10

After the Cyber Pearl Harbor

Vulnerability and Resiliancy in a Networked World

AARON BRANTLY

> I fear all we have done is to awaken a sleeping giant and fill him with a terrible resolve.
>
> —ADMIRAL ISOROKU YAMAMOTO, IN *TORA! TORA! TORA!*

When the last of the fires had been put out and the final screams from the sunken USS Arizona had been forever silenced, the United States rose from an act of strategic and tactical surprise unlike any it had previously experienced. Less than a day after the attacks on Pearl Harbor, President Roosevelt was able, with the support and approval of Congress, to declare war. In the following weeks, months, and years, millions of citizen soldiers would be mobilized and the entire industrial base of a nation would be placed on war footing. An isolationist nation became a nation reinvigorated by a warrior's resolve. A sleeping giant had risen to action.

Seventy-three years later the image of a nation caught unawares haunts us and forces us to consider the implications similar attacks. But post-World War-II conflicts have rarely been so straightforward. Since World War II the United States has not formally declared war on another country. War carries unprecedented risk in the nuclear age, and what constitutes an act of war is not always clear.

What follows is a conflict scenario followed by a discussion of policy issues that would need to be addressed during and after a catastrophic cyber attack on the United States. The conflict scenario, while extreme, is nevertheless plausible. How U.S. policymakers would respond, however, is uncertain.

I. Operation Rockets Red Glare

At 12:00 EST on July 3, 2016 a link is posted to the Facebook page of five of the nation's top music artists, each of whom is holding a concert in a different U.S. city on July 4th. The link entices visitors with an offer of free concert tickets as well as special backstage passes. Less than twenty seconds later the first user has clicked on the link and is taken to a false domain website that serves

malware. This website is mobile, tablet, and desktop enabled. Each device that accesses this website is served a customized virus designed to do several things: first, it reposts the link to the user's own Facebook page without their permission; second, it scans their contacts and sends an email to all of their contacts with a brief message telling them to look at some recent photos; finally, it installs a botnet script that allows a remote computer to activate a Distributed Denial of Service attack on this device.[1] The email that has been sent to all of their contacts contains a copy of the virus disguised to look like an image that, when clicked, installs the same virus on whatever device they are using.

By 18:00 EST on July 3, the Facebook links alone have generated nearly one million clicks, and the fake image in the email has been clicked ten million times. Less than six hours after introduction, without anyone knowing, the virus has infected eleven million devices. By 24:00 EST the count is upwards of fifty million devices. At the same time this mysterious virus is spreading, one hundred prepositioned Federal government employees with previously unknown associations to the Chinese government have logged onto their computers in twenty cities and thirty different federal agencies, and they have inserted thumb drives into their computer workstations. Leaving their computers turned on but their monitors turned off, all one hundred employees exit their buildings. Meanwhile, employees of the Yankee Nuclear Power Station, Calvert Cliffs Nuclear Power Plant, the Edwin I. Hatch Nuclear Plant, Turkey Point Station, and the Diablo Syn Nuclear Power Plant, show up to work and insert Bluetooth-enabled USB thumb drives into their work stations.

By 06:00 EST on July 4, more than one hundred million network-connected devices have been infected in the United States alone. At this time applications start appearing in the Android Play Store and the Apple App Store for the Fireworks displays in New York, Washington, D.C., San Francisco, Chicago, Dallas, and Atlanta. The stores describe these applications as unofficial guides to the day's festivities in each of these cities. As the country wakes up on the 4th of July each of these applications is downloaded thousands of times.

During the days preceding the 4th of July, news agencies release reports indicating the U.S. intelligence community's efforts to thwart all possible terrorist attacks from Islamist extremists. The U.S. government has not seen any additional signals chatter to indicate problems from any nation state or non-state groups in the days and weeks preceding the 4th of July.

