Cyber Attacks

The New WMD Challenge to the Interagency

by Quan Hai T. Lu

The Ubiquitous Cyber Threat

The President of the United States recently said that "cyber threat is one of the most serious economic and national security challenges we face as a nation."[1,2] Advances in transistor design and integrated circuits have accelerated technologies exponentially. U.S. civil society's reliance on these modern digital systems has, itself, made the U.S. vulnerable to cyber attacks. Cyber attacks are becoming more sophisticated, making detection and attribution difficult. Simultaneously, the "Internet of Things" (IoT) is growing exponentially in the U.S., making every citizen vulnerable to a cyber-attack. Computing and networking systems are vulnerable because integrated circuits and processors are complex—making subversive counterfeit microchips easily replaced and nearly impossible to detect; internet anonymity is pervasive; the building blocks of software are open-sourced or developed by third parties; widespread commercial-off-the-shelf (COTS) software and hardware are manufactured with low or no concerns for security; foundries for microchip manufacturing are located overseas; lines of codes for software now number in the tens of millions and are growing; integrated circuits have over two billion transistors and are also growing; testing and verifying all systems for vulnerabilities is infeasible if not impossible; and development and production processes are now automated—relying on third-party or open-source libraries for hardware and source code.[3]

The IoT links individuals' daily lives to that of the internet. This interconnectedness between people and cyberspace gives criminals, extremists, and adversary nation-states a vector to target individuals, private and governmental organizations, and U.S. civil society as a whole, and, in the

U.S. Army Major Quan Hai T. Lu is the Deputy Chief of Systems Vulnerability & Assessment at the Defense Threat Reduction Agency. He served as a company commander with the 82d Airborne Division in support of Operation Iraqi Freedom. He holds a M.S. degree in nuclear engineering and is a Countering WMD Graduate Fellow at National Defense University.

process, it has inspired a fear of the unknown. In short, cyber is the new weapon of mass destruction (WMD) threat, and addressing it will require marshalling the resources of the entire interagency.

The methods and means may be different, but a cyber attack on chemical facilities, biological research labs, nuclear power plants, and the nuclear command and control nodes is, in important ways, effectively equivalent to an adversary using WMD. Cyber attacks causing an explosion at a chemical factory and releasing toxic industrial chemicals/toxic industrial materials (TICS/TIMS) into the surrounding environment may have the same physical and psychological effects as chemical weapons. Similarly, cyber attacks on nuclear power plants that cause a reactor meltdown and release harmful radioactive material may cause psychological and economic impacts similar to a radiological dispersal device (RDD). Genetic information for biological weapons stolen through cyber attacks from bioresearch facilities may accelerate adversaries' ability to acquire or develop biological WMDs. Insider cyber attacks on nuclear command and control systems may result in an unintentional detonation of a nuclear weapon or the disablement, disruption, and destruction of critical systems during a national emergency. The approaches and devices are nontraditional, but cyber attacks on chemical, biological, nuclear power, and military nuclear command and control facilities can have effects comparable to those of a WMD.

Cyber attacks on other U.S. critical infrastructure can also cause mass damage and casualties. For example, an attack on the power grid that stops the supply of power for a long time over a wide area may cause a humanitarian crisis. Cyber attacks on commerce may cause hundreds of billions of dollar in damages, hurting people at every socioeconomic level. Cyber attacks on one or more nodes in the complex system of infrastructures that sustains the U.S. may massively disrupt—or perhaps destroy—the conduct of U.S. civil society. Indeed, damages resulting from a successful cyber attack on critical infrastructure can be worse than some WMD attacks.

Because of the comprehensive nature of the cyber threat, the interagency cannot ignore the possible WMD-like consequences that a cyber attack could pose.

The cyber threat is not lurking somewhere over a distant horizon; it is here. News reports about a security breach or cyber attacks occur daily. Everything is connected to the internet or is in the process of being connected, and a cyber attack on these interconnected systems has the potential for WMD-like consequences. Millions of electronic devices transformed U.S. civil society into a world economic and military superpower in the latter half of the twentieth century. Trillions of devices—from planes, trains, and automobile to thermostats, smart watches, and everything in between—are increasingly getting connected to the internet. Because of the comprehensive nature of the cyber threat, the interagency cannot ignore the possible WMD-like consequences that a cyber attack could pose. Technology is advancing at an exponential rate, rendering traditional defensive measures or even simple legislation remedies to protect U.S. interests inadequate to the threat. Even if adequate, both are liable to become obsolete before they can be effectively implemented. A defensive posture alone is inadequate to protect the U.S. against cyber attacks because the U.S. cannot defend everywhere at all times. A determined adversary will only need to find one weakness and concentrate its resources to conduct a successful cyber attack. Hence, interagency partners—and not just the Department of Defense—must consider their respective roles in both cyber-defensive and cyber-offensive operations.

