Wilson Briefs | October 2015

Arms Control in Cyberspace?

Wilson Center

By Robert Litwak and Meg King

SUMMARY

U.S. policymakers have compared the challenge of managing threats in the cyber domain to that of controlling nuclear weapons during the Cold War. The United States and China are currently negotiating what would be the first cyber arms control agreement to ban attacks on each other's critical infrastructure in peacetime. The Obama administration believes such an agreement could lead to a broader "international framework" of norms, treaties, and institutions to govern cyberspace. Arms control and deterrence are longstanding U.S. policy instruments that are being revived and retooled to meet contemporary cyber challenges. But the utility of these Cold War strategies, which constitute necessary but not sufficient measures, will be inherently limited owing to fundamental differences between the nuclear and cyber domains.

THE POLICY CONTEXT

At the conclusion of President Xi Jinping's state visit to Washington on September 25, 2015, the United States and China announced a limited agreement "that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[1] Reactions of U.S. cyber experts to the Chinese commitment to forego state-sponsored cyber commercial espionage were mixed—with some characterizing the move as a "sea change" and others viewing it as consistent with previous Chinese statements made even as the country engaged in the large-scale theft of foreign intellectual property. "The question now," President Barack Obama declared, is 'Are words followed by actions?'"

In addition to this discrete measure, the world's two major powers committed, according to a joint statement issued by the White House, to "identify and promote appropriate norms of state behavior in cyberspace within the international community."[2] This "generic embrace" of a code of conduct, as a senior Obama administration official characterized it, could pave the way for future U.S.-Chinese ministerial talks whose objective would be to negotiate the first cyber arms control agreement banning state-sponsored cyberattacks on each other's critical infrastructure during peacetime.[3] The two countries affirmed that this high-level channel would also be used "to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side."

The Xi visit came in the aftermath of the bombshell revelation in June 2015 that Chinese state hackers had breached the Office of Personnel Management's website and obtained the personal information on some 22 million current and former U.S. government employees. President Obama, a major theme of whose presidency has been to promote a "rules-based international order," has called for the creation of an "international framework" to regulate great power competition in cyberspace. Such a state-based framework, the president acknowledges, will not be "perfect" because it will not solve cybersecurity threats posed by "non-state actors and hackers who are very good." But among states, the president declared, "there has to be a framework that is analogous to what we've done with nuclear power because nobody stands to gain. And, frankly, although the Chinese and Russians are close, we're still the best at this. And if we wanted to go on offense, a whole bunch of countries would have some significant problems."[4]

Obama's comments surrounding the Xi visit reflect an emerging two-pronged strategy that would apply Cold War-era concepts—arms control and deterrence—to the cyber domain. In advocating the establishment of a new "international framework" to govern cyberspace, the president invoked the nuclear precedent—the decades of arms control experience between the United States and the Soviet Union to stabilize the balance of terror, and among the 190-plus states that have acceded to the Nuclear Non-Proliferation Treaty. But complementing this cooperative offer to negotiate the bounds of acceptable behavior in cyberspace was a deterrent threat: "There comes a point at which we consider this a core national security threat," Obama asserted. Administration officials have referred to the possible imposition of sanctions on Chinese hackers as a punitive instrument to affect the Beijing regime's calculus of decision.

Arms control and deterrence are longstanding U.S. policy instruments that are being revived and retooled to meet contemporary cyber challenges. But the utility of these Cold War strategies, which constitute necessary but not sufficient measures, will be inherently limited owing to fundamental differences between the nuclear and cyber domains. U.S. policymakers, analogizing from the historical experience with nuclear arms control and proliferation (as well as other weapons of mass destruction), are primarily focused on developing state-based strategies.

However, unlike the nuclear weapons under the control of states, cyberspace (along with the oceans, air, and outer space) is part of the world's shared spaces—what the United Nations calls the "global commons"—that is integral to globalization and a domain in which non-state actors can increasingly exercise power and influence rivaling that of states.

