Cyber Domain Conflict in the 21st Century

by Frank J. Cilluffo and Sharon L. Cardash

The U.S. military recently accorded cyberspace the status of a "domain," which means that it is a potential battle-space like land, sea, air, or outer space, and will be treated accordingly. What is the nature of conflict and threats in this digital landscape? What key policy questions will arise for the United States, as a result, and how might these matters be best addressed? Looking forward, these emerging questions will be top priorities for policymakers. Our aim here is to explore these issues and help spark discussion, thereby helping to shape some of the contours of these important policy debates as this new and distinct domain continues to touch and impact all the others.

The Digital Ecosystem: Threat Spectrum

The digital revolution has unleashed and empowered a host of new actors with previously little clout in the realms of national and international security. The added significance and potency of these actors, together with traditional and continuing sources of threat in the form of nation-states and their proxies, makes for a complex ecosystem. Effective countermeasures are complicated by the anonymity that cyberspace affords, otherwise called the attribution problem, and by the pace of cyber activity, which includes the speed and volume of action as well as the rates of change and development of the technologies used.

Who is behind the clickety-clack of the keyboard? It could be a foreign intelligence service seeking to steal secrets related to national or economic security, a criminal organization turning to online theft to make a substantial profit, a terrorist group trying to execute an attack and instill fear in the targeted civilian population, a "hacktivist" committed to a particular cause, or even a bored ankle-biter looking for a challenge.

In terms of state actors, Russia and China currently dominate the espionage business, siphoning out U.S. intellectual property that was the product of heavy U.S. investment in research and development, to such an extent that the U.S. National Counterintelligence Executive has labeled these countries "a national, long-term, strategic threat to the United States of America."[1] Chinese state entities have also

Frank J. Cilluffo directs the George Washington University Homeland Security Policy Institute (HSPI) and co-directs GW's Cyber Center for National & Economic Security (CCNES).
Sharon L. Cardash is Associate Director of HSPI and a founding member of CCNES.

aggressively pursued computer network exploitation to collect intelligence to further China's strategic aspirations.[2] In addition, Iran and North Korea make up for in intent what they presently lack in capability. Any domestic shortfalls in their capacity are further limited by the existence of a thriving market in cyber weapons. Cash plus intent can take a determined and persistent adversary, or one of their proxies, a long way.

ONCE A SOPHISTICATED ATTACKER USES A PARTICULAR ATTACK TOOL OR EXPOSES A PARTICULAR VULNERABILITY, IT IS OUT IN THE WILD FOR OTHERS TO GRAB AND USE, REVERSE ENGINEER, OR EMPLOY TO ADVANTAGE.

Convergence or hybridization of the threat in various ways is also a potential concern. Once a sophisticated attacker uses a particular attack tool or exposes a particular vulnerability, it is out in the wild for others to grab and use, reverse engineer, or employ to advantage. For instance, state actors with specific aims that are quite different from criminal actors' objectives may nevertheless adopt criminal tactics, tools and/or procedures. The good news is that, in terms of cyber-terrorism, we have not yet seen the convergence of the really bad guys with the really good stuff. It would be a mistake though, to allow ourselves to slide into complacency as a result. In this regard, General Keith Alexander, who leads U.S. Cyber Command, warned that al-Qaeda and others who wish to do harm to the United States "could very quickly get to" a state in which they possess "destructive" cyber capability that could be directed against the U.S. [3]

Besides being the newest battle-space, cyberspace also meets, merges with, and intersects the physical battlefield in various ways. In the lead-up period to the NATO intervention in Libya, the Obama Administration reportedly gave thought to using cyber means to disable Libyan radar and other defense mechanisms in order to prepare the battlefield. [4] In the end, a more conventional course was pursued; but the episode serves to illustrate the idea of networked warfare. Networked warfare has already occurred, as shown in the 2008 conflict between Russia and Georgia in which Russia attacked and disrupted Georgia's communications network. As Ambassador David Smith observes, "Russia has integrated cyber operations into its military doctrine, though not fully successful,…Russia's 2008 combined cyber and kinetic attack on Georgia was the first practical test of this doctrine…[and] we must assume that the Russian military has studied the lessons learned…". [5] Consider also Iraq, where insurgents and other extremists used networked technologies to their advantage by sharing lessons learned in real-time, thereby rendering attacks on the U.S. and allied forces more deadly. [6] Likewise, as noted by the U.S.-China Economic and Security Review Commission, "computer network operations have become fundamental to the PLA's strategic campaign goals for seizing information dominance early" in a military conflict. [7]

