The Rise of Cyber-Attacks-Short-of-War: *The Case for a New Cyber Treaty*

Asan Institute for Policy Studies
Kim Kildong

2017.02.27

They called it Operation Olympic Games. Huddled with his staff in the basement of the White House, President Obama secretly authorized cyber attacks against the computer systems that operate Iran's Natanz uranium enrichment plant. The worm, later dubbed Stuxnet, was designed to randomly speed up or slow down the centrifuges that process highly enriched uranium until they self-destructed. The beauty of the attack was, even when the centrifuges broke down, none of the plant operators suspected it was caused by a malicious code. It simply looked like a routine break down. Elated with the operation's success, President Obama authorized an even larger scale cyber attack.[1]

Some 6000 miles away in Natanz, Iranian scientists were enjoying another hot summer day. Everything seemed to be running as usual. Then suddenly, approximately 1,000 centrifuges spun out of control and self-imploded. The nuclear scientists panicked, while the plant operators turned to their computers to identify the problem. There was none. The computer screens indicated that everything was working just fine. The Iranians had no clue what had just hit them. And the devastation unraveling in front of their very eyes could not be stopped.[2]

[1] David Sanger, "Obama Order Sped Up Wave of Cyber Attacks against Iran," *The New York Times,* June, 12, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
[2] Ibid; Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired,*

Just when the operation seemed to be a complete success, the unexpected happened: Stuxnet went loose on the Internet. The malware, which was intended to be contained within the Natanz nuclear facility, was exposed when the USB drive containing the malware was connected to a computer with Internet access. The malware instantly replicated itself and spread around the world. It was only then did the Iranians finally realize that Natanz had been sabotaged.[3]

Enraged, the Iranians got hold of the code and weaponized it themselves. Whether they feared that a direct retaliatory attack on the U.S. would invite further attacks is unknown. But the Iranians ultimately opted to retaliate against Saudi Arabia, one of the U.S.' closest allies in the Middle East. In August 2012, Iran launched a massive cyber attack on Saudi ARAMCO, the world's largest oil company. The cyber attack wiped out the hard drives of 35,000 computers, instantly crippling the company's digital infrastructure. ARAMCO's ability to provide 10 percent of the world's oil supply was put in immediate jeopardy.

This is the new uncomfortable reality. Warfare is no longer limited to bombs and bullets. Bits and bytes can inflict as much damage as a Tomahawk missile. An adversary can paralyze a state's nuclear reactor from thousands of miles away and jeopardize a country's economy with a simple click. Countries with asymmetric capabilities find cyber attacks to be an irresistible method of warfare due to its minimal cost of operations, the wide availability of computers, and the near impossibility of attribution. Twenty-nine countries have already set up cyber units in their military to incorporate cyber weapons to their conventional planning for war. Pessimists warn that the proliferation of cyber

Nov. 03, 14,https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[3] Ibid.

weapons is inevitable.[4] Keith Alexander, former head of National Security Agency (NSA) and U.S. Cyber Command confirms: "Mark my words, it's going to get worse."[5]

While world leaders and legal practitioners rightfully fear and prepare for the worst kinds of "destructive" cyber attacks (i.e. Stuxnet), there looms a glaring need to regulate "disruptive" cyber attacks which may not cause actual physical damage, but nevertheless have severe consequences on the society, economy, and government. This report coins the term "cyber-attacks-short-of-war" (CASoW) to characterize these new cyber attacks as "**a politically motivated cyber attack by both state and non-state actors on private and public property with the intent to create severe disruptions in the society, economy, and government, without causing actual physical damage or death.**"[6] This report concedes that cyber attacks that cause physical damage and loss of human life fall under traditional laws of war. But "cyber-attacks-short-of-war" operates in an anarchic, ungoverned space that begs for a new set of regulations. It is CASoW, not cyber war, that poses the most pressing challenge for contemporary society.

The UN Charter and Cyber Warfare

The concept of just war theory (jus ad bellum) and conduct governing activities during war (jus in bello) have endured the test of time and are enshrined in

[4] Jennifer Valenito-Devries and Danny Yadron, "Cataloging the World's Cyberforces," *The Wall Street Journal*, Oct. 11, 2015, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710; McAfree Report, In the Crossfire: Critical Infrastructure in the Age of Cyber War, 2010, 11, http://resources.mcafee.com/content/NACIPReport.
[5] Andrea Shalal-Esa, "Top General Says U.S. under Constant Cyber Attack Threat," *Reuters*, May, 14, 2013, http://www.reuters.com/article/us-cyber-summit-alexander-idUSBRE94D12L20130515.
[6] This term is not to be confused with cyber crime, which are carried out by individuals with personal economic motives and generally has less impact.

