Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace

Colonel Gary P. Corn*

Introduction

When the first host-to-host message was sent across the ARPANET in October 1969, few could have fully anticipated the degree to which the internet, and now the internet of things, would explode across the globe and revolutionize nearly every facet of public and private life.[1] Nor could anyone have predicted the degree to which it would establish an entirely new realm—cyberspace[2]—through which states could engage in traditional, and not-so-traditional, statecraft and conflict. However, it is now clear that states have fully embraced cyber operations[3] as a means to pursue their national interests and gain low-cost asymmetric advantages over their adversaries. With this new instrument of statecraft has come novel and challenging questions about the applicability of existing legal orders.[4]

The technological structure and global interconnectedness of cyberspace offer states and non-state actors a unique medium through which to operate against a broader array of targets, with decreased risk of attribution and free from the physical constraints of geography and territorial

* Judge Advocate, United States Army. Presently assigned as Staff Judge Advocate, United States Cyber Command. Previous assignments include Chief, Operational Law Branch, International and Operational Law Division, Office of the Judge Advocate General of the Army; Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff; Staff Judge Advocate, U.S. Army South; Chief of International and Operational Law, and Chief of Criminal Law, I Corps and Fort Lewis; Chief of International Law, Combined Forces Command-Afghanistan; Special Assistant United States Attorney, United States Attorney's Office for the District of Columbia; and Litigation Attorney, U.S. Army Litigation Division. The views and opinions expressed herein are those of the author and do not necessarily state or reflect those of the Department of the Army, the Department of Defense, or the United States Government.

[1] *See generally* ANDREW BLUM, TUBES: A JOURNEY TO THE CENTER OF THE INTERNET 39-67 (2012) [hereinafter TUBES].

[2] A baseline challenge for any discussion of "cyber" issues and challenges, whether technical, policy, or legal, is the lack of a commonly accepted lexicon. *See Resources: Cyber Definitions*, NATO COOPERATIVE CYBER DEF. CTR. OF EXCELLENCE, https://ccdcoe.org/cyber-definitions.html (last visited June 15, 2017) (compilation of cyber related terms and varying definitions from different states and organizations). For purposes of this chapter, I use the official Department of Defense (DoD) definition of cyberspace: "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." U.S. DEP'T OF DEF., DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 58 (Aug. 2017) [hereinafter DOD DICTIONARY].

[3] "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace." DOD DICTIONARY, *supra* note 2, at 58. *See also*, Paul Duchaine, *The Notion of Cyber Operations, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 214 (Nicholas Tsagourias & Russell Buchan eds., 2015) ("Suitable or not, the term cyber operations seems to become a common denominator for activities in cyberspace, undertaken with the aim of achieving objectives in or through this digital domain.").

[4] States have been testing the proverbial waters in cyberspace since at least 2007, when Estonia came under broad and sustained cyber operations, which some attribute to Russia, after the Estonian government moved a Soviet-era statue commemorating World War II from the center of Tallinn, its capital. ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 60-66 (2016) [hereinafter THE HACKED WORLD ORDER]. Despite a steadily increasing number of aggressive, malicious, and complex cyber operations since then, states have struggled to achieve clarity or consensus on the applicable normative frameworks governing cyber operations, creating continued and at times debilitating uncertainty. *See* Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, 8 HARV. NAT'L SEC. L. J. 239, 242 (2017).

DRAFT

boundaries.[5] Not only does cyberspace defy geopolitical borders, but it is predominantly owned, operated, and managed by the private sector, resides largely outside of national control, is integrated with the operation of critical infrastructures, and forms the backbone of commerce, governance, and national security.[6] At an increasing rate, adversaries are leveraging and exploiting the numerous technical, policy, and legal ambiguities surrounding cyberspace to conduct a range of intrusive and increasingly aggressive activities to the point where cyber threats are now considered a major, if not the most significant, strategic threat to the United States.[7]

While some of these cyber operations have been conducted as part of on-going armed conflicts,[8] the vast majority have taken place in the so-called "Gray Zone"—the far more uncertain space between war and peace. Alternatively described as gray-zone challenges or gray-zone conflicts, these activities are more accurately understood as actions that are coercive and aggressive in nature and rise above normal, everyday peacetime geo-political competition, "but that [are] deliberately designed to remain below the threshold of conventional military conflict and open interstate war."[9] Although these activities are not limited to any single domain or modality, cyberspace offers fertile terrain for gray-zone confrontation.[10] Russia's hacking of the

---

[5] *See* Jeffrey M. Reilly, *Multi-domain Operations: A Subtle but Significant Transition in Military Thought*, AIR & SPACE POWER J. (2016) ("The integrated nature of cyberspace in the realm of power grids, transportation networks, communications, and financial systems represents a lucrative target that would allow an adversary to cause massive physical damage and economic disruption to the US homeland.").

[6] JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-12(R), CYBERSPACE OPERATIONS I-1 (Feb. 5, 2013) (hereinafter JP 3-12].

[7] U.S. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 9 (2015) [hereinafter DOD CYBER STRATEGY].

[8] States, to include the United States, have embraced cyber capabilities as a means and method of warfare, are accelerating efforts to incorporate them into their warfighting arsenals, and in some cases have conducted cyber operations as part of on-going hostilities. *See* Barak Obama, Statement by the President on Progress in the Fight Against ISIL (Apr. 13, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/04/13/statement-president-progress-fight-against-isil ("Our cyber operations are disrupting [ISIS] command-and-control and communications."); Lolita C. Baldor, *APNewsBreak: US Military Launches Campaign of Cyberattacks Against Islamic State*, ASSOCIATED PRESS (Feb. 26, 2016), https://apnews.com/9c93a8c408c443399ebaf88ecc7f3d2e/apnewsbreak-dod-launches-aggressive-cyberwar-against. *See generally* ENEKEN TIKK ET AL., INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 66-89 (2010) (discussing Russia's use of cyber operations during the 2008 Georgia conflict); NATO COOPERATIVE CYBER DEF. CTR. OF EXCELLENCE, CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE (Kenneth Geers ed., 2015) (discussing Russia's use of cyber operations against and during its conflict with Ukraine). When employed during an existing armed conflict, there is little question that the *jus in bello* rules apply to cyber operation, even if subsidiary questions remain as to precisely how specific provisions apply to this developing technology. *See* U.S. DEP'T OF DEF. OFFICE OF GEN. COUNSEL, DEPARTMENT OF DEFENSE LAW OF WAR MANUAL (UPDATED DEC. 2016) 994, 996-97 (2015) [hereinafter DOD LAW OF WAR MANUAL]. There is far less clarity on how international law regulates states' conduct of cyber operations below the threshold of armed conflict.

