Warfare in the Cyber Domain

Welton Chang
Sarah Granger

Making sense of cyber warfare requires understanding the cyber domain. The inherent characteristics of the cyber domain make it challenging to determine the implications of cyber warfare on national security policy. Accurately defining the cyber environment is essential. Understanding how the environment functions and behaves as well as understanding the implications of concepts, like convergence (the integration of multiple technologies into a smaller number of platforms and the increasing blending of the virtual and physical worlds), help frame the big picture.

The cyber environment shapes the "warfare" part of cyber warfare. Unfortunately, discussions about cyber warfare have been polarized by commentators, some who believe that a "cyber Pearl Harbor" is inevitable and others who believe just the opposite. Reality lies somewhere in the middle. It is important to remember that warfare is an extension of politics and that this axiom applies in the cyber domain. Operational planning must take into account a spectrum of threats. Understanding the implications of complexity and the intentions of actors in the system will be key to developing effective cyber warfare strategies.

Introducing the cyber domain: complexity and openness

What constitutes the cyber domain?[1] The Internet, of course, but also much more. The cyber domain includes the Internet's organizing architecture, devices connected to the Internet, and wired and wireless networks. Some of these networks are managed by government and private sector entities, some connected to the wider Internet and some that are not. The scale of the Internet makes it difficult to comprehend. This leads to an overreliance on imprecise analogies. While the Internet is technically the first purely human-created domain, its structure can be difficult to conceptualize. Rather than existing within finite borders, it mimics other natural systems such as bacterial colonies and expanding galaxies, where billions of nodes expand in all directions.[2] As a result, the cyber domain, principally networks of networked computers, operating on a ubiquitous data transfer protocol, is both interactively and structurally complex.[3]

Complexity makes the cyber domain difficult to study. Structural complexity results from the exponential growth of computing power and the number of devices connected to the Internet. Interactive complexity derives from human involvement in the system. Exponential technological change has made the environment more complex than ever. The numbers exemplifying this change are astounding: over 2.1 billion people connected via the Internet, 1.8 zettabytes of electronic data created in 2011 and 555 million total websites.

The number of mobile devices connected to the Internet is projected to outnumber the total people on the planet in 2016.[4] Transaction of information between any of these devices is possible, leading to a multitude of interactions and consequences humanity has yet to fully understand.[5]

Security was not a part of the original design of cyberspace. The cyber domain was designed for openness. Standardized protocols for data transmission make up the glue that holds the Internet together and domain name services help to direct data to where it needs to go. A design focused on openness means that security is not inherent in the system and must be grafted on after the fact. There was little concept of mass computer malware when the protocols were developed. Networks and the software built on top of them ride on an inherently open backbone, and as a result, multiple layers of security need to be built in to ensure system and data integrity.[6] Widespread vulnerabilities are akin to deficiencies in the human immune system. The lack of genetic variance amongst human beings means that contagious disease can affect a lot of people. Cyberspace has a similar kind of genetic uniformity: the ubiquity of operating systems like Microsoft Windows running programs like Internet Explorer means that unaddressed vulnerabilities will be widespread.

Describing the cyber domain: convergence, the human element, speed, and asymmetry

Beyond complexity and openness, several important characteristics of the cyber environment shape cyber warfare, including rising levels of convergence, the speed of interactions, the inextricable human element, and the empowerment of the individual within the cyber domain.

Convergence is an oft-written about, sometimes understood, and much maligned concept. Convergence has referred mostly to the seemingly inexorable march of the integration of digital technologies into fewer and fewer delivery platforms. For example, the distinction between email, television, and voice communications has been blurred by the wide-scale adoption of smartphones capable of all three functions operating on Internet protocols. Convergence is also the blending of the virtual and physical worlds. As more systems are connected to the wider Internet for purposes of efficiency and convenience, many physical objects will have a presence in the virtual world. At one extreme, virtual deletion becomes the equivalent of physical destruction. For example, most of the world's finances exists as data only, and fixing data corruption would be reliant on electronic data in the absence of physical records.[7] The merger of the virtual and physical worlds has also extended to humans and technology. Convergence also means that vulnerabilities currently identified in computer programs that control physical entities like industrial control systems (ICS) will grow more widespread.[8] ICS is the umbrella term for a class of electronic systems that control a wide-range of infrastructure such as water, gas, and electric systems. In an inherently open system convergence means more virtual vulnerabilities some analogous to physical ones.

