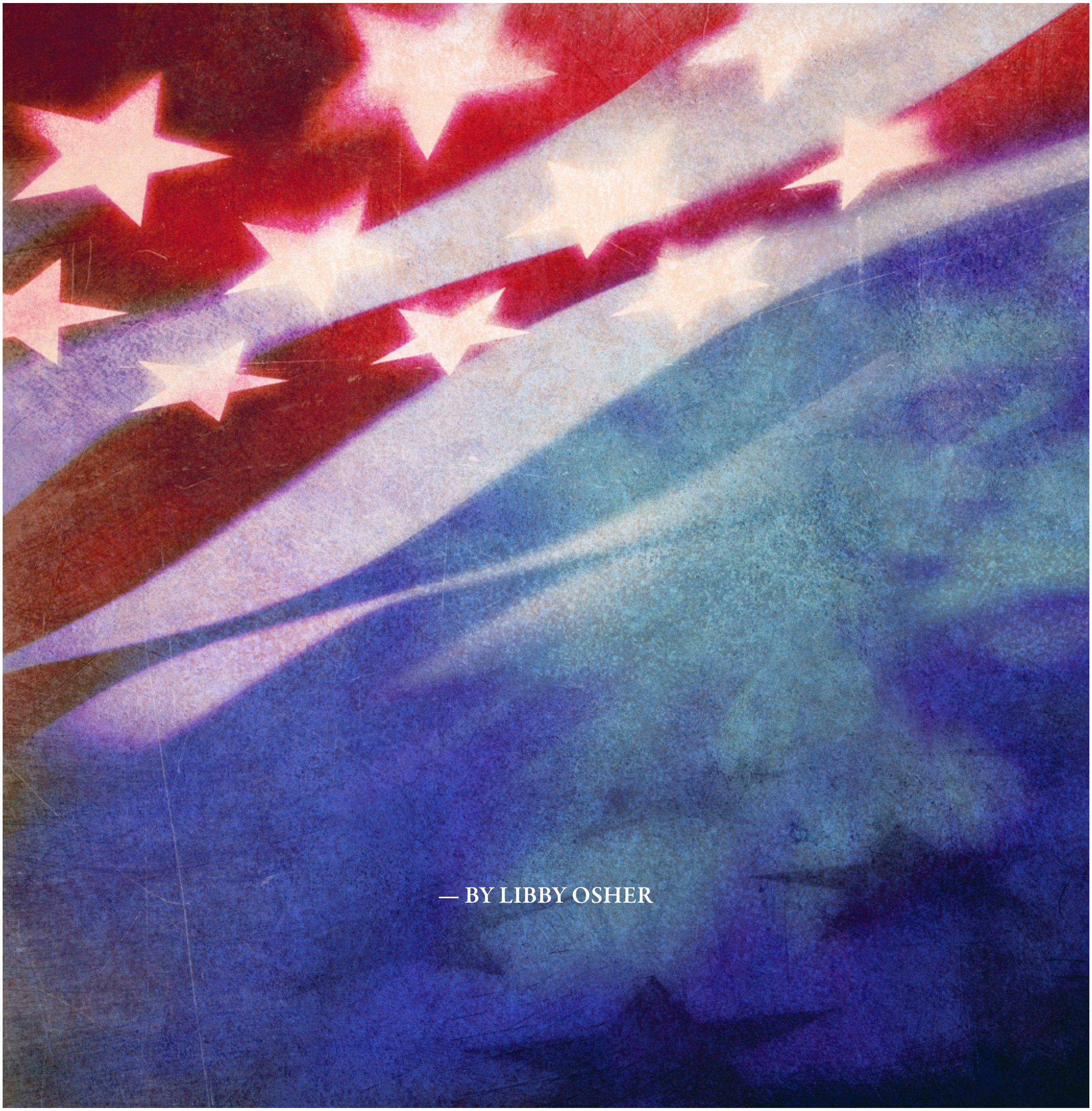
Debugging America's Cyber Policy



— BY LIBBY OSHER

Information leaks and faulty programming[1] revealed to the world that the United States developed and deployed offensive cyber attacks. Although it wasn't discovered until late 2010, Stuxnet was deployed at least in 2009 and was probably developed as early as the end of the Bush administration.[2] As details emerged, the way the U.S. weaponized cyber technology was eerily reminiscent of the way it weaponized nuclear technology some 70 years ago. In both cases, the United States weaponized new technology with little understanding of the consequences for the broader international community. And yet, the United States disregarded legitimate concerns over their offensive use in favor of its perceived vital national security:[3] war with Japan and Iranian nuclear proliferation.[4]

Stuxnet is a highly sophisticated U.S.-Israeli computer worm that corrupted centrifuges at Iran's nuclear facility in Natanz. It is a complex piece of malware designed to inject code into SCADA (industrial control systems), all the while hiding its presence from the operator. Stuxnet's ultimate goal was to reprogram these industrial control systems and sabotage the centrifuges.