Article 2(4) and Article 51 of the UN Charter. Article 2(4) clearly prohibits "the threat or *use of force* against the territorial integrity or political independence of any state...."[7] [emphasis added] The exception is promulgated in Article 51: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of the United Nations."[8] [emphasis added] In short, other than self-defense, a state can only resort to the legal use of force when it is authorized or mandated by the UN Security Council.

Although the UN Charter does not explicitly define "use of force" and "armed attack," decades of statecraft and rulings by the International Court of Justice (ICJ) provide some guidance and precedent. Considered to have a lower threshold than an armed attack, a "use of force" can include, but is not limited to, missile tests and bombardment of an unpopulated area. Considered "the most grave forms of the use of force"[9] by the ICJ, an "armed attack" can include, but is not limited to, aerial bombardment, ground assault, missile strikes, and territorial incursions.

Categorizing an attack as a "use of force" or an "armed attack" is critical because the aggrieved state is permitted to take appropriate, lawful, and legitimate responses against the aggressor. In the case of a "use of force," the attacked state can lawfully retaliate with countermeasures such as economic sanctions. But force still cannot be employed as retaliation. In case of an "armed attack," under Article 51's self-defense clause, the attacked state can lawfully retaliate with force that is proportional and discriminating.

[7] UN Charter
[8] Ibid.
[9] International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua *v.* United States of America), accessed at: http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5

But when does a cyber attack rise to the level of an illegal "use of force" or an "armed attack" under international law? The most authoritative work that tackles this pivotal question is *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013), a non-binding academic study sponsored by NATO.[10] *The Manual* argues that a cyber attack constitutes a "use of force" when its scale and effects[11] are comparable to non-cyber operations rising to the level of a "use of force." If it produces the same effect that a bomb would, the cyber attack would be considered a "use of force."

For a cyber attack to be considered an "armed attack," the attack must result in either physical destruction of property or death of person(s).[12] It is not difficult to imagine the types of cyber attacks that would rise to the level of an armed attack: (1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction and death, and (3) operations that disable air traffic control resulting in airplane crashes.[13] Such scenarios have fortunately remained in the realm of the imagination. But were they to occur, there would be visible, tangible, and measurable consequences.

But what happens when a cyber attack does not cause any actual physical damage or death? Would such cyber attacks be considered a "use of force" or even an "armed attack," triggering a state's right to self-defense? If not, what

[10] In 2009, NATO Cooperative Cyber Defence Centre of Excellence convened a group of international law experts to examine whether existing international law could account for the newly emerging technologies. The full manuscript of *The Manual* can be accessed at: https://ccdcoe.org/tallinn-manual.html.

[11] The experts offer nine categories as reference, severity, immediacy, directness invasiveness, measurability, military character, state involvement, and presumptive legality. For more detail: https://ccdcoe.org/tallinn-manual.html

[12] Michael N. Schmitt, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, (New York: Cambridge University Press, 2013).

[13] Harold H. Koh, "International Law in Cyberspace," *Harvard International Law Journal* (2012) Vol. 54

would be the appropriate response? And if the cyber attack was conducted by a state sponsored proxy, would a state-to-state statute like the UN Charter be applicable?

Cyber-Attacks-Short-of-War

Retired military lawyer, Major General Charles Dunlap drily notes: "A cyber attack is governed by basically the same rules as any other kind of attack."[14] But he fails to ask the corollary question—should it?

These modern cyber attacks do cause "severe disruptions" in society, economy, and government, but with the exception of Stuxnet, no known cyber attack has ever caused physical damage. The fact that state entities rarely conduct cyber attacks compounds the problem. In most cases, nation-states orchestrate cyber attacks using patriotic hackers, giving them ample room for plausible deniability. Because "cyber-attacks-short-of-war" fall outside the purview of the UN Charter and fail to trigger *jus ad bellum* principles, a new set of regulations governing cyber attacks is needed.

So what exactly are "cyber-attacks-short-of-war?" These attacks run the range from cyber espionage, cyber sabotage, to cyber subversion. To evaluate whether a cyber attack qualifies as a CASoW, three categories must be weighed: 1) the perpetrator(s)' intent; 2) its relationship to the government; 3) the level and scope of "severe disruption." More significance is placed on the first two categories because, while the intent and affiliation of the perpetrator can be rather quickly determined, the term "severe disruption" *ipso facto* is subjective

[14] Peter W. Singer, Allan Friedman, *Cybersecurity: What Everyone Needs to Know,* (Oxford University Press: New York), 2014.

and difficult to measure. Thus, if the perpetrator is shown to have close relations with a government and is motivated politically to cause "severe damage," the cyber attack would qualify as a CASoW. The following examples illustrate the disastrous consequences of a CASoW.