At 12:00 EST on July 4, all Bluetooth-enabled USB sticks have been successfully installed on nuclear power station computers, and on one hundred different computers at fifty different Federal agencies. Although some security

researchers have started to pick up on the rapid spread of a new virus, by this time the virus has spread to more than two hundred million connected devices worldwide. The number of devices is growing rapidly.

Just as people are sitting down for fireworks across the United States, the virus, embedded now in more than four hundred million devices globally, goes active. The virus is programmed to force infected devices to participate in a DDoS attack against various network-connected infrastructures. Once a DDoS attack reaches maturation, subsequent devices begin pinging other pre-identified targets. Within minutes all credit card transactions in the United States grind to a halt. ATMs are inoperable. Cell networks are clogged with data traffic making voice calls difficult if not impossible. Of the nearly four hundred million connected devices approximately one hundred million are programmed to attack networked Industrial Control Systems for major mass transportation systems in New York, Washington, Chicago, and Philadelphia.[2] Within minutes a dozen subway and metro trains have crashed, resulting in several hundred casualties. First responders are called, but by now the DDoS attack has changed its focus to target networked city traffic grids, creating gridlock as people head downtown to watch fireworks displays. All subway systems nationwide are shut down due to an inability to safeguard riders. Thousands of passengers are stranded in tunnels, and emergency personnel are unable to reach them. Mobile phone networks are clogged with traffic and few calls are going out.

As chaos begins to spread in major cities, the virus implanted on each of the USB sticks at the fifty different Federal Agencies begins spreading across Federal networks. The virus, modeled after CryptoLocker, is designed to encrypt and make all data on targeted computers inaccessible.[3] Thousands of computers are affected; quickly the call goes out to shut down all networked federal computers. Many agencies with limited duty staffs are ordering a complete disconnect of their buildings from the Internet. All digital Federal communications move towards a complete standstill, and all processing of payments, payrolls, health benefits, verifications of identities at border crossings, and hundreds of other systems become inoperable.

As the virus spreads through Federal networks, individuals sitting in cars outside the five nuclear power plants point with powerful directional Bluetooth antennas at the facilities. Leveraging intelligence gained through the Edward Snowden intelligence leaks of 2013–14, these individuals begin systematically breaking into the computer control systems regulating the temperature of the reactors. They do not change the temperatures of the core; instead, they manipulate the output to indicate overheating. This sets off alarms and immediately

all five reactors begin emergency shutdown procedures. As these reactors shut down, the power grid is strained and rolling blackouts start occurring. The blackouts cause panic in cities where subway systems are shut down and traffic is already snarled. At 20:00 EST the President activates the emergency alert system and all TVs and radios begin broadcasting a message for people to return to their homes in a safe and orderly fashion. The minute the Emergency Alert Broadcast begins, all infected digital devices target defense networks simultaneously. The virus that has spread through Federal networks now penetrates and disrupts classified Command, Control Computers, Communications and Intelligence Surveillance and Reconnaissance (C4ISR) network capabilities. The U.S. defense establishment is under the most severe and sustained attack it has ever experienced.

As code enters the classified networks, C4ISR services begin to degrade. The ability for PACCOM, the Pacific Fleet, and Washington to communicate is severely degraded; by 22:00 EST on July 4, communications between them have come to a virtual standstill. Isolated, Carrier Strike Group 1, currently stationed in the East China Sea, establishes a war-time footing and begins preparations for an imminent attack. Because it has lost communications with PACCOM and with Washington, its C4ISR is severely degraded; it maintains only an analog radio range defensive perimeter.