The human element is a fundamental part of the cyber domain that cannot be ignored. Because humans built the cyber architecture, it will be inherently imperfect. In addition, enforcing security measures such as installing anti-virus software, creating hard passwords, and rebuffing social engineering tactics like "phishing" all fall upon the user. And in most cases, the software itself has bugs and holes in it, whether it is running as an operating system or at the application level.

Speed is also an important element of the cyber domain to consider when operating in cyberspace. Action in cyberspace can be faster and lead to further reaching geographic effects than in other domains. However, the operators of computer systems are humans who do not work at light speed. Humans act as functional constraints on the environment to the extent that they are in control of the device and program in operation. While electrons move at light speed, bottlenecks in network architecture and the average processor speed across a data route are also constraints. Finally, while electrons are faster than ground forces, when operations in cyberspace support wider-scale military operations in other domains, the boots constrain the pace of operations. The main effort ultimately dictates the effectiveness of the electrons as well.

The cyber domain is an operating environment in which the effectiveness of the individual is amplified because of automation, the agility of small groups, and the spread of knowledge across geographies. An individual operating anywhere in the world with an Internet connection can commandeer a large and oftentimes unwitting botnet (a group of computers clandestinely and remotely controlled) to conduct denial-of-service attacks. An individual can also create a program that replicates and spreads on its own, through the same vulnerability. Because knowledge transmission is now nearly costless, individuals in loose networks can rapidly learn the most effective attack techniques and exploit previously unknown vulnerabilities. Such loose networks and networks of networks begin to exhibit emergent intelligence, replicating centrally directed action where no such authority exists. This means that individuals such as the group Anonymous, using a botnet, can have the same impact as computer operatives who took down large numbers of public and private Estonian networks in 2007.[9]

Lastly, the asymmetry between the resources, costs, values, stakes, and organization of groups like Anonymous as compared to government organizations such as the United States Cyber Command stems from an environment that is more amenable to virtual insurgency than it is to conventional warfare.[10] Because of the open design of the cyber domain, defense is inherently more costly and time consuming than offense. Also, expensive and highly technical cyber weapons developed by governments can be easily and inexpensively repurposed by others in the cyber domain. Asymmetry in the cyber domain generally favors smaller and more agile actors. These actors often don't have a permanent physical address and can mask their virtual ones. This is a key point that large bureaucracies must embrace in order to develop effective mitigation strategies.

Cyber Clausewitz

The primacy of politics in the execution of any kind of war means that war is ultimately a contest of political will. When strategies are properly developed, political objectives will be the ultimate goal of cyber warfare. Some commentaries on cyber warfare focus on the unique features of the cyber domain, while ignoring the idea that war is an extension of politics. In the arguments about whether or not a "cyber Pearl Harbor" is inevitable, commentators rarely consider the idea that such an extreme action would be undertaken for political purposes.[11] Similarly, when cyber terrorism is discussed, a "cyber 9/11" is described as either impossible or inevitable.[12]

A "cyber Pearl Harbor" is unlikely to occur unless the benefits of taking such an action clearly outweigh the costs for a state. For example, integration of state economies raises the costs of unilateral action. Some seem to think that the plural of cyber attacks is cyber warfare, but we shouldn't forget that warfare requires a political objective. Even terrorist acts are designed to achieve some kind of political or religious objective, whether it be demoralizing a populace or forcing a government to negotiate, not merely destruction for destruction's sake. Understanding the intentions of adversaries is paramount and so is recognizing the extent to which an adversary might be dependent on other actors in the system. In the hyper-integrated world in which we live, not taking into account dependence leads to missing a key factor in the likelihood or unlikelihood of the outbreak of war. Lastly, cyber warfare need not occur at the extreme parts of the capability spectrum. Focusing the discussion on extreme scenarios only serves to polarize arguments and obfuscate real dangers that exist.