A cyber attack that successfully shuts down the electrical grid for prolonged periods over a large geographic area may have WMD-like consequences.

The U.S. Electric Grid

A cyber attack that successfully shuts down the electrical grid for prolonged periods over a large geographic area may have WMD-like consequences. The vulnerability of the national electric grid to cyber attack is not a new revelation. The electric grid is the U.S. technological center of gravity. Transnational extremists and nation-states whose aims are to disrupt or destroy U.S. civil society have many ways to attack this U.S. center of gravity. In particular, the vulnerability of the electric grid industrial control systems (ICS) to cyber attacks and other critical infrastructures has given U.S. adversaries a relatively easy way to disrupt or destroy U.S. civil society. The outages could severely disrupt the delivery of essential services such as communications, food, water, waste water removal, health care, and emergency response. Moreover, cyber attacks—unlike traditional threats to the electric grid such as extreme weather—are unpredictable and more difficult to anticipate, prepare for, and defend against.

The Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works across the interagency "to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures."[4] In 2012, the ICS-CERT responded to 198 cyber incidents. More than 41 percent of these incidents involved the energy sector, particularly electricity.[5] Thwarting these attacks will require effective information sharing among interagency partners and state and local agencies working over a dispersed area, in addition to close collaboration with private sector entities.

The U.S. Chemical Industry

Chemical facilities share the same cyber-network commonalities as other U.S. critical infrastructures. Their industrial control systems have the same network vulnerabilities that can be exploited by adversaries. From 2006 to 2009, the Government Accountability Office found a 400 percent increase in cyber attacks on chemical facilities.[6]

The ubiquitous reliance on TICs/TIMs and their proximity to the civilian population make the chemical industry a target for terrorist hackers. A recent study found that one in three American schoolchildren attend school within the danger zone of a hazardous chemical facility. Some 19.6 million children in public and private schools in forty-eight states are within the vulnerability zone of at least one chemical facility, according to data the facilities provided to the Environmental Protection Agency.[7] In 2006, Congress established the Chemical Facility Anti-Terrorism Standards program to help regulate high-risk chemical facilities. However, in 2013, a massive chemical explosion that killed 15 people and injured another 226 at a fertilizer plant in the town of West, Texas, showed that the speed with which the DHS is able to inspect high-risk chemical plants is inadequate.[8]

A cyber attack on chemical facilities designed to release TICs/TIMs is no different in effect than using chemicals in warfare or terrorist attacks. In fact, the effect might be greater, as the affected population is likely to be almost entirely unprotected. For example, hydrogen cyanide gas released from a deliberately staged industrial fire may cause severe respiratory distress to an unsuspecting civilian population. Hydrazine released in an improvised explosive device can cause skin burns and blisters. To take a historical example, the 1984 methyl isocyanate accident in Bhopal, India, killed thousands and injured over a hundred thousand civilians.[9] The triggering and dispersal method may be different, but the consequence of releasing TICs/TIMs could result in the same WMD-like consequences.

The Conventional Energy Sector

U.S. petroleum and gas systems are also vulnerable to cyber attacks. Vulnerabilities exploited in petroleum and gas facilities abroad presage possible similar exploitations in U.S. facilities. For example, the data-destruction attacks on Saudi Aramco and on Qatar's RasGas gas company in 2013 represent a major shift from cyber spying on oil and gas companies to more widespread destruction of their operations.[10] In June 1982, the Central Intelligence Agency (CIA) was alleged to have caused a Siberian pipeline to explode with a so-called logic bomb. The target was a Soviet pipeline and the resulting explosion was detected by U.S. early warning satellites.[11] The covert operation sabotaged the pipeline's control systems with malicious code. Even though the attack caused no direct casualties, harm came to the Soviet economy.[12] Coupled with the Soviet's weak economy and U.S. military build-up, one could argue that the cyber attack contributed to the fall of the Soviet Union. More recently and closer to home, in March 2012, the DHS reported ongoing cyber intrusions among U.S. natural gas pipeline operators.[13] A successful cyber attack on the U.S. petroleum and gas distribution and production system could cause significant harm to the U.S. economy.

