Getting Serious About Cyberwarfare

Frank J. Cilluffo & J. Richard Knop

The future of military conflict will certainly include a cyber component. Computer network operations, including exploits and attacks, will be integrated into military planning, doctrine and operations. Cyber warfare will simultaneously be its own domain and will also impact other domains (land, sea, air, and space)—from intelligence preparation of the battlefield (IPB), to computer network attack (CNA).

Nations that can best marshal and mobilize their cyber power—defined as "the ability to use cyberspace to create advantages and influence events in all other operational environments and across the instruments of power"—and integrate it into strategy and doctrine will ensure significant national security advantage into the future.[1]

The U.S. cybersecurity community is evolving and developing in response to the threat climate that prevails, but remains in a nascent stage of maturity. To date, the cybersecurity community has not reached anything approaching the level of acumen displayed by the U.S. counterterrorism community. Its current state is akin to where our anti-terrorism efforts found themselves shortly after the 9/11 attacks. While our defense and intelligence architectures and capabilities in the cyber field outmatch and outcompete those on the civilian side, the future of U.S. cyberdefense and cyber-response is not assured even in a military context. The threat and the technology that supports it have markedly outpaced U.S. prevention and response efforts as a whole.

Frank J. Cilluffo is an associate vice president at The George Washington University, where he directs the Cyber Center for National & Economic Security. He previously served as a Special Assistant to President George W. Bush for Homeland Security.

J. Richard Knop is the founder and co-manager of FedCap Partners, LLC. He also serves as a member of The George Washington University Board of Trustees, where he oversees the University's Cybersecurity Initiative.

Despite multiple incidents that could have served as galvanizing events to shore up U.S. resolve to formulate and implement the changes that are needed (and not just within Government) we as a country have yet to take the steps needed to enhance our security, readiness and resilience. As General Keith Alexander, Commander of U.S. Cyber Command and director of the National Security Agency, noted recently, "The country is a 'three' on a scale of one to ten when it comes to cyber preparedness."[2]

While bits and bytes are unlikely to replace bullets and bombs, terrorist groups may increase their cyber savvy as time wears on and may affect our threat and vulnerability calculus accordingly.

Threat matrix

The cyber threat is multifaceted. At the time of a breach, just who is behind the clickety-clack of the keyboard is not readily apparent. It could be an ankle-biter, a hacker, hacktivists, criminal or terrorist groups, nation-states or those that they sponsor. The Internet is a medium made for plausible deniability. From a homeland security perspective, however, our principal concerns are by and large foreign states—specifically those that pose an advanced and persistent threat. Russia and China fall in this category although their tactics and techniques may—and likely have been—exploited by others.

The U.S. National Counterintelligence Executive (NCIX) pulls no punches in its assessment: "The nations of China and Russia, through their intelligence services and through their corporations, are attacking our research and development... This is a national, long-term, strategic threat to the United States of America."[3] The Chairman of the Joint Chiefs of Staff likewise expressed concern in testimony to the Senate Armed Services Committee earlier this year: "I believe someone in China is hacking into our systems and stealing technology and intellectual property."[4] He declined to link this activity directly to the People's Liberation Army (PLA). However, Chinese Army officers have publicly expressed significant interest in and support for non-traditional means to yield military advantage.[5]

As a report issued by the U.S.-China Economic and Security Review Commission has outlined, "Computer network operations have become fundamental to the PLA's strategic campaign goals for seizing information dominance early in a military operation."[6] The report also notes that even during peacetime, computer network exploitation has likely become central to PLA and civilian intelligence collection operations to support national military and civilian strategic goals.[7]

As foreign intelligence services engage in cyber espionage against us, they often combine technical and human intelligence in their exploits.[8] These activities permit others to leapfrog many bounds beyond their rightful place in the innovation cycle. As the Office of the NCIX observes in its *2011 Report to Congress*, "Moscow's highly capable intelligence services are using HUMINT [human intelligence], cyber, and other operations to collect economic information and technology to support Russia's economic development and security."[9]

After Russia's war with Georgia in 2008, the military appraised its campaign and made note of its poor performance in the domain of Information Warfare.[10] This led to a call for "Information Troops" within the Russian armed forces; however, no such body has yet to appear. Professor Igor Panarin, of the Ministry of Foreign Affairs' Diplomatic

Academy, notes that "the objective is… certainly, to create centres which would envisage so-called hacker attacks on enemy territory."[11] The present absence of defined "Information Troops" within the armed forces does not preclude a preoccupation with their "lack of capacity to prosecute or defend against CNO within the military" and will continue to incite calls to action.[12]

At worst, such exploits hold the potential to bring the United States and its means of national defense and national security to a halt—thereby undermining the trust and confidence of the American people in their government. This is a dark scenario. Yet one wonders what purpose the mapping of critical U.S. infrastructure (by our adversaries) might serve other than intelligence preparation of the battlefield. In 2009, the *Wall Street Journal* reported that cyberspies from Russia and China had penetrated the U.S. electrical grid, leaving behind software programs. These intruders didn't cause any damage to U.S. infrastructure, but sought to navigate the systems and their controls.[13] Indeed, the line between this type of reconnaissance and an act of aggression is thin, turning only on the matter of intent.