At 23:59 EST China, which had been conducting naval drills in the South China Sea, immediately changes course and sends most of its naval and air assets towards Taiwan. China deploys one hundred JH-7 fighter-bombers accompanied by one hundred J-11 air superiority fighters to take out all surface-to-air Radar installations. The initial wave of attacks are followed immediately by one hundred H-6 bombers and an additional fifty J-11 fighters with designated targets, including Air Force and Army installations, across Taiwan. The air defenses of Taiwan are immediately overwhelmed. Carrier Strike Group One is unable to respond. Within six hours Elements of the South China Sea and East China Sea Fleets begin an assault on Taiwan with support from several hundred ships, 12,000 PLA Marines, and 10,000 Paratroopers from the 15th PLA Airborne Corps. Within twenty-four hours the fighting has all but stopped on Taiwan, its defense forces having been caught by surprise and overwhelmed. The United States is unable to respond. Instead of participating in the defense of Taiwan U.S. forces would now be required to liberate Taiwan, necessitating significant assets and risking a nuclear conflict.

By July 6, China has possession of Taiwan, U.S. critical infrastructure has been severely damaged by widespread chaos on public transportation, roads,

and electric grids, U.S. government computers are inaccessible as a result of the encryption of their contents, and U.S. commerce has reverted to cash alone as a result of the inability to process credit cards. The penetration of nuclear power plants has resulted in all nuclear power plants nationwide being shut down until their security can be ensured. Internet-connected devices are still engaging in DDoS attacks and the volume of devices affected is unable to be diminished as people continue to attempt to use their devices that they had come to depend upon.

Events of the previous days are in line with China's cyber strategy.[4] China has invested a significant amount of time and resources developing what it refers to as "informationization" strategy. *China National Defense News*, in February 2007, defined *informationization* or cyber warfare as the struggle for the information advantage in the realms of politics, military affairs, economics, and technology and utilizes a broad array of cross-functional areas of applicability in which it desires to make its efforts succeed.[5] The focus of Chinese information warfare development is not the ability to wage network-centric warfare as the United States has demonstrated in previous conflicts, but rather to attack and significantly degrade the ability of an enemy to wage effective combat operations.[6] Much of China's cyber capability development to date has been focused on obtaining a wide array of capabilities as part of a broad process of military modernization.[7] Of seven cases of economic or industrial espionage prosecuted between 2009 and 2011, six were of individuals with links to China.[8]

The President, sitting in the situation room, looks at representatives from the National Security Council and asks what he should do. The room is silent. This crisis, both military and civilian in nature, has already impacted almost every Federal agency and department. How should policymakers respond?

II. Policy Problems in the Digital Age

On February 16, 2010, the Bipartisan Policy Center ran a simulation similar to the scenario described above. Analysis of the scenario, called "Cyber Shock-Wave," revealed that in a severe cyber crisis the legal authorities and functions of U.S. government agencies and officials would be ambiguous, at best. The subsequent report divided its key findings into four areas where weaknesses were discovered: government organization, legal authorities, international protocols, and public education and awareness.[9] The specific weaknesses include the inability of government officials to deal with issues outside of .mil and .gov

networks, the lack of clear lines of authority, the inability to provide timely and accurate decision-making, policy, legal and organizational constraints, missing or underdeveloped statutory authorities, international response mechanisms, a significant lack of public education on proper behavior in cyberspace, and general network security issues.[10]

Attempts to resolve these weaknesses are ongoing. Policy and strategic frameworks that comprise any potential response to significant cyber incidents are being formulated at virtually every level of government. For more than a decade the U.S. Government has been researching, formulating, and reformulating its national and international cybersecurity strategy to stay in step with this rapidly evolving domain of interaction. Deputy Secretary of Defense William J. Lynn III noted in 2010 that the creation of U.S. Cyber Command was a direct result of challenges faced by the pervasiveness of information technology across the U.S. Government.[11] Policy documents including the 2003 *National Strategy to Secure Cyberspace*, the 2009 *Cyberspace Policy Review*, the 2011 Department of Defense *Strategy for Operating in Cyberspace*, and the 2011 *International Strategy for Cyberspace*, have all become roadmaps for cross-governmental and cross-societal integration of a fuller and more comprehensive approach to dealing with the multitude of issues arising from cyberspace.