The current state of play

Have we seen cyber warfare already?[13] Purported Russian actions during the 2007 conflict with Estonia are the earliest and most oft-cited example. Some experts believe the employment of cyber tactics during the 2007 Estonia dispute was more akin to cyber conflict, not rising to the threshold of war.[14] However, states and populations were not as dependent on the cyber domain in 2007 as they are now. Cloud computing was just getting its start and dependence on the Internet for commerce and banking was vastly different.

The inherent vulnerabilities in the cyber domain, coupled with the development of capabilities by various actors (some with malign intentions) means that cyber warfare is a very real possibility in the future. Any national cyber strategy that seeks to deal with the cyber environment must take into account the risks involved if vulnerabilities go unaddressed. Based on our level of dependence on the cyber domain for both national security capabilities and the functioning of daily life, the risks are great.[15]

But what is the current level of threat? This is difficult to define for several reasons, although we can say for certain that over the past two years,

attacks on major networks and systems have been steadily increasing, in both public and private sector situations.[16] Exact statistics with regards to attacks are difficult to collect and analyze, and a focus on attack statistics glosses over the more insidious threat of undetected attacks and unexploited software and hardware vulnerabilities.[17] Different organizations and sectors may harbor parochial interests with regards to inflating or diminishing the threat picture.[18] Whether those interests are bureaucratic or profit-driven, threat analyses must be aggregated and distilled to get a more holistic and unbiased understanding of the current state of play. It is also possible that large-scale attacks may look vastly different from what has been experienced previously.[19]

When it comes to cyber warfare a spectrum of threats and tactics exist, from denial of service and disruption to the destruction of physical hardware connected via industrial control systems. This spectrum of threats touches all of the other domains of warfare—ground, sea, air, and space.[20] The economic dimension is tremendous as well - General Keith Alexander, head of both U.S. Cyber Command and the U.S. National Security Agency, said existing cyber threat and cyber attacks constitute the "greatest transfer of wealth in the history".[21] For a U.S. defense establishment that is so dependent on an overwhelming economic and material advantage, this amounts to a virtual "death by a thousand cuts".[22]

A reasonable conclusion is that we could suffer from a wide range of possible attacks, especially in a real world conflict that occurs across domains.[23] Cyberterrorism may also become more likely as knowledge about industrial control systems spreads while vulnerabilities go unaddressed. Lastly, while there has been some movement towards precision cyber attacks, complex computer programs operating as designed could unintentionally result in catastrophic consequences in the absence of human interaction.[24]

In conclusion: educating, training and coordinating

If our cyber vulnerabilities are allowed to go unaddressed, we are leaving the virtual drawbridge down.[25] Our job now is to improve information exchange, intelligence efforts, and security coordination mechanisms so that we can prevent, adapt and react should the time come that critical infrastructure or other key networks are compromised. We must act now because critical infrastructure powers our economy and our national security apparatus.

Moving forward, continuing to educate all military and civilian stakeholders is of paramount concern, in addition to securing the networks and nodes themselves. One looming problem is that the number of Americans being trained, educated and developed within the US (including college students majoring in computer science and related fields) is not scaling appropriately to match the increased threat. It is also critical to educate average citizens about enhancing the security of their own computers and networks. A hybridized approach to cyber threat management, incident

response, and pre-planned defensive measures must be adopted in order to develop a more resilient defensive architecture.[26]

In the near future, we will see more intelligence-gathering software in our networks, we will experience more widespread attacks of various kinds, and we should expect to encounter unintended consequences and as of yet unseen disruptions. While in most cases the nature of future attacks may be unpredictable, history may be a reliable guide for others. What we do know is adversaries of various sorts - individuals, rogue groups and sophisticated organizations - already dwell in networks and can penetrate them at will in many cases.

