Maneuver Warfare in the Cyber Domain

A proposal to update the existing legal framework to facilitate decentralized decision making in cyber operations

by Capt Joe McGinley

War is both timeless and ever changing. While the basic nature of war is constant and methods we use evolve constantly … [o]ne major catalyst of change is the advancement of technology. As the hardware of war improves through technological development, so must the tactical, operational, and strategic usage adapt to its improved capabilities to counteract our enemy's.[1]

>Capt McGinley is currently the Deputy Staff Judge Advocate at Marine Corps Base Hawaii. Prior to MCBH, he was a trial counsel at MCAGCC Twentynine Palms, CA and deployed with the Marine Rotational Force-Darwin.

This excerpt from *MCDP 1, Warfighting,* has proven particularly relevant with the advent of cyber warfare. Recent technological advances have allowed hackers to conduct cyberattacks against the United States and countries around the world. The 2015 Office of Personnel Management hack, for example, resulted in the theft of 21.5 million Federal employees' personal information. In 2007, a series of coordinated cyberattacks crippled the Estonian government, banks, media, and other institutions—bringing the country "to a virtual standstill."[2] Most recently, Russia has employed cyber operations as part of the conflict in Ukraine.[3]

In the absence of treaties or statutes, the DOD and Marine Corps have taken steps to adapt to and regulate this new wrinkle in modern warfare. Several DOD documents relevant to this discussion are classified; those documents will not be addressed and limit this article's permissible scope.

The United States does not stand alone in its quest to regulate cyberspace and cyber warfare. An international group of experts developed the *Tallin Manual* and *Tallin Manual 2.0*, which seek to establish an international code to govern cyber operations. While the *Tallin Manual* and the *Tallin Manual 2.0* provide useful guidelines, they are not binding on the United States. It would benefit the United States to take a leading role in the development of domestic and international standards, both as a world leader and because such standards will improve America's ability to act and react decisively, consistently, and in coordination with our allies.

Current Legal Framework

Modern warfare is analyzed under two primary sources of authority: the U.N. Charter and the Law of Armed Conflict (LOAC). Cyber warfare, however, presents several challenges that the definitions in the U.N. Charter and the LOAC may not adequately address.

The U.N. Charter. The U.N. Charter establishes many of the basic principles for international relations. Various interpretations of the U.N. Charter have occasionally resulted in political tensions, such as balancing a state's right to sovereignty with a state's right to preemptive self-defense. Sovereignty versus preemptive self-defense remains an ongoing source of friction in international relations and international law—a problem that will be exacerbated if the conduct of cyber warfare is analyzed within a framework that does not account for its intricacies.

Article 2 of the U.N. Charter grants states the right sovereignty, stating,

> [a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[4]

Article 51 grants states the right to self-defense. It reads, in part,

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security [emphasis added].[5]

The U.N. Charter, understandably, does not address issues specific to cy-

ber warfare in several ways. The U.N. Charter does not define the "force" that may not be used "against the territory integrity" of any state, nor does it define "armed attack." Cyberattacks resulting in physical damage, and thus having the effect of a physical attack, would likely constitute force in violation of Article 2. One could argue, however, that cyberattacks that *do not* result in the manipulation of physical objects (such taking information from an electronic database) may not constitute "force" against a state's "territorial integrity" as the terms are commonly understood. This represents a potentially dangerous gray area, and one that our enemies could exploit.

Additionally, as with traditional warfare, no clear guidance exists on how far the right to self-defense, as articulated by Article 51, extends. A state's right to self-defense is not absolute, and it remains unclear when action in cyberspace crosses the line between "preemptive self-defense"[6] and a violation of another state's sovereignty.[7]

The LOAC. The DOD applies the LOAC to all military operations. The LOAC is a combination of the "Hague Tradition" and "Geneva Tradition."[8] The Hague Tradition regulates the means and methods of warfare, such as the tactics, weapons, and targeting criteria.[9] All military operations must be evaluated in terms of necessity, proportionality, distinction, and humanity.[10]

The LOAC applies to both international armed conflicts (IACs) as well as non-international armed conflicts (NIACs). However, the distinction between the two categories of conflict could prove critical to other issues such as use of force and the status of enemy combatants. The ability to attribute an attack to its source will be crucial in determining whether an IAC or NIAC framework applies.

IACs. The U.N. classifies armed conflict between two states as IACs. It bases this classification on Common Article 2,[11] which is supplemented by Additional Protocol I.[12] Cyber warfare in an IAC poses few legal problems. If a foreign military or government conducts cyberattacks against the United States as part of a conflict, the United States could respond in accordance with U.N. Charter Article 51 and the LOAC, constrained only by the principles of necessity, distinction, proportionality, and humanity. Those foreign operatives working on behalf of the state would be entitled to the same protections as any other prisoner of war.

