The Cyber Domain

Dr. Glenn Alexander Crowther

ABSTRACT

Both the Department of Defense (DoD) and the North Atlantic Treaty Organization (NATO) have declared that cyber is a "domain", co-equal with air, land, and sea. DoD also recognizes space as a domain. Merriam-Webster defines a domain as a sphere of knowledge, influence, or activity.[1] Although DoD does not define "domain", it does define cyberspace as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] No one has yet proposed what the cyber domain is, where militaries should be operating in cyberspace, and what missions' militaries should be doing in cyberspace. This article identifies what DoD says their missions are in cyberspace and discusses what areas are appropriate for military operations in cyberspace. Additionally, it argues that militaries must be very careful about what missions they accept in cyberspace, and must circumscribe their forays into cyberspace lest they are overwhelmed by the sheer scope of the domain.

CIRCUMSCRIBING THE MILITARY CYBER DOMAIN

The military must limit its activities within cyberspace. Just as modern megacities could absorb entire armies, the Internet would swallow the entire cyber capability of not only the DoD but also the capabilities of partners and Allies. It is therefore important to choose how to circumscribe military cyber activities within cyberspace. This is not meant to limit where military cyber units may operate, but rather to limit what functions military cyber resources participate in, thereby preserving cyber capabilities for mission requirements rather than frittering cyber capabilities pursuing wills-o'-the-wisp through cyberspace.

Dr. Glenn Alexander Crowther is the Senior Research Fellow for NATO/Europe and Cyber Policy in the Institute for National Strategic Studies (INSS) at NDU. His work at the strategic level includes tours at the Army Staff, the Joint Staff J5, and as a Research Professor at Strategic Studies Institute. He was personally selected to be a Counterterrorism Advisor for the US Ambassador to Iraq, a Political Advisor for the MNC-I Commander, and a Special Assistant for the SACEUR. He has published in a variety of formats and locations, has experience teaching at the graduate level and has extensive experience as a public speaker in a wide variety of locations. Alex has a BA in International Relations from Tufts, an MS in International Relations from Troy University, and a Ph.D. in International Development from Tulane. He was also an International Security Studies Fellow at the Fletcher School of Law & Diplomacy.

In the United States, 90% of cyber activity is in private hands.[3] In Europe, the statistics are similar.[4] Thus, the military should not be operating within 90% of the Internet unless it pertains to one of the mission sets that this article identifies as appropriate for military participation. When pursuing these mission sets, the military can go where they need to in cyberspace, however, they should avoid entering into most private and commercial cyber interactions, not only for the sake of privacy and limitations on the use of military instruments (such as *posse comitatus,* the 1877 U.S. law that proscribes military activities inside U.S. territory) but also to retain freedom of maneuver. As an example, military cyber operators should not be concerned with PayPal interactions with Amazon, unless the person initiating the payments is involved in something that would make them the target of intelligence operations.

DoD has three primary cyber missions: Defend DoD networks, systems, and information; Defend the US homeland and US national interests against cyberattacks of significant consequence; and Provide cyber support to military operational and contingency plans.[5] In order to perform those missions, reports estimate that DoD has a "cyber workforce of more than 160,000 military and civilian personnel": 3777 for defensive operations, 145,457 for operation and maintenance and 13,910 working on information assurance. Another 6200 in the Cyber Mission Force adds up to 169,344 cyber operators.[6] Although this sounds like a great many resources for the Department to wield in cyberspace, this number represents a requirement for the military to accept a circumscribed mission set because of finite resources. Although eventually everyone in DoD will eventually be involved in cyber-enabled operations, they will not be performing defensive and offensive cyber operations. This points to the need to be parsimonious in the allocation of cyber resources.

Just like the U.S. Army could be absorbed by future megacities like Lagos, Nigeria [7], the vast and growing expanse of the Internet would swallow the DoD cyber workforce, whether it be 170,000 or 1.7 million workers. There is pressure on DoD to participate in cyber operations outside of their three stated mission sets. If national security policy makers insist that DoD should expand their cyber mission set, and should DoD accept the new, expanded missions, then DOD would court disaster.

U.S. joint doctrine recognizes the nine principles of war: objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, and simplicity. [8] Not circumscribing military missions in cyberspace violates at least three principles: mass, economy of force, and simplicity.

An expanded mission set might include helping to protect Internet users in the US. In 2016, there were 287 million Internet users in the US. [9] If there are 170,000 cyber warriors helping to protect US persons using the Internet would mean one DoD cybernaut is helping almost 1700 internet users. If this example is too extreme, some people believe that DoD assets could help businesses. As large businesses typically have some cybersecurity, small businesses would need the most help. As there were 28.8 million small businesses in the United States in 2016 [10], there would be one cyberwarrior helping 170 small businesses. These two examples should suffice to prove that DoD does not possess the resources to help the private sector.