[9] Hal Brands, *Paradoxes of the Gray Zone*, FOR. POL. RESEARCH INST. (Feb. 5, 2016), https://www.fpri.org/article/2016/02/paradoxes-gray-zone; *see also*, U.S. SPECIAL OPERATIONS COMMAND, WHITE PAPER: DEFINING GRAY ZONE CHALLENGES 1 (Apr. 2015), https://army.com/sites/army.com/files/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf. ("[G]ray zone challenges are defined as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality.") [hereinafter U.S. SPECIAL OPERATIONS COMMAND, WHITE PAPER].

[10] Some of the literature on the so-called "gray zone" speaks in terms of gray-zone conflict. *See, e.g.*, Nora Bensahel, *Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex*, FOR. POL.

Democratic National Committee and its related attempt to interfere with the 2016 presidential election are prime examples.[11]

Defending against gray-zone cyber threats undoubtedly starts with improving the protection and resilience of information technology and telecommunications (ITT) networks and systems. But cybersecurity[12] alone is not enough. Information technology and the internet were not constructed with security in mind, and efforts to eliminate vulnerabilities are erratic, dependent on immature and ineffective market forces and regulatory schemes, and consistently outpaced by relatively low-cost exploitation technologies and techniques.[13] In the parlance of deterrence strategy, denying the benefit of cyber operations to adversaries—especially in the limited sense of internal cybersecurity measures—will only be marginally effective at best.[14] At least for the near- to mid-term, confronting the growing national security threat posed by cyber threats will require more holistic strategies that incorporate both traditional deterrence and counter-cyber operations conducted outside the context and below the threshold of armed conflict.

Today's threat environment also necessitates the employment of cyber capabilities[15] in pursuit of broader national security objectives—for example, to collect intelligence, deter adversaries,

---

RESEARCH INST. (Feb. 13, 2017), https://www.fpri.org/article/2017/02/darker-shades-gray-gray-zone-conflicts-will-become-frequent-complex (discussing in terms of gray-zone conflicts); MICHAEL J. MAZARR, MASTERING THE GRAY ZONE: UNDERSTANDING A CHANGING ERA OF CONFLICT 55-78 (2015) (same); David W. Barno & Nora Bensahel, *Fighting and Winning in the "Gray Zone"*, WAR ON THE ROCKS (May 19, 2015) https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone (same). Because of the specific *jus ad bellum* and *jus in bello* connotations raised by the term conflict, the author prefers the term confrontation to describe the aggressive cyber activities short of a use of force or armed conflict that are the focus of this chapter.

[11] *See* Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html; *see also* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. 1, 2 ("The DNC hacks epitomized the grey zone strategy.").

[12] Cybersecurity, distinct from, albeit overlapping with, cyber defense, is defined as the "[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." U.S. DEP'T OF DEF., INSTRUCTION 8500.01, CYBERSECURITY 55 (Mar. 14, 2014) (quoting THE WHITE HOUSE, NAT'L SECURITY PRESIDENTIAL DIRECTIVE-54/HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-23, 3 (Jan. 8, 2008)).

[13] As the Defense Science Board noted in a recent study, "Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures." Memorandum from the Co-Chairs, Defense Science Board Task Force to the Chairman, Defense Science Board, subject: Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence (Feb. 2017), *in* DEP'T OF DEF., DEF. SCIENCE BOARD, TASK FORCE ON CYBER DETERRENCE (Feb. 2017).

[14] *See id.* at 3-7.

[15] The term "cyberspace (or cyber) capabilities" is, like most cyber terms, susceptible to varied meanings. For example, for purposes of its instruction governing legal reviews of weapons and cyber capabilities, the United States Air Force defines cyber capabilities narrowly as "any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities" but excludes from this definition "a device or software that is solely intended to provide access to an adversarial computer system for data exploitation." DEP'T OF AIR FORCE, INSTRUCTION 51-402, LEGAL REVIEWS OF WEAPONS AND CYBER CAPABILITIES (Jul. 27, 2011). In contrast, the *DoD Cyber Strategy* uses the term in the broader sense of discrete cyber-related means and ways, to include devices and software, which can be employed to perform a set of tasks to execute a specified course of action and achieve a desired effect. *See generally*, DOD CYBER STRATEGY, *supra* note 7, at 9 (stating, for example, that it is a DoD goal to build and maintain ready forces and capabilities to conduct cyberspace

control conflict escalation, and achieve lawful ends in war. What is needed is a comprehensive national strategy that fully integrates cyber capabilities and operations into wider efforts to deter, defend against, and respond to both cyber and non-cyber gray-zone challenges, as well as more traditional national security threats, and to control conflict escalation and defeat adversaries should deterrence and escalation control fail.[16] While a number of technical and policy questions complicate comprehensive strategy development, this chapter focuses on the legal complexities, both domestic and international, associated with employing cyber capabilities in defense of the United States and in furtherance of national security objectives in the complex and ambiguous security environment below the threshold of armed conflict, especially in the so-called zone of twilight (i.e., the gray-zone) between peace and war.[17] Understanding how existing legal frameworks apply to gray-zone cyber operations is critical to properly characterizing threats and defining available response options under domestic and international law.

For example, consider Iran's well documented distributed denial-of-service (DDoS) campaign against the U.S. financial sector from 2011 to 2013, involving a sophisticated, globally-distributed network of compromised computer systems—a botnet.[18] According to the Department of Justice, "attacks disabled victim banks' websites, prevented customers from accessing their accounts online and collectively cost the victims tens of millions of dollars in remediation costs as they worked to neutralize and mitigate the attacks on their servers."[19] Did

operations); *see also* U.S. DEP'T OF DEF., DIRECTIVE 7045.20, CAPABILITY PORTFOLIO MANAGEMENT, 8 (Sept. 25, 2008) (defining capability). Unless otherwise stated, the term is used throughout this chapter in the broader sense reflected in the *DoD Cyber Strategy* as any cyber-related means or ways.

[16] *See* DOD CYBER STRATEGY, *supra* note 7, at 13-15 (listing five strategic goals). The development of a comprehensive national strategy for effectively developing and employing cyber capabilities to confront gray zone challenges is complicated by a number of cross-cutting policy goals and other factors, to include legal uncertainties. For example, it is United States policy "to promote an open, interoperable, secure, and reliable internet that enables international trade and commerce, strengthens international security, and fosters free expression and innovation." BARRACK OBAMA, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 8 (May 2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE]; s*ee also*, DOD CYBER STRATEGY, *supra* note 7, at 1. If the internal tensions among these goals are not readily apparent, one need only consider the growing number of events, such as the Democratic People's Republic of North Korea's hack of Sony Pictures, China's hack and exploitation of the Office of Personnel Management, and Russia's hack of the DNC, to realize that the very openness and interoperability we seek creates inherent security vulnerabilities. The policy goal of exercising due diligence and the need to assert jurisdiction and control over domestic cyber infrastructure in order to achieve any measurable degree of cybersecurity at some level risks conflict with commitments to free expression and privacy, and arguably undercuts the United States' advocacy for a multi-stakeholder governance model for the Internet. *See* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra*, at 10. *See generally* Kristen Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317 (2015) (discussing the various proposed approaches to international internet governance).