CYBER THREATS

The Internet—short for inter-networking—emerged in the 1970s through pioneering work supported by the Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense. What started as an initiative to facilitate scientific research among a small community of essentially approved users expanded exponentially when the Internet went commercial in the late 1980s. The number of global users of the Internet has now topped 3 billion people, and concerted efforts in the developing world to close the digital divide will add billions more. In tandem with the skyrocketing growth of the Internet, which now permeates all facets of our society and economy, has been a dramatic increase in security threats.

Cyber expert James Lewis likens the Internet to the "Wild West" in which "we pit weak defenses against skilled opponents."[5] Those opponents range from individual hackers to terrorist groups, and from criminal organizations to state sponsors. The cyber threats generated by these perpetrators are likewise diverse. Indeed, there is no universally accepted definition as to what precisely constitutes a cyberattack. The term is often used interchangeably with cyberespionage, cyberterrorism, cybercrime, and cyberwarfare. To clarify these eliding and confusing usages, Yale Law School scholars, writing in "The Law of Cyber-Attack," offered a concise, narrow definition: "A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose."[6]

Under this definition, politically motivated cyberterrorism would meet the criteria of a cyberattack, whereas cybercrimes (such as credit card fraud) that do not have a political or national security objective would not. Nor would cyberespionage (which, of course, the United States itself extensively employs) constitute a "cyberattack" if the action did not compromise the functioning of a computer network. President Obama told President Xi that the Chinese government's large-scale cyber-enabled theft of intellectual property for commercial advantage "has to stop" because it had essentially crossed the line from cyberespionage to large-scale cybercrime.[7]

At the other end of the threat continuum, a cyber*attack* crosses the definitional threshold into cyber*warfare* if its effects are equivalent to an armed attack.[8] In 2012, State Department Legal Adviser Harold Koh explicitly confirmed that a cyberattack whose consequences amounted to an armed attack could trigger the right of self-defense under UN Charter Article 51, and that international law governing armed conflict (e.g., the norm distinguishing between military and civilian targets) would apply to cyberwarfare. The U.S. approach to cyberattacks potentially triggering an armed counter-response focuses on consequences—deaths, damage, and large-scale disruption. Addressing the thorny issue of attribution—identifying the perpetrator of a cyberattack—Koh declared that "states are legally responsible for activities undertaken through 'proxy actors,' who act on the State's instructions or under its direction or control."[9] In an apparent reference to China, Koh noted that not all countries accept the principle that international law applies in cyberspace. Indeed, on the core issue as to what constitutes a cyberattack, China, as well as Russia and other members of the Shanghai Cooperation Council, view the issue through a political prism, emphasizing the use of information technology by adversarial parties to engage in "mass psychological brainwashing to destabilize society and state."[10] This expansive definition of cyberattack is a bald effort to block political content on the Internet that the Beijing and Moscow regimes find potentially threatening to regime stability and survival.

In the cyber domain, the United States faces a multiplicity of threats generated by a multiplicity of hostile parties. In 2012, Defense Secretary Leon Panetta declared that the vulnerability of the U.S. power grid, transportation system, financial networks, and government institutions created the specter of a "cyber-Pearl Harbor." The most destructive such scenario, he stated, would be "cyber-actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack."[11] When discussing the possibility of a cyber-Pearl Harbor, one must distinguish between state and non-state actors. Cyber experts question whether a non-state actor would be capable of conducting a mass-casualty cyberattack. Such an attack, according to U.S. Naval Academy professor George R. Lucas, "simply outstrips the intellectual, organizational and personnel capacities of even the most well-funded and well-organized terrorist organization, as well as those of even the most sophisticated international criminal enterprises."[12] As cyber analysts P.W. Singer and Allan Friedman note, taking down critical infrastructure, such as the power grid, "doesn't just require the skills and means to get into a computer system. It requires knowing what to do once you're there."[13] This assessment parallels that of WMD specialists who are skeptical that a non-state terrorist group, lacking the industrial capabilities of a state, could construct an unconventional nuclear, chemical, or biological weapon to carry out a mass-casualty attack. That judgment holds for now. But for both the cyber and WMD domains, the open question regarding non-state threats is how long these practical constraints on mass-casualty weaponization will remain.