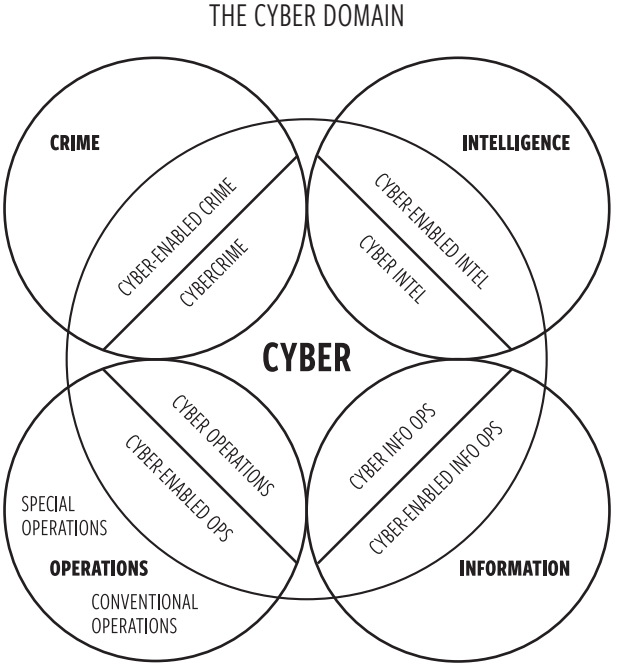

Figure 1. The Military Cyber Domain

Where Should the Military Operate in Cyberspace?

If the military should not be supporting the private sector, what should they be doing in cyberspace? There are four sets of cyberspace activities that pertain to the military: intelligence, information, crime and military operations.[11] Militaries participate in intelligence operations, conduct information operations, conduct and support conventional and special operations, and respond to a limited subset of crime. Together these four areas make up the military cyber domain.

Although the military has equities in all of these areas, the only area that the military predominates in is the military operations portion. There are, however, intelligence, information and criminal activities that involve the military. Figure 1 illustrates the Military Cyber Domain. In any of these four fields, there is a spectrum of activity, from the conventional activity to cyber-enabled activity to cyber activity in that field to purely cyber operations. The remainder of this paper examines each of the four areas that are appropriate for military operations.

Cyber Operations

In the center are pure cyber operations that the Department would be doing anyway: Information and Communications Technology (ICT), Network Operations, and Defensive Cyber Operations (DCO). This is the manifestation of the first DoD cyber mission: to defend DoD networks, systems, and information.

The first mission set under "cyber operations" is ICT.

> ICT refers to all the technology used to handle telecommunications, broadcast media, intelligent building management systems, audiovisual processing and transmission systems, and network-based control and monitoring functions. Although ICT is often considered an extended synonym for information technology (IT), its scope is broader. ICT has more recently been used to describe the convergence of several technologies and the use of common transmission lines carrying very diverse data and communication types and formats.[12]

Information and Communications Technology, therefore, provides the backbone of all military activities. Can anyone imagine running a modern military without telecommunications and diverse data and communications types? This includes all of the communications devices including computers and telephones. The DoD Chief Information Officer (CIO) is the Principal Staff Assistant and senior advisor to the Secretary of Defense for information technology (including national security systems and defense business systems), information resources management and efficiencies. As such, the CIO is responsible for ICT in the Department, and is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; cybersecurity; positioning, navigation, and timing (PNT) policy; and the DoD information enterprise that supports DoD command and control (C2).[13]

Network operations is the next mission set under "cyber operations." The Defense Information Systems Agency (DISA) is overall responsible and provides, operates, and assures command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of military operations.[14] The global DoD network is called the Department of Defense Information Network (DODIN). DISA operates DODIN while each of the services has their own portion of DODIN such as the U.S. Army Network Enterprise Technology Command (NETCOM) and the Air Force Information Network (AFIN). DISA also provides direct telecommunications and IT support to the president, vice president, their staff, and the U.S. Secret Service through the White House Communications Agency.[15]

Defensive Cyber Operations is the last mission under "cyber operations." According to the DOD Joint Publication 3–12 (R), Cyberspace Operations, "DCO are Cyberspace Operations (CO) intended to defend DOD or other friendly cyberspace ... (and) are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[16]

These three cyber operations areas underlie all military functions. Although it is possible to perform other military functions (such as fires) without ICT, network operations, and DCO, it has become more and more difficult to do so. The facts that the U.S. Naval Academy have had to add a class to teach Midshipmen to navigate with sextants[17] and the U.S. Army Infantry School has realized the importance of teaching their Infantry Officers to use a map and compass[18] illustrates how rare it is for operations to do without these three cyber functions.

