HARVARD INTERNATIONAL LAW JOURNAL ONLINE
VOLUME 62 / 2020

SOME CONSIDERATIONS FOR CONDUCTING LEGAL REVIEWS OF U.S. MILITARY CYBER OPERATIONS

*The Hon. Paul C. Ney, Jr.**

General Nakasone, Colonel Smawley, distinguished panelists, and guests, thank you for the opportunity to speak with you today. Since its inception in 2012, the U.S. Cyber Command legal conference has provided the Department of Defense (DoD), other U.S. Government agencies, our Allies and partners, and interested members of the academy and the general public, with a unique opportunity to explore some of the complex legal issues facing our military and our Nation in cyberspace.

I have two objectives today. First, I'll offer a snapshot of how we in DoD are integrating cyberspace into our overall national defense strategy. Second, I will summarize the domestic and international law considerations that inform the legal reviews that DoD lawyers conduct as part of the review and approval process for military cyber operations. We at DoD now have considerable practice advising on such operations and are accordingly in a position to begin to speak from experience to some of the challenging legal issues that cyber operations present.

To set the scene, when I talk about "cyberspace," I am referring to "the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems,

---

* General Counsel, U.S. Department of Defense. This Essay is based on remarks given at the U.S. Cyber Command Legal Conference on March 2, 2020. Footnotes have been added and updated as of the date of publication of this Essay. I am grateful to Charles A. Allen, Eliana V. Davidson, Thomas H. Lee, Guillermo R. Carranza, Commander Robin Crabtree, Karl S. Chang, Matthew McCormack, John L. Muelheuser, Gary Corn, and Lieutenant Commander Lynn M. Cherry, for their assistance in preparing this Essay.

and embedded processors and controllers."[1] Physically, and logically, the domain is in a state of perpetual transformation. It enables the transmission of data across international boundaries in nanoseconds—controlled much more by individuals or even machines than by governments—spreading ideas to disparate audiences and, in some cases, the generating of physical effects in far-flung places.

I. TODAY'S CYBER THREAT ENVIRONMENT AND DOD'S RESPONSE

As we enter the third decade of the twenty-first century, people are imagining, developing, and creating new technologies and devices at a faster rate than ever before. These new technologies update on a near daily basis—think of the software update that your phone automatically uploaded today.

Sophisticated technologies are now a part of nearly all aspects of military operations, creating opportunities and challenges. A recent Brookings paper makes the point well: "By . . . building Achilles' heels into everything they operate, modern militaries have created huge opportunities for their potential enemies. The fact that everyone is vulnerable . . . is no guarantee of protection."[2]

Constantly changing vulnerabilities exist not only within our Armed Forces but also in the private and public sectors, which provide critical support to our operations. This includes contractors that manage networks and other services; the defense industrial base that is the foundation of the United States' military strength; and critical public

---

1 DEP'T OF DEF., DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 55 (June 2020), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf [https://perma.cc/E428-M2FP].

2 MICHAEL O'HANLON, THE BROOKINGS INST., FORECASTING CHANGE IN MILITARY TECHNOLOGY, 2020-2040 16 (2018), https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf [https://perma.cc/YKA6-5FQL].

infrastructure upon which the entire country, including the Armed Forces, relies for water, electricity, and transportation.

From a strategic competition perspective, too, cyberspace is increasingly dynamic and contested, including as a warfighting domain. In the past few years, other nations, in part to make up for gaps in conventional military power vis-à-vis the United States, have developed cyber strategies and organized military forces to conduct operations in cyberspace. China's Strategic Support Force, for example, provides its People's Liberation Army with cyberwarfare capabilities to "establish information dominance in the early stages of a conflict to constrain [U.S.] actions . . . by targeting network-based [command and control,] . . . logistics, and commercial activities."[3] Russia consistently uses cyber capabilities for what it calls "information confrontation" during peacetime and war.[4] All of this is unsurprising because cyber is a relatively cheap form of gaining real power, especially for impoverished adversaries like North Korea: a cyber operation can require nothing more than a reasonably skilled operator, a computer, a network connection, and persistence.