STATE-SPONSORED CYBERATTACKS

In March 2011, on the eve of the U.S.-led NATO intervention in Libya to topple Qaddafi, the Obama administration debated whether to open the air campaign with a cyber-offensive to penetrate the Libyan military's computer network and disrupt the air defense system. After internal deliberations, the administration refrained, fearing the move would set a precedent Russia and other countries could seize on to mount their own cyber-offensives. A few weeks later, on May 2, 2011, the Obama administration also balked at a narrower proposed cyberattack to prevent Pakistan's radar from spotting the helicopters carrying U.S. special forces on the mission targeting Osama bin Laden.[14] Neither of these attacks would have met the definitional criteria for cyberwarfare because the disruption operations aimed at these defense facilities would not have generated the deaths and damage of an actual armed attack. Despite these instances of reticence, several states have been charged with conducting cyberattacks either directly or through proxies. These cyberattacks, the most prominent of which are discussed below, vary by *type*, *attribution*, and *consequence*.

Russia's cyberattack on Estonia, 2007—In spring 2007, Estonia was the target of a *denial-of-service* attack that forcibly shut down websites and other online platforms. The attack overloaded the servers and crashed the websites of the Estonian parliament and government ministries, political organizations, newspapers, and banks. The scale of the attack, which proved more disruptive than damaging, suggests that botnets (a global network of compromised computers) were used to flood the websites. The precipitant of the attack was evidently the Estonian government's decision to relocate a Soviet-era statue commemorating the victory over Nazi Germany. The Estonian government publicly accused Russia of perpetrating the attack. Though the attack was eventually attributed to Russian nationalist "hacktivists," no definitive link between them and the Russian government was established. A former chief scientist at the Pentagon's Defense Advanced Research Projects Agency, described the attacks as "more like a cyber riot than a military attack," while another former senior U.S. cybersecurity official said that the "prevailing assessment" was that no "state actor" was involved in this denial-of-service attack.[15] Nonetheless, this episode has been called "the first explicit large-scale attack for political rather than economic purposes."[16]

Russia's cyberattack on Georgia, 2008—Like the Estonian attack of 2007, a denial-of service attack employing botnets compromised Georgian government and media websites in summer 2008, but the country's critical infrastructure was not disrupted. Because this cyberattack immediately preceded Russia's late August military incursion across the Georgian border in support of ethnic separatists in the Abkhazia and Ossetia, Georgia attributed it to the Russian government. But subsequent analysis could not establish a direct link between the Russian "patriotic hackers" who launched the cyberattack and the Russian government.

The U.S. Stuxnet attack on Iran, 2008-2010—The U.S. cyberattack on Iran's nuclear program utililizing the Stuxnet computer virus marked the first sustained use of a cyberweapon against an adversarial state's industrial infrastructure. As reported by David Sanger of the *New York Times*, the incoming Obama administration accelerated the attacks, code-named Olympic Games, which the Bush administration had initiated in response to the growth of Iran's uranium enrichment site at Natanz.[17] The focus of the cyberattack were the thousands of centrifuges spinning at Natanz to produce what the Iranians claimed was low-enriched uranium to fuel (nonexistent) civil nuclear reactors, but that were capable of yielding highly-enriched, weapons-grade uranium. The U.S. National Security Agency, assisted by a secret Israeli cyber-unit, developed a computer worm—what the Americans called "the bug"—to sabotage the centrifuges by ordering them to spin out of control. The worm, introduced by exploiting a vulnerability of the German-made Siemens computer on use at the Natanz site, resulted in the destruction of more than 1,000 centrifuges in 2010. In launching the Stuxnet attack, the Bush and Obama administrations had to weigh the benefits of slowing Iran's nuclear program with the risks of a precedent-setting use of a cyberweapon.