[17] Johnson v. Eisentrager, 339 U.S. 763, 769 (1950); *see also*, Michael Jefferson Adams, *Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace*, 5 HARV. NAT'L SEC. L. J. 377, 422-25 (2014).

[18] Dep't of Justice, Office of Pub. Affairs, *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector* (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged [hereinafter DoJ Press Release]. A DDoS attack involves flooding a target server, website or other network resource with incoming messages, connection requests or malformed packets sent from multiple compromised computer systems or devices—a botnet—distributed globally across geographic borders. The flood of traffic to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems. *Definition: Distributed Denial of Service (DoS) Attack*, TECHTARGET http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

[19] DoJ Press Release, *supra* note 18.

the individual DDoS attacks or the campaign as a whole constitute a use of force against the United States? If not, did they constitute a prohibited intervention under customary international law (CIL) or the breach of some other established international obligation? What do domestic and international law say about employing cyber capabilities to deter, prevent, or counter such a DDoS or similar threats in the future?

Consider also former Chairman of the Joint Chiefs of Staff General Martin Dempsey's comments when announcing what has been dubbed the Department of Defense's "Left-of-Launch" air and missile defense program in 2013, where he noted the importance of integrating new, non-kinetic capabilities such as cyber operations into the traditional anti-ballistic missile toolset.[20] The strategy envisions using cyber and other kinetic and non-kinetic capabilities to prevent adversaries "from effectively employing any of [their] air and missile weapons" against the United States or its allies.[21] In contrast to other capabilities, cyber operations generally require gaining advanced, persistent, and clandestine access to the target system to be effective in such a preemptive role. Would such an operation constitute intelligence exploitation, traditional operational surveillance and reconnaissance, or operational preparation of the environment? Does the President have unilateral authority to direct this type of operation, or must Congress play a role? Would the clandestine nature of the operation bring it within the ambit of covert action or might it be conducted under the intelligence or traditional military activities exceptions to the Covert Action Statute?[22] From an international law perspective, would such an operation constitute a use of force or the imminent threat thereof, or would it be governed by the less well-defined legal framework regulating inter-state activities below the use-of-force threshold?

These are just a sampling of the myriad complex legal questions implicated by cyber operations conducted outside the context of armed hostilities.[23] In such a rapidly evolving environment, the development of legal and policy parameters for governing state behavior in cyberspace—

---

[20] David E. Sanger & William J. Broadmarch, *Trump Inherits a Secret Cyberwar Against North Korean Missiles*, N.Y. TIMES (Mar. 4, 2017), https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=span-ab-top-region&region=top-news&WT.nav=top-news&_r=0.

[21] MARTIN E. DEMPSEY, JOINT INTEGRATED AIR AND MISSILE DEFENSE: VISION 2020 (Dec. 5, 2013); *see also* Riki Ellison, *Left of Launch*, MISSILE DEFENSE ADVOCACY ALLIANCE (Mar. 16, 2015), http://missiledefenseadvocacy.org/alert/3132 ("The strategy is based on a preemptive strike with new non kinetic technologies, such as electromagnetic propagation, cyber as well as offensive force to defeat nuclear ballistic missile threats before they are launched, known as 'left of launch.' The strategy is to attack by electronic embedment or through the electronic radar signatures of the threat's command and control systems and the targeting systems of the threatening ballistic missiles.").

[22] 50 U.S.C. § 3093 (2012).

[23] Many of these difficult issues can also arise during the course of armed hostilities. As noted, *supra* note 8, cyber capabilities constitute means and methods of warfare subject to the LOAC. But not all cyber tools and operations are the same, and while some may by design involve destructive consequences, more often than not they will employ elegantly simple and precisely targeted technical means that generate minimal effects on the functionality of the targeted system, but support or achieve greater operational objectives. Recognizing the truism that LOAC applies to these operations is much easier than identifying which specific provisions of the LOAC are triggered and how they apply. For instance, does the particular cyber effect to be delivered constitute an in bello attack subject to the full panoply of the LOAC targeting rules, or is it something less? If less, how exactly does the LOAC regulate the operation? *See* DOD LAW OF WAR MANUAL, *supra* note 8, at 1003-05; TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 414-20 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

domestically and internationally—have failed to keep pace with the threat.[24] Suffice it to say, attorneys charged with reviewing and advising on the legality of cyber operations are continuously called on to address difficult issues of first impression. This chapter will identify and consider some of the more challenging domestic and international legal issues raised by the conduct of cyber operations in the gray zone between peace and war. Before turning to these questions, the chapter offers a brief description of the gray-zone concept in Part I, followed by a description of the cyberspace domain and the general nature of cyber operations in Parts II and III respectively. The chapter then turns in Part IV to a selective review of the domestic and international law challenges to conducting gray-zone cyber operations.

I. "Gray Zone" Security Challenges

In November 2014, a group calling itself the Guardians of Peace (GOP) began releasing a trove of Sony Pictures Entertainment's confidential and proprietary information—exploited data that included copies of previously un-released films, personal information about Sony Pictures employees and their families, e-mails between employees, and information about executive salaries at the company.[25] The GOP's stated purpose was to force Sony to cancel the release of its film *The Interview*, a satirical comedy about a plot to assassinate North Korean leader Kim Jong-Un.[26] The data releases were accompanied by various threats against the company and its employees, as well as threats of terrorist attacks against cinemas planning to screen the film. The hack also involved significant wiping of data and damage to Sony's IT systems.[27] In December 2014, the Federal Bureau of Investigation officially attributed the malicious cyber operations to the Democratic Republic of North Korea (DPRK), and the United States levied sanctions on the DPRK in response.[28]

In his initial statements addressing the Sony hack, President Obama vowed the United States would "respond proportionately and in a space, time and manner that we choose," but did not categorize the nature of the attack.[29] And although his Secretary of Homeland Security described the episode as "not just an attack against a company and its employees," but rather as "an attack on our freedom of expression and way of life,"[30] days later President Obama stated his view that the Sony hack was not an act of war, but instead "an act of cyber vandalism."[31] Senator John McCain, among others, disagreed, noting, "It's more than vandalism. It's a new form of warfare that we're involved in, and we need to react and react vigorously."[32] The varied descriptions and categorizations of the Sony hack were indicative of legal and political