A key element of the U.S. military's strategy in the face of these cyber-threats is to "defend forward."[5] Implementing this element of the strategy begins with "continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver"—which we refer to as

---

3 DEF. INTELLIGENCE AGENCY, CHINA MILITARY POWER: MODERNIZING A FORCE TO FIGHT AND WIN 46 (2019), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf [https://perma.cc/R53S-NMFN].

4 DEF. INTELLIGENCE AGENCY, RUSSIA MILITARY POWER: BUILDING A MILITARY TO SUPPORT GREAT POWER ASPIRATIONS 38 (2017), https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf [https://perma.cc/ATQ8-DLEB] (citations omitted).

5 DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [https://perma.cc/N9F9-GKWZ] [hereinafter DOD CYBER STRATEGY].

"persistent engagement."[6] "Persistent engagement recognizes that cyberspace's structural feature of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace."[7] As General Nakasone has said, "[i]f we find ourselves defending inside our own networks, we have lost the initiative and the advantage."[8] In short, the strategy envisions that our military cyber forces will be conducting operations in cyberspace to disrupt and defeat malicious cyber activity that is harmful to U.S. national interests.[9]

Cyber operations are also becoming an integral part of other military operations. As the 2018 National Defense Strategy emphasizes, "[s]uccess no longer goes to the country that develops a new technology first, but rather to the one

---

6 C. Todd Lopez, *Persistent Engagement, Partnerships, Top Cybercom's Priorities*, DEFENSE.GOV (May 14, 2019), https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/ [https://perma.cc/RV8Z-G6GE]. *See also id.*; *Securing the Nation's Internet Architecture: Hearing Before the H. Armed Services Subcomm. on Intelligence & Emerging Threats & Capabilities & the H. Oversight & Reform Subcomm. on Nat'l Sec.* (Statement of Edwin Wilson, Deputy Assistant Secretary of Defense for Cyber Policy at 3) (Sep. 10, 2019), https://docs.house.gov/meetings/AS/AS26/20190910/109894/HHRG-116-AS26-Bio-WilsonB-20190910.pdf [https://perma.cc/T4S7-5NFG] [hereinafter *Hearing*]; U.S. CYBER COMMAND, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR US CYBER COMMAND (2018) https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 [https://perma.cc/7866-EHZY].

7 Michael P. Fischerkeller & Richard J. Harknett, *Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace*, LAWFARE (Nov. 9, 2018), https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace [https://perma.cc/U4W2-LE4U].

8 *An Interview with Paul M. Nakasone*, JOINT FORCES Q. (Jan. 2019), at 4, 7, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf [https://perma.cc/CCP7-9RBD].

9 *See Hearing*, *supra* note 6, at 3 (U.S. Armed Forces "defend forward by conducting operations that range from collecting information to gain insight about hostile cyber actors and their intent, to exposing malicious cyber activities and associated infrastructure publicly, to disrupting malicious cyber activities directly.").

that better integrates it and adapts its way of fighting."[10] For example, during operations in Iraq in 2017, U.S. forces used cyber and space capabilities to disrupt communications to and from the enemy's primary command post, forcing the enemy to move to previously unknown backup sites, thereby exposing their entire command-and-control network to U.S. kinetic strikes.[11] Operations like this will become increasingly common.

Because of the complexity and dynamism of the domain and the threat environment, the need for persistent engagement outside U.S. networks, and the critical advantage that cyber operations provide our Armed Forces, DoD must develop, review, and approve military cyber operations at so-called "warp-speed." To this end, the U.S. Government has made meaningful strides. You heard in 2018 that the President had issued National Security Presidential Memorandum-13, *United States Cyber Operations Policy*, or "NSPM-13" for short, which allows for the delegation of well-defined authorities to the Secretary of Defense to conduct time-sensitive military operations in cyberspace. Congress also has clarified that the President has authority to direct military operations in cyberspace to counter adversary cyber operations against our national interests and that such operations, whether they amount to the conduct of hostilities or not, and even when conducted in secret, are to be

---

10 DEP'T OF DEFENSE, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA 10 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/R5KF-EXG7].