The U.S. Health Care System

On August 18, 2014, one of the largest U.S. hospital groups reported that it was the victim of a cyber attack from China. Personal data including Social Security numbers belonging to 4.5 million patients were stolen in the largest cyber attack recorded to date by the U.S. Department of Health and Human Services.[14] Hospitals are soft targets where a cyber attack can cause a lot of damage easily.

A cyber attack can shut down an entire hospital network by threatening information security, system functionality, or device operation.

A cyber attack can shut down an entire hospital network by threatening information security, system functionality, or device operation. For example, a patient receiving chemotherapy for cancer attends a therapy session where an automated pump administers the prescribed chemo. A cyber attack causes the routine automated procedure to spike the dose of the chemo into the patient's system, causing irreversible harm. The malfunction of one of the pumps puts in question the reliability of the remaining pumps. Meanwhile, the cyber attack also disrupts or halts normal hospital operations. New patients cannot be admitted and current patients' information is inaccessible. Now imagine similar cyber attacks occurring during or as part of a mass casualty event. The complex attack would cause mass fatalities.

Nuclear Reactors

Cyber attacks that result in release of significant amounts of radioactive material may cause psychological and economic impact similar to that of an RDD. The number of cyber attacks on nuclear power plants is increasing at an alarming rate.[15] Radiological dispersal—whether from a bomb or a power plant explosion—may have the potential to cause significant loss of life, radiation casualties, lasting psychological trauma, and extensive property damage and contamination that will have lasting effects. Radiation released into the environment likewise has the potential for great harm. Even if a cyber attacker's objective is not to cause physical harm per se, the attacker still could inflict economic catastrophe on a populace worried with the "How clean is clean?" problem in the aftermath of a radiological release. Moreover, cyber attacks not calculated to cause physical harm could still result in the theft of proprietary information that could be used in later attacks. An increase number of attacks with few or no effects may simply be a case of hackers perfecting their skill or probing for vulnerabilities as they wait for a more opportune time to inflict substantial damage. The motives for attacks are elusive and have as many possible permutations as there are attackers. The rationale for why a disaster has yet to occur from a cyber attack is just as elusive. Nevertheless, the already-known certainties surrounding possible cyber attacks against nuclear reactors require the interagency apparatus to confront the cyber threat vigorously.

The computer systems at the National Nuclear Security Administration (NNSA) are under continuous cyber attacks. The NNSA experiences nearly six million hacking attempts daily...

The U.S. Nuclear Weapon Enterprise

U.S. Air Force General Robert Kehler, former Commander of the U.S. Strategic Command, stated in a 2013 Senate hearing that he was very concerned with the cyber-related attacks on the U.S. nuclear command and control (NC2) and weapon system.[16] Much of the NC2 system is analogous to the systems that control nuclear power plants. Even though the point-to-point and hard-wired nature of the system makes it resilient to external cyber-attacks, the system is still vulnerable to insider attacks.

A possible indirect effect of a cyber attack is the theft of nuclear weapons designs that, in turn, can advance an adversary's capability to threaten the U.S. For example, in April, 2013, the Department of Energy's Oak Ridge National Laboratory was successfully hacked and several megabytes of data were stolen.[17] The computer systems at the National Nuclear Security Administration (NNSA) are under continuous cyber attacks. The NNSA experiences nearly six million hacking attempts daily, thousands of which are categorized as "successful." Even without causing significant damage, the NNSA has already expended nearly $150 million just to identify and mitigate cyber attacks.[18]

Cyber attacks can also indirectly impact NC2 and U.S. weapon systems. The ability to maintain communication between the President and intercontinental ballistic missile (ICBM) installations, nuclear ballistic submarines (SSBNs), and nuclear bombers relies on a series of networks that are vulnerable to cyber attacks. The system relies on a communication and electrical backbone that a catastrophic cyber attack could disrupt or destroy for a prolonged period and thus have a profound effect on the U.S. ability to conduct its nuclear command and control.