North Korea's cyberattack on Sony Pictures, 2014—According to U.S. officials, North Korea was "centrally involved" in the hacking of Sony Pictures computers to steal data in December 2014. The disruption (including the online posting of stolen emails, salary information, and unreleased movies) was more embarrassing than damaging. The precipitant of the cyberattack was the Sony studio's impending release of a comedy film ridiculing North Korea's supreme leader, Kim Jong Un. The FBI was able to attribute the cyberattack to North Korea because of "sloppy" efforts to use proxy servers to disguise the trail of evidence. The Obama administration's announced a "proportional response," imposing sanctions on 10 officials involved in "many of North Korea's major cyberoperations."[18] But in tandem with this official reaction was a covert operation, denied by U.S. officials, which temporarily cut off North Korea's limited access to the Internet.[19] Because of North Korea's reliance on China for Internet access, the Obama administration reportedly asked the Beijing government for assistance in blocking the Kim Jong Un regime's ability to carry out cyberattacks.[20]

China's cyberattack on the OPM database, 2015—The Obama administration, while privately attributing the hack of the U.S. Office of Personnel Management's huge database to China, have refused to do so publicly. The breach, which compromised the personal data of some 22 million current and former U.S. government employees, was revealed in June 2015. The reticence in naming China was reportedly due to concern that such a revelation would require the United States to disclose details of its own espionage and cyberspace capabilities. Indeed, according to the *Washington Post*, Director of National Intelligence James R. Clapper even expressed grudging admiration for the OPM hack, saying U.S. spy agencies would do the same against other governments.[21]

Assessment—Three major issues emerge from this select review of cyberattack cases: (1) attribution remains a fundamental challenge because cyber forensics to track a cyberattack to its source is a major technological hurdle and state perpetrators may utilize non-state proxies to carry out an attack; (2) the Stuxnet attack crossed "a rubicon," in the phrase of a former CIA director, because it resulted in significant destruction (i.e., equivalent to an armed attack) in Iran's nuclear infrastructure; and (3) cyberespionage, even on the scale of the OPM hack by China, falls within the traditional parameters of espionage and does not cross the definitional thresholds of a cyberattack or cybercrime.

ARMS CONTROL AND DETERRENCE

Escalating Threats

Attacks among states in cyberspace are escalating. In the wake of the U.S. Stuxnet attack on Iran's nuclear infrastructure, the Tehran regime retaliated with three waves of cyberattacks on American banks in August 2012. That same month, according to former National Security Agency director Keith Alexander, Iran launched a cyberattack on the Saudi Arabian national oil company's computer network.[22] The sharp escalation in state-sponsored cyberattacks prompted the *New York Times* to editorialize: "The best way forward is to accelerate international efforts to negotiate limits on the cyberarms race, akin to the arms-control treaties of the Cold War."[23] President Obama has similarly analogized between the nuclear and cyber arms races.

In the nuclear domain, the United States has advanced state-based strategies to curb capabilities and manage the escalatory risks of superpower competition. Unlike cyber capabilities, nuclear weapons have been in the sole custody of states. State-based strategies have been pursued to reassure non-nuclear states to forego the weapons option, and to induce or compel nuclear weapons states to secure their arsenals to prevent the "leakage" of a weapon to a terrorist group. The same state-based rationale has been applied to terrorism. State sponsorship has sharply declined since the 1970s because of the punitive costs that the international community has imposed on states that use terrorism as an instrument of policy. A persisting challenge is "passive sponsors," states that turn a blind eye because they lack the capacity to control their sovereign space or are sympathetic to the political goals of the terrorist groups operating on their territory.