NIACs. The more complex scenario would involve one or more non-state actors that conduct cyberattacks against the United States. One can easily imagine a scenario in which a terrorist organization, or other organizations operating independently of any nation-state, attempts to bring down all or parts of the DOD or Marine Corps network. These actions and actors would likely fall within the NIAC framework.

NIACs, or "armed conflict[s] not of an international character occurring in the territory of one of the High Contracting Parties,"[13] trigger additional Protocol II obligations for the state party involved in the conflict.[14] NIACs have traditionally involved the imposition of international regulations on entirely internal conflicts, such as the Colombian government's struggle against the Revolutionary Armed Forces of Colombia. But this definition has expanded in recent years; multiple international courts have recognized that NIACs may exist across international borders.[15]

Unlike combatants in IACs, combatants in NIACs do not receive combatant immunity, prisoner of war status, or protections for their actions.[16] Foreign cyber operatives will likely fall somewhere along a spectrum between "no state support" and "state or military employee." The Marine Corps should have a plan for how to classify actors at various points along this spectrum, providing various levels of support, and train Marines on what protection those actors are entitled to. Once we accurately categorize these actors, we will next have to determine at what point they become valid military targets depending on their actions in cyberspace. Commander's intent should then empower decision-makers at the appropriate level.

How far does our right to self-defense go? *(Photo by LCpl Angela Wilcox.)*

Improving our Combined Arms

The Marine Corps relies on maneuver warfare to defeat its enemies. Part of this approach includes the use of combined arms, which *MCDP 1* defines as "the full integration of arms in such a way that to counteract one, the enemy must become more vulnerable to another."[17] Speed provides a crucial means to exploit the enemy's gaps that the combined arms dilemma exposes. The cyber domain is no different.

The Marine Corps is aware that its reliance on electronics could prove to be a critical vulnerability in battle. A successful enemy cyberattack could act as a

force multiplier for an otherwise inferior force, drastically slow our operational tempo such that we lose relative speed over the enemy, and severely limit the Marine Corps' ability to use combined arms. In a near-peer engagement, the ability to move our personnel and aircraft close to and into enemy territory both undetected and unimpeded will be critical for shaping operations. Developing cyber capabilities organic to the MEFs and empowering decision-makers at the MEF level would allow for a quicker response, thus improving our relative speed and exposing our enemies to a combined arms dilemma earlier in the fight.

Moving Forward

Domestically, the United States has recognized the immediacy of the cyber threat, as evidenced by the 2017 *National Security Strategy* and the 2018 *National Defense Strategy* (NDS). While discussing how to protect the United States in the cyber era, the *National Security Strategy* noted that information sharing and layered defenses will be key to deterring and defeating rogue actors.[18] The NDS enacted this intent, stating that we will

> invest in cyber defense, resilience, and continued integration of cyber operations into the full spectrum of military operations.[19]

The Marine Corps Cyberspace Command addresses and develops defenses to cyberattacks, assesses system vulnerabilities, and prepares to digitally "maneuver" in support of operational forces.[20]

Internationally, the *Tallinn Manual* distinguishes between "use of force" and "armed attack"[21] and concludes that cyber operations can qualify as an armed attack, particularly in cases involving substantial injury or physical damage.[22] Additionally, some members of the group posited that a "sufficiently severe non-injurious or destructive cyber operation, such as that resulting in a state's economic collapse, can qualify as an armed attack."[23]

These domestic and international measures represent a great deal of progress and a useful baseline in an emerging field. The United States should seek to lead the global community in this area. The DOD will benefit from having a set of rules for responses and engagement criteria. While not a necessity, signing and ratifying a single international framework can both improve relations with our allies and allow the DOD to improve interoperability during combined operations. Such a framework will also facilitate decentralized decision-making as to whether an "attack" has occurred and allow MEFs to respond quickly and decisively in fluid situations.

We rely on maneuver warfare to out think our enemies. *(Photo by Cpl Mark Lowe.)*

Decentralized decision-making remains especially important to the Marine Corps. Our structure and doctrine place decision-making responsibility on our personnel closest to the ground. Predictability and known rules of engagement may become critical considerations for these individuals. Our MAGTFs and MEFs would benefit from an organic cyber warfare element

The personnel closest to the ground are the responsible decision makers. *(Photo by Cpl Mark Lowe.)*

that could react instantaneously to an enemy cyberattack, conduct a counterattack, and relay relevant information to the GCE, ACE, or LCE. Such decentralization is also consistent with the NDS's directive to integrate operations "into the full spectrum of military operations." Cyber and electronic warfare will likely take on an increasingly prominent role in future conflicts; we owe our Marines the power to make critical decisions with confidence and consistency so we may continue to win battles in any clime and place.

Notes

1. Headquarters Marine Corps, *MCDP 1, Warfighting*, (Washington, DC: 1997).

2. LTC Scott W. Beidleman, USA, *Defining and Deterring Cyber War*, (Carlisle, PA: U.S. Army War College, 2009).

3. Laurens Cerulus, "How Ukraine Became a Test Bed for Cyperweaponry," *POLITICO*, (February 2019), available at https://www.politico.

