DIIS POLICY BRIEF

Challenges to international regulation of cyber technology at war

Kenneth B. Moss, kenneth.moss@gc.ndu.edu

May 2014

Cyber technology could change not only the conduct of war itself; it could alter the way governments and others initiate hostilities and war. Existing international laws need to be reviewed to make sure they address the capabilities and accountability of cyber operations in conflict and war, and the participation of China, Russia and other states in negotiations is critical.

Assessing the impact of cyber technology on the conduct of military operations and war is a serious question for the international community. Not only could this technology change the conduct of war itself; it could alter the way governments and others initiate hostilities and war. As the international community lacks a standard definition of "war," it is not surprising to find the absence of a common vocabulary regarding cyber and war. "Cyberwar," "cybered conflict," and "wartime cyber-attacks" are among the terms used, and each carries different meanings – war fought by cyber technologies, war's conduct aided by the cyber domain, and cyber technology as an actual form of attack during war.

Contrasted against the content and meaning of international humanitarian law – the law of armed conflict – the characteristics of the cyber domain in war do not seem at first glance to match what this law governs.

RECOMMENDATIONS

- Do not advocate a thorough revision of international humanitarian law (law of armed conflict) to accommodate cyber technology. Existing law provides a sound foundation. Use the Tallinn Manual or comparable studies as a baseline.
- Participation of China, Russia, and other states in negotiations is critical. Both Moscow and Beijing have proposed negotiation of a code of conduct for cyber security. The Tallinn Manual's origins will cause suspicion that this is a NATO-driven initiative, so this subject must be addressed in fora related to the International Committee of the Red Cross or the UN.
- Enable extensive public involvement in the debate in order to inform and educate not only the public but elected representatives and government officials.
- Revise existing national laws and processes concerning governmental decisions to use force to assure that they adequately address the capabilities and accountability of cyber operations in conflict and war.
- Revise existing domestic laws that address acts by private citizens that could be defined as criminal measures, forms of armed attack, or illegal intrusion into the sovereign matters of other states.

Its area of responsibility is state-to-state interaction. Discussion of the cyber domain often occurs in transnational terms that suggest it is beyond state control and involves hundreds of millions of non-state actors. This description is partly true, of course, but it is important to remember that every part or actor in cyber still has to contend in some way with the jurisdiction or sovereignty of a state. That said, the attributes of cyber do not match intuitively with the characteristics of war that shaped international law. The United Nations Charter rests on the premise that the attacker is identifiable (a state's government) and can be held accountable and punished by the international community. Even though war has involved non-physical measures, most governments, leaders, and citizens automatically think of war in physical terms: missiles, planes, bombs, bullets, etc. It is tempting, therefore, to conclude that existing international law and practice must undergo major revision to accommodate the changes that cyber technology in war requires.

Land, sea, air, and space are domains where governments have sought to govern the initiation and conduct of war – and in the case of space to try to prevent its militarization. In July 2011 the U.S. Department of Defense Strategy for Operating in Cyberspace identified cyberspace as "an operational domain to organize, train, and equip." Yet, what cyberspace exactly is evades an exact definition. Peter W. Singer and Allan Friedman in a recent study tabulate that the U.S. Department of Defense alone has offered "at least twelve different definitions." Furthermore, the revelations since June 2011 about the extensive capabilities of the National Security Agency (NSA) in the United States as well as other foreign agencies have stimulated public and official awareness and expanded definitions as to what cyberspace may encompass. Is it just the technologies and the related infrastructure or does this domain include everything these technologies affect? Defining the traditional domains where operations and war may occur is difficult in the cyber domain.

As the United States maintains strong capabilities in numerous categories of cyber operations, its adherence to international law in this domain is critical for the world community.

What Is "Use of Force" in Cyberspace?