The Military and Cyber Intelligence

Militaries have participated in intelligence operations as long as there have been organized forces. Sun Tzu wrote about the use of intelligence by the military.[19] The modern manifestation of US national intelligence demonstrates this strongly as the US Intelligence Community admits that no less than eight of their 17 members belong to DoD.[20] Therefore, it makes sense that the military should be operating in cyberspace as part of their intelligence mission.

Normal intelligence operations would be the traditional approach to intelligence before the advent of cyberspace: stealing secrets, developing sources, etc. As modern societies become more informationized, fewer intelligence operations will occur without technology. Infiltrating terrorist cells and other traditional methods of gathering the data that eventually becomes intelligence will continue to be important in areas that are not integrated into the global information system, such as remoter areas in the Middle East, Central Asia, and Africa. Traditional spycraft will also be required to infiltrate organizations that specifically adopt approaches to minimize or avoid vulnerability to advanced intelligence-gathering techniques (such as signals intelligence), such as al-Qaeda and Daesh.

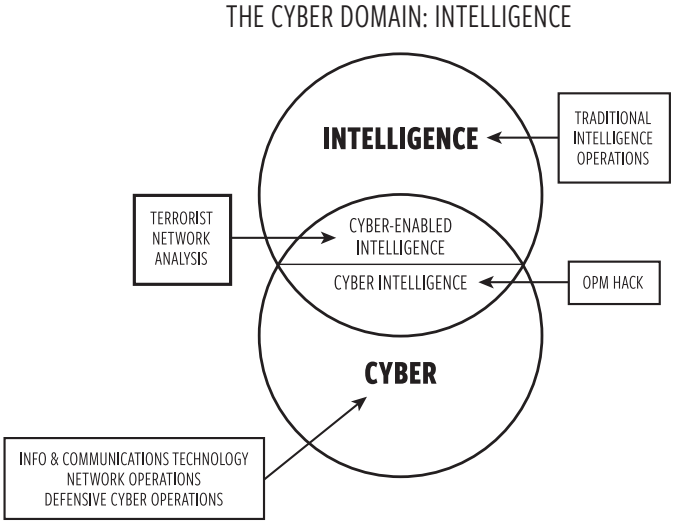

Figure 2. Relationship between Cyber and Intelligence

Cyber-enabled intelligence operations would use cyber capabilities in support of intelligence operations. One example would be terrorist network analysis using data that had been gathered by traditional intelligence means such as human intelligence. More and more of these intelligence operations are becoming cyber-enabled intelligence. In the long run, almost all traditional intelligence operations will be cyber-enabled intelligence operations as collection and analysis methods are significantly improved through the use of nanotechnology and artificial intelligence.

Cyber intelligence operations would be where the intelligence operation occurs entirely in cyberspace. Examples include the 2012 operation by Chinese hackers that penetrated Indian Navy computers and compromised sensitive information [21] or the 2015 hack on the US Office of Personnel Management, where the personnel records for at least 22.1 million people were "affected by cyber intrusions that U.S. officials have privately said were traced to the Chinese government". [22] As more and more records are maintained electronically, more intelligence operations will be executed entirely within cyberspace. Although pure cyber intelligence operations will increase in number, there will always be a need for traditional intelligence operations until human beings are no longer involved.

The Military and Cyber Crime

At first blush, it makes no sense at all that a military would be involved in any crime protection, much less cybercrime. In the United States, the Department of Justice has the lead for cybercrimes while the Department of Homeland Security has responsibility for cybercrimes under their jurisdiction. [23] However, the ubiquity of cybercrime and the specific targeting of defense-related industrial and personnel information requires that militaries at least pay attention to cybercrime.

The Defense Cyber Crime Center (DC3) serves as the operational focal point for the Defense Industrial Base (DIB) Cybersecurity Program. They provide digital forensics and multimedia (D/MM) lab services, cyber technical training, technical solutions development, and cyber analytics for the following DoD mission areas: cyber security (CS) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT).[24] DC3 also leads efforts to deal with any cybercrime that involves DoD personnel.