Countries such as Iran and North Korea are not yet on a par with Russia and China insofar as capabilities are concerned; but what Iran and North Korea lack in indigenous capability they make up for in terms of intent. Here motivation supersedes sophistication. From a U.S. perspective, the challenge is asymmetric in character and of course complicated by the nuclear backdrop.

Iran is increasingly investing in bolstering its own cyberwar capabilities. According to press reports, the government there is investing the equivalent of one billion dollars to build out its offense and defense.[14] Iran has organized an "Iranian Cyber Army," and has also employed pro-government hackers who have managed to shut down Twitter, block websites and execute complex cyberattacks within Iran.[15] Also, it is useful to keep in mind that many of the capabilities that Iran does not yet have may be purchased. A veritable arms bazaar of cyber weapons exists, and the bar to entry continues to get lower while the cyber weapons continue to become more user-friendly (i.e., point-and-click).[16] Our adversaries just need the cash and the intent.

> Our cyber-offense and defense both require work. The two go hand-in-hand, with the one bolstering and reinforcing the other. Imbalance between them may give rise to significant potential peril.

Unfortunately there is no lack of evidence of intent. By way of example, U.S. officials are investigating "reports that Iranian and Venezuelan diplomats in Mexico were involved in planned cyberattacks against U.S. targets, including nuclear power plants." Press reports based on a Univision (Spanish TV) documentary that contained "secretly recorded footage of Iranian and Venezuelan diplomats being briefed on the planned attacks and promising to pass information to their governments," allege that "the hackers discussed possible targets, including the FBI, the CIA and the Pentagon, and nuclear facilities, both military and civilian. The hackers said they were seeking passwords to protected systems and sought support and funding from the diplomats."[17]

Iran itself is not a monolith when it comes to its cyber (or terrorist) activities. Indeed, Iran's Islamic Revolutionary Guard Corps (IRGC) operates as a semi-independent entity, and it is unclear just how much they coordinate with Iranian intelligence (the Ministry of Intelligence and Security, or MOIS). This complicates U.S. efforts in terms of both threat assessment and response. Moreover, despite the imposition of sanctions on Iran, it is quite clear that the IRGC is not running out of money; the Corps has a substantial economic enterprise internal and external to Iran including telecommunications.[18] This coupled with the foreign terrorist organizations (FTOs) Iran supports and sponsors, notably Hezbollah, makes Iran a key threat.[19] Note further that Iran's ability to conduct electronic warfare, including the jamming and spoofing of radar and communications systems, has been enhanced by acquisition of advanced jamming equipment. In the event of a conflict in the Persian Gulf, Iran could combine electronic and computer network attack methods to degrade U.S. and allied radar systems, thereby frustrating or at least complicating both offensive and defensive operations.[20]

From the standpoint of defense, the nation would be well served by a cyber-deterrence strategy that is clearly and powerfully articulated. Having singled out certain adversaries in open-source government documents, logic dictates that we should specify (without divulging sensitive or compromising details) the broad outlines of what we are doing about these activities directed against us.

If past is prelude, Iran has leaned on proxies in the past to do its bidding, and this factors into the cyber domain as well. Hezbollah has also entered the fray, establishing the Cyber Hezbollah organization in June 2011. Law enforcement officials note that the organization's goals and objectives include training and mobilizing pro-regime (Government of Iran) activists in cyberspace. In part this involves raising awareness of and schooling others in the tactics of cyberwarfare. Hezbollah is deftly exploiting social media tools such as Facebook to gain intelligence and information. Even worse, each such exploit generates additional opportunities to gather yet more data as new potential targets are identified, and tailored methods and means of approaching them are discovered and developed.[21]

Looking beyond the horizon, the outlook is likewise concerning. While bits and bytes are unlikely to replace bullets and bombs, terrorist groups may increase their cyber savvy as time wears on and may affect our threat and vulnerability calculus accordingly. As Gen. Alexander observed recently, 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 us.[22] Bear in mind that cyberterrorism (and terrorism in general) is a small numbers business. Big numbers are not needed to generate serious consequences. Indeed, nineteen hijackers were able to take nearly three thousand lives and cause substantial economic damage in the 9/11 terrorist attacks.

How prepared are we?