11 *See* Matthew Cox, *US, Coalition Forces Used Cyberattacks to Hunt Down ISIS Command Posts*, MILITARY.COM (May 25, 2018), https://www.military.com/dodbuzz/2018/05/25/us-coalition-forces-used-cyberattacks-hunt-down-isis-command-posts.html?utm_source=Mike%27s+Daily+Blast&utm_campaign=8d4307f510-EMAIL_CAMPAIGN_2018_04_27_COPY_02&utm_medium=email&utm_term=0_beae3dbeb1-8d4307f510-51475081) [https://perma.cc/7Z8G-J6YU].

considered traditional military activities and not covert action, for purposes of the covert action statute.[12]

Even as the United States takes action to secure its vital national interests and to support its Allies and partners in this complex environment, it is a Nation dedicated to the rule of law. Consequently, we must ensure that our efforts are not only effective but also consistent with law and wider U.S. Government efforts to promote stability in cyberspace and adherence to the rules-based international order. DoD lawyers have an important role to play as the Department develops and executes cyber operations to meet these mandates.

Let me turn now to providing you a sense of how DoD lawyers analyze proposed military cyber operations for compliance with domestic and international law.

II. FRAMEWORK FOR LEGAL ANALYSIS

To evaluate the legal sufficiency of a proposed military cyber operation, we employ a process similar to the one we use to assess non-cyber operations. We engage our clients to understand the relevant operational details: What is the military objective we seek to achieve? What is the operational scheme of maneuver and how does it contribute to achieving that objective? Where is the target located? Does the operation involve multiple geographic locations? What is the target system used for? How will we access it? What effects—

---

12 *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232 (2018) [hereinafter "NDAA for FY 2019"]. Several provisions in the NDAA for FY 2019 provide authority and express support for the conduct of cyber operations to disrupt, defeat, and deter "active, systematic, and ongoing campaign[s] of attacks against the Government or people of the United States in cyberspace, including [attempts] to influence American elections and democratic political processes" by Russia, China, North Korea, or Iran. *Id*. § 1642. The NDAA for FY 2019 also affirms the authority of the President and Secretary of Defense to conduct clandestine military operations in cyberspace, including operation short of hostilities (as such term is used in the War Powers Resolution) or in areas in which hostilities are not occurring. *Id*. § 1632.

such as loss of access to data—will we generate within that system? How will those effects impact the system's functioning? Which people or processes will be affected by anticipated changes to the system's functioning? Are any of those likely to be impacted civilians or public services? Answers to these questions will drive the legal analysis.

A. U.S. Domestic Law

Let's take up considerations of U.S. domestic law first. We begin with the foundational question of domestic legal authority to conduct a military cyber operation. The domestic legal authority for the DoD to conduct cyber operations is included in the broader authorities of the President and the Secretary of Defense to conduct military operations in defense of the nation. We assess whether a proposed cyber operation has been properly authorized using the analysis we apply to all other operations, including those that constitute use of force. The President has authority under Article II of the U.S. Constitution to direct the use of the Armed Forces to serve important national interests, and it is the longstanding view of the Executive Branch that this authority may include the use of armed force when the anticipated nature, scope, and duration of the operations do not rise to the level of war under the Constitution, triggering Congress's power to declare war.[13] Furthermore, the Supreme Court has long affirmed the President's power to use force in defense of the

---

13 *See*, *e.g.*, April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities, 42 Op. O.L.C. slip op. at 9–10 (2018); Authority to Use Military Force in Libya, 35 Op. O.L.C. slip op. at 8 (2011) (quoting Deployment of United States Armed Forces to Haiti, 18 Op. O.L.C. 173, 179 (1994)); *see also* The President's Power in the Field of Foreign Relations, 1 Op. O.L.C. Supp. 49, 56 (1937) (describing President Thomas Jefferson's actions leading to the Barbary War, the invasion of Mexico by Presidents Polk and Wilson, President McKinley's agreement to suppress the Boxer Revolution, and President Roosevelt's use of the military to support Colombia to acquire the Panama Canal Zone as examples of the exercise of presidential authority to use the military without Congressional approval.).

nation and federal persons, property, and instrumentalities.[14] Accordingly, the President has constitutional authority to order military cyber operations even if they amount to use of force in defense of the United States. Of course, the vast majority of military operations in cyberspace do not rise to the level of a use of force; but we begin analysis of U.S. domestic law with the same starting point of identifying the legal authority.