Water, Food, and Agriculture Infrastructure

The risk to the U.S. posed by cyber attacks with the intention to harm consumer confidence in the U.S. food, water, and the agricultural system can cause severe damage and have large economic impact. In theory, cyber attacks on the food, water, and agricultural system are less costly and have a lower technology threshold than traditional WMD. Targets are more vulnerable, and the impact from a successful cyber attack may be more significant. The cost, lower technology barrier, and vulnerability of targets may make cyber attacks against the U.S. food, water, and agriculture system more likely than other kinds of WMD threats, thus requiring special interagency attention to protect against such attacks.

Similar to other U.S. critical infrastructure, the water and wastewater utilities rely on a network of computers and automated data acquisition and control systems to operate and monitor them. The delivery of potable water to hundreds of millions of people has become, like many other conveniences, routine. Prolonged interference in the delivery of the water or removal of wastewater may precipitate a severe environmental issue. A cyber attack that interferes with the purification process—either leaving the water under or over treated—may result in contaminated water being delivered to the local population and cause a significant public health problem. A cyber attack that interferes with the distribution of water or wastewater removal could likewise lead to an overflow of sewage in public waterways and drainage systems. An attack in a drought-stricken area may exacerbate the problem and have tremendous economic implications. Successful cyber attacks that interrupt or halt the delivery of potable water or removal of wastewater for prolonged periods over a wide geographic area may have WMD-like consequences.

The future of food and agriculture is in automation via large-scale robotics. Envision dozens or hundreds of robots with thousands of digital sensors monitoring, predicting, cultivating, and extracting crops from the land. The automation also produces meats genetically designed and grown from test tubes—completely independent of a living animal. Working with little or no human intervention, the automated system feeds the hundreds of millions. Implementation of the systems on a limited scale is already underway.[19] Now imagine a cyber attack that alters the genetic makeup of the meat to sicken the consumer or to destroy the crops. The cyber attacks would starve millions. The growing reliance on the automated systems—all vulnerable to cyber attacks—has the potential of producing mass damage and disruption to U.S. civil society.

The growing reliance on the automated systems—all vulnerable to cyber attacks—has the potential of producing mass damage and disruption to U.S. civil society.

The Task Ahead

Some critics argue that cyber attacks that cause WMD-like consequences may not be that easy and that technology is keeping pace to counter the problem. On the contrary, cyber attacks are relatively easy when compared to the increasingly sophisticated security software required to protect systems. Figure 1 (pg. 54) shows the exponentially growing complexity required to protect systems versus the relative constant size of malicious software.

With respect to hardware, the trend is just as troubling. Integrated circuits have over 2 billion transistors, and this number doubles every

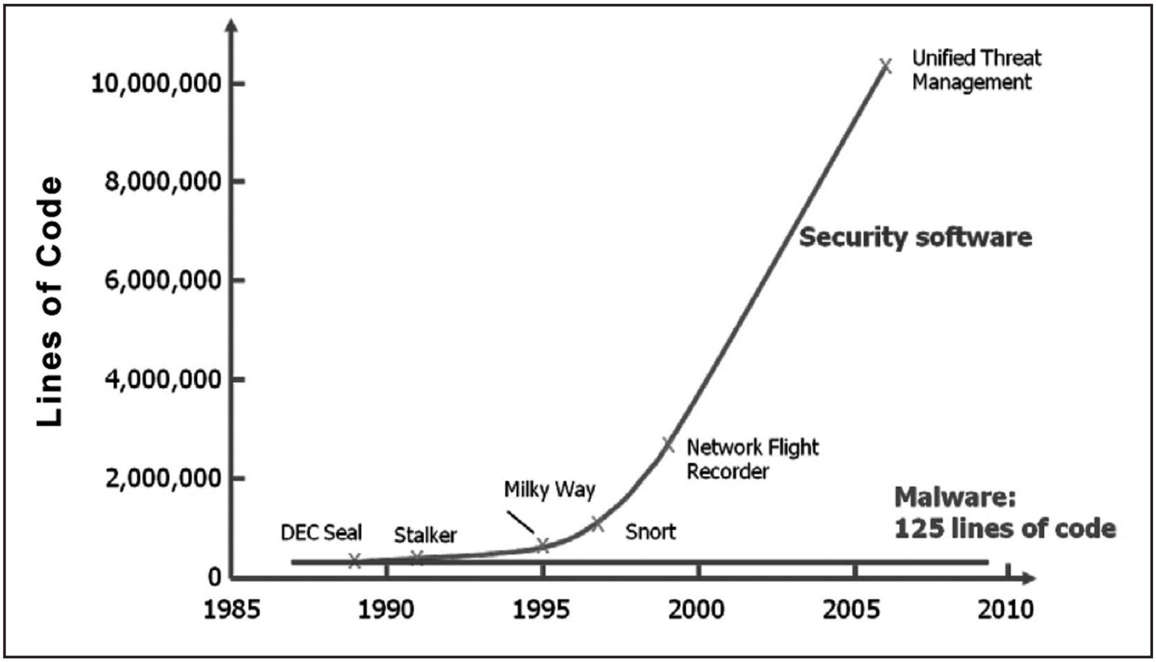

Figure 1: Complexity of Defensive Code vs. Offensive Code[20]