Their involvement in the DIB is particularly important as the US depends on technological advantages on the battlefield, while adversaries seek to steal the technology and sell it, use it themselves, or figure out how to mitigate effects on the battlefield. An excellent example of that is the theft of C-17 plans, where hackers stole 630,000 files from Boeing's system, totaling some 65 gigabytes of data, and volumes of data on the Lockheed Martin F-35 and F-22.[25] The DIB Cybersecurity (CS) Program DoD is designed to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified networks or information systems. It is a public-private cybersecurity partnership designed to improve DIB network defenses, reduce damage to critical programs, and increase DoD and DIB cyber situational awareness. Under the DIB CS Program, DoD and DIB participants share unclassified and classified cyber threat information.[26]

Conventional criminal operations would be an old-school crime, such as entering a bank with a pistol and a bag to steal money. As long as there is cash and people are vulnerable to crimes such as kidnapping, these crimes will continue. Cyber-enabled criminal operations fuse technology and crime. One example is ATM-skimming, where criminals use hidden electronics to steal the personal information stored on your card and record your PIN number. They then later access your account.[27] Keylogging is a similar cyber-enabled crime, where hackers gather account information via the technique of recording keystrokes and then later using the information to log into other people's accounts. Pure cybercrime would be a criminal operation that occurs wholly in cyberspace, such as the use of the SWIFT system to steal $81 million from the Bank of Bangladesh.[28]

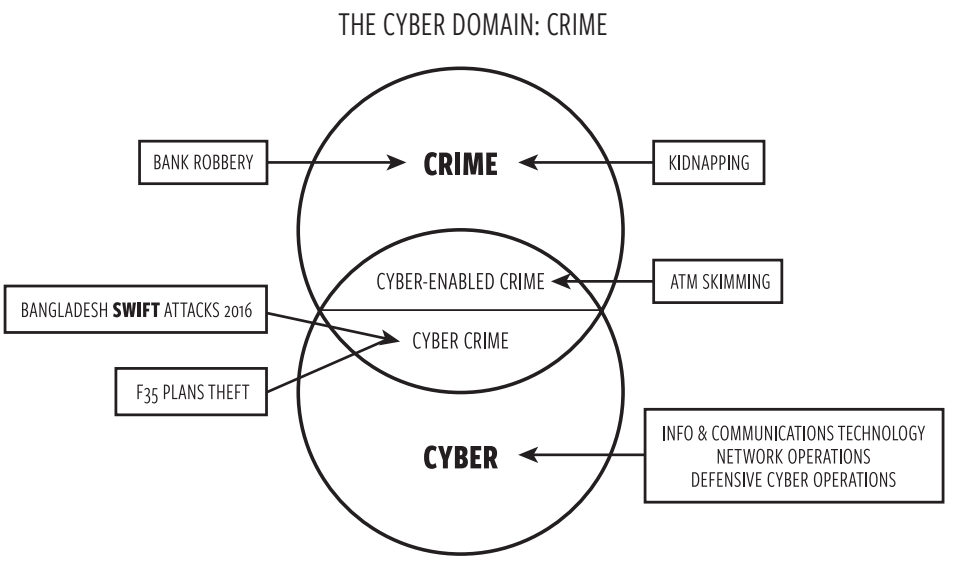

Figure 3. Relationship between Cyber and Crime

One major gain for the United States and global allies and partners is the codification of cybercrime as the equivalent of non-cyber or traditional crime. Robbing a bank at gunpoint is now recognized to be the same as using cyber means to steal money from a bank. Russia and China had previously felt that cyberspace was like the Wild West, where the law did not prevail.[29] During the 2015 meetings of the UN Group of Government Experts, China and Russia both joined the rest of the participants in agreeing that international law does run writ in cyberspace. That means that both intelligence and crime in cyberspace are covered by extant law that deals with the two subjects. The U.S. Congress has an ongoing effort to update laws within Title 50 (War and National Defense) and Title 18 (Crimes and Criminal Procedure) of the United States Code to ensure that cybercrimes are captured in U.S. law.[30]

The Military and Information Operations

Militaries have been using operations in the information environment to shape cognition for the entire history of warfare. Sun Tzu refers to all warfare being based on deception, a form of information operations. Information operations[31] featured strongly during the Cold War and have returned to importance as a global China and a resurgent Russia conceptualize the informationization of modern societies.[32] Russia has returned to the aggressive use of Active Measures or Political Warfare against NATO Allies and partners, in particular, their neighbors over who the Government of Russia seeks to reestablish hegemony.[33] China has developed the concept of the "Three Warfares" which includes lawfare, media warfare, and propaganda warfare.[34] All three have strong connections to the use of information.