We have been lucky to a certain extent. On some occasions, attacks on critical infrastructure and other important systems have been thwarted and that information shared with the public.[27] These episodes dispel the myth that there is no motive for attackers to go after such systems. Resilience models prove effective in planning for recovery and response, particularly due to the asymmetric nature of the domain and the likelihood of multi-pronged and/or multi-phased attack patterns. Successful education in this area should include resilience training, hands-on scenario response, as well as technical and social engineering. The development of rapidly deployable training modules may be extremely helpful. In many cases, the process of obtaining permission to provide training and education programs can be a hurdle in its own right, preventing personnel at all levels from obtaining much needed skills that can be helpful in identifying and combating cyber attacks.

In the end, complexity and the inherent properties of the cyber environment shouldn't stop us from strategizing and planning.[28] While the vastness of the cyber domain currently overwhelms our stove-piped government infrastructure, our collective understanding improves each year although the threat continues to grow. But by building in resilience to the system and distributing defensive responsibility to all end-users, conducting warfare in the cyber domain will become more costly and less effective for the attacker. Cyber warfare may not have occurred yet, but it is certainly a future threat that must be taken seriously by governments, private companies, and individuals. The threat is only trending higher, and by taking action now to increase security, we decrease the risk of being caught off guard.

Notes

1. Joint Publication 1-02 defines cyberspace as "a global domain within the information environment consisting of the independent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." United States Department of Defense, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, (Washington D.C.: November 8, 2010), pp. 79-80; accessed at: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>.

2. Forthcoming: Sarah Granger, Lorelei Kelly, "Cybersecurity and Modern Grand Strategy", Institute for the Study of Diplomacy, Georgetown University School of Foreign Service, 2012; p. 1.

3. See: United States Army Training and Doctrine Command, "TRADOC Pamphlet 525-5-500: Commander's Appreciation and Campaign Design", January 28, 2008, pp. 5-7; accessed at: <http://www.tradoc.army.mil/tpubs/pams/p525-5-500.pdf>.
4. See: Pingdom, "Internet in 2011 in numbers", Royal Pingdom, January 17, 2012; accessed at: <http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/>. Jon Brodkin, "Mobile internet devices will outnumber humans this year, Cisco predicts", Ars Techica, February 14, 2012; accessed at: <http://arstechnica.com/business/2012/02/mobile-internet-devices-will-outnumber-humans-this-year-cisco-predicts/>; IDC, "The 2011 Digital Universe Study: Extracting Value From Chaos", June 2011; accessed at: <http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm>.
5. A study by MITRE's JASON on cyber security states, "There are no intrinsic "laws of nature" for cyber-security as there are, for example, in physics, chemistry or biology. Cyber-security is essentially an
applied science that is informed by the mathematical constructs of computer science such as theory of automata, complexity, and mathematical logic." JASON, "Science of Cyber Security", MITRE Corporation, November 2010, p. 4; accessed at: <http://www.fas.org/irp/agency/dod/jason/cyber.pdf>.
6. See: Paul A. Strassaman, "The Internet's Vulnerabilities Are Built Into Its Infrastructure", AFCEA, Signal Online, November 2009; <http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2109&zoneid=3>
7. For an example of the dangers of convergence see: Robert O'Harrow Jr., "Tridium's Niagara Framework: Marvel of Connectivity Illustrates New Cyber Risks," *Washington Post*, July 11, 2012, accessed at: <http://www.washingtonpost.com/investigations/tridiums-niagara-framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html>
8. See: Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems", National Institute of Standards and Technology", NIST Special Publication 800-82, p. 2-1; accessed at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800.82.pdf>. Supervisory Control and Data Acquisition Systems (SCADA) are a class of industrial control systems. Programs like SCADAscan detect SCADA networks connected to the Internet. See also: Bill Brenner, "#BSidesSF: Why SCADA security is such an uphill struggle", CSO Online, February 27, 2012; accessed at: <http://blogs.csoonline.com/critical-infrastructure/2044/bsidessf-why-scada-security-such-uphill-struggle>
9. Russian or pro-Russian hackers are suspected to have perpetrated the denial of service attacks against Estonian government and private sector sites during a conflict over the relocation of a war memorial. See: William C. Ashmore, "Impact of Alleged Russian Cyber Attacks", US Army School of Advanced Military Studies, May 2009, pp. 5-8; accessed at: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA504991>.
10. For a discussion on asymmetry and cyber warfare see: Michael Breen, Joshua A. Geltzer, "Asymmetric Strategies as Strategies of the Strong", *Parameters*, Spring 2011, pp. 48-49; accessed at: <http://www.carlisle.army.mil/usawc/parameters/Articles/2011spring/Breen-Geltzer.pdf>. See also: Quinn Norton, "How Anonymous Picks Targets, Launches Attacks, and Takes Down Powerful Organizations", *Wired*, July 3, 2012, accessed at: <http://www.wired.com/threatlevel/2012/07/ff_anonymous/all/>.
11. A "cyber Pearl Harbor" in our estimation would be a massive, intentional, unexpected debilitating attack on U.S. critical infrastructure and defense capabilities. See: Jake Tapper, "Leon Panetta: A Crippling Cyber Attack Would Be An Act of War", ABC News, May 27 2012; accessed at: <http://abcnews.go.com/blogs/politics/2012/05/leon-panetta-a-crippling-cyber-attack-would-be-act-of-war/>.
12. Sunlen Miller, "Despite Threat of 'Cyber 9/11', Lawmakers Punt Cyber Security Bill", ABC News, August 2, 2012; accessed at: <http://abcnews.go.com/blogs/politics/2012/08/despite-threat-of-cyber-911-lawmakers-punt-cyber-security-bill>