When the U.S. dropped the bomb on Hiroshima in 1945, it signaled to the world that nuclear weaponization was possible and acceptable. States soon scrambled to assemble their own offensive nuclear programs.

It is a complex piece of malware designed to inject code into SCADA (industrial control systems), all the while hiding its presence from the operator. American cyber attacks send a similar message that the offensive use of cyber technology could become a norm. Russia and China are sure to ramp up their cyber programs in response to American aggression[5] leading all three to cite the other's programs as justification for their own, just as American and Soviet nuclear regimes did less than a decade ago. Without immediate action, another arms race-driven by short-term paranoia, will occur at the expense of long-term national security.

In the years that followed World War II, there was a window of opportunity when international controls were still theoretically possible, but neither the U.S. nor the USSR made sufficient efforts to establish them. A nuclear arms race ensued, and today no less than nine countries possess nuclear weapons.[6]

It is impossible to know if a greater effort to instill international control through efforts like the Baruch Plan would have succeeded in avoiding, or at least containing, the Cold War conflict. The establishment of norms is a far easier task than to outlaw existing capabilities.

> **The average American will never handle radioactive material like uranium (U-235) or plutonium (Pu-239), let alone a nuclear weapon, but most will use the Internet.**

Fortunately, this is the preliminary stage of cyber warfare and there is still time to formulate domestic policies and establish international regulations.
The more accessible, under-regulated,
and poorly understood features of the
cyber
domain hasten the need for a comprehensive strategy and international cooperation. The United States must act to safeguard its virtual networks.

While there are some parallels, the weaponization of nuclear and cyber technology is very different in regards to their peaceful and military functions. Unlike nuclear material, for example, the Internet is a universal and fundamental service relied on by many institutions and integral to the daily lives of billions of people worldwide, not to mention hundreds of millions in the United States. In addition, the Internet is vital to the world economy, including essential industries such as electricity providers and financial institutions.

The average American will never handle radioactive material like uranium (U-235) or plutonium (Pu-239), let alone a nuclear weapon, but most will use the Internet. Public education of safe computer practices must be emphasized and marketed as a first line of defense against cyber attacks.

Despite habitual use, most people — from teenagers to Fortune 500 corporations —do not practice safe online behavior and sometimes fall victim to the most basic Internet scams.[7] For example, phishing emails bait the recipient to provide confidential information and often include malicious links to websites infected with malware. While victims could avoid this scam by displaying the true hyperlink or researching the purported sender, these attacks are prevalent and costly.

The pervasiveness of phishing attacks demonstrates the vulnerability of cyber technology. In 2007, a multitude of cyber attacks were attributed to non-state actors like criminal organizations, terrorists, and hacktivists, including the April 2007 denial of service attack on Estonia and major intrusions of the Departments of Defense, Homeland Security, State, and Commerce.[8] These groups and individuals benefitted from the accessibility of cyber technology, the low operational cost, and the abundant technical expertise available to launch a sophisticated cyber attack, in comparison

We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.

aspect, which is completely unattainable in the nuclear arena. While nuclear technology is confined to state-level policy, the increased opportunity for abuse by diverse actors in cyber necessitates the adaptation of a defensive policy. Conventional retaliatory measures effective in the deterrence of a nuclear attack would not work against targets that cannot be identified, or punished with the tools used to address state aggression. This dynamic threat requires a revised national security policy.

Non-state actors invade cyber space instead of a nuclear weapons depot because states have monopolized nuclear technology since its inception, safeguarding it from abuse through efforts such as the Nunn-Lugar program and Global Threat Reduction Initiative. Apart from a few regulatory committees, such as the Internet Engineering Task Force (IETF) which sets technical standards for internet protocol and the Internet Corporation for Assigned Names and Numbers (ICANN) which assigns domain names, cyber space has remained largely independent of government control.[9] Because of their limited role in the regulation of cyber technology, governments must make every effort to avoid backroom deliberations and open up policy decisions to think tanks, private technology firms, and industries that specialize in cyber security. Discussion of cyber regulations and policy should include input from the public. Policymakers need to ensure that regulations do not trample on civil liberties or violate a right to privacy on the Internet.