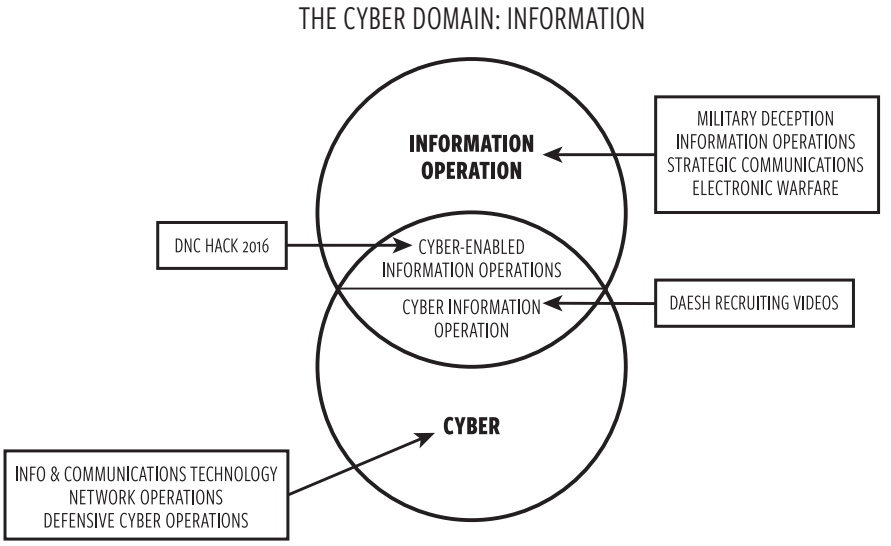

Figure 4. Relationship between Cyber and Information

In addition to the Three Warfares, China has made advances in conceptualizing "strategic information war". This concept "refers to the use of information and information technology in the political, economic, (science & technology), diplomatic, cultural, and military arenas to secure information advantage. In this broad sense, information war spans military and civilian spheres, peacetime and wartime, and has a global nature." [35] Although there are a variety of names for the Russian approach, the most accurate appears to be "new generation warfare" which "is manifested in five component elements: political subversion, proxy sanctuary, intervention, coercive deterrence and negotiated manipulation." [36] Together these two approaches provide a significant threat to the United States, NATO Allies and like-minded partners around the world. This means that we all need to be competing in the information space. Information competition is so important that the Chairman of the Joint Chiefs of Staff recently designated "information" to be a joint function, co-equal with the existing joint functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment. [37]

The military has five functions that partially exist in the information environment and seven that exist entirely within the environment: Information Operations (IO), Military Deception, Psychological Operations (PSYOPs, also known as Military Information Support Operations or MISO), Public Affairs, and Strategic Communications are entirely within the environment. Communications & Signals, Cyber, Electronic Warfare (EW), Intelligence, Space operations and Operations Security (OPSEC) exist partially within. Physical operations also have an information effect, as when a US Army unit goes to a firing range in eastern Poland. All of these functions are legitimate military operations within cyberspace.

Conventional information operations are the age-old arts of persuasion. They are sometimes called propaganda (if your opponents are performing the operations), educational material (if your side is doing it) or even advertising via printed text, radio waves or television. Since tribes formed before history was captured, human beings have shaped the cognition of other human beings, both in the 'in group' and the 'out group.' Even though operations in the information environment have been central to civilization from the beginning, these operations expanded dramatically with the communications revolution inherent in the advent of the telegraph in the 1800s and accelerated with the further evolutionary additions of radio and television.

A new category of operations in the information environment is cyber-enabled information operations, which began with the arrival of the Internet. This takes the form of a traditional operation which uses cyber to magnify the Impact of the operation or to enable the operation itself. The hack of the Democratic National Committee would be an example of a cyber-enabled information operation. The information was obtained through cyber operations (the enabling function) but released via Wikileaks and thence to mainstream media outlets, a more traditional method of disseminating information.

Cyber information operations are a relatively new set of information operations that takes place entirely in cyberspace. An example would include Daesh recruiting videos. Videos are smoothly produced in a variety of languages and are aimed at global youth. As their target audience are digital natives, Daesh builds their products to be consumed as they do other digital materials. [38]

Countering these types of operations requires that the same techniques be used. As the Carter Center says, "The implementation of preventative community-based policies will equip trusted Islamic scholars and religious leaders with the necessary analysis and digital tools" [39] meaning that people hoping to counter them must use digital techniques to compete. This makes operations in the information environment a key cyber mission for militaries.

Military Operations and Cyberspace

Military operations can also be cyber-enabled or executed purely in cyberspace. This analytic framework discusses two types of military operations: conventional and special operations.