---

[24] For example, despite the rapidly increasing rate and severity of malicious cyber activity, especially state-sponsored, the United Nations Group of Governmental Experts (UNGGE) has made limited, incremental progress.
[25] THE HACKED WORLD ORDER, *supra* note 4, at 51-54.
[26] *Id.*
[27] *Id.; see also* David E. Sanger et al., *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014), https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0.
[28] THE HACKED WORLD ORDER, *supra* note 4, at 51-54.
[29] David E. Sanger et al., *Obama Vows a Response to Cyberattack on Sony*, N.Y. TIMES (Dec. 19, 2014), https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0.
[30] *Id*.
[31] David Jackson, *Obama: We're not at cyberwar with North Korea*, USA TODAY (Dec. 21, 2014), https://www.usatoday.com/story/news/politics/2014/12/21/obama-cnn-hack-attack-north-korea-sony/20723053.
[32] *Id*.

ambiguities that persist with respect to cyber operations, ambiguities that the DPRK exploited through aggressive tactics in an attempt to influence behavior in the United States—the hallmark of what many now describe as gray-zone conflict.[33]

Although frequently described as a specific type of conflict or security challenge, the gray zone is better understood as a distinct operating environment falling along the conflict continuum somewhere between normal, peacetime geo-political interactions and overt warfare.[34] It is an environment characterized by inherent legal, policy, and factual ambiguities which state and non-state actors exploit to engage in particularly aggressive actions designed to alter the status quo and achieve strategic objectives normally associated with war, but without clearly violating established international norms or crossing conventional thresholds.[35] In this way, gray-zone actors pursue their objectives while reducing the risk of triggering open warfare. Gray-zone threats manifest in and through all domains, not just cyberspace.[36] However, the *sui generis*, dynamically evolving, and normatively uncertain nature of cyberspace offers a particularly lucrative medium for gray-zone threat actors.[37]

Some point to gray-zone approaches as "mostly the province of revisionist powers—those actors that seek to modify some aspect of the existing international environment" to achieve objectives "normally associated with victory in war."[38] Certainly, there are a number of states engaging in what some describe as "shadow wars"—employing highly aggressive tactics that, although they "may not trigger conventional military responses . . . nonetheless pose great strategic risks" to targeted states.[39] Aggressive cyber operations like the previously discussed Sony hack frequently feature prominently in these gray-zone strategies, and failure to actively counter these threats essentially cedes strategic initiative to revisionist states and non-state actors and steadily erodes the rules-based, international order.[40]

DRAFT

---

[33] The gray-zone concept is not new, but has gained increased attention among policymakers, strategists, and scholars as of late. *See* Joseph L. Votel et al., *Unconventional Warfare in the Gray Zone*, 80 JOINT FORCES Q. 101, 102 (2016); JOHN CHAMBERS, COUNTERING GRAY-ZONE HYBRID THREATS: AN ANALYSIS OF RUSSIA'S "NEW GENERATION WARFARE" AND IMPLICATIONS FOR THE US ARMY 13 (2016), https://mwi.usma.edu/countering-gray-zone-hybrid-threats-mwi-report ("Recently, the concept of gray-zone conflict emerged amongst scholars, strategists, and, particularly, members of the United States special operations community); Brands, *supra* note 9 (describing gray-zone challenges as both the wave of the future and a blast from the past).

[34] CHAMBERS, *supra* note 33, at 13 ("Consequently, the gray zone is an [operating environment] and not a type of conflict, in the same way that urban or desert warfare refers to the [operating environment] in which conflict takes place and is not a distinct form of conflict.").

[35] U.S. SPECIAL OPERATIONS COMMAND, WHITE PAPER, *supra* note 9, at 1 (Gray-zone challenges "are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks.").

[36] Russia's actions aimed at destabilizing and dismembering Ukraine, China's "creeping expansionism" in the South China Sea, and Iran's use of subversion and proxy warfare to expand its influence in the Middle East are all cited as examples of gray-zone security challenges. CHAMBERS, *supra* note 33, at 16; Brands, *supra* note 9.

[37] *See, e.g.,* Andy Greenberg, *How An Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017), https://www.wired.com/story/russian-hackers-attack-ukraine (discussing Russia's cyber operations against the Ukraine power grid as a test bed for operations against the United States).

[38] Brands, *supra* note 9.

[39] Barno & Bensahel, *supra* note 10.

[40] *See generally*, Schmitt, *Grey Zones in the International Law of Cyberspace*, *supra* note 11.

However, recalling that the gray zone is properly understood not as a specific form of conflict, but rather as a description of the strategic environment constituting a "segment along the conflict continuum," it becomes clear that non-revisionist states must also be prepared and willing to operate in the gray zone to shape strategic conditions, deter and counter adversaries, and deny them "decisive positional advantage."[41] As was the case throughout the Cold War, today's threat environment calls for "'the employment of all the means [of national power], short of war, to achieve . . . national objectives.'"[42] To be effective, deterrence and counter-cyber strategies must incorporate cyber capabilities and operations, not just in a cyber-on-cyber construct, but more broadly across the full spectrum of military operations conducted below the threshold of armed conflict. Furthermore, regardless of how gray the zone may be, legitimacy and adherence to the rule of law remain key components to executing successful strategies and military operations within it. This requires navigating the relatively unchartered legal waters of the unique and constantly evolving terrain of cyberspace.

II. The Cyberspace Domain

The novel, hyper-dynamic, and highly technical nature of the globally-interconnected ITT environment of cyberspace has generated significant uncertainty about the application of existing legal frameworks.[43] Adding to this uncertainty is the fact that cyber operations can generate a wide range of effects in both scope and scale, from subtle manipulation to significant destruction, directly within and against components of cyberspace as well as indirectly against the external systems and users that depend on it.[44] Also, cyber operations frequently leverage or are conducted in conjunction with other capabilities such as space, electronic warfare, and information operations, all of which are governed by distinct authorities and raise additional legal complexity.[45]

Much of the present domestic and international legal order is founded on certain baseline premises about, *inter alia*, Westphalian geography and related concepts of sovereignty and the sovereign equality of states, the notion of state responsibility and the associated legal and political requirement of attribution, and traditional dichotomies between war and peace and the corresponding roles of intelligence, military, and law enforcement operations. The construct of cyberspace challenges each of these premises in fundamental ways.[46]

Although the internet is still relatively young, military doctrine has quickly evolved to add cyberspace as the newest of five interdependent domains through which military forces must be able to defend and operate, just as they have traditionally done in the physical domains of air,

---

[41] Votel et al., *supra* note 33, at 108.
[42] *Id.* at 102 (quoting George F. Kennan, *Policy Planning Staff Memorandum* (May 4, 1948), *available at* http://academic.brooklyn.cuny.edu/history/johnson/65ciafoundings3.htm.).
[43] *See*, *e.g.,* Schmitt, *Peacetime Cyber Responses*, *supra* note 4, at 242.
[44] The Russians use of cyber operations to generate effects in the information space is an example.
[45] JP 3-12, *supra* note 6, at II-1.
[46] *See* Gary D. Brown et al., *Military Cyberspace Operations*, 158-62, *in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE (Geoffrey S. Corn et al. eds.) (2016) [hereinafter Brown et al., *Military Cyberspace Operations*]; Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. OF NAT'L SECURITY LAW & POL'Y 539, 580 (2012).

land, maritime, and space.[47] From a military perspective, the basic operational objectives in cyberspace are the same as in the four physical domains: secure freedom of action to create desired military effects and the ability to deny such freedom of action to adversaries.[48] But cyberspace differs from the physical domains in significant ways. Cyberspace is a man-made, ubiquitously interconnected environment stretching and operating across international boundaries, under constant construction and modification.[49] It is built on predominantly civilian infrastructure that functions according to its own evolving protocols and logic. Further, some portion of cyberspace resides in all the other domains, and operations in all the other domains are dependent, to an increasing degree, on cyberspace and cyber operations.[50] The domain is a multifaceted, layered eco-system, each component of which has unique characteristics and complexities that may be relevant to assessing the legality of any particular cyber operation.