In the context of cyber operations, the President does not need to rely solely on his Article II powers because Congress has provided for ample authorization. As I noted earlier, Congress has specifically affirmed the President's authority to direct DoD to conduct military operations in cyberspace.[15] Moreover, cyber operations against specific targets are logically encompassed within broad statutory authorizations to the President to use force, like the 2001 Authorization for the Use of Military Force, which authorizes the President to use "all necessary and appropriate force" against those he determines were involved in the 9/11 attacks or that harbored them.[16] Congress has also expressed support for the conduct of military cyber operations to defend the nation against Russian, Chinese, North Korean, and Iranian "active,

---

14 *See, e.g.*, The Prize Cases, 67 U.S. (2 Black) 635, 668–70 (discussing the authority of the President to resist foreign invasion and suppress insurrection); Fleming v. Page, 50 U.S. 603, 615 (1850) ("As commander-in-chief, [the President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy.").

15 *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81 § 954, 125 Stat. 1298, 1551 (2011) ("Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution (50 U.S.C. 1541 *et seq*.).").

16 Authorization for the Use of Military Force, Pub. L. No. 107–40, 115 Stat. 224 (2001).

systematic, and ongoing campaigns of attacks" against U.S. interests, including attempts to influence U.S. elections.[17]

In addition to questions of legal authority, DoD lawyers advise on the Secretary of Defense's authority to direct the execution of military cyber operations as authorized by the President and statute,[18] "including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power,"[19] and to conduct related intelligence activities.[20] Our lawyers ensure that U.S. military cyber operations adhere to the President's specific authorizations as well as the generally applicable NSPM-13.

After concluding that the operation has been properly authorized, DoD lawyers assess whether there are any statutes that may restrict DoD's ability to conduct the proposed cyber operation and whether the operation may be carried out consistent with the protections afforded to the privacy and civil liberties of U.S. persons. To illustrate, I am going to talk about two statutes and the First Amendment as examples of laws that we may consider, depending on the specific cyber operation to be conducted.

First, let's look at federal criminal provisions in Title 18 of the U.S. Code that prohibit accessing certain computers and computer networks "without authorization,"[21] or transmitting a "program, information, code, or command,"[22] that intentionally causes "any impairment to the integrity or availability" of the computer or data on it[23]—provisions found in the Computer Fraud and Abuse Act or "CFAA," as amended.[24] These provisions contain exceptions for lawfully

---

17 NDAA for FY 2019, *supra* note 12, § 1642 (2018).

18 *See* 10 U.S.C. § 113(b) (2019) (the Secretary has "authority, direction, and control over the Department of Defense").

19 10 U.S.C. § 394(a) (2018).

20 *See* 50 U.S.C. § 3038 (2016).

21 18 U.S.C. § 1030(a)(2) (2018).

22 *Id*. § 1030(a)(5)(A).

23 *Id*. § 1030(e)(8).

24 *Id*. § 1030.

authorized activities of law enforcement agencies and U.S. intelligence agencies but do not refer to U.S. military cyber operations.[25] Common sense and long-accepted canons of statutory interpretation suggest, however, that the CFAA will not constrain appropriately authorized DoD cyber operations.[26]

The CFAA was enacted to protect U.S. Government computers and critical banking networks against thieves and hackers,[27] not vice versa; it expresses no clear indication of congressional intent to limit the President from directing military actions;[28] and the more recent statutes I mentioned earlier specifically authorize or reaffirm the President's authority to direct DoD to conduct operations in cyberspace. In light of these considerations, it would be unreasonable and counterintuitive to interpret the CFAA as restricting properly authorized military cyber operations abroad against foreign actors.[29]

Second, DoD lawyers typically analyze whether the proposed cyber operation may be conducted as a traditional

---

25 *See* 10 U.S.C. § 1030(f) ("This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.").