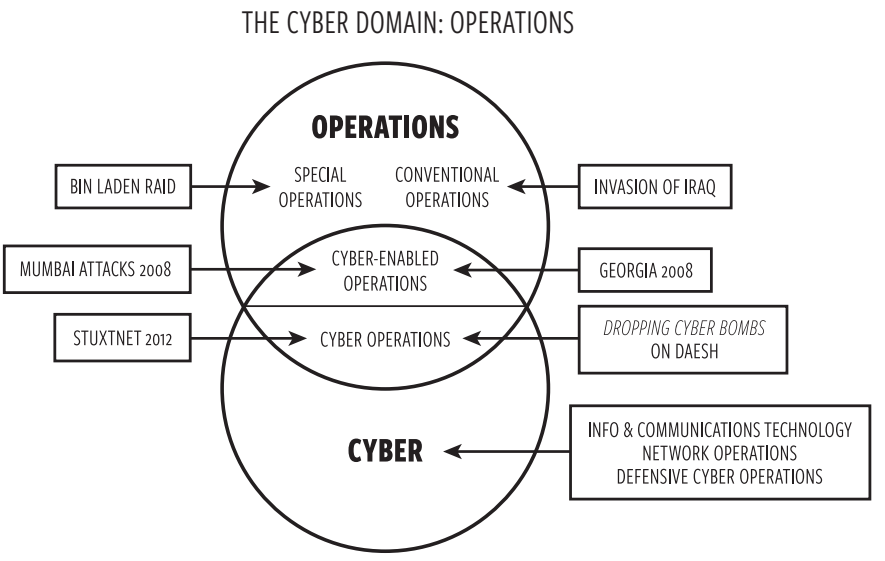

Figure 5. Relationship between Cyber and Operations

Cyber can either enable an operation or can be the operation itself. As such, there are cyber-enabled conventional operations, cyber-enabled special operations, conventional cyber operations and special cyber operations. Cyber-enabled conventional operations happen on a daily basis while almost all special operations (due to the availability of resources) are cyber-enabled. It is probably safe to assume that cyber conventional operations happen frequently and regularly. Cyber special operations, like their kinetic namesake, probably do not occur often.

An example of a conventional or normal military operation would be the invasion of Iraq. An example of a special operation would be the raid to eliminate Osama bin Laden. Although these operations occurred with a minimum of cyber enabling, as time goes on and cyber capabilities suffuse militaries, more and more of these operations will become cyber-enabled. Eventually, all conventional and special operations will become cyber-enabled unless specific counter-cyber operations negate that advantage.

An example of a cyber-enabled conventional military operation would be Russian operations in Georgia in 2008. Although Russia previously conducted purely cyber operations against Estonia in 2007, Georgia was different in that Russia conducted cyber operations against targets in Georgia to affect Georgian command and control in support of conventional military operations on the ground and air. [40]

An example of a cyber-enabled special operation would be the Mumbai attacks of 2008. Planners used a Go-Pro camera and walked the route so everyone could see videos of their routes during their preparation for the operation. Planners used Google Earth during their planning process. The command and control element monitored Indian social media

and traditional media (such as radio and television) to track the response by Indian security forces and steered the attacking force away from reacting Indian forces, enabling the operation to continue much longer than expected. [41]

As mentioned, cyber military operations also come in two flavors: conventional and special operations. A conventional cyber operation would be like "dropping cyber bombs on Daesh". Secretary of Defense Ash Carter explained at an event at US Northern Command that "We're using these tools to deny the ability of ISIL leadership to command and finance their forces and control their populations; to identify and locate ISIL cyber actors; and to undermine the ability of ISIL recruiters to inspire or direct Homegrown Violent Extremists," [42] Although the operations may be classified, mere classification would not be sufficient to label this a special operation. This is a conventional operation in that it does not require special techniques or unique modes of employment, and does not require a covert approach to the operation.

According to Joint Publication 3-05, Special Operations, these operations require:

> ... unique modes of employment, tactics, techniques, procedures, and equipment. They are often conducted in hostile, denied, or politically and/or diplomatically sensitive environments, and are characterized by one or more of the following: time-sensitivity, clandestine or covert nature, low visibility, work with or through indigenous forces, greater requirements for regional orientation and cultural expertise, and a higher degree of risk...Special operations may differ from conventional operations in degree of strategic, physical, and political and/or diplomatic risk; operational techniques; modes of employment; and dependence on intelligence and indigenous assets. [43]

A cyber special operation would be the Stuxtnet attacks on Iran. It meets many of the criteria for a special operation as defined above. It required unique modes of employment, tactics, techniques, procedures, and equipment. It was conducted in a hostile, denied, or politically and/or diplomatically sensitive environments. It was a low visibility operation characterized by a clandestine or covert nature, as manifested by the fact that no one has yet proved who conducted the operation.

As militaries routinely conduct conventional and special operations, these types of operations involving cyberspace are appropriate for militaries to conduct. All operations will eventually be cyber-enabled while there will be more and distinct cyber operations.

CONCLUSION

Because cyberspace is so large, and so much cyber activity occurs in the private sector, militaries do not have any business operating in most of cyberspace. Although militaries should be able to range anywhere throughout cyberspace to complete appropriate missions, most cyber activity should not involve the military at all.