In broad terms, cyberspace is composed of three interdependent layers—physical, logical, and persona—in or against which cyber operations can be conducted.[51] At any given moment (or nano-second in the case of the logical layer), the operationally relevant components of each layer reside somewhere on the globe, usually within the sovereign territory of or subject to the control of at least one state. Although less than precise, planners and operators conceptualize this geographic aspect as blue (friendly), red (adversary), and gray (third-party) space.

The physical network layer of cyberspace is comprised of both a geographical and physical network component. Simply put, the hardware, networking devices, wires, cables, optical links, satellite uplinks, and other physical infrastructure that make up ITT are tangible objects located somewhere in the geographic realm.[52] This geographic reality implicates matters of sovereignty and jurisdiction, highly relevant considerations in assessing the applicability of particular domestic or international legal regimes.[53]

The logical layer of cyberspace is more difficult to conceptualize, and is often untethered from geography. Generically referred to as the "code," it is comprised of the software and protocols[54]

---

[47] JP 3-12, *supra* note 6, at I-2. *See also*, DOD LAW OF WAR MANUAL, *supra* note 8, at 995 ("As a doctrinal matter, DoD has recognized cyberspace as an operational domain in which the armed forces must be able to defend and operate, just like the land, sea, air, and space domains."). The North Atlantic Treaty Organization (NATO) also recognizes cyberspace as an operational domain. *See* NATO, *Warsaw Summit Communiqué*, ¶ 70 (July 9, 2016), http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[48] LARRY D. WELCH, CYBERSPACE—THE FIFTH OPERATIONAL DOMAIN 7 (2011), https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf.

[49] "Every computer, router, or device attached, or removed, from cyberspace changes the cyberspace domain as a whole." WILLIAM D. BRYANT, INTERNATIONAL CONFLICT AND CYBERSPACE SUPERIORITY: THEORY AND PRACTICE 58 (2016). So to do changes to the various protocols and programs running in cyberspace, as well as advancements in the computing power and capability of ITT writ large. *See id.*

[50] WELCH, *supra* note 48, at 3.

[51] JP 3-12, *supra* note 6, at I-2. *See also* ALEXANDER KLIMBURG & PHILIPP MIRTL, CYBERSPACE AND GOVERNANCE—A PRIMER 5-9 (2011), https://issafrica.org/acpst/uploads/Klimburg_Cyberspace_and_Governance-A_primer.pdf; DAVID CLARK, CHARACTERIZING CYBERSPACE: PAST, PRESENT AND FUTURE 1-4 (2010), https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf.

[52] JP 3-12, *supra* note 6, at I-2 to I-3.

[53] *See* TALLINN 2.0, *supra* note 23, chs. 1, 3 (discussing sovereignty and jurisdiction respectively).

[54] A protocol "defines the rules or conventions that are necessary to obtain a certain goal (e.g. communication)." KLIMBURG & MIRTL, *supra* note 51, at 7. Software "is the computer program

that combine to generate specific outputs or services, which can themselves combine to create inexhaustible possibilities of new outputs or services such as websites, search engines, podcasts, encrypted communications platforms, and social networking sites.[55] The logical layer also includes the content or information that is created, captured, stored, processed, and transmitted in or through cyberspace.[56] With the accelerating move to cloud-based computing, this data can be stored on servers or in data centers anywhere around the globe, and be dynamically transferred from one location to another in milliseconds. The intangible, highly-mutable, and often ephemeral nature of the logical layer is laced with vulnerabilities (defects in the basic code) and "opens inexhaustible possibilities to create" not only new outputs or services, but also malware—software programs designed to damage or do other unwanted actions on a computer system such as Trojans, viruses, and worms.[57]

Lastly, the persona layer of cyberspace, sometimes referred to as the social layer, is made up of the people, either individually or as representatives of public or private entities, who use the rules that apply in the logical network layer to develop a digital representation of themselves through which they interact in and with cyberspace to achieve outcomes.[58] For example, john.doe@email.com is an alias that allows its owner to transact in cyberspace. To interact in cyberspace, the actor must first "access" cyberspace through a device capable of connecting to the internet. Generally, each device has a unique identifier such as an Internet Protocol (IP) address[59] or a Mobile Equipment Identifier (MEID).[60] These identifiers are not always static, and the degree of ownership or affiliation of the device to the actor can vary.

The nature of the logical layer affords individuals and entities in cyberspace the ability to easily create multiple cyber aliases, which can vary in the degree to which they accurately reflect the true identity of the owner, and each single virtual identity can have multiple users.[61] The components of these virtual identities, or cyber-personas, are normally not linked to any single physical location, and thus do not necessarily correspond to the location of the actual owner. The logical layer of cyberspace also affords these actors a constantly expanding and evolving array of technical means to obfuscate their identity and internet activity. These include instruments such as IP anonymizers like The Onion Router (TOR)[62] and Virtual Private Networks (VPN),[63] as well as the use of coopted nodes. In short, the attributes of cyberspace

---

that implements these protocols." *Id.*

[55] *Id*.

[56] Some consider the information that is stored, transmitted, and transformed in cyberspace to be a fourth layer. *See* KLIMBURG & MIRTL, *supra* note 51, at 5-9; CLARK, *supra* note 51, at 1-4.

[57] KLIMBURG & MIRTL, *supra* note 51, at 7.

[58] JP 3-12, *supra* note 6, at I-3 to I-4; KLIMBURG & MIRTL, *supra* note 51, at 8-9.

[59] An identifier assigned to each computer and other device connected to the internet that is used to locate and identify the node in communications with other nodes on the network.

[60] An electronic serial number assigned to every mobile computing device, such as cell phones.

[61] JP 3-12, *supra* note 6, at I-3 to I-4; KLIMBURG & MIRTL, *supra* note 51, at 8-9.