13. This is a debate that has occurred numerous times over the past ten years. See: Intelligence Squared, "The Cyber War Threat Has Been Greatly Exaggerated", June 8, 2010; accessed at: <http://intelligencesquaredus.org/debates/past-debates/item/576-the-cyber-war-threat-has-been-grossly-exaggerated>. See also: David Betz, "'Cyberwar' is not coming", *Infinity Journal*, Volume 1 Issue 3,
14. Vice Admiral (ret.) Michael McConnell, "Cyber-Power and Cyber-Security", Aspen Security Forum, July 1, 2012; accessed at: <http://www.aspenideas.org/session/cyber-power-and-cyber-security>. Thomas Rid argues the threshold that cyber war must meet is that it must be "potentially violent, it has to be purposeful, and it has to be political." Those who argue that cyber war has not occurred believe that the lack of violence and physical destruction make cyber action not on the order of cyber warfare. Thomas Rid, "Think Again: Cyberwar", *Foreign Policy*, March/April 2012, accessed at: <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full>.
15. A critical area where both civilians and military depend on that is increasingly connected to cyberspace is the power generation sector. See: Reuters, "Senators to hear pitch for tougher cyber security", March 12, 2012, accessed at: <http://www.reuters.com/article/2012/03/07/us-usa-cybersecurity-congress-idUSTRE82621W20120307>.
16. David Sanger, Eric Schmitt, "Rise is Seen in Cyber Attacks Targeting U.S. Infrastructure", *The New York Times*, July 26, 2012, accessed at: <http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html>. See also: James A. Lewis, "Significant Cyber Events", Center for Strategic and International Studies, last updated May 2012; accessed at: <http://csis.org/publication/cyber-events-2006>.
17. Previously unknown but existing vulnerabilities include both hardwired hardware vulnerabilities and software vulnerabilities called "zero-day" exploits. The difficulty in attributing the attack (knowing who did it) is also a key concern in the cyber domain. See also: Sergei Skorobogatov, Christopher Woods, "In the blink of an eye: There goes your AES key", May 28, 2012, accessed at: <http://eprint.iacr.org/2012/296.pdf>.
18. For a discussion of this subject see: accessed at: Peter Maass, Megha Rajagopolan, "Does Cybercrime Really Cost $1 Trillion?", Propublica, August 1, 2012; <http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion>.
19. Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, accessed at: <http://www.potomacinstitute.org/index.php?option=com_content&view=article&id=77:-conflict-in-the-21st-century-the-rise-of-hybrid-wars&catid=40:books&Itemid=62>.
20. Danny Steed, "Cyber Power and Strategy: So What?", *Infinity Journal,* Vol. 1 Issue 2, accessed at: <http://www.infinityjournal.com/article/11/Cyber_Power_and_Strategy__So_What?>.
21. Michael Riley and Dune Lawrence, "Hackers Linked to China's Army Seen from E.U. to D.C.", Bloomberg, July 26, 2012; accessed at: <http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html>.
22. Cheryl Pellerin, "Cyber Operations Give Leaders New Options, Official Says", *American Forces Press Service*, April 12, 2012; accessed at: <http://www.defense.gov/news/newsarticle.aspx?id=67918>. Both James Lewis of CSIS and Richard Clarke have used this analogy as well.