The Internet also reinforces and exponentially magnifies one of the hallmarks of terrorism, namely, that it is a small numbers business in which the few can cause a degree of harm that is well out of proportion to the size of the attacking group. This was seen in the 9/11 attacks, where 19 hijackers caused almost 3,000 deaths as well as substantial economic damage. The Internet serves as a powerful enabler for U.S. adversaries' activities and aims by being a means of connecting, inspiring, radicalizing, recruiting, training, planning, executing and implementation, as well as fundraising for those who wish to do the U.S. harm. As such, cyberspace amplifies and brings to the fore the voices of the individual and the small group, and ramps up their impact to an extent arguably never before seen or felt. The so-called "lone wolf" who derives only his inspiration from others, perhaps even exclusively through the Internet, represents a particularly vexing challenge for U.S. law enforcement authorities since this type of case offers very few, if any, indicators or tripwires that could facilitate successful prevention efforts.

THE INTERNET ALSO REINFORCES AND EXPONENTIALLY MAGNIFIES ONE OF THE HALLMARKS OF TERRORISM, NAMELY, THAT IT IS A SMALL NUMBERS BUSINESS IN WHICH THE FEW CAN CAUSE A DEGREE OF HARM THAT IS WELL OUT OF PROPORTION TO THE SIZE OF THE ATTACKING GROUP.

Key Policy Questions and Selected Action Principles

Almost two years ago, we wrote the following which, unfortunately, is still a fair evaluation of the state of play in this field:

> *Both offense and defense are complicated in an ecosystem characterized by ambiguity, where basic questions remain unanswered. National and international authorities continue to struggle with definitional issues such as: What constitutes an act of war in cyberspace? Do we need a cyber equivalent of NATO Article V, which enshrines the principle of collective defense? How might cyber deterrence capability be best developed?* [8]

To this list of open questions we would now add several more. Looking over the horizon, what should the United States be prepared for in terms of cyber tools, techniques and weapons? What strategic threat indicators ought to be developed? How should the US best design a tactical and strategic indications and warning (I&W) capability? What should be the constituent principles and redlines for each of U.S. cyber defense and U.S. cyber offense? What are the appropriate roles and responsibilities, and who should be the lead Federal agencies to carry out various components of the mission areas? How might information be shared with the private sector in real time? Should there be a greater role for active defense, meaning the ability to immediately attribute and counter attacks, in order to address future threats in real-time? What should U.S. rules of engagement look like?

Over and above these strategic and doctrinal questions, we would also ask the following: How might the United States synergize military and intelligence community efforts in cyberspace to best shape the ecosystem to advantage? The wars in Iraq and Afghanistan, the U.S. campaign against al Qaeda and its ilk, and other battle-spaces have demonstrated the leverage that may be attained over adversaries when U.S. operations are efficiently networked and our military and intelligence community work to support one another. What are the recent lessons learned from counter-terrorism and counter-insurgency planning and operations that ought to be modified and applied to the cyber domain? What safeguards and limitations should be adopted and respected to prevent improper cross-realm–military to civilian and vice versa–encroachment?

While each of these questions could easily be the sole subject of a journal article or book chapter, here a more limited task is tackled, by offering a select number of action principles that are intended to help guide and inform the elaboration and articulation of cyber policy and doctrine.

Look to past practice and translate it

History often proves a valuable guide and present context is no exception. What has served the United States well in other domains may also be applicable or at least adaptable to cyberspace. One example would be the laws of armed conflict. Though developed in a pre-cyber world, this body of law rightfully remains a touchstone. However, going forward, it may prove constructive to engage in robust—national—discussions as to whether certain aspects might be tailored to the digital age, and how. Past practice is also relevant to combating Internet-facilitated radicalization. Political campaigns have long used the power of negative imagery to undermine the appeal and credibility of opponents, in the eyes of their peers and followers. Taking a similar tack, by exposing the hypocrisy and inconsistencies in the narratives that continue to fuel violent extremism both online and off, is an idea that holds promise yet has not been pursued in a systematic and sustained way. [9]

Think through the current alignment of capabilities and authorities

As things now stand there is, in respect to domestic cyber defense, a gap that exists between the Department of Defense, which has many of the requisite capabilities but lacks some of the authorities, and the Department of Homeland Security, which has many of the authorities but lacks some of the capabilities. How the United States should go about bridging that gap, in ways that preserve both privacy and civil liberties, is a vexing question and one that should be given serious and careful thought. Recalibration may be in order but this outcome is not predetermined. What is certain is that any discussion should proceed deliberately by calling the question and reaching a conclusion that best serves national objectives.