26 *See, e.g.*, Nardone v. United States, 302 U.S. 379, 383–84 (1937); Hancock v. Train, 426 U.S. 167, 179 (1976) ("Statutes which in general terms divest pre-existing rights or privileges will not be applied to the sovereign without a clear expression or implication to that effect." (citations omitted)); Dibble v. Fenimore, 545 F.3d 208, 215 (2d Cir. 2008) (describing the "canon of construction that limits the reach of statutes of general applicability to military affairs when Congress has not explicitly provided for application to the military"); United States Assistance to Countries that Shoot Down Civil Aircraft Involved in Drug Trafficking, 18 Op. O.L.C. 148, 164 (1994) (explaining that statutes should not be "be construed to have the surprising and almost certainly unintended effect of criminalizing actions by military personnel that are lawful under international law and the laws of armed conflict").

27 *See* H.R. REP. No. 98-894, at 4 (1984).

28 *See Nardone*, 302 U.S. at 383–84.

29 *Cf.* Application of the Neutrality Act to Official Government Activities, 8 Op. O.L.C. 58, 78–80 (1984) (reasoning that subsequent Congressional enactment of provisions regulating the use of the military and covert actions provided further evidence of Congressional intent that the Neutrality Act did not apply to the activities of the Department of Defense or the Central Intelligence Agency).

military activity—or "TMA"—such that it would be excluded from the approval and oversight requirements applicable to covert action under the Covert Action Statute.[30] Because the statute does not define TMA, we look to the legislative history and a provision in the National Defense Authorization Act for Fiscal Year 2019 that clarifies that in general clandestine military activities in cyberspace constitute TMA for purposes of the Covert Action Statute, and reaffirms established congressional reporting requirements for military cyber operations.[31]

Third, DoD lawyers must assess whether a proposed operation will impact the privacy and civil liberties of U.S. persons. The practical reality of cyberspace today is that U.S. military cyber operations aimed at disrupting an adversary's ability to put information online or to distribute it across the worldwide web have the potential to affect U.S. persons' rights and civil liberties in ways that operations in physical domains do not.

Let me give you a concrete example. A core part of DoD's mission to defend U.S. elections consists of defending against covert foreign government malign influence operations targeting the U.S. electorate. The bulk of DoD's efforts in this area involve information-sharing and support to domestic partners, like the Department of Homeland Security and the Federal Bureau of Investigation. But what about a U.S. military cyber operation to disrupt a foreign government's ability to disseminate covertly information to U.S. audiences via the Internet by pretending that the information has been authored by Americans inside the United States? Can we conduct such an operation in a manner that contributes to the defense of our elections but avoids impermissible interference with the right of free expression under the First

---

30 *See* 10 U.S.C. § 3093(e) (2019); H.R. REP. No. 102-166 at 29–30 (1991) (Conf. Rep.); *see also* S. REP. No. 102–85 at 46 (1991).

31 NDAA for FY 2019, *supra* note 12, § 1632.

Amendment—including the right to *receive* information?[32] The analysis often turns on the specifics of the proposed operation—but, in short, we believe we can.

Few precedents address this issue directly; but, U.S. case law does provide a framework with at least three key strands. First, there are judicial decisions that stand for the proposition that the U.S. Government, in carrying out certain appropriately authorized activities, may incidentally burden the right to receive information from foreign sources without violating the First Amendment.[33] Second, courts have recognized a compelling government interest in protecting U.S. elections from certain types of foreign influence—especially when that influence is exercised covertly.[34] Third, government action based on the content of the speech will be suspect.[35]

In light of these precedents, DoD lawyers analyzing particular cyber operations for First Amendment compliance will consider a number of factors, including: whether the operation is targeting the foreign actors seeking to influence U.S. elections covertly rather than the information itself; the extent to which the operation may be conducted in a "content neutral" manner; and, the foreign location and foreign government affiliation of the targeted entity.