two years. Moreover, manufacturing the chips without flaws is nearly impossible. The flaws—whether accidental or by design—make modern IT systems built around the integrated circuits vulnerable to cyber attacks. Modern IT systems are ubiquitous in U.S. critical infrastructure. A well-resourced and determined adversary will be able to exploit the flaws and could cause WMD-level damage and fatalities.

Some may also argue that if the U.S. truly were vulnerable to cyber attacks that have WMD-like consequences, adversaries would have already attempted a catastrophic attack. In point of fact, attacks on the U.S. critical infrastructure occur routinely, and terrorists have announced their intention of using WMD against the U.S. Conducting a WMD-like attack through cyberspace would be an attractive option—providing a certain level anonymity while having plenty of media appeal. Adversaries, such as states or terrorists, could launch attacks and cause severe physical and psychological damage without leaving their safe havens.

Several plausible explanations may explain the lack of a successful cyber attack that would qualify as cyber terrorism—let alone a WMD-like attack. Many analysts believe that transnational terrorists lack the technical know-how to carry out a sophisticated WMD cyber attack. Sophisticated cyber attacks require a level of software literacy that may be beyond the capabilities of current terrorist cells. However, a determined terrorist cell may eventually bridge the capabilities gap by recruiting more computer-savvy extremists or by developing the capability themselves. Naturally, the interagency cannot wait until such a time to marshal its resources. It may also be that the U.S. has yet to face a WMD-like cyber attack because nation-states that have the means to do so are deterred by fear of U.S. instruments of power, including conventional and nuclear retaliation. Finally, the most probable reason why the U.S. has yet to experience a crippling cyber attack is because adversaries, with the capability and means to inflict mass death and casualties to the U.S., would rather steal from the wealthiest nation in the world. Billions if not trillions of dollars in intellectual property, trade secrets, and military technology—including information that could accelerate adversaries' ability to develop or acquire WMD—have been lost as the result of cybercrime. Some economists have called it the greatest transfer of wealth in history.[21]

The Pentagon, in an annual report on China, directly charges that Beijing's government and military have conducted computer-based attacks against the U.S., including efforts to steal information from federal agencies. Hackers associated with the Chinese government broke into the computers of airlines and military contractors over 20 times in a single year, according to the U.S. Senate. The Senate report alleged that cyber attacks were targeted at systems tracking movement of troops and equipment. They included breaking into computers on a commercial ship and uploading malicious software on to an airline's computers.[22]

To characterize the point another way, a cyber attack that causes WMD-like damages is a "black swan event." Made famous by Nassim Nicholas Taleb, [23] a "black swan event" is a highly improbable event that has a significant impact. Events such as the creation of the internet and the attacks on 9/11 are examples of such events. No one could have predicted how the internet would transform the U.S. economy, military, and society. Cyber attacks that cause WMD consequences are difficult if not impossible to forecast in terms of the precise time or place they might occur. In some cases, critics are simply unaware or biased against the idea that cyber attacks and WMD are increasingly interconnected in the twenty-first century and pose a significant threat to the U.S. Nevertheless, as argued above, the possible WMD-like consequences of cyber attacks are sobering possibilities that the interagency must consider with all due gravity.