Puzzling through this difficult issue will entail grappling with larger related matters such as the most desirable ratio of defense to offense for U.S. cyber efforts.

CYBERSPACE IS NOT A DOMAIN IN WHICH THE UNITED STATES CAN GO IT ALONE. INTERNATIONAL ALLIANCES ARE AND WILL REMAIN CRUCIAL.

Remember that transnational threats require transnational solutions

Cyberspace is not a domain in which the United States can go it alone. International alliances are and will remain crucial. Current platforms and structures, including the “Five Eyes” intelligence and information sharing partnership comprised of the U.S., the U.K., Australia, Canada and New Zealand, as well as the Council of Europe’s Convention on Cybercrime, may offer a foundation on which to build. Such possibilities should be explored thoughtfully, particularly in today’s financially resource-scarce environment at home and abroad, before turning to create new structures. NATO could prove an important partner in this regard by offering a venue in which threat-related information may be shared, though it may be necessary to first put in place additional mechanisms and safeguards that would enhance not only information-sharing, but also cyber defense efforts more generally, within the context of this particular alliance. NATO’s experience on the cyber front, especially its reaction to the 2007 cyber attacks on Estonia, could form the basis of a multilateral dialogue—and ideally, ultimately, an associated action plan—concerning what might be done differently were the same or similar facts, if not worse, to recur in future. Recall that in 2007, Estonia’s government, banks and other entities were the targets of “large and sustained distributed denial of service attacks (DDoS attacks)…many of which came from Russia.” NATO declined to invoke Article V/collective defense.[10]

Leverage technology but recognize that it will take us only part of the way

Three elements form the crux of the cyber domain: technology, policy, and people. The first two generally receive their due but, too often, the human aspect of the equation is either left out or under appreciated. Consider the field of intelligence, for instance, whose findings help power U.S. cyber defense—and offense—efforts. While sophisticated technologies may yield highly valuable information that furthers our national security, there is still no substitute for a human source (HUMINT). Collecting and exploiting all-source intelligence is therefore the most robust way forward, even in the cyber realm. As things now stand, however, we are not even fully leveraging domestic resources that would require relatively little cultivation: those who work for privately owned and operated critical infrastructure enterprises such as water and electric power, possess critical knowledge and expertise which could and should be invoked for building situational awareness, related to threat and for undergirding response, that is both broad and deep. Yet these human sources of intelligence presently feed into only a fraction of the country’s Fusion Centers, composed of State and local law enforcement and other entities, and designed to gather and analyze threat-related information such as signatures, hostile plans, and techniques to degrade, disrupt or destroy systems, derived from the public and private sectors in order to bolster U.S. prevention and response efforts, including in the cyber domain.[11]

Have a national conversation—which is past due

Democracy and transparency are, or at least should be, mutually reinforcing. The American people are, likewise, a powerful resource. As with any valuable resource, however, it is important to treat it with the respect and care that it deserves. So far, the bulk of discussions regarding cyber policy and strategy have taken place within and across specific niche communities in Government and private industry—especially sectors that constitute critical infrastructure—rather than nationwide and at all levels, despite the far-reaching implications that these policy and strategy decisions hold for the country as a whole. The better course would be to engage in a national conversation that extends beyond these rarified circles, so as to work through and come to terms as a nation with the roles that the government and the private sector should each play in this area, whether our laws need to be updated, and the meaning of national and economic security, privacy and civil liberties, and other long-cherished values and ends in the digital age. Identifying our goals and objectives in this way, and discussing how best to meet and protect them in this manner, is the path most likely to generate and sustain national support for policy and strategy as well as, ultimately, operations. In recent weeks we have seen the beginnings of a countrywide dialogue, with the President's reference to cybersecurity in his February 2013 State of the Union address and the release of an Executive Order—"Improving Critical Infrastructure Cybersecurity"[12]; and following the publication by U.S. security firm Mandiant of a provocative report alleging and detailing state-sponsored Chinese cyber espionage targeting corporations and other entities in the United States and other countries.[13] The conversations sparked by these developments are notable and will, hopefully, raise awareness of these complex issues and challenges as well as serve as a spur to action.