[62] The Onion Router, or Tor, is a network designed to provide anonymous access to the internet. Tor uses layered encryption and routes a user's internet traffic through a number of nodes, each of which decrypts only a layer of the transmission data, and is only aware of the IP addresses in front of the node and behind it, so that the sender and cannot be identified at any point along the transmission chain. *See What is Tor?,* TOR VS.VPN, https://www.bestvpn.com/tor-vs-vpn (last visited Aug. 22, 2017).

[63] A Virtual Private Network (VPN) is a way of ensuring privacy when accessing the internet. When using a VPN, a user's computer or mobile device connects through an encrypted tunnel to a VPN server through an Internet Service

facilitate anonymity, complicating accurate identification of cyber actors and attribution of actions conducted in cyberspace for purposes of assessing legal obligations and responsibilities.[64]

To illustrate the complexities presented by the interrelated components of cyberspace and the unique nature of cyber operations, consider the example of a non-state terrorist organization that uses the internet as a means to command and control its operations, recruit members, develop and distribute propaganda, and conduct malicious cyber activities against its adversaries. The group's cyber actors, through multiple cyber personas, may operate from within the sovereign territory of one or several different states, utilizing commercially procured or coopted physical and virtual civilian ITT infrastructure located in yet other states. They may use various tools and techniques to obscure their identities and activities, and cause data to transit the internet globally. Cyber operations aimed at disrupting these activities raise layered questions about the appropriate domestic legal basis and framework for conducting them, as well as the international law rights of and obligations owed to the various other states whose territory and sovereignty may be implicated. Addressing these issues requires an in-depth, case-by-case understanding and review of the exact nature of the cyber operation in question, and the effects it is intended or anticipated to generate.

For sound reasons, many of the details regarding existing cyber capabilities and employment options are not publically available. However, some general observations about how cyber operations are constructed and executed are possible.

III. The Anatomy of Cyber Operations

A. Three Purpose-based Categories of Cyberspace Operations

Recall that cyber capabilities are considered the means and ways used to achieve specific ends, or effects, in and through cyberspace.[65] In this sense, cyber is not unlike traditional military operations, where the doctrinal characterization and corresponding legal regulation of the means and methods used to achieve military ends depend on the context within which, and the purpose for which, they are employed. Thus, consistent with other military operations, DoD doctrine divides cyber operations into three broad, purpose-based categories: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense Information Network (DODIN) operations, which are strictly limited to measures internal to DoD networks.[66]

Provider, or ISP. Because the traffic is encrypted, the ISP can see only that data is being transferred to the VPN server. The data is protected in transit from decryption and view. *See id.*

[64] *See* TALLINN 2.0, *supra* note 23, at 115-16; Scott C. Shackleford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem* 200-01, *in* CONFERENCE ON CYBER CONFLICT PROCEEDINGS 2010 (C. Czosseck and K. Podins eds. 2010) (discussing the technical and legal challenges of attribution in cyberspace, and stating that "[a]ttribution of a cyber attack to a State is a, if not *the*, key element in building a functioning legal regime to mitigate . . . attacks." (emphasis in original)), https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf.

[65] *Supra* note 3.

[66] JP 3-12, *supra* note 6, at II-2 to II-3. Both DODIN operations, as well as the internal defensive measures component of DCO, are limited to actions internal to DoD networks, and are at times indistinguishable from

Offensive cyberspace operations are defined as "cyberspace operations intended to project power by the application of force in or through cyberspace."[67] The definition is somewhat misleading, in that the "force" applied rarely involves actual physical damage or harm, and so the effect delivered often times will not constitute force in the *jus ad bellum* or *jus in bello* senses of the term.[68] Essentially, OCO can be analogized to traditional fire and maneuver operations conducted to obtain positional advantage over and defeat an adversary, usually, but not exclusively, in the context of an already existing armed conflict.[69] For example, a cyber operation might be conducted to temporarily disable an adversary's anti-aircraft radar system, achieving the same operational effect as electronic jamming through a different means. Another example is an operation directed at disrupting or degrading the functionality of strategic-level targets, like the supervisory control and data acquisition (SCADA) systems[70] of adversary railroads or ports.[71]

In contrast, DCO are defined as "[p]assive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems."[72] This definition of DCO can be confusing, because of its reference to both passive and active operations, as well as its overlap with DODIN operations.[73] That is, a significant portion of DCO are limited to internal measures, best understood as falling under the protection function of joint military operations.[74] For purposes of this chapter, the more salient component of DCO are DCO response actions (DCO-RA), which are defined as "[d]eliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems."[75] Again, this definition is imprecise due to its under inclusiveness. Like any military capability, cyber operations can be a viable option for defending the Nation and its interests in more than a counter-cyber role.[76] Accordingly, like OCO, DCO-RA are intended to generate effects outside of friendly, or blue-space, networks and systems.[77] But where the intent of conducting the cyber operation is to counter or respond to actual or imminent threats directed against the United States or its interests, *to include* malicious cyber activity, the operation would be a DCO, not an OCO.

---

cybersecurity measures. S*ee supra* note 12. While these operations implicate a number of domestic legal issues, starting with the Fourth Amendment, they are not addressed in this chapter.

[67] JP 3-12, *supra* note 6, at GL 4.

[68] *Id.* at II-5.

[69] *See generally*, JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-0, OPERATIONS, ch. III (discussing joint functions, to include fires and movement and maneuver)[hereinafter JP 3-0].

[70] A system of software and hardware elements used by industrial organizations to, *inter alia*, control industrial processes locally or at remote locations and directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software. *See What is SCADA?*, INDUCTIVE AUTOMATION, https://inductiveautomation.com/what-is-scada (last visited Aug. 24, 2017).

[71] *See* DOD LOW MANUAL, *supra* note 8, at 210 & n. 161 (describing ports and railroads as legitimate war supporting military objectives).

[72] JP 3-12, *supra* note 6, at II-2.

[73] *See id.*, at II-2 to II-3.

[74] JP 3-0, *supra* note 69, at II-35 to II-42 (describing the joint function of protection).

[75] JP 3-12, *supra* note 6, at II-3.

[76] *See*, *e.g.*, *supra* notes 20-21 and accompanying text (discussing "Left-of-Launch" strategy); DOD CYBER STRATEGY, *supra* note 7, at 26 (discussing integrating cyber options into broader DoD plans).

[77] JP 3-12, *supra* note 6, at II-7.

The operational categories laid out in DoD doctrine are further broken down into more specific operational tasks that generally align with traditional kinetic constructs. As in other domains, cyber operations normally start with and are driven by intelligence, surveillance, and reconnaissance (ISR) activities designed to collect, process, exploit, and disseminate information necessary to inform military planning and decision making.[78] While all means of ISR, to include traditional activities such as human intelligence or electronic intelligence, may be leveraged to inform cyber operations, a substantial amount of the data collection needed to support follow on cyber operations occurs directly in and through cyberspace.