We at DoD realize that military involvement in protecting U.S. elections is a sensitive mission, even when conducted in compliance with First Amendment protections and consistent with congressional intent. Virtually any military involvement

---

32 The First Amendment protects the rights of U.S. persons "to receive information and ideas, regardless of their social worth." Stanley v. Georgia, 394 U.S. 557, 564 (1969); *see also* Martin v. City of Struthers, 319 U.S. 141, 143 (1943); Lamont v. Postmaster General, 381 U.S. 301, 306–07 (1960).

33 *See, e.g.*, Kleindienst v. Mandel, 408 U.S. 753 (1972); United States v. Alvarez, 567 U.S. 709 (2012) (plurality opinion).

34 *See* Bluman v. FEC, 800 F. Supp. 2d 281 (D.D.C. 2011), *aff'd by* Bluman v. FEC, 565 U.S. 1104 (2012).

35 *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 384 (1992) (explaining that content-based regulation of speech is permissible only when the content itself is "constitutionally proscribable").

in U.S. elections implicates the bedrock premise of maintaining civilian control of the military and our long tradition of keeping the military out of domestic politics. Accordingly, in assessing proposed operations related to elections, DoD lawyers pay particular attention to whether the proposed operation may be conducted consistent with legal and regulatory limits on the use of official positions to influence or affect the results of U.S. elections or to engage in, *or create the appearance of engaging in*, partisan politics.[36]

B. International Law

Those are some highlights of U.S. domestic law considerations that may be implicated by proposed military cyber operations; let me turn now to international law.

We recognize that State practice in cyberspace is evolving. As lawyers operating in this area, we pay close attention to States' explanations of their own practice, how they are applying treaty rules and customary international law to State activities in cyberspace, and how States address matters where the law is unsettled. DoD lawyers, and our clients, engage with our counterparts in other U.S. Government departments and agencies on these issues, and with Allies and partners at every level—from the halls of the United Nations to the floors of combined tactical operations centers—to understand how we each apply international law to operations in cyberspace. Initiatives by non-governmental groups like those that led to the Tallinn Manual can be useful to consider, but they do not create new international law, which only states can make. My intent here is not to lay out a comprehensive set of positions on international law. Rather, as I have done with respect to domestic law, I will tell you

---

36 *See* 5 U.S.C. § 7323(a)(1); DEP'T OF DEF., DIRECTIVE 1344.10, POLITICAL ACTIVITIES BY MEMBERS OF THE ARMED FORCES, ¶ 4.1.2.2 (Feb. 19, 2008), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/134410p.pdf [https://perma.cc/775C-XAR5].

how DoD lawyers address some of the international law issues that today's military cyber operations present.

I will start with some basics. It continues to be the view of the United States that existing international law applies to State conduct in cyberspace. Particularly relevant for military operations are the Charter of the United Nations, the law of State responsibility, and the law of war. To determine whether a rule of customary international law has emerged with respect to certain State activities in cyberspace, we look for sufficient State practice over time, coupled with *opinio juris*—evidence or indications that the practice was undertaken out of a sense that it was legally compelled, not out of a sense of policy prudence or moral obligation.

As I discussed a few minutes ago, our policy leaders assess that the threat environment demands action today—our clients need our advice today on how international legal rules apply when resorting to action to defend our national interests from malicious activity in cyberspace, notwithstanding any lack of agreement among States on how such rules apply. Consequently, in reviewing particular operations, DoD lawyers provide advice guided by how existing rules apply to activities in other domains, while considering the unique, and frequently changing, aspects of cyberspace.

First, let's discuss the international law applicable to uses of force. Article 2(4) of the Charter of the United Nations provides that "All 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."[37] At the same time, international law recognizes that there are exceptions to this rule. For example, in the exercise of its inherent right of self-defense a State may use force that is necessary and proportionate to respond to an

---

37 U.N. Charter art. 2, ¶ 4.

actual or imminent armed attack.[38] This is true in the cyber context just as in any other context.