Policy Opportunities and Challenges

An analogous state-based strategy for the cyber domain would leverage the mutual interests of states as stakeholders in preserving the "global commons." All states have an interest in ensuring that the Internet operates smoothly—for example, by eliminating "botnets"—and combatting cybercrime.[24] This is the starting point—"the low-hanging fruit," as two cyber experts put it—for creating the "international framework" of norms and institutions that President Obama has proposed.

Another priority should be to bring to fruition the negotiations between the United States and China on a cyber arms control agreement to ban state-sponsored cyberattacks on critical infrastructure during peacetime. The Obama administration views that potential bilateral agreement as a base upon which to develop a global consensus of states.

The bedrock of a state-based strategy to address cyber challenges is sound *national* policies, codified in domestic law and enforced. Such measures address the cyber analogue to the passive sponsor challenge in counter-terrorism. But key to this approach is incentivizing states to rein in non-state actors (individuals and groups) conducting proscribed activities. The bind is that authoritarian states like Russia and China have an interest in preserving "patriotic hackers" as a policy instrument (while maintaining plausible deniability) and in controlling politically threatening Internet content that would be protected speech in democratic states.

These elements of what one could characterize as "arms control in cyberspace" are necessary, but not sufficient. As during the Cold War, arms control needs to be buttressed by a robust strategy of deterrence in both its variants—deterrence by denial and deterrence by punishment.

In the cyber realm, *deterrence by denial* would entail defensive measures that frustrate an adversary's ability to achieve its objective. On the individual level of personal computers, anti-virus and anti-malware software that block outside intrusions are a form of deterrence by denial. As significant as a "cyber arms control agreement" to ban attacks on critical infrastructure might be in normative terms, the necessary complement are effective cyber defense mechanisms—strengthening computer networks to block unauthorized access and increase their resilience—that would frustrate a potential attacker. In these terms, the Chinese hack of the OPM database was a stunning failure of deterrence by denial. Deterrence by denial has important implications for crisis stability because, in the "cyber Pearl Harbor" nightmare scenario, it can significantly reduce the incentive that an adversary like Russia might see in initiating a preemptive strike. Crisis stability is a thorny issue as cyber probes of computer networks that fall within the realm of espionage could have unintended escalatory consequences if perceived by the target state to be the prelude to an attack.

Deterrence by punishment would hold states accountable for cyberattacks which either they or their proxies conduct. This variant of deterrence is the more familiar of the two from the Cold War era. A stable nuclear deterrent relationship between the United States and the Soviet Union—captured by the fitting acronym MAD, mutual assured destruction—fostered what historian John Lewis Gaddis describes as "the long peace" by making the use of nuclear weapons unthinkable. But that system relied on an ability to accurately attribute a potential attack to a specific adversary. In the cyber realm, attribution is a major problem. In the case of the Sony hack, the FBI was able to trace the attack back to North Korea only because of its "sloppy" use of proxy servers to mask its action. And, in response, the Obama administration responded covertly with a form of deterrence by punishment when it essentially shut down North Korea's Internet for a short period. As cyber expert Benjamin Brake argues, "a credible retaliatory threat will depend on perceptions of U.S. attribution capabilities." That requires investments in cyber forensics to improve the United States' real and perceived attribution capacities.[25] An enhanced attribution capability can affect an adversarial state's calculus of decision if a cyberattack entails a significant risk of being traced back to its perpetrator. Any adversarial state contemplating a cyberattack (particularly one crossing the threshold into cyberwar by being equivalent of an armed attack) must be made to believe through the credibility of U.S. attribution capabilities that the regime would be held accountable for its action or that of a proxy acting indirectly on its behalf.

In sum, the goal is to make the Internet Wild West less wild. Retooled versions of Cold War strategies—arms control and deterrence—will be essential policy tools for U.S. policymakers. But as essential as they are, their utility will be limited by the challenging character of the cyber domain.

ENDNOTES

The authors gratefully acknowledge the research assistance of Olivia Kantor in the preparation of this Policy Brief.

[1] White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015 <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

[2] Ibid.