Just as in the kinetic realm, the ability to deliver an intended effect against a specified target in furtherance of the commander's intent depends on the collection and analysis of sufficient information to map and understand the cyber "terrain," identify and characterize the target and the path to the target (to include identifying any exploitable vulnerabilities), and to tailor or pair the right tool or capability to the target. Traditionally, this initial data collection and processing has been done under intelligence authorities, but can also be done as non-intelligence enabling actions, such as surveillance and reconnaissance maneuver operations or operational preparation of the environment (OPE).[79]

These preparatory activities are intended to inform and facilitate follow on cyber operations. Ultimately, they are conducted to enable the specific tactical action of cyberspace attack—the degradation, disruption, destruction, or manipulation of data or systems to generate offensive or defensive effects.[80]

Although the current doctrinal framework and terminology is nascent and evolving, the importance of distinguishing the broad purpose-based categories of cyber operations should not be understated. From the perspective of assessing legality, understanding the primary purpose of an operation is nearly always relevant, and takes on further significance in an environment like cyber where the specific tactics, techniques, and procedures (TTPs) used to collect information and to deliver defensive or offensive effects may be indistinguishable.[81] In addition to

---

[78] *Id.* at II-8. *See also*, JOINT CHIEFS OF STAFF, JOINT PUBLICATION 2-0, JOINT INTELLIGENCE (Oct. 22, 2013) (describing intelligence operations) [hereinafter JP 2-0]. Although often discussed as a single action or capability, intelligence, surveillance and reconnaissance, or ISR, is in fact a synchronizing function of three discrete but related intelligence and operations activities. DOD DICTIONARY, *supra* note 2, at 116 (defining ISR as an integrated intelligence and operations function "that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations."). Surveillance and reconnaissance are non-intelligence maneuver operations conducted to collect data and information. *See* JP 2-0, *supra*, at I-11.

[79] *See*, *e.g.,* U.S. DEP'T OF THE ARMY, FIELD MANUAL 3-55, INFORMATION COLLECTION 1-1 to 1-12 (May 2013) (discussing reconnaissance and surveillance operations). *See also* JP 3-12, *supra* note 6, at II-4 to II-5 (describing cyberspace intelligence, surveillance, and reconnaissance, and cyberspace operational preparation of the environment).

[80] JP 3-12, *supra* note 6, at II-5. The doctrinal term of cyberspace attack is a misnomer, as it does not correspond to the legal terms of armed attack and attack in the *jus ad bellum* and *jus in bello*, respectively. *See infra* note 316 and accompanying text.

[81] Where the code or technique to be used can have "simultaneous utility as a tool to collect intelligence and an instrument to influence events," traditional "distinctions among intelligence collection, covert action, and military activity are hard to bring to bear . . . ." Chesney, *Law of the Title 10/Title 50 Debate*, *supra* note 46, at 580.

understanding the specific task and purpose of an operation, much deeper factual granularity about the specific target to be affected, the tools and TTPs to be employed, and the expected direct and collateral effects to be generated, is also critical to providing ex ante legal advice to commanders and policy makers.

B. Tactical Cyber Actions

The unique attributes of cyberspace compel one truism: no two cyber operations are (or better stated, can be) the same. A cyber operation's "attack" profile, including tool design and weaponeering, must be tailored particularly to account for variables such as the target configuration (i.e., its operating system, resident software, system vulnerabilities, and security software such as intrusion detection systems and anti-virus programs that may be running on the target system) and the type, scope, and scale of intended effect.[82] As noted earlier, the cyber operational environment—including adversary security awareness and postures, intrusion detection systems and forensic capabilities of service providers, third-party cybersecurity vendors, and system owners along the path to target, as well as individual target characteristics—is constantly changing.[83] The available vectors and opportunities to access a target system or device and successfully deliver effects can be extremely fleeting. Once an adversary is aware of its vulnerabilities it can mitigate or eliminate them, and it can adapt its security and defensive measures to render offensive tools ineffective.[84] Operational security and the attendant concealment and secrecy it requires—achieved through a combination of clandestine operational TTPs and obfuscated infrastructure—are therefore vital in the cyber domain. Details about operations and capabilities are therefore highly classified. However, the general contours of most tactical cyber actions are commonly understood, and provide helpful background to framing the legal issues discussed in Section IV.

Ultimately, tactical cyber effects, whether for offensive or defensive purposes, are achieved through the degradation, disruption, or destruction of a targeted system.[85] The intended tactical effects may be achieved immediately through direct denial or, alternatively, through obfuscated manipulation that results in time- or conditions-based delayed effect. Consequently, while a taxonomy of cyber operations that focuses on consequential effects is useful, it is equally (if not more) important to delineate how those effects are achieved.

Each cyber operation will vary in accordance with the nature of the targeted system or device, its specific vulnerabilities, and the nature and combination of the tools employed against it. Notwithstanding these variables, several models have been developed to describe the basic steps commonly employed in a typical cyber operation. Although described differently, these models generally include the following phases: 1) reconnaissance (target discovery and enumeration); 2) exploitation (initial access); 3) privilege escalation and sustainment; 4) exfiltration or effect; and

[82] Customizing software code to exploit specific vulnerabilities and/or cause specific effects.
[83] *See* BRYANT, *supra* note 49, at 58 (describing the ephemeral nature of cyberspace).
[84] JP 3-12, *supra* note 6, at I-7 ("Another challenge [for cyber operations] is that the use of a capability may reveal its functionality and compromise future effectiveness.").
[85] Degradation is a quantifiable limitation to access to a target that can be represented as a percentage of denial of capacity and/or time. Disruption is a total, but temporary, degradation of a target. Destruction is the permanent, irreparable disruption of a target. Manipulation, on the other hand, is the control or change of adversary information, information systems, and/or networks.

5) assessment and concealment.[86] Most operations, whether external or internal, start in the reconnaissance phase in order to identify and understand the target and the operational environment and proceed through the following four phases.[87]

As noted, situational awareness of the target in cyberspace can be achieved through both intelligence and non-intelligence enabling actions. Regardless of authorities employed, the reconnaissance phase involves the identification and selection of targets that align with the commander's operational intent, as well as scanning and other techniques aimed at characterizing the target and identifying potential access and attack vectors, whether they be human or system vulnerabilities.[88] Reconnaissance identifies basic information about potential targets needed to access or affect them, such as network information (e.g., IP addresses, domain names, and network topology), host information (e.g., user and group names, and operating system and version), human information (for both target identification and human exploitation), and security measures and posture (e.g., password complexity and change frequency requirements, firewalls, intrusion detection systems).[89] Target reconnaissance can be developed over a period of time and generally with relative stealth, and may involve both passive and active measures, such as IP address and port scans, and running network mappers.[90] Initial reconnaissance may be sufficient to support a basic external effect operation, or may continue through follow-on phases to provide deepening insight into the targeted network or end-point device.

