Failed Cyberdefense

The Environmental Consequences of Hostile Acts

Jan Kallberg, Ph.D., and Rosemary A. Burk, Ph.D.

(FEMA, David Valdez)

A FAILED CYBERDEFENSE CAN have wider effects than discussed in earlier debates of potential consequences of a cyberattack. The need for cyberdefense to protect the environment has not drawn the attention it deserves as a national security matter. Adversarial nations are covertly pursuing methods to damage and disrupt the United States in a cyberconflict in the future. The president of the United States noted this in *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*:

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

Jan Kallberg is an assistant professor at Arkansas Tech University and a research associate at the Cyber Security Research and Education Center, the University of Texas at Dallas. He holds a Ph.D. from the University of Texas at Dallas. His works have been published in Joint Force Quarterly, Strategic Studies Quarterly, Air and Space Power Journal, IEEE Access, *and* IEEE Security and Privacy.

Rosemary Burk is an assistant professor in biology at Arkansas Tech University. She holds a Ph.D. from the Department of Biological Sciences at the University of North Texas. Her research has been published by International Journal of Water Resource Development *and* Journal of Freshwater Ecology.

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

> These attacks mark a significant escalation of the cyberthreat, and they have renewed concerns about still more destructive scenarios that could unfold. For example, we know that foreign cyberactors 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, others consider the likelihood of a cyberwar as marginal. One of the leading arguments against the possibility of future cyberwar has been the premise that such an attack would cause no long-term damage.[3] This argument is based on a marginalization of cyberattacks as intermittent disruptions of client computers by crude and unsophisticated malign software that creates temporary havoc.[4] The perception is that damage is limited to the attacked computer networks—not the external environment that relies on these networks. However, the concerns aired by Panetta, originating from the assessment made by the president, convey a wider, more holistic perception of potential damage beyond computer networks.

In this article we present a tangible argument that cyberwar can inflict continuing damage on a targeted society beyond the actual destruction of a defending computer network. The long-term environmental consequences of a lost cyberwar and failed national cyberdefense are not well recognized. The last decade's intense study of cybersecurity, with its focus on networks and network security, has left the risk to physical environments that rely upon cybercontrolled networks unaddressed.[5]

The Concept of Cyberwar

In cyberwar conflicts, state actors are seeking to force a policy change in the other party. Therefore, cyberwar should be regarded 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 seeks to subdue. Nuclear weapons are feared because of their validated and graphically devastating effects. Cyberweapons will need to show they are catastrophic; otherwise, the threat or deterrence of those weapons evaporates.

In earlier studies of cyberwar, the focus was on disruptions in technical or military capacity and the resilience to operate in a degraded environment. The potential to destroy opposing systems through digital lethality has recently been introduced.[6] In these scenarios, the factual long-term damage is limited. For an adversary seeking to affect U.S. policy, current vulnerabilities in our industrial control systems are an inviting opportunity. Their targeting could have significant societal impacts—fear, uncertainty, and public pressure on political leadership if environmental damage occurs.

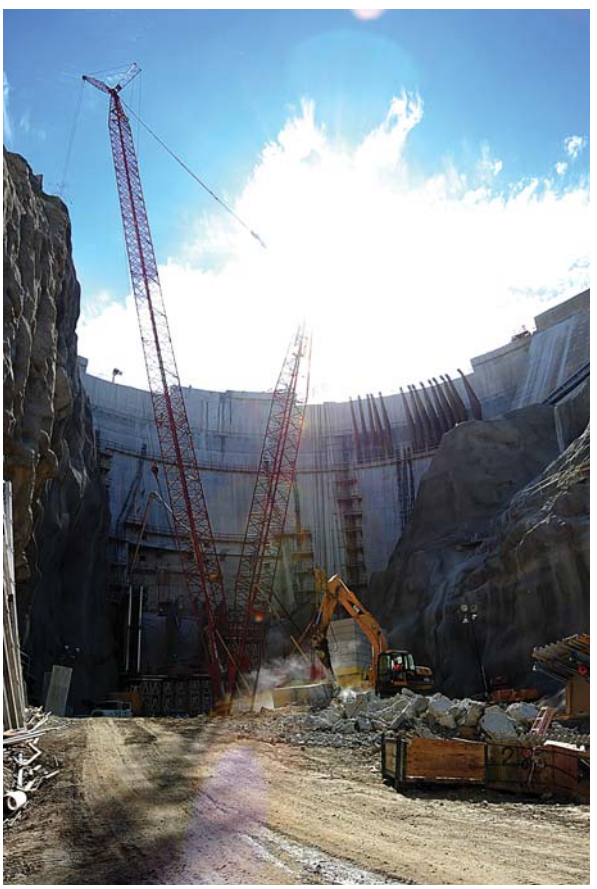
Attacking industrial control systems to damage the environment is a grave act of war. However, as long as attribution is unknown and there is no punitive mechanism in place, the prohibitions against such acts in international law are at the attacker's discretion to recognize. Today, there are limited options, if any, to enforce accountability for cyberattacks through international law.