Similar to the Y2K problem at the turn of the present century, the whole of government will need to work together to deter, defend, and mitigate against sophisticated cyber attacks. Unlike Y2K, the threat posed by cyber attacks will be a persistent threat that the U.S. must be vigilant in defending against. In principle, catastrophic cyber attacks are preventable. This much, however, is certain: Left unchecked, the attacks may have WMD-like consequences—billions of dollars in damages, thousands of lives in jeopardy, and military operations compromised. The interagency, working with state and local agencies and in cooperation with the international community, can mitigate the risk and impact of cyber attacks. DoD and DHS should jointly develop a comprehensive plan to handle a catastrophic attack should one occur. In addition, government organizations should also share lessons learned across the interagency, both vertically and horizontally. Placing greater emphasis on offensive measures to prevent cyber attacks will also be necessary. All interagency partners should continue to invest in people, organizations, and technologies to build and maintain a robust cyber-security capability. No one strategy, no single organ or level of government, no one piece of technology, and no one person can prevent and deal with the consequences of a catastrophic cyber attack on U.S. critical infrastructure. ***IAJ***

NOTES

[1] The views expressed herein are those of the author and do not necessarily reflect the official views of the U.S. government or any of its entities.

[2] Barack Obama, “Remarks by the President on Securing our Nation’s Cyber Infrastructure,” White House, Washington, May 29, 2009, <http://www.whitehouse.gov/the_press_office /Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>, accessed on January 12, 2015.

[3] Defense Science Board, “Resilient Military Systems and the Advanced Cyber Threat,” <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>, accessed on October 10, 2014.

[4] Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, <https://ics-cert.us-cert.gov>, accessed on January 8, 2015.

[5] “National Electric Grid Remains at Significant Risk for Cyber-Attacks,” *Info Security*, <http://www.infosecurity-magazine.com/news/national-electric-grid-remains-at>, accessed on October 14, 2014.

[6] Chemical Sector Coordinating Council and the Department of Homeland Security, “Securing Industrial Control Systems in the Chemical Sector, Roadmap Awareness Campaign —A Case for Action,” <http://www.dhs.gov/xlibrary/assets/oip-chemsec-case-for-action-042011.pdf>, accessed on December 8, 2014.

[7] “DHS Slow to Inspect High-Risk Chemical Plants,” Homeland Security News Wire, <http://www.homelandsecuritynewswire.com/dr20140423-one-in-ten-american-schoolchildren-in-school-near-risky-chemical-facility>, accessed on December 2, 2014.

[8] Ibid.

[9] Richard Davies, “Bhopal Still Haunts Union Carbide 30 Years Later,” ABC News, <http://abcnews.go.com/blogs/business/2014/12/bhopal-still-haunts-union-carbide-30-years-later>, accessed on December 2, 2014.

[10] Kelly Jackson Higgins, “Destructive Attacks on Oil and Gas Industry a Wake-Up Call,” <http://www.darkreading.com/attacks-breaches/destructive-attacks-on-oil-and-gas-industry-a-wake-up-call/d/d-id/1140525?>, accessed on November 13, 2014.

[11] “Are the Mouse and Keyboard the New Weapons Of Conflict?” *The Economist*, <http://www.economist.com/node/16478792>, accessed on January 16, 2014.

[12] Gus W. Weiss, “The Farewell Dossier,” <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm>, accessed on January 16, 2015.

[13] Paul W Parfomak, “Pipeline Cybersecurity Federal Policy, ” Congressional Research Service, August 16, 2012.

[14] Jim Finkle and Caroline Humer, “Community Health Says Data Stolen in Cyber-Attack from China,” <http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818>, accessed on December 3, 2014.

[15] Mark Holt, “Nuclear Power Plant Security and Vulnerabilities,” Congressional Research Service Report, No. RL34331, Washington, 2014, <http://fas.org/sgp/crs/homesec /RL34331.pdf>, accessed on January 16, 2015.

[16] General C. Robert Kehler, USAF, Commander, U.S. Strategic Command, statement before the Senate Armed Services Committee, 2004, <http://www.armed-services.senate.gov /imo/media/doc/13-09%20 -%203-12-13.pdf>, accessed on January 16, 2015.

[17] "U.S. Nukes Face Up to 10 Million Cyber Attacks D," *US News*, <http://www.usnews .com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily>, accessed on November 6, 2014.

[18] Ibid.

[19] Michell Zappa, "15 Emerging Agriculture Technologies That Will Change the World," *Business Insider*, <http://www.businessinsider.com/15-emerging-agriculture-technologies-2014-4>, accessed on January 16, 2015.

[20] Department of Defense, Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat," <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems .CyberThreat.pdf>, accessed on October 10, 2014.

[21] "NSA: Cybercrime Is 'the Greatest Transfer of Wealth in History'," ZDNet, <http://www.zdnet.com/article/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history>, accessed on December 8, 2014.

[22] Kehler.

[23] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Random House, New York, 2007.