Depending on the circumstances, a military cyber operation may constitute a use of force within the meaning of Article 2(4) of the U.N. Charter and customary international law. In assessing whether a particular cyber operation—conducted by or against the United States—constitutes a use of force, DoD lawyers consider whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine.[39] Even if a particular cyber operation does not constitute a use of force, it is important to keep in mind that the State or States targeted by the operation may disagree, or at least have a different perception of what the operation entailed.

Second, the international law prohibition on coercively intervening in the core functions of another State, such as the choice of political, economic, or cultural system,[40] applies to State conduct in cyberspace.[41] For example, "a cyber operation by a State that interferes with another country's ability to hold an election" or that tampers with "another country's election results would be a clear violation of the rule

---

38 *See* DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 1.11.5 (rev. Dec. 2016) [hereinafter DOD LAW OF WAR MANUAL], https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190 [https://perma.cc/2KW4-MXVY].

39 *See* Harold Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012*, 54 HARV. INT'L L.J. ONLINE 1, 3–4, https://harvardilj.org/2012/12/online_54_koh/ [https://perma.cc/8GTK-7D8C]; *see also* DOD LAW OF WAR MANUAL, *supra* note 38, § 16.3.1.

40 *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, at 108 (June 27, 1986), https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf [https://perma.cc/9MPA-QE3F].

41 *See* Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 175 (2017). https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf [https://perma.cc/9945-XV39].

of non-intervention."[42] Other States have indicated that they would view operations that disrupt the fundamental operation of a legislative body or that would destabilize their financial system as prohibited interventions.[43]

There is no international consensus among States on the precise scope or reach of the non-intervention principle, even outside the context of cyber operations. Because States take different views on this question, DoD lawyers examining any proposed cyber operations must tread carefully, even if only a few States have taken the position publicly that the proposed activities would amount to a prohibited intervention.

Some situations compel us to take into consideration whether the States involved have consented to the proposed operation. Because the principle of non-intervention prohibits "actions designed to coerce a State . . . in contravention of its rights,"[44] it does not prohibit actions to which a State voluntarily consents, provided the conduct remains within the limits of the consent given.[45]

Depending on the circumstances, DoD lawyers may also consider whether an operation that does not constitute a use of force could be conducted as a countermeasure. In general, countermeasures are available in response to an internationally wrongful act attributed to a State. In the

---

42 *Id*. at 175.

43 *See, e.g.*, U.K. Att'y Gen. Jeremy Wright QC, MP, Address on Cyber and International Law in the 21st Century (May 23, 2018) [hereinafter "U.K. Att'y Gen. Speech"], https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [https://perma.cc/L5N6-HKX8] (archived Sept. 26, 2019)) ("[T]he practical application of the principle [of non-intervention] in this context would be the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system. Such acts must surely be a breach of the prohibition on intervention in the domestic affairs of states.").

44 Memorandum from George H. Aldrich, Acting Legal Adviser, Dep't of State, on Intervention in the Internal Affairs of Other States (Oct. 25, 1974).

45 *See, e.g.*, Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 72–74 (2001).

traditional view, the use of countermeasures must be preceded by notice to the offending State, though we note that there are varying State views on whether notice would be necessary in all cases in the cyber context because of secrecy or urgency.[46] In a particular case it may be unclear whether a particular malicious cyber activity violates international law. And, in other circumstances, it may not be apparent that the act is internationally wrongful and attributable to a State within the timeframe in which the DoD must respond to mitigate the threat. In these circumstances, which we believe are common, countermeasures would not be available.

For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory. This proposition is recognized in the Department's adoption of the "defend forward" strategy: "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[47] The Department's commitment to defend forward including to counter foreign cyber activity targeting the United States—comports with our obligations under international law and our commitment to the rules-based international order.

The DoD OGC view, which we have applied in legal reviews of military cyber operations to date, shares similarities with the view expressed by the U.K. Government in 2018.[48] We recognize that there are differences of opinion among States, which suggests that State practice and *opinio juris* are presently not settled on this issue. Indeed, many States' public silence in the face of countless publicly known

---

46 *See, e.g.*, U.K. Att'y Gen. Speech, *supra* note 43.