Environmental Effects of Cyberwar

If an adversary could cause major irreversible environmental damage to the United States through cyberattacks on industrial control systems, or merely establish control over numerous systems, it could limit U.S. policy options. The threat and risk of a cyberattack would 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 cyberattacks 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 supervisory control and data acquisition (SCADA) systems, which are a subset of industrial control systems. SCADA systems control

the processes in our energy, transportation, water management, and other industries. They 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 cybersecurity challenges. Many of these systems were never intended nor designed to be connected to any other computer, let alone linked to a global information network such as the Internet. 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 cybersecurity features. The hardening and increased protection of American SCADA systems is likely to take decades; the majority of the SCADA systems are not upgraded once installed and 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—if cyberdefense fails, what could happen? The environmental ramifications deserve as much attention as the potential threat to computer systems.



The Big Tujunga Dam is under construction to reinforce the walls due to an increased debris flow from recent severe winter storms, La Canada Flintridge, Calif., 2 August 2010. (Adam DuBrowa, FEMA)

Hydroelectric Dams and Reservoirs

For example, a series of dam failures in a large watershed would have significant environmental impacts. Hydroelectric dams and reservoirs are controlled using different forms of computer networks, either cable or wireless, and the control networks connect to the Internet. A breach in the cyberdefenses of an electric utility company could lead 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 for generating energy. A cyberattack on several upstream dams could release water that would increase pressure on downstream dams. With rapidly diminishing storage capacity, downstream dams would risk being breached by the oncoming water. Eventually, the attack could have a cascading effect, literally and figuratively, through the river system and result in a catastrophic flood. The traditional cybersecurity way to frame the problem is to consider the loss of function and disruption in electricity generation—overlooking the potential environmental effect of an inland tsunami. This is especially troublesome where the population and the industries are dense along a river, such as in Pennsylvania, West Virginia, and other areas with cities built around historic mills. If the cyberattack occurred during a heavy rain when the dams were already stressed, any rapid increase in water level could trigger successive dam collapses.[8] This could lead to a catastrophic loss of lives and property and a critical 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 soil heavily eroded or

completely washed away. Fish populations would be decimated along with fisheries that rely upon them. The short-term and long-term effects would be substantial, and restoration efforts could be too costly for the nation to pursue. The environmental damage would be permanent.

U.S. Chemical Industry

The sizeable U.S. chemical industry provides another example of the potential environmental impact of a cyberattack. Manufacturing plants and storage facilities store large quantities of industrial chemicals. The U.S. chemical industry produced $759 billion of chemical products in 2011.[9] Over 96 percent of all manufactured products in the United States rely on the input of chemical material. The United States produces 15 percent of the world's chemicals. Each year the United States transports 847 million tons of chemicals on railways, highways, and freight ships.[10] The transportation routes are adjacent to or passing creeks, rivers, ground water aquifers, urban areas, and agricultural land. These chemical fluids could, once released, create contamination that requires long-term mitigation, restoration, and in some cases land subsidence equal to an EPA superfund site.[11]

Chemicals could infiltrate groundwater and make it a health hazard, pollute the air, contaminate the soil, and make land unsuitable for housing, agriculture, and development. Environmental damage could be irreversible if the national cyberdefense failed.

Environmental Defense

Defending American infrastructure from cyberattacks is not only protecting information, network availability, or the global information grid. It is also safeguarding the lives of citizens, protecting property, and preserving ecosystems and the ecosystem services that we rely on. An attack leading to environmental damages could impact our societal stability.[12]

The national cyberdefense organized by the Department of Defense and other government agencies is on a "green" mission to ensure cyberattacks do not create irreversible environmental damage within the United States. Successful cyberdefense mitigates the risk for significant damage to domestic freshwater drinking sources, aquatic and adjacent terrestrial ecosystems, and biological diversity. This mission must continue to protect the natural resources essential for life. ***MR***

NOTES

1. Barack Obama and Leon E. Panetta, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Vol. 1 (Washington DC: Government Printing Office, 2012).

2. Leon E. Panetta, "Defending the Nation from Cyber Attack" (speech given to Business Executives for National Security, New York, 11 October 2012).

3. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

4. Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (2012): 6-13.

5. 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. Jan Kallberg and Adam Lowther, "The Return of Dr. Strangelove," *The Diplomat*, 20 August 2012.

7. William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (2010): 97.

8. "Isaac Leaves Hundreds of Homes Underwater; Dam Shows Stress," *Los Angeles Times*, 30 August 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, <http://www.americanchemistry.com/chemistry-industry-facts>.

11. Environmental Protection Agency. Superfund Sites, <http://www.epa.gov/superfund/sites/npl/where.htm>.

12. Jan Kallberg and Bhavani Thuraisingham. "State Actors's Offensive Cyber Operations—The Disruptive Power of Resourceful Systematic Cyber Attacks," *IEEE IT Professional* 15, no. 3 (2013): 32-35.