4. United Nations, *Charter of the United Nations,* (San Fransico, CA: October 1945). See Article 2 (4).

5. *Charter of the United Nations*. See Article 51.

6. U.N. Special Rapporteur Philip Alston has stated that

> [a] targeted killing conducted by one State in the territory of a second State does not violate the second State's sovereignty [where] ... the first, targeting State has a right to international law to use the force in self-defen[s]e under Article 51 of the U.N. Charter, [and] the second state is unwilling or unable to stop armed attacks against the first State launched from its territory.

U.N. Human Rights Council, *Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Study on Targeted Killings, U.N. Document A/HRC/14/24/Add.6*, (Geneva, CH: May 2010). For other examples of preemptive self-defense in international law, see William H. Taft IV, *The Legal Basis for Preemption*, Council on Foreign Relations, (2002), available at http://www.cfr.org

7. In traditional warfare, absent consent, a "victim" state may only violate another state's sovereignty in the name of self-defense if the host state is "unwilling or unable" to stop the threat to international peace. Additionally, the victim State's operations must conform to the LOAC's principles of necessity and proportionality. A similar standard would be useful cyber warfare, especially considering the clandestine and secretive nature of some hacking groups in countries like China and Russia. See Ashley S. Deeks, "'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense," *Virginia Journal of International Law*, (Charlottesville, VA: University of Virginia School of Law, December 2011). Citing Permanent Rep. of the Russian Federation to the U.N., Letter dated Sept 11, 2002 from the Permanent Rep of the Russian Federation to the United Nations addressed to the Secretary-General, Annex, U.N. Doc. S/2002/1012/Annex.

8. LTC Richard P. DiMeglio, Judge Advocate, USA, et al., *Law of Armed Conflict Deskbook*, (Charlottesville, VA: United States Army Judge Advocate General's Legal Center and School, 2012).

9. Hague tradition consists of the Hague Conventions of 1899, as revised in 1907, the 1954 Hague Cultural Property Convention, and the 1980 Certain Conventional Weapons Convention. Geneva Tradition focuses on respecting and protecting victims of warfare; Geneva Tradition is composed of the four Geneva Conventions of 1949, each of which protects a different category of war victim. *Law of Armed Conflict Deskbook*: *supra* n. 8 at 19.

10. *Law of Armed Conflict Deskbook.*

11. "Common Article" refers to articles that are common to all four Geneva Conventions.

12. "[T]he present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more High Contracting Parties, even if the state of war is not recognized by one of them." Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field ["Geneva I"] article 2 (1949). The United States has not signed or ratified Protocol I, in part because it expands Common Article 2 to include conflicts previously classified as non-international armed conflicts. Under Protocol I, Common Article 2 would include "armed conflicts in which people are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination." Protocol Additional to Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts art. 1, para. 4. The United States has resisted ratifying Protocol I because it expands liability for commanding officers for the actions of subordinates (*id.*, at arts. 86, 87) and because it states enemy combatants have not distinguished themselves from civilians until they have engaged in preparatory or combat activities (*id.*, at art. 44[3]). For a fuller discussion of the reasons that some States have chosen not to ratify Protocol I; see Harvey Rishikof, "Institutional Ethics: Drawing Lines for Militant Democracies," *Joint Force Quarterly,* (Washington, DC: National Defense University Press, 2009). See also David McGrogan, "Whither Now, Additional Protocol I?" *International Law Observer,* (January 2009), available at http://www.internationallawobserver.eu.

13. *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field ["Geneva I"] art. 3 (1949).*

14. *Law of Armed Conflict Deskbook.*

15. See Supreme Court of the United States, *Hamdan v. Rumsfeld, 548 U.S. 557,* (Washington, DC: 2006). Holding that "the term 'conflict not of an international character' is used here in contradistinction to a conflict between nations" and thus recognizing that Common Article 3 conflicts can expand beyond the territory of one States. See also International Court of Justice, 2005 I.C.J. 337, *Case Concerning Armed Activities on the Territory of Congo (Democratic. Republic of Congo v. Uganda),* (The Hague, NL: December 2019).

16. For further reading, see Supreme Court of Israel, *HJC 769/02, The Public Committee Against Torture in Israel, et al., v. The Government of Israel, et al.*, (Jerusalem, IL: December 2005).

17. *MCDP 1.*

18. *National Security Strategy of the United States of America, 2017.*

19. *National Defense Strategy of the United States of America, 2018.*

20. James K. Sanborn, "Cyber Battlefield Grows in Importance," *Military Times,* (April 2009), available at http://www.militarytimes.com.

21. Collin Allan, "Was the Cyber Attack on a Dam in New York an Armed Attack?" *Just Security,* (January 2016) available at https://www.justsecurity.org.

22. Ibid.

23. Ibid.