Any substantive debate focusing on the aftermath of a major cyber incident necessarily focuses four phases of political reaction.[12] These phases constitute a decision matrix upon which to build policy recommendations at each stage of a crisis. These phases of reaction include triage, treatment, risk mitigation, and response.

Stage One: Triage

Triage occurs after an incident has occurred or has been identified as in progress. As in the case above, a fast-moving incident might only be recognizable after initial losses have occurred. Triage involves identifying the type of incident(s) and prioritizing treatments. As in a medical emergency, different specialists might be required to respond to different situations; different aspects of government and society might be called upon to respond following a major cyber incident. Triage asks the question: "how can we minimize further damage in the most efficient manner?"

During the triage phase, immediately following a significant cyber incident, the first priority of the government is to maintain the security of the homeland. The incident is a cyber and kinetic incident, yet the cyber incident poses the greatest challenge to the homeland. Therefore, policymakers iden-

tify national territorial integrity, economic stability, and civil order as the initial treatment areas.

Stage Two: Treatment

Treatment involves the application of the specific organizational and functional units to halt, slow, and repair damage. Treatment could involve private, local, state, federal, and international assets all with the goal of halting further losses and repairing those that have already occurred. The treatment phase requires significant levels of coordination, escalation processes, legal and statutory authorities, and leadership.

Treatment should include, but is not limited to, the activation of all National Guard units nation-wide to ensure territorial integrity and provide additional resources for civil order, the elevation of the national alert status military installations, the grounding of all air-traffic, the closure of all public transportation, and suspension of the markets. Lastly, all nuclear power stations should be shut down and begin a software-reset process. Although initial treatments do not solve the broader problems caused by the cyber incident, they facilitate an organized approach and enable subsequent treatments.

Stage Three: Risk Mitigation

Risk mitigation occurs in tandem with treatment and can occur during and after response phases. Because an incident in cyber occurs within a system of systems environment, a nesting of networks and computing devices, it can be vital to shut down assets prior to their manipulation, corruption, or degradation. Risk mitigation comes into play as soon as triage occurs. It can be both a short-term and a long-term process; often, it is best examined in a lessons learned or after action report. Risk mitigation is a crucial aspect of facilitating resilience and minimizing vulnerabilities.

Risk mitigation in this scenario requires the shutting down of all mobile networks and the dissemination of Public Service Announcements (PSAs), on the national emergency alert system requesting all citizens reinstall their phone software and shut down their computers until such time as an antivirus solution can be developed. Federal networks should be shut down and each computer should be removed from the network and independently verified. Those devices found to contain malicious programs should be immediately erased, re-imaged and inspected before returning them to the network. Long-term risk mitigation includes policy changes and incentive programs to increase cybersecurity across civilian and military infrastructure.

Stage Four: Response

A response is a highly political action and often forms the center of the political debate associated with a particular incident. A response can serve as a deterrent to dissuade future actions; it can be punitive, to demonstrate resolve; or it can be defensive, to pre-empt future attacks. A response can take many forms and can be sought through legal, criminal, military, formal, and informal mechanisms. A response is often the product of a bureaucratic decision-making process.

The degradation of command and control capabilities makes most forms of military response difficult; additionally, China's nuclear status complicates any potential response. Economic interdependencies with China make any potential economic sanctions difficult if not equally harmful to the United States. A diplomatic démarche through the United Nations is likely to have little effect on China, but is a clear first step. Second, as U.S. capabilities return, the U.S. should forcefully re-establish its Pacific position in control of key shipping lanes and should work to foster increased military and diplomatic ties with Asian nations to counterbalance Chinese aggression. Last, the United States should institute a policy of controlled interdependence to ensure all strategic goods can be produced within the continental United States to alleviate potential supply constraints with an increasingly belligerent nation.