Does the nature of the cyber domain undermine the key provisions of international law related to war? These are specifically Article 2 (4) of the UN Charter that requires states to "refrain from the threat or use of force against the territorial integrity or political independence of any state" and Article 51 that allows self-defense in instances of "armed attack." Such questions as well as others about the characteristics and effect of such operations and the perception of such action by both the targeted and the international community at large have reportedly figured in President Barack Obama's reluctance to initiate cyber attacks against Syria.

As the United States maintains strong capabilities in numerous categories of cyber operations, its adherence to international law in this domain is critical for the world community. The outgoing commander of U.S. Cyber Command as well as the director of the National Security Agency, General Keith Alexander, testified to Congress the determination of use of force" or "armed attack" would be "made within the bounds of U.S. and international law." The pivotal question is what determines the threshold where these enter into effect. Alexander's answer relied on criteria well-grounded in both international law as well as Just War theory – "scope," "duration," and "intensity." He is also implying that such operations could produce results as destructive as some physical attacks. Were there attributes of the Stuxnet operation against Iranian nuclear centrifuges that would have made it analogous to a use of force and thus an arguable violation of the UN Charter? Was it too specifically targeted; was the "intensity" or 'scope" of the operation too limited? From the other perspective was it like an "armed attack" and thus a justification for self-defense? If so, what would have been the appropriate, justifiable form and level of response?

While government officials, scholars, and others answer these concerns in a variety of ways, the most important international effort to date to determine some common answers is the work of the International Group of Experts or the Tallinn Group who released in early 2013 The Tallinn Manual on the International Law Applicable to Cyber Warfare. Although sponsored by the NATO Cooperative Cyber Defense Center of Excellence, the manual bears no official support from NATO or any member government. Nevertheless, the Tallinn Manual is so far the best place to start for any serious discussion of accommodating international humanitarian law to the realities of the cyber domain. From it and other commentaries a valid question emerges whether or not it is best to leave the law as it is to encompass these capabilities or to revise or rewrite it however necessary. Either avenue poses risks. More general law may be more effective and inclusive than law that

tries to confront specific capabilities or characteristics. Yet, it may be more ambiguous and open to contrasting interpretation.

Is it best to leave the law as it is to encompass the capabilities of cyber technologies or to revise it however necessary? Either avenue poses risks.

Cyber technology in war poses questions ranging from the strategic to the operational and technical levels. Could a cyber war be a form of war all on its own or will any cyber attack or -operation be part of larger operations that supplement traditional means of war? Many writers anticipate cyber technological measures especially in the initial and early phases of a conflict, although such operations could continue through the duration of the conflict. A particular concern is that the non-physical and sometimes evasive characteristics of the cyber domain make it especially tempting to use for early, preventive, or pre-emptive attack. It may be covert, undetected, and well below thresholds that would enable early determination about "use of force" or "armed attack." Thus, will it make conflict more probable while simultaneously, as some argue, enable it to be more targeted but less destructive?

Cyberspace decreases accountability

International law as well as the domestic laws of many states, especially those with democratic institutions, place accountability at the very center of their frameworks to restrict and regulate war – whether it is the identity of the state using force or the responsibility of select individuals or institutions to make the decision to use force or respond with self-defense. More than any other domain of known war, the cyber domain seriously challenges accountability. In the cyber domain, unlike most forms of war, its means and conduct may not be restricted to states and governments. Domestic laws often govern the conduct of citizens, including actions they can take against other countries or foreign nationals, so states are not helpless, but the commercial pervasiveness of the cyber domain complicates the challenge of enforcement. The governments of the United States and its allies depend on commercial networks; well over ninety percent of U.S. Government communications move on commercial networks. Leading edge conceptualization and writing of programming predominantly occur in the commercial world.

The global availability of the technology as well as the dispersed population using it makes determination of the source or initiator of an attack difficult. Nearly seven years after the cyber attack on Estonia, the exact originators are unknown. Much evidence points to individuals or groups in Russia, but proof of government responsibility is unclear, and the arrival of attacks from other countries, including the United States, shows how successful the intentional rerouting was. If the source of attack is unknown, it is harder to determine intent (attack or simply malice) or to decide on the nature of and target for response. As in any form of conflict, there is a risk of disproportionate response and mistaken targeting.