[3] David E. Sanger, "U.S. and China Seek Arms Deal for Cyberspace," *New York Times*, September 19, 2015 <http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html?_r=0>.

[4] White House, "Remarks by the President to the Business Roundtable," September 16. 2015 <https://www.whitehouse.gov/the-press-office/2015/09/16/remarks-president-business-roundtable>.

[5] James Andrew Lewis, "The key to keeping cyberspace safe? An international accord." *Washington Post*, October 7, 2014 <http://www.washingtonpost.com/postlive/key-to-keeping-cyberspace-safe-international-accord/2014/10/07/ae50a35e-4812-11e4-b72e-d60a9229cc10_story.html>.

[6] Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," *Yale Law School Faculty Scholarship Series*, paper 3852, 2012, p. 11 <http://digitalcommons.law.yale.edu/fss_papers/3852>.

[7] White House, "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," September 25, 2015 <https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>.

[8] Hathaway and Crootof, "The Law of Cyber-Attack," pp. 21-22.

[9] Department of State, Legal Advisor Harold Hongju Koh, "International Law in Cyberspace," address at USCYBERCOM, September 18, 2012 <http://www.state.gov/s/l/releases/remarks/197924.htm>; and Ellen Nakashima, "Cyberattacks could trigger self-defense rule, U.S. official says," *Washington Post*, September 18, 2012 <https://www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html>.

[10] Hathaway and Crootof, "The Law of Cyber-Attack," p. 9.

[11] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012 <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>.

[12] Quoted in P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), p. 98.

[13] Ibid.

[14] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," New York Times, October 17, 2011 <http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0>.

[15] Shaun Waterman, "Analysis: Who cyber smacked Estonia?," UPI, June 11, 2007 <http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/26831181580439/>.

[16] Edward Skoudis, "Information Issues in Cyberspace" in Franklin D. Kramer, et al., eds., *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), p. 178.

[17] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012 <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0>.

[18] David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony Case," *New York Times*, January 2, 2015 <http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html?ref=topics&mtrref=topics.nytimes.com&assetType=nyt_now>.

[19] Martin Fackler, "North Korea Accuses U.S. of Staging Internet Failure," *New York Times*, December 27, 2014 <http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html?ref=topics>.

[20] David E. Sanger, Nicole Perlroth, and Eric Schmitt, "U.S. Asks China to Help Rein In Korean Hackers," *New York Times*, December 20, 2014 <http://www.nytimes.com/2014/12/21/world/asia/us-asks-china-to-help-rein-in-korean-hackers.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news>.

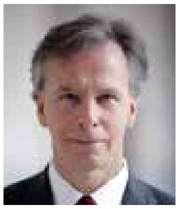
[21] Ellen Nakashima, "U.S. decides against publicly blaming China for data hack," Washington Post, July 21, 2015 <https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html>.

[22] David E. Sanger, "Document Reveals Growth of Cyberwarfare Between the U.S. and Iran," *New York Times*, February 22, 2015 <http://www.nytimes.com/2015/02/23/us/document-reveals-growth-of-cyberwarfare-between-the-us-and-iran.html>.

[23] Editorial Board, "Arms Control for a Cyberage," *New York Times*, February 26, 2015 <http://www.nytimes.com/2015/02/26/opinion/arms-control-for-a-cyberage.html?_r=0>.

[24] Singer and Friedman, *Cybersecurity and Cyberwar*, p. 187.

[25] Benjamin Brake, "Strategic Risks of Ambiguity in Cyberspace," *Contingency Planning Memorandum* no. 24, Council on Foreign Relations, May 2015 <http://www.cfr.org/cybersecurity/strategic-risks-ambiguity-cyberspace/p36541>.



Robert Litwak is Vice President for Scholars and director of International Security Studies at the Wilson Center.

Meg King is director of the Wilson Center's Digital Futures Project.

The Wilson Center

@TheWilsonCenter

facebook.com/WoodrowWilsonCenter

www.wilsoncenter.org

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

Wilson Center