The Greatest Transfer of Wealth

States do not go to war over espionage. But what if the spy is caught stealing sensitive information that is a direct threat to national security? The U.S. alone loses approximately $350 billion dollars annually on cyber attacks, an ongoing phenomenon Keith Alexander calls "the greatest transfer of wealth in history."[15] The digital revolution has given perpetrators an unprecedented advantage of gaining invaluable information without needing a physical human asset. States no longer need to rely solely on expensive satellites, airplanes, submarines, and human spies to collect information. A few laptops with a high speed connection and highly skilled hackers will suffice. This significantly lowered barrier of entry has been fueling the proliferation of cyber espionage.

However, the scale of operations is not the only growing problem. The sensitive information and the economic quality of the information that are being stolen deeply impact a state's long term national security interests and economic competitiveness.

In May 2009, the Pentagon acknowledged that Chinese hackers successfully infiltrated some U.S. government and defense contractors'

[15] Josh Rogin, "NSA Chief: Cybercrime Constitutes the Greatest Transfer of Wealth in History," *Foreign Policy,* July 9, 2012, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/
https://www.wsj.com/articles/SB10001424127887324328904578621880966242990.

computer systems.[16] One of the most sensitive information stolen was the design and manufacturing process of F-35 fighter jets, the next generation combat aircraft designed to protect America for the next 55 years. The U.S. spent approximately $1.5 trillion and 14 invaluable years in research and development (R&D).[17] By stealing the F-35 design data, China was able to build its J-31 fighter while obviating the need for R&D investments. Former Defense Acquisition Chief Frank Kendall observed: "What it does is reduce the costs and lead time of our adversaries to doing their own designs, so it gives away a substantial advantage."[18] The influential Defense Science Board argues that what is more worrisome is that the Chinese were able to gain knowledge of operational concepts and system use (e.g., which processes are automated and which are person controlled) developed from decades of U.S. experience—the type of information that cannot simply be recreated in a laboratory or factory environment. Such information also helps the adversary to rapidly develop countermeasures against these new technologies.[19]

West Virginia Senator Joe Manchin criticized the Obama administration's failure to retaliate against China for stealing the F-35 designs: "They're making leaps, which are uncommon, at the behest of us, and we know this...but we're not taking any actions against them." [20] The Obama

[16] Office of the Secretary of Defense, "Military Power of the People's Republic of China 2009," accessed at: https://www.defense.gov/Portals/1/Documents/pubs/China_Military_Power_Report_2009.pdf

[17] Naval Air Warfare Center, "Joint Strike Fighter F-35 Lightning II Fact Sheet," accessed at: http://www.jsf.mil/news/docs/20160324_Fact-Sheet.pdf

[18] David Alexander, "Theft of F-35 Design Data Is Helping U.S. Adversaries," *Reuters*, June, 19, 2013, http://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619

[19] Defense Science Board, "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," *DOD*, January 2013, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

[20] Brendan McGarry, "Lawmaker: Chinese J-31, J-20 Mirror American F-35, F-22," *Defensetech*, September, 29, 2015, https://defensetech.org/2015/09/29/lawmaker-chinese-j-31-j-20-mirror-american-f-35-f-22/.

administration charged a private citizen named Su Bin, one of the three hackers in charge of the operation. Mr. Su has been sentenced to a mere *five* years in prison for the attacks.[21] There were no formal diplomatic protests. There were no resolutions proposed to the UN Security Council. There were no economic sanctions.

Widespread social disruption in Estonia

In 2007, Russia and Estonia clashed over the removal of the Bronze Soldier Soviet War Memorial in central Tallinn, Estonia. While ethnic Russians in Estonia saw the statute as a tribute to fallen WWII soldiers, Estonians viewed it as a symbol of Soviet occupation. When the Estonian government was contemplating whether to remove the statue, ethnic Russians in Estonia took to the streets to protest and President Vladimir Putin warned of "irreversible consequences" if the Estonian authorities were to follow through.[22] Despite the warning, the Estonian authorities relocated the statue to the Tallinn Military Cemetery on April 27, 2007.

On that very day, Estonia was hit with crippling distribution of denial of service (DDoS) attacks. Credit card transactions and bank accounts were frozen. Public fear intensified as news agencies could not broadcast, internet websites were inaccessible, and mobile phone networks were completely shut down. With their hands effectively tied, the Estonian government was unable to communicate with the public. It took nearly three weeks for the Estonian Cyber Emergency Response Team to fend off the perpetrators and restore vital services.

