defending American infrastructure from cyber attacks is not only protecting information, network availability, or the global information grid, it is also safeguarding the lives of citizens and property and protecting ecosystems and the ecosystem services that we rely upon. Attacks on the environment and the quality of life of the citizenry directly affect the confidence the population has in the government's ability to govern.

The national cyberdefense organized by the Department of Defense and other government agencies is on a "green" mission to ensure that cyber attacks do not create irreversible environmental damage within the United States and loss of quality of life. For an adversarial nation that seeks to influence our population and inject fear, cyber-created environmental damages have a high payoff, especially if the cyber operations are covert and unlikely to be attributed. Successful cyberdefense mitigates the risk for significant damage to domestic freshwater drinking resources and aquatic and adjacent terrestrial ecosystems and protects biological diversity. The risk posed by the adversarial nations' pursuit to hijack industrial control systems in covert cyber operations cannot be ignored as a national security concern. Cyberdefense is, due to the consequences of failing, not only a military matter but an environmental protection issue.

Endnotes

1. Obama, Barack, and Leon E. Panetta. Sustaining US global leadership: Priorities for 21st century defense. Vol. 1. Washington DC: The White House, 2012.
2. Defending the Nation from Cyber Attack (Business Executives for National Security), as delivered by Secretary of Defense Leon E. Panetta, New York, October 11, 2012.
3. Rid, Thomas. Cyber war will not take place. *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.
4. Rid, Thomas, and Peter McBurney. Cyber-Weapons. *The RUSI Journal* 157, no. 1 (2012): 6–13.
5. Turk, Robert J. Idaho National Laboratory. 2005. US-CERT Control Systems Security Center. Cyber Incidents Involving Control Systems. INL/EXT-05-00671. http://www.inl.gov/technicalpublications/documents/3480144.pdf.
6. Kallberg, Jan, and Adam Lowther. The Return of Dr. Strangelove. *The Diplomat*, August 20, 2012.
7. Lynn III, William F. Defending a New Domain—The Pentagon's Cyberstrategy. *Foreign Affairs* 89 (2010): 97.
8. Susman, Tina, Molly Hennessy-Fiske, and John M. Glionna. Isaac leaves hundreds of homes underwater; dam shows stress. *Los Angeles Times,* August 30, 2012. http://articles.latimes.com/2012/aug/30/nation/la-na-isaac-storm-20120831.
9. American Chemistry Council. http://www.americanchemistry.com/Jobs/EconomicStatistics/Industry-Profile/Global-Business-of-Chemistry
10. American Chemistry Council. Global Business of Chemistry. http://www.americanchemistry.com/chemistry-industry-facts.
11. EPA. Superfund Sites. National Priorities List. http://www.epa.gov/superfund/sites/npl/where.htm.
12. Waldo, Dwight. (1948) 1984. *The Administrative State*. New York: Holmes & Meier.

13. Waldo, Dwight. 1980. *The Enterprise of Public Administration*. Novato: Chandler & Sharp.
14. Pennsylvania Historical & Museum Collection. Manuscript Group 471: Harold and Lucinda Denton Papers. Accident at Three Mile Island. http://www.portal.state.pa.us/portal/server.pt/community/documents_from_1946_-_present/20426/three_mile_island/999081.
15. PBS. People and Events: Harold R. Denton. http://www.pbs.org/wgbh/amex/three/peopleevents/pandeAMEX87.html.