Conclusion

The cyber domain has empowered a range of new actors. Against this background, there is no shortage of forms that conflict could take in the 21st century. Prudence and preparedness dictate that we look over the horizon to identify potential threats and the best ways to defeat them in this new and ever-evolving environment. The challenge is considerable given the speed at which action does—and reaction must—take place in cyberspace.

Further magnifying the complexity inherent in the tasks ahead is the governing principle that, in this context, you are only as strong as your weakest link. An important part of the national conversation should therefore be the idea that security is a responsibility that extends from the public sector into the private sector and beyond to the level of the individual. Indeed the time to act is now, before events may spur a potentially more draconian response later. The proverbial power of one—both to cause harm and to suffer it, the latter with potentially significant and possibly much broader knock-on effects—is not to be underestimated in the cyber context.

Though the scope and nature of the challenge may seem intimidating, recall that we have risen successfully in the past to a similar call; outer space was once as new and daunting a domain as cyberspace. Moving forward, U.S. policy and strategy will undoubtedly be tested, especially in the current climate marked by financial resource constraints. Leadership, determination, and concerted effort, however, could help take the U.S. a long way towards meeting crucial goals.

Notes

[1] Siobhan Gorman. "China Singled out for Cyber spying", *The Wall Street Journal*, citing Robert Bryant, November 4, 2011. http://online.wsj.com/article/SB10001424052970203716204577015540198801540.html#ixzz1ckLNwAJX. See also: "Foreign Spies Stealing U.S. Secrets in Cyberspace" *Report to Congress on Foreign Economic Collection*, 2009-2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[2] *2011 Report to Congress of the U.S.-China Economic and Security Review Commission*. http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf.

[3] Robert Burns. "Cybersecurity chief urges action by Congress," *The Seattle Times*, July 9, 2012. http://seattletimes.nwsource.com/html/politics/2018645510_apuscybersecurity.html?syndication=rss.

[4] Eric Schmitt and Thom Shanker. "U.S. Debated Cyber warfare 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=1&pagewanted=print.

[5] David J. Smith. "How Russia Harnesses Cyberwarfare," *American Foreign Policy Council Defense Dossier*, August 2012. http://www.afpc.org/files/august2012.pdf.

[6] Frank J. Cilluffo and Sharon L. Cardash. "Defining 'War' in the Cyber Era" in *#CyberDoc: No Borders–No Boundaries. National Doctrine for the Cyber Era*, Timothy R. Sample and Michael S. Swetnam (eds), Arlington, VA: Potomac Institute Press, December 2012.

[7] The PLA refers to China's Armed Forces. *2011 Report to Congress*. http://www.uscc.gov/annual_report/2011/annual_report_full_11.pdf.

[8] Sharon L. Cardash and Frank J. Cilluffo. "Managing Complexity in a WikiLeaks World" *HSPI Commentary*, (December 13, 2010). http://www.gwumc.edu/hspi/policy/commentary020_wikileaks.cfm.

[9] Testimony of Frank J. Cilluffo before the Senate Committee on Homeland Security and Governmental Affairs "The Future of Homeland Security: Evolving and Emerging Threats", (July 11, 2012.). http://www.gwumc.edu/hspi/policy/Testimony%20-%20SHSGAC%20Hearing%20-%2011%20July%202012.pdf.

[10] Jason Healey and Leendert van Bochoven. "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council Issue Brief*, (2011). http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf at page 2

[11] Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing, and Keith D. Squires "Counterterrorism Intelligence: Fusion Center Perspectives" *HSPI Counterterrorism Intelligence Survey Research* (CTISR), (June 2012). http://www.gwumc.edu/hspi/policy/HSPI%20Counterterrorism%20Intelligence%20-%20Fusion%20Center%20Perspectives%206-26-12.pdf.

[12] Barack Obama. "Improving Critical Infrastructure Cybersecurity." Executive Order, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (February 12, 2013).

[13] "APT 1: Exposing one of China's Cyber Espionage Units," *Mandiant*, February 19, 2013, http://intelreport.mandiant.com/.