The path of operational and political accountability behind such decisions in the cyber domain becomes difficult even within the boundaries of government. One reason is already evident – the laws, political processes, and chains of command that exist developed in environments dependent on physical or traditional deployment and weaponry. Even if they are adequate for cyber operations, political leaders in particular are not comfortable addressing the cyber domain because of a lack of expertise and informed debate. No better example exists than in the U.S. where there is general agreement that the law concerning joint congressional/executive consultation for the use of force, the War Powers Resolution, does apply to the cyber domain – but how it does so is unclear.

More than any other domain of known war, the cyber domain seriously challenges accountability.

A second reason why cyber technology impairs accountability is that the difficulty in tracing origin or verifying intent, etc. makes it a measure of special value in the realms of both intelligence and warfare. The institutions, procedures, and laws governments use in these realms are different, and in most countries the parliamentary or legislative arm is excluded or involved in intelligence operations in only general terms. Intelligence is not armed force or war, and international law does not prohibit, restrict, or regulate it. However, governments can move the conduct of what are arguably uses of force into the intelligence domain. Numerous allied missions during the Second World War were of such nature. An ongoing illustration of this matter is in the debate in the U.S. as to whether or not the NSA (an intelligence agency) and Cyber Command (a military command) should

have the same person as director and commander. In December 2013 President Obama decided to retain this structure– a decision some interpreted as a way to preserve stronger, more flexible capabilities in both intelligence and military arenas.

A third complicating reason is the increased dependence by militaries and intelligence agencies on private contractors. Questions about their role and capability add more ambiguity to a domain of conflict where the commercial world is already so prominent. Many governments have sought changes to laws to define and regulate the place of contractors in operational theaters, but cyber technologies can enable a theater to be almost anywhere. International humanitarian law excludes private contractors from enjoying the rights of uniformed combatants (even if companies provide uniforms in theater that closely resemble or duplicate those of the military). However, the distinction made by law does not deter a growing reliance on contractors due to costs, the forms of specialized support needed in the cyber domain, and, arguably, the value of having access to actors whose status is not as well-controlled or defined in policy and law.

Holding the Cyber Genie in the Bottle?

The realization of the capacity and ease of attack in the cyber domain, as drawn from the Edward Snowden affair and the extensive penetration of private data banks by both private and state actors, has sharpened awareness that the cyber domain is indeed a setting for uses of force and attack and not just intelligence and criminal conduct. Heightened cyber security and awareness are recurrent and obvious responses to prepare and defend against such occurrences. So, too, is consideration of stricter corporate and national domains in the networked world, which would try to insulate state and non-state actors from intrusion and attack and diminish dependence on a global network significantly shaped by the United States. However, these are private and state-level actions that would have slight effect on the political and legal treatment of cyber war in the international community. Multilateral discussions are the only means that may develop effective steps to restrict and regulate the course of cyberwar.

RECOMMENDED READING

P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: *What Everyone Needs to Know* (Oxford and New York: Oxford University Press, 2014).

Derek S. Reveron, editor, Cyberspace and National Security: *Threats, Opportunities, and Power in a Virtual World* (Washington, D.C.: Georgetown University Press, 2012)

Michael N. Schmitt, editor, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge and New York: Cambridge University Press, 2013)

The opinions expressed in this policy brief are those of the author alone and do not necessarily reflect the official opinion of the Danish Institute for International Studies.

DIIS · DANISH INSTITUTE FOR INTERNATIONAL STUDIES
Østbanegade 117, DK-2100 Copenhagen, Denmark · tel: +45 32 69 87 87 · Fax: +45 32 69 87 00 · e-mail: diis@diis.dk · www.diis.dk