47 DOD CYBER STRATEGY *supra* note 5, at 1.

48 *See, e.g.*, U.K. Att'y Gen. Speech, *supra* note 43.

cyber intrusions into foreign networks precludes a conclusion that States have coalesced around a common view that there is an international prohibition against all such operations (regardless of whatever penalties may be imposed under domestic law).

Traditional espionage may also be a useful analogue to consider. Many of the techniques and even the objectives of intelligence and counterintelligence operations are similar to those used in cyber operations. Of course, most countries, including the United States, have *domestic* laws against espionage, but international law, in our view, does not prohibit espionage *per se* even when it involves some degree of physical or virtual intrusion into foreign territory. There is no anti-espionage treaty, and there are many concrete examples of States practicing it, indicating the absence of a customary international law norm against it. In examining a proposed military cyber operation, we may therefore consider the extent to which the operation resembles or amounts to the type of intelligence or counterintelligence activity for which there is no *per se* international legal prohibition.[49]

Of course, as with domestic law considerations, establishing that a proposed cyber operation does not violate the prohibitions on the use of force and coercive intervention does not end the inquiry. These cyber operations are subject to a number of other legal and normative considerations.

As a threshold matter, in analyzing proposed cyber operations, DoD lawyers take into account the principle of State sovereignty. States have sovereignty over the information and communications technology infrastructure within their territory. The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not

---

49 *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 38, § 16.3.2. That is not to say that a military cyber operation that is *not* analogous to traditional or counterintelligence activity is necessarily unlawful; such an operation may, however, warrant closer scrutiny and additional analysis.

appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.

It is also longstanding DoD policy that U.S. forces will comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations.[50] Even if the law of war does not technically apply because the proposed military cyber operation would not take place in the context of armed conflict, DoD nonetheless applies law-of-war principles.[51] This means that the *jus in bello* principles, such as military necessity, proportionality, and distinction, continue to guide the planning and execution of military cyber operations, even outside the context of armed conflict.

DoD lawyers also advise on how a proposed cyber operation may implicate U.S. efforts to promote certain policy norms for responsible State behavior in cyberspace, such as the norm relating to activities targeting critical infrastructure. These norms are non-binding and identifying the best methods for integrating them into tactical-level operations remains a work in progress. But, they are important political commitments by States that can help to prevent miscalculation and conflict escalation in cyberspace. DoD OGC, along with other DoD leaders, actively supports U.S. State Department-led initiatives to build and promote this framework for responsible State behavior in cyberspace. This includes participation in the UN Group of Governmental Experts and an Open-Ended Working Group on information and communications technologies in the context of international peace and security. These diplomatic engagements are an important part of the United States'

---

50 *See* DEP'T OF DEF., DIRECTIVE 2311.01, DOD LAW OF WAR PROGRAM ¶ 1.2 (July 2, 2020), available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101p.pdf?ver=2020-07-02-143157-007 [https://perma.cc/9NRH-Q2W6]; s*ee also* DOD LAW OF WAR MANUAL, *supra* note 38, § 18.1.1.

51 DOD LAW OF WAR MANUAL, *supra* note 38, § 3.1.1.2.

overall effort to protect U.S. national interests by promoting stability in cyberspace.

Of course, the real work of analyzing specific military cyber operations in light of the domestic and international legal considerations I have mentioned falls to judge advocates and civilian attorneys at the tactical and operational levels—which is to say, many of you. As one of my predecessors, Jennifer O'Connor, noted in a speech in 2016, military operations—including cyber operations—are subject to a rigorous targeting process that involves both policy and legal reviews to ensure that specific operations are conducted consistent with the relevant authorization, domestic and international law, and any additional restraints imposed by the applicable orders. Particularly in areas like this one, in which not only the law but the domain itself is constantly evolving, I am extremely proud of the legal work many of you do for the Department of Defense and am humbled every day by your dedication to our Nation's defense.

Thank you all for what you do and for the opportunity to speak with you today.