With national and economic security at stake, the imperative of preparedness is clear. Yet we have a way to go on this front before it could be reasonably concluded that the United States is giving enough focus to cyberdefense and cyberresponse in the military realm. (Of course, the cyber threat spectrum impacts more than the defense community alone. The broader public sector, the private sector, the interface and intersections between them, as well as individual citizens, are also at risk. This article, however, relates simply to the military domain.)

Prevention and response requires, among other things, capabilities and capacities that can be executed and implemented in real time against sophisticated and determined adversaries. Underlying those abilities and the exercise of that power, in turn, must be fundamental operating principles carefully derived, defined and debated in the clear light of day, that represent the product of a national conversation on the subject.

Policy and strategy in this area have suffered to date because concepts and categories which constitute the evolution and end-product of our thinking as a nation have lagged behind both technology and practice (particularly that of our adversaries). These various elements may still be brought into better alignment, but doing so will require concerted effort and commitment on the part of our military and civilian leaders. Remember that we have risen in the past to similar challenge successfully, forging strategy and policy in another new domain devoid of borders, namely outer space.

Our cyber-offense and defense both require work. The two go hand-in-hand, with the one bolstering and reinforcing the other. Imbalance between them may give rise to significant potential peril. Fortunately discussions are under way at the Pentagon and elsewhere regarding the rules of engagement that should, do, and will inform and guide U.S. actions in cyberspace. Contingency planning that incorporates attacks on U.S. infrastructure is needed, as is red-teaming and additional threat assessments which should include modalities of attack and potential consequences.

From the standpoint of defense, the nation would be well served by a cyber-deterrence strategy that is clearly and powerfully articulated. Having singled out certain adversaries in open-source government documents, logic dictates that we should specify (without divulging sensitive or compromising details) the broad outlines of what we are doing about these activities directed against us.[23] It may be that the equivalent of an above-ground nuclear test is needed in order to demonstrate U.S. wherewithal to actual and prospective adversaries, who might thereby be dissuaded from a course of action or, alternatively, compelled toward specific steps. What that equivalent test may be is not altogether clear nor is the feasibility or possible consequences of conducting it, but these are the sorts of questions that merit national reflection at this time. Force protection is another, as second-strike capabilities may be needed to ensure it.

Before going on the offensive, prudence dictates that we first inoculate ourselves against the very measures that will be visited upon others. Blowback is always a risk in military engagement and all the more so in the cyber context, where unintended consequences may materialize once a cyber-weapon is released into the wild.

An "active defense" capability, meaning the ability to immediately attribute and counter attacks, is needed to address future threats in real-time. Active defense is a complex undertaking, however, as it requires meeting the adversary closer to its territory, which in turn demands the merger of our foreign intelligence capabilities with U.S. defensive and offensive cyber capabilities (and potentially may require updating relevant authorities). A significant breakthrough in the counterterrorism realm post-9/11 was the synchronization of Title 10 and Title 50 of the United States Code—a development that harmonized military and intelligence functions. Similarly, this synchronization can be leveraged to strengthen our active defenses in the cyber domain. We cannot simply firewall our way out of this problem.

Before going on the offensive, however, prudence dictates that we first inoculate ourselves against the very measures that will be visited upon others. Blowback is always a risk in military engagement and all the more so in the cyber context, where unintended consequences may materialize once a cyber-weapon is released into the wild. Identifying and implementing the necessary precautions should therefore be an integral part of taking the offensive—and indeed a precursor to it.

Readiness is no simple matter in this context, certainly not across the board. Government entities with the greatest capabilities (such as NSA) do not have all the authorities, while departments whose capacities are less fully developed (such as DHS) are endowed with relatively greater authority. The result is a range of knock-on effects including challenges for computer network defense (CND) and computer network exploit and attack (CNE and CNA). Figuring out how best to bridge the gap between authorities and capabilities is a vexing challenge, but one that would serve us well to think through carefully, taking into account all competing equities (security, privacy, civil liberties, etc.).

All-source intelligence that underpins and enables prevention and response is and will continue to be crucial for military and civilian efforts. As much as technology matters in this area, there is simply no substitute for HUMINT. A human source—whether a recruit in place inside a foreign intelligence service, a criminal enterprise, or a terrorist organization—is the most valuable force multiplier, bar none. By helping to create a "rich picture" of the threat, HUMINT keeps our blind spots to a minimum.

Input and insights from the private sector, including the owners and operators of critical infrastructure, are also an important component for building robust (national) situational awareness and a shared knowledge of the battle-space. These owners and operators should be part of our Fusion Centers. Yet this is not the case for more than half of the nation's Centers—despite the fact that a sizable majority of Fusion Centers are (according to survey research conducted recently by The George Washington University's Homeland Security Policy Institute) believed by their membership to have "relatively weak capabilities in regard to the gathering, receiving, and analyzing of cyber threats."[24]

The road ahead

History offers guidance on how to move forward smartly. We must find the cyber equivalents of Billy Mitchell, George Patton, Curtis LeMay and Bill Donovan—leaders who understand both the tactical and strategic uses of new technologies and weapons. Such leadership, together with the elaboration and articulation of doctrine to guide and support the development and use of U.S. cyber capabilities of all kinds, will propel the nation much closer to where it needs to be.