23. For a discussion of the so-called cyber arms race see: Michael Riley, Ashlee Vance, Cyber Weapons: The New Arms Race, *Bloomberg Businessweek*, July 20, 2011, accessed at: <http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p1>
24. For example, see the impact of high-speed automated trading on Wall Street. Nathaniel Popper, "Knight Capital Says Trading Glitch Cost it $440 Million," *The New York Times*, August

2, 2012, accessed at: <http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/>.
25. Stewart Baker, Natalia Filipiak, Katrina Timlin, "In the dark: Crucial industries confront cyberattacks", McAfee, Center for Strategic and International Studies, 2011; accessed at: <http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf>.
26. American strategist T. X. Hammes stated that to deal with "super empowered small groups" requires an "all of society response" and that such a model is present in "the defense of the internet". See: Jim Zirin, "Will the war in the 21st Century be fought in cyber space?", Digital Age, November 25, 2007, 20:26-20:28; accessed at: <http://www.youtube.com/watch?v=j1_QG0NIwdE>. Charles Billo, Welton Chang, Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States, Institute for Security Technology Studies, (Hanover, NH: Dartmouth College, December 2004), p. 133; accessed at: <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>.
27. Mark Clayton, "Report: Cyberattacks on critical US targets surge," *Christian Science Monitor*, June 29, 2012, accessed at: <http://www.csmonitor.com/USA/2012/0629/Report-Cyberattacks-on-critical-US-targets-surge>. Operation Night Dragon was a publicized group of attacks against energy companies. Operation Shady Rat reportedly targeted 70 government, private sector, and non-profit victims in 40 countries. See: Dmitri Alperovitch, "Revealed: Operation Shady RAT", McAfee, version 1.1, 2012, accessed at: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf> and McAfee, "Global Energy Cyberattacks: Night Dragon", February 10, 2011, accessed at: <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.
28. Michael J, Gallagher, Joshua A. Geltzer, and Sebastian L.V. Gorka, "The Complexity Trap", *Parameters*, Spring 2012, accessed at: <http://www.carlisle.army.mil/usawc/Parameters/Articles/2012spring/Gallagher_Geltzer_Gorka.pdf>. See also: Forthcoming: Sarah Granger, Lorelei Kelly, "Cybersecurity and Modern Grand Strategy", Institute for the Study of Diplomacy, Georgetown University School of Foreign Service, 2012.

Contributors

Mr. Welton Chang is a Defense Department analyst. He was the senior civilian advisor to Iraq's National Intelligence Cell in 2011. From 2005-2012, Welton served as an active and reserve Army officer during which he deployed to Iraq and South Korea. Welton graduated cum laude from Dartmouth College in 2005 with departmental high honors. While at Dartmouth, Welton worked at the Institute for Security Technology Studies where he co-authored and published a widely-cited monograph on cyber warfare. He is currently an MA candidate in Georgetown University's Security Studies Program. He is also a Truman National Security Fellow.

Ms. Sarah Granger is the founder of the Center for Technology, Media & Society (CFTMS). She is currently a Fellow at the Truman National Security Project, co-chairing their cybersecurity group. She began her career working in cybersecurity for the Lawrence Livermore National Laboratory, followed by work as a network security consultant for several years before founding CFTMS. Sarah was a contributing author of Ethical Hacking, and she has edited books on mobile security, cryptography and biometrics. She has also written for Spectrum, Security Focus, and Forbes Russia. Follow her on Twitter @sarahgranger.

The views expressed in the article are those of the authors and do not reflect the official policy or position of the Defense Intelligence Agency, the Department of Defense, or any U.S. Government agency.