There are pressures for the military to become more involved in cyberspace. DoD leaders have thus far managed to avoid being dragged into additional areas, mainly by sticking to DoD's three cyber missions: Defend DoD networks, systems, and information; Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and Provide cyber support to military operational and contingency plans. These are legitimate cyber missions for any military. These have been clearly articulated by the U.S. military; however, other militaries probably have not thought this through as they are busy building their cyber forces.

As manifestations of these legitimate cyber missions, there are four areas in cyberspace that are appropriate for the military to operate in crime, intelligence, information operations and military operations. This article has provided examples of how the military would be involved in all four of these areas. Although military forces are involved in these areas, they are not involved in all operations in these areas (for instance, the Department of Justice handles most cybercrime) but are involved in these areas. This, then, is the circumscribed area that should be called the military cyber domain. Militaries and Alliances like NATO around the world would do well to conceptualize these missions as appropriate for military cyber forces, understand why they should not be performing cyber missions outside of these areas, and inform their political masters that expanding cyber operations away from those four missions risks frittering away cyber combat, which would put at risk the overall mission of the military, the defense of the nation.

NOTES

1. https://www.merriam-webster.com/dictionary/domain.

2. DOD Dictionary of Military and Associated Terms, 60, as of March 2017, available at http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf.

3. G. Alexander Crowther and Shaheen Ghori. "Detangling the Web – A Screenshot of US Government Cyber Activity". Joint Force Quarterly #78, available at http://ndupress.ndu.edu/Media/News/Article/607658/detangling-the-web-a-screenshot-of-us-government-cyber-activity/.

4. House of Lords. "Protecting Europe against large-scale cyber-attacks". European Union Committee 5th Report of Session 2009–10", page 54, available at https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf

5. The Department of Defense Cyber Strategy, available at https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/.

6. J. Li, Jennifer, and Lindsay Daugherty, "Training Cyber Warriors - What Can Be Learned from Defense Language Training?" Washington, DC: RAND, 2015, http://www.rand.org/pubs/research_reports/RR476.html. See also Spidalieri, Francesca and Jennifer McArdle, "Transforming the Next Generation of Military Leaders into Cyber-Strategic Leaders: The role of cybersecurity education in US service academies." Arlington, VA: The Potomac Institute, 2016, http://www.potomacinstitute.org/images/CDR_Spidalieri-McArdle_p141-p163_041216.pdf. Both refer to a 2011 the DOD report "Cyber Operations Personnel Report." Washington DC, 2011, available at http://www.nsci-va.org/CyberReferenceLib/2011-04-Cyber%20Ops%20Personnel.pdf which report a total of 163,144 military and civilian personnel for FY09: 3777 Defensive Operations, 145,457 Operation and Maintenance and 13,910 Information Assurance. Since this antedates the National Mission Force, we would have to add 6200 personnel for a total of 169,344.

7. U.S. Army. Megacities and the United States Army – Preparing for a Complex and Uncertain Future, June 2014, available at: https://www.army.mil/e2/c/downloads/351235.pdf.

8. Joint Publication (JP) 3-0, Operations, January 17, 2017, ix.

9. Statista. "Internet usage in the United States - Statistics & Facts," https://www.statista.com/topics/2237/internet-usage-in-the-united-states, accessed August 1, 2017.

10. United States Small Business Administration. "2016 United States Small Business Profile," 2016, https://www.sba.gov/sites/default/files/advocacy/United_States.pdf.

11. Military operations as used here include military or paramilitary operations that other security (such as the Italian Carabinieri) or intelligence forces (such as the CIA) could perform but are mainly military in nature.

12. Technopedia. Information and Communications Technology (ICT). Technopedia goes on to explain that "Converging technologies that exemplify ICT include the merging of audiovisual, telephone and computer networks through a common cabling system. Internet service providers (ISPs) commonly provide internet, phone and television services to homes and businesses through a single optical cable. The elimination of the telephone networks has provided huge economic incentives to implement this convergence, which eliminates many of the costs associated with cabling, signal distribution, user installation, servicing and maintenance costs." Available at https://www.techopedia.com/definition/24152/information-and-communications-technology-ict.

13. DOD Directive (DoDD) 5144.02, DoD Chief Information Officer (DoD CIO), November 21, 2014, available at http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/514402p.pdf.

14. DISA. Our Work/DISA 101, available at http://disa.mil/About/Our-Work.

15. DISA's Mission Partner Support, available at http://disa.mil/About/Our-Work/Mission-Partners.

16. Joint Publication 3-12 (R), Cyberspace Operations, February 5, 2013, II-2, available at http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

17. Geoff Brumfiel, U.S. Navy Brings Back Navigation By The Stars For Officers, National Public Radio, February 22, 2016, available at http://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers.