At the end of the day, the ability to reconstitute, recover and get back on our feet is perhaps the best deterrent. The storms that recently battered the National Capital Region, leaving close to a million people without power during a week-long heat wave, are instructive in terms of our shortcomings on resilience. Mother Nature may be a formidable adversary, but just imagine the level of damage and destruction that a determined and creative cyber-enemy could have wrought.

[1] Franklin Kramer, Stuart Starr and Larry Wentz, *Cyberpower and National Security* (Washington, DC: National Defense University, Center for Technology and National Security Policy, 2009).

[2] General Keith Alexander, "Protecting the Homeland from Cyber Attacks," The Aspen Institute, July 26, 2012, http://www.aspeninstitute.org/about/blog/general-keith-alexander-protecting-homeland-cyber-attacks.

[3] As cited in Siobhan Gorman, "China Singled Out for Cyber Spying," *Wall Street Journal*, November 4, 2011, http://online.wsj.com/article/SB10001424052970203716204577015540198801540.html#ixzz1ckLNwAJX.

[4] General Martin Dempsey, testimony before the Senate Committee on Armed Services, February 14, 2012, http://www.armed-services.senate.gov/Transcripts/2012/02%20February/12-02%20-%202-14-12.pdf.

[5] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: China's People's Liberation Army, 1999).

[6] Patton Adams, George Bakos and Bryan Krekel, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, March 3, 2012, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

[7] Ibid.

[8] Frank J. Cilluffo and Sharon L. Cardash, "Commentary: Defense Strategy Avoids Tackling the Most Critical Issues," *Nextgov*, July 28, 2011, http://www.nextgov.com/cybersecurity/2011/07/commentary-defense-cyber-strategy-avoids-tackling-the-most-critical-issues/49494/.

[9] National Counterintelligence Executive of the United States, "Foreign Spies Stealing U.S. Secrets in Cyberspace," *Report to Congress on Foreign Economic Collection, 2009-2011*, 5, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[10] Keir Giles, "Information Troops—A Russian Cyber Command?" Conflict Studies Research Centre, Oxford, UK, 2011.

[11] "Russia is Underestimating Information Resources and Losing Out to the West," *Novyy Region* (via BBC World Monitoring), October 29, 2008.

[12] Ibid.

[13] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html.

[14] Yaakov Katz, "Iran Embarks on $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864.

[15] Tom Gjelten, "Could Iran Wage a Cyberwar on the U.S.?" NPR, April 26, 2012. http://www.npr.org/2012/04/26/151400805/could-iran-wage-a-cyberwar-on-the-u-s

[16] Frank J. Cilluffo, "Preparing for a More Aggressive Iran," *Huffington Post*, July 30, 2012, http://www.huffingtonpost.com/frank-j-cilluffo/preparing-for-a-more-aggr_b_1718725.html.

[17] Shaun Waterman, "U.S. Authorities Probing Alleged Cyberattack Plot by Venezuela, Iran," *Washington Times*, December 13, 2011, http://www.washingtontimes.com/news/2011/dec/13/us-probing-alleged-cyberattack-plot-iran-venezuela/?page=all.

[18] Julian Borger and Robert Tait, "The Financial Power of the Revolutionary Guards," *Guardian* (London), February 15, 2010, http://www.guardian.co.uk/world/2010/feb/15/financial-power-revolutionary-guard.

[19] Frank J. Cilluffo, Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, July 11, 2012, http://www.gwumc.edu/hspi/policy/publicationType_testimonies.cfm.

[20] Michael Puttre, "Iran Bolsters Naval, EW Power," *Journal of Electronic Defense* 25, no. 4, April 2002, 24; Robert Karniol, "Ukraine Sells Kolchuga to Iran," *Jane's Defense Weekly* 43, no. 39, September 27, 2006, 6; Stephen Trimble, "Avtobaza: Iran's Weapon in Alleged RQ-170 Affair?" *The DEW Line*, December 5, 2011, http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html.

[21] Cilluffo, Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs.

[22] Robert Burns, "Cybersecurity Chief Urges Action by Congress," *Seattle Times*, July 9, 2012, http://seattletimes.nwsource.com/html/politics/2018645510_apuscybersecurity.html?syndication=rss.

[23] See Krekel et al., "Occupying the Information High Ground"; Office of the NCIX, *Report to Congress on Foreign Economic Collection*, 2009-2011.

[24] 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.