[21] Justin Ling, "Man Who Sold F-35 Secrets to China Pleads Guilty," *Vice News*, March 25, 2016, https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty
[22] Gary Peach, "Statue Symbolizes Grudges Against Russia," *The Associated Press*, April, 22, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/04/22/AR2007042200617_pf.html

While the worst had passed, and no physical damage and death occurred, fear and panic spread among the general public. Estonians compare these series of events as their own 9/11.[23]

When Estonian authorities traced the attack to Russia, the Kremlin simply denied involvement and blamed Nashi, a state-sponsored group of young pro-Kremlin hackers.[24]Initially, Estonia contemplated invoking Article 5 of the North Atlantic Treaty, but reconsidered in light of the reluctance of other NATO members to deem the cyber attacks as an "armed attack" in the absence of physical damage.[25] With no viable retaliation, Estonia turned to its domestic laws and regulations to prosecute the suspects. Under the Mutual Legal Assistance between Russia and Estonia, Russia was legally obligated to cooperate with Estonia's criminal investigation. True to form, the Russian Supreme Procurator rejected Estonia's request. With no support from allies and unable to compel Russia to cooperate, Estonia convicted a single ethnic Russian student living in Tallinn. He was fined a "whopping" $1,642, for the havoc he wrought on the entire nation of Estonia.

Did Russia Cross the Red Line?

In October 2016, the Obama Administration accused Russia of interfering with the U.S. presidential election. Two months earlier, the U.S. intelligence community had warned of Russia's attempt to influence the election. This fear

[23] http://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/
[24] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, *Berkeley Journal of Law* (27), 2009, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil
[25] Scheherazade Rehman, "Estonia's Lessons in Cyberwarfare," *US News*, Jan. 14, 2013, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

was realized when the Russians hacked into the Democratic National Committee (DNC) and leaked presidential candidate Hillary Clinton's emails to WikiLeaks.[26] Although Russia disclaimed these accusations, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) concluded with high confidence that the attacks were traced back to Advanced Persistent Threat (APT) 29 and APT 28, both considered proxy actors of the Kremlin.[27] The Central Intelligence Agency (CIA) assessed that the attacks were intended to help Donald Trump win the presidency.[28] Though Russia's intervention may not have directly influenced the outcome of the election, there is no denying that the cyber attacks took place.[29] As President Obama noted: "…that does not in any way, I think, detract from the basic point that everyone during the election perceived accurately—that in fact what the Russian hack had done was create more problems for the Clinton campaign than it had for the Trump campaign."[30] Admiral Michael S. Rogers, the Director of the NSA and Commander of CYBERCOM, concurred, "There shouldn't be any doubt in

[26] Adam Entous, Ellen Nakashima, and Greg Miller, "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House," *The Washington Post,* Dec. 9, 2016, https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.8253de2f0c12; Assange has repeatedly disputed claims that the emails came from the Russian government. Yet, in a December interview on Hannity's radio show, he left open the possibility that Guccifer 2.0 (the hacker that actually leaked the emails) activities were linked to the Russians. For more read, https://www.washingtonpost.com/news/fact-checker/wp/2017/01/05/julian-assanges-claim-that-there-was-no-russian-involvement-in-wikileaks-emails/?utm_term=.b18da842ee3a.

[27] President Obama stated, "These data theft and disclosure activities could only have been directed by the highest levels of the Russian government."

[28] Miller, "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House."

[29] Philip Rucker and Ashley Parker, "Trump Admits to Russian Hacking Even as He Attacks U.S. Intelligence Community," *Washington Post*, Jan. 11, 2017, https://www.washingtonpost.com/politics/trump-admits-to-russian-hacking-even-as-he-attacks-us-intelligence-community/2017/01/11/40941a34-d817-11e6-b8b2-cb5164beba6b_story.html?utm_term=.945272cd7e98

[30] Scott Detrow, "Obama on Russian Hacking: We Need to Take Action. And We Will." *NPR,* December 15, 2016, http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-need-to-take-action-and-we-will

anybody's mind…This was not something that was done casually, this was not something that was done by chance, this was not a target that was selected purely arbitrarily…This was a conscious effort by a nation-state to attempt to achieve a specific effect."[31] Even President Trump, who at first downplayed the allegations as "fake news," admitted that Russia was behind the attack.[32]