18. Major John P. Vickery, The Lost Art of Dismounted Land Navigation. *Infantry Magazine* October-December 2015, available at http://www.benning.army.mil/infantry/magazine/issues/2015/OCT-DEC/pdf/4)%20Vickery%20-%20Land%20Nav.pdf.

NOTES

19. Sun Tzu, The Art of War, Chapter 13: The Use of Spies.

20. Office of the Director of National Intelligence. Members of the IC. "Eight Department of Defense Elements—the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial- Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the four DoD services; the Army, Navy, Marine Corps, and Air Force," available at https://www.odni.gov/index.php/what-we-do/members-of-the-ic.

21. "Lately, a bug that infiltrated the Indian Navy computers at its Eastern Command headquartered at Visakhapatnam enabled Chinese hackers to break into the system. A bulk of sensitive information, which reportedly details the position of marine forces, was compromised in the attack." Indian Defense. Indian Navy Raises Army For Cyber Front: Recruiting Cadets Against Chinese Hackers, July 13, 2012, available at http://indiandefence.com/threads/indian-navy-raises-army-for-cyber-front-recruiting-cadets-against-chinese-hackers.20159/.

22. Washington Post, Hacks of OPM databases compromised 22.1 million people, federal authorities say, available at https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.9b8c1d3e3fcf.

23. G. Alexander Crowther and Shaheen Ghori. "Detangling the Web – A Screenshot of US Government Cyber Activity". Joint Force Quarterly #78, available at http://ndupress.ndu.edu/Media/News/Article/607658/detangling-the-web-a-screenshot-of-us-government-cyber-activity/.

24. DC3 Web Page, available at http://www.dc3.mil/.

25. Justin Ling, Vice.com, "Man Who Sold F-35 Secrets to China Pleads Guilty", March 24, 2016, available at https://news.vice.com/article/man-who-sold-f-35-secrets-to-china-pleads-guilty.

26. About the DIB CS Program, available at https://dibnet.dod.mil/portal/intranet/Splashpage/RegisterThemed .

27. How Stuff Works, ATM Skimming, available at http://money.howstuffworks.com/atm-skimming.htm.

28. Kim Zetter, That Insane, $81M Bangladesh Bank Heist? Here's What We Know, *Wired,* May 17, 2016, available at https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/.

29. Mark Pomerleau, Intelligence officials: Cyber domain is still the 'Wild West', September 30, 2015, available at https://defensesystems.com/articles/2015/09/30/ic-congress-cyber-wild-west.aspx.

30. Examples include the Cyber Intelligence Sharing and Protection Act and the Strengthening State and Local Cyber Crime Fighting Act.

31. This article uses 'information operations' to be synonymous with 'operations in the information environment', as opposed to the U.S. Army Information Operations specialty.

32. China's Military Strategy, The State Council Information Office of the People's Republic of China, Beijing, May 2015.

33. Jeffrey V. Dickey, Thomas B. Everett, Zane M. Galvach, Matthew J.Mesko, Anton V.Soltis, "Russian Political Warfare: Origin, Evolution, and Application", Naval Postgraduate School, June 2015, available at https://calhoun.nps.edu/handle/10945/45838.

34. Stefan Halper. "China, The 'Three Warfares'": May 2013, available at http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/Litigation%20Release%20-%20China-%20The%20Three%20Warfares%20%20201305.pdf.

35. Dean Cheng. PLA Views on Informationized Warfare, Information Warfare and Information Operations, 61.

36. Phillip A. Karber, Ph.D. Russia's New Generation Warfare, NGA Pathfinder, June 4, 2015, https://medium.com/the-pathfinder/russia-s-new-generation-warfare-471066cb37d#.93qob470m.

37. Joint Publication 3-0, Operations, January 17, 2017, Chapter III, Joint Functions.

38. Mohammed Jamjoom, ISIS recruiting Western youth with English-language video, CNN, Jun 21, 2014, available at https://www.youtube.com/watch?v=jdgzCbrPqzQ.

39. The Carter Center, Religious Appeals in Daesh's Recruitment Propaganda, September 2016, available at https://www.cartercenter.org/resources/pdfs/peace/conflict_resolution/countering-isis/religious-appeals-in-daesh-recruitment-propaganda-091316.pdf.

NOTES

40. AFCEA, The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict, May 24, 2012, available at http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

41. RAND, The Lessons of Mumbai, 2009, available at http://www.rand.org/pubs/occasional_papers/OP249.html.

42. Colin Clark. Carter Details Cyber, Intel Strikes Against Daesh At NORTHCOM Ceremony. DefenseOne. May 13, 2016. Available at http://breakingdefense.com/2016/05/carter-details-cyber-intel-strikes-against-daesh-at-northcom-ceremony/.

43. Joint Publication 3-05, Special Operations, I-1.