While the destructive power of a cyber attack pales in comparison to the physical devastation of a nuclear weapon attack, the insidious nature of virtual attacks can have numerous lasting effects, which include the economic toll of intellectual property theft, infiltration of military databases, and the disruption of financial systems. The possibility of infiltrating a cyber network to facilitate a remote physical attack on the command and control centers of a power grid or worse, a nuclear site, is very much alive.

Corporations lose time and money spent on innovation when designs are stolen and counterfeited, which includes the violation of intellectual property rights and can ultimately result in the loss of jobs. According to the FBI, intellectual property theft costs American businesses billions of dollars every year. [10] In 2010 Yu Qin and Shanshan Du stole GM hybrid vehicle trade secrets in order to sell the information to Chery Automobile, a Chinese automotive manufacturer and foreign competitor of GM. GM estimated that the value of the stolen documents was more than $40 million.[11] And in 2009, Chinese hackers infiltrated military databases to access the design of the Joint Strike Fighter (F-35) by Lockheed Martin. [12]

Cyber security norms and best practices need to be established before non-state actors carry out a lethal attack and before states develop large-scale offensive cyber programs. On the global stage, the U.S. should collaborate with the international community to call for the categorical prohibition of cyber attacks directed at power grids. An effective treaty will include monitoring

The potential for disaster is very real. The greater accessibility of cyber weapons to non-state actors, advantage of anonymity for states, and absence of stigma against an attack increases its likelihood and compounds the importance of the cyber policy debate. National dialogue, international cooperation, and regulations on cyber activity that mirror the policy response to nuclear weapons must be emphasized. However, the need to learn from nuclear security strategy should not be misconstrued as advocacy of the same policy constructs used to address previous forms of warfare. The Cold War doctrine should not be applied to cyber warfare, just as pre-industrial age war-gaming strategies would not be applied to post-industrial military operations. ■

Libby Osher is a master's degree candidate in nonproliferation and terrorism studies at the Monterey Institute of International Studies and a Security Scholar at the Federation of American Scientists where she researched cyber security and bioterrorism. In 2011, she graduated from the George Washington University with a BA in international affairs with a regional concentration in the Middle East, and a minor in Semitic languages. In her third year at GWU, Libby spent a semester at the American University of Cairo in Egypt where she focused on Arab and Muslim political and religious movements and furthered her Arabic language studies.

REFERENCES AND NOTES

[1] Rosenbaum, R. (2012, April). "Richard A. Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian Magazine*, April 2012: http://www.smithsonianmag.com/history-archaeology/richard-clarke-on-who-was-behind-the-stuxnet-attack.html

[2] Falliere, N., Liam O. Murchu, & Eric Chien. (February 2011). W32. stuxnet dossier. Symantec: Version 1.4

[3] Glenny, Misha. "A Weapon We Can't Control," *The New York Times,* June 24, 2012: http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html

[4] Benedict, Kennette. "Stuxnet and the Bomb," *The Bulletin of the Atomic Scientists*, June 15, 2012: http://thebulletin.org/web-edition/columnists/kennette-benedict/stuxnet-and-the-bomb

[5] Steinbruner, John D. (2011). *The Cybersecurity Situation*. CISSM working paper, Center for International and Security Studies at Maryland, University of Maryland, College Park.

[6] Kristensen, Hans. Status of World Nuclear Forces, FAS.org, 2012: http://www.fas.org/programs/ssp/nukes/nuclearweapons/nukestatus.html

[7] Boulton, Clint. "CIOs: DNSChanger Malware Won't Knock Us Offline," *Wall Street Journal,* July 8, 2012: http://blogs.wsj.com/cio/2012/07/08/cios-say-dnschanger-malware-will-not-knock-us-offline/

[8] Lewis, J. A., Langevin, J. R., McCaul, M. T., Charney, S., & Raduege, H. CSIS Commission on Cybersecurity for the 44th Presidency, (2008). Securing Cyberspace for the 44th Presidency. Washington, DC: Center for Strategic and International Studies.

[9] Nye Jr, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Winter 2011, p. 30: http://www.au.af.mil/au/ssq/2011/winter/nye.pfd

[10] Federal Bureau of Investigation, Intellectual Property Theft: http://www.fbi.gov/about-us/investigate/cyber/ipr/ipr

[11] Federal Bureau of Investigation, Detroit Division, Press Release, "Two Charged in Conspiracy to Steal GM Trade Secrets," July 22, 2010: http://www.fbi.gov/detroit/press-releases/2010/de072210.htm

[12] Gorman, Siobhan. "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009: http://online.wsj.com/article/SB124027491029837401.html