Despite the severity of this breach, the Obama Administration's response was disproportionately weak. On December 29, 2016, the administration announced that the U.S. would expel 35 Russian diplomats and add Russian intelligence officials on the Office of Foreign Assets Control (OFAC) list of Specially Designated Nations and Blocked Persons (SND List). [33] The administration also closed two recreational Russian compounds that were used for intelligence activities. Obama also stated that the administration will take covert retaliations. Nevertheless, many share the arguments of U.S. Senators John McCain (R-AZ) and Lindsey Graham (R-SC): "Ultimately, the sanctions are a small price for Russia to pay for its brazen attack on American democracy."[34]

Recommendations: A New Cyber Treaty for CASoW

These three examples of CASoW showcase the devastating implications of

[31] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html
[32] Philip Rucker and Ashley Parker, "Trump Admits to Russian Hacking Even as He Attacks U.S. Intelligence Community," *Washington Post*, Jan. 11, 2017, https://www.washingtonpost.com/politics/trump-admits-to-russian-hacking-even-as-he-attacks-us-intelligence-community/2017/01/11/40941a34-d817-11e6-b8b2-cb5164beba6b_story.html?utm_term=.945272cd7e98
[33] The White House, "Fact Sheet: Actions in Response to Russian Malicious Cyber Activities and Harassment," December, 29, 2016, accessed at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and
[34] Senate Press Release. http://www.mccain.senate.gov/public/index.cfm/press-releases?ID=DFAE6FFD-976A-468C-B53B-15D548E46BD7. Accessed February 16, 2017.

cyber attacks. While they caused "severe damage," the affected states failed to respond in a proportionate manner that could have deterred future attacks. Because traditional laws of war are useless for managing cyber attacks, this report calls for a new international treaty that clearly delineates the threshold and consequences of any cyber attack and holds states accountable for the actions of proxy agents.

By clearly spelling out the threshold for a CASoW and defining retaliatory proportionality, both the aggressor and the victim will know beforehand the consequences of launching any cyber attack. If the agreed upon threshold and consequences were to be codified in a binding treaty, the victim state will be legally permitted to execute a proportionate response that is legitimate in the eyes of the international community. More importantly, this new treaty would make the adversary reevaluate its cost-benefit calculation before launching a CASoW. Unless the cyber attack accrues significant benefits and gains for the initiator, there is little incentive for the state to risk bearing the anticipated consequences.

The new treaty must also address the attribution problem. Digital forensics is difficult as it is. But even in cases where the perpetrator is identified, states can simply claim deniability. By shifting the blame to a private citizen or a sub-group, nation-states have been able to avoid meaningful repercussions. The new treaty holds states accountable for any and all of their proxies. This is an approach the United States took to justify its attack on the Taliban in Afghanistan in 2001. Lastly, this new treaty must include an obligatory assistance clause, requiring all states to fully cooperate with a victim state(s)' investigation. An extradition clause that allows the victim(s) to request extraditions of suspects and convicted cyber hackers would be a prominent part

of the new treaty. Noncompliance by any parties would be viewed as a sign of collaboration between the suspects and the state in which the former operated.

Conclusion

Richard Clarke, former cyber security and cyber terrorism adviser to the White House is worth quoting at length: "My greatest fear is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts.… ***And we never really see the single event that makes us do something about it. That it's always just below our pain threshold***…After a while you can't compete."[35] [emphasis added]

Clarke's words go the heart of the cyber problem: traditional laws of war do not adequately address "cyber-attacks-short-of-war." A cyber attack can cause severe disruptions in the economy, government, and society without causing any tangible, physical damage or death. As it falls below the traditional trigger for war, nation-states have not been able to execute proportionate responses to deter future attacks. To exacerbate the problem, these cyber attacks are not perpetrated by someone "sitting on their bed who weighs 400 pounds,"[36] but by individuals and groups of professionals with deep financial and technical resources, often with government toleration, and in some cases, explicit support.[37] Today, states can passively claim deniability and obviate meaningful consequences by the simple act of shifting blame to compliant proxies.

[35] Ron Rosenbaum, "Richard Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian Magazine,* April 2012, http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/

[36] During the first presidential debate on September 26, 2016, Trump declared that the hacking may have been the work of "someone sitting on their bed weighing 400 pounds."

[37] Remarks by Eugene Spafford in James Fallows, "Cyber Warriors," *The Atlantic,* March 2010,https://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/

The three incidents cited in this report proffer ample evidence and conditions for consideration of a new codified cyber treaty. Failing to agree to a cyber treaty that regulates CASoW poses a serious threat to the national security and economy of highly connected modern states. Thomas Hobbes once said, “Hell is truth seen too late.” The need to address this portentous development looms large. It would be tragic but well deserved if this cyber Wild West is left untamed.