A significant cyber incident can theoretically achieve as much damage, destruction, and confusion as many conventional kinetic attacks. For policymakers, it is important to move quickly and efficiently to reestablish control over a situation before it spirals too far. How, then, should policymakers respond to a "Cyber Pearl Harbor" like the one described here?

As noted in a February 2013 Government Accountability Office report, "no integrated, overarching strategy exists that articulates priority actions, assigns responsibilities for performing them, and sets time frames for their completion."[13] Therefore, to address vulnerability and resiliency in a networked world following a cyber Pearl Harbor first requires addressing specific policy and statutory issues hindering an adequate response. Whereas the original Pearl Harbor attack necessitated rapid after-incident coordination and response, it is possible that anticipatory policy and statutory developments might reduce the potential severity of a significant cyber incident.

Networks are always going to have vulnerabilities, yet the ability of a government to respond and adapt to changes as they arise will foster resilience and minimize bureaucratic vulnerabilities.

RECOMMENDED READINGS

Bronk, Christopher. 2011. "Blown to Bits: China's War in Cyberspace, August-September 2020."

Cyber ShockWave: Simulation Report and Findings. 2010. Bipartisanpolicy.org (February).

Lynn, William J. 2010. "Defending a New Domain." *Foreign Affairs* (September 1).

Masters, Jonathan. 2011. "Confronting the Cyber Threat." Council on Foreign Relations Backgrounder (May 23).

Thomas, Timothy L. 2009. "Nation-state Cyber Strategies: Examples from China and Russia." In Kramer, Franklin D, and Stuart H Starr, eds. *Cyberpower and National Security*. Washington, DC.

GOVERNMENT DOCUMENTS RELATED TO CYBER

Carter, Ashton. 2015. The Department of Defense Cyber Strategy. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Obama, Barack H. 2013. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.

Obama, Barack H. 2011. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.

U.S. Government Accountability Office. 2013. Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. Washington, DC.

Wortzel, Larry M. 2013. Testimony in "U.S.-China Economic and Security Review Commission 2013 Report to Congress: China's Military Modernization, U.S.-China Security Relations, and China's Cyber Activities." United States House of Representatives, 113th Congress 26. Washington, DC.

NOTES

[1]Distributed Denial of Service attacks (DDoS) is the process by which a networked connected computing device or multiple devices are used to overwhelm a target with a flood of external communications requests causing the target system to become inaccessible, unusable or simply fail. The more nodes or bots attached to a DDoS attack the more powerful and distributed the attack.

[2]Industrial Control Systems (ICS) are automated systems that manage industrial processes including subway, transportation, electrical and other systems. Failures of these types of systems have been linked to accidents involving various industrial processes. The STUXNET virus was a virus designed to manipulate various ICS systems.

[3]Cryptolocker is a form of ransomware (subset of malware) that targeted windows computers via email attachments. Once activated the malware encrypts certain files on the target system using RSA public-key cryptography making the files inaccessible until a ransom is paid and the files are unlocked).

[4]Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, eds. Franklin D. Kramer and Stuart H Starr (Washington, DC: Potomac Books, 2009), 466.

[5]Ibid.

[6]Ibid., 467.

[7]Larry M. Wortzel, Testimony to the U.S. House of Representatives Armed Services Committee Hearing on "2013 Report to Congress of the U.S.-China Economic Security Review Commission" (November 12, 2013), http://origin.www.uscc.gov/sites/default/files/WortzelL-20131120_2013%20Annual%20Report.pdf.

[8]Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011" (October 2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[9]"Cyber ShockWave: Simulation Report and Findings," Bipartisanpolicy.org, Washington, DC (February 2010), 4.

[10]Ibid.

[11]William J. Lynn III, "Defending a New Domain," *Foreign Affairs* (September 1, 2010), accessed August 6, 2014, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

[12]This should be distinguished from the responses of a computer emergency response team (CERT) or other network specific security protocols.

[13]U.S. Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented," (Washington, DC: GPO, 2013).