C. External and Internal Cyber Operations

The means of achieving operational cyber effects generally can be divided into two broad categories: "those that attack from outside enemy systems [external], and those that attack from within [internal]."[91] External effects operations, such as a denial of service (DoS) attack, focus on temporarily disrupting or degrading an adversary system's ability to communicate or access data.[92] Internal operations involve gaining unauthorized access—hacking—into an adversary system to steal data, manipulate information, or degrade or disrupt the system's functionality.[93]

An example of an external cyber operation is a denial-of-service (DoS) attack. A DoS attack degrades or disrupts the availability of information to a user of a machine or network resource by

---

[86] *See, e.g.,* ERIC M. HUTCHINS ET AL., INTELLIGENCE-DRIVEN COMPUTER NETWORK DEFENSE INFORMED BY ANALYSIS OF ADVERSARY CAMPAIGNS AND INTRUSION KILL CHAINS 4-5, https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (describing a seven-phase process); Ross Brewer, *The Six Stages of a Cyber Attack Lifecycle*, HELPNETSECURITY (Mar. 6, 2017), https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle (describing a six-phase process); *The Seven Steps of a Successful Cyber Attack*, INFOSEC INSTITUTE (Jun. 11, 2015), http://resources.infosecinstitute.com/the-seven-steps-of-a-successful-cyber-attack/#gref (describing a seven-phase process); Duchaine, *supra* note 3, at 229-30 (describing a six-phase process).
[87] JP 3-12, *supra* note 6, at II-8 to II-10.
[88] HUTCHINS ET AL., *supra* note 86, at 4; *The Seven Steps of a Successful Cyber Attack, supra* note 86.
[89] *See* U.S. Naval Acad., Cyber Dep't, */SY110/Phases of a Cyber Attack/Cyber Recon*, https://www.usna.edu/CyberDept/sy110/lec/cyberRecon/lec.html (last visited Aug. 24, 2017).
[90] *Id.*
[91] BRYANT, *supra* note 49, at 60.
[92] *Id.*
[93] *Id.* at 60-61.

flooding it with information or requests for information.[94] Every transmission between networks involves the transmission of information, or the transmission of a request for information. For example, typing a Uniform Resource Locator (URL)—the address for webpages or files on the internet—for a particular website into a browser sends a request to the website's computer server to view the page. Servers can only process a finite number of requests before they become overloaded and, consequently, crash. A distributed DoS (DDOS) amplifies this effect exponentially through the use of multiple compromised computers and servers (a botnet).

As noted, the objective of internal cyber operations—those that involve penetration of a target computer or network—is to gain sufficient access to an end-point device (such as a mobile phone or laptop) or a host within a network (a connected computer, router, or server) to either introduce a "payload" (the tool employed to carry out the cyber operations intended effects) or gain remote, root-level control of the device or host to achieve the operational objective of data exfiltration or system disruption, denial, degradation, or destruction. Leveraging information obtained during the reconnaissance phase to identify available access points, or vulnerabilities,[95] the operation will move to the exploitation phase to gain initial, unauthorized access into the targeted system or node. Initial access might be achieved using, among other means, stolen credentials (usernames and passwords), spearphishing, a Trojan horse,[96] or infiltrating an exploit through normal internet traffic. From this initial foothold, the operation may pivot to establish deeper access into the device, or establish access to other nodes within the network as a pathway to the ultimate target. Throughout its course, the operation will move into the privilege escalation phase as necessary to increase privileges within the host or the broader network to a level that will allow sustained access and remote control of the system. When the necessary conditions are set, the operation will move into the exfiltration or effect phase to achieve the ultimate operational objective. Finally, an assessment will be done to determine whether the operational objectives have been met, at which point the operator will back out of the system, possibly leaving a backdoor to allow follow on operations. Whether or not follow on operations are contemplated, the operator will employ TTPs to erase traces of the operation.[97]

As we have seen, operational effectiveness in the unique environment of the cyberspace domain often depends on developing and employing specifically tailored TTPs in a security intensive operational environment. Throughout each phase of an operation, concealment and detection avoidance are frequently critical to mission success. These operational-security imperatives require not only the use of boutique cyber tools designed to avoid detection, but may also call for

[94] *Security Tip (ST04-015) Understanding Denial-of-Service Attacks*, US-CERT: UNITED STATES COMPUTER EMERGENCY RESPONSE TEAM (Feb. 26, 2013), https://www.us-cert.gov/ncas/tips/ST04-015.

[95] These vulnerabilities are flaws in software, hardware, the site, or personnel, and are collectively known as the attack surface. A vulnerability may be a publically known but unpatched flaw or it may be an undisclosed flaw, known as a zero-day—a flaw in computer software unknown to the developer or user but discovered by researchers and exploited before the developer or user can patch it. *See What Is a Zero-Day Exploit?*, FIREEYE, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html (last visited Aug. 24, 2017).

[96] A Trojan horse "is a program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes exploiting legitimate authorizations of a system entity that invoked the program." U.S. Naval Acad., Cyber Dep't, */SY110/CyberOperations/Malware*, https://www.usna.edu/CyberDept/sy110/lec/malware/lec.html (last visited Aug. 24, 2017).

[97] After operations involving the delivery of an effect, a battle damage assessment will typically be performed through sustained target access, or other intelligence or non-intelligence enabling actions.

the use of covered or concealed ITT infrastructures.[98] Applying existing legal paradigms in this *sui generis* operational environment raises a host of novel and challenging questions, especially in the gray zone of sub-armed conflict cyber operations.

IV. The Law of Gray-Zone Military Cyber Operations

Like the internet itself, the operational domain of cyberspace is in its infancy, and the attendant operational concepts and doctrine governing military cyber operations are even more nascent. Not surprisingly, so too are the understandings of how existing legal paradigms apply to this emerging means and method of statecraft and warfare. Manning, training, equipping, and, ultimately, employing the military to conduct cyber operations implicates a host of novel and challenging issues of domestic and international law. This is especially true for operations executed outside of a clearly defined armed conflict, where legal ambiguity predominates.[99]

Despite best efforts, international bodies such as the United Nations Group of Governmental Experts (UNGGE) have made little progress in clarifying the role of international law in regulating cyber operations beyond generalized statements that it applies to such operations.[100] Nor have states provided much clarity individually on their views, despite increasing pressure and a growing body of academic work on the subject.

Yet it is beyond contention that cyber operations must comply with applicable domestic and international law, and ambiguity as to the specifics of application in no way relieves commanders or the lawyers advising them of this obligation.[101] As with any military operation, cyber operations must be reviewed prior to execution for consistency with domestic law to ensure they are both grounded in an affirmative authority to act and will be executed consistent with any applicable constitutional or statutory constraints or proscriptions. With the exception of certain operations that are strictly limited to domestic matters, cyber operations must also comply with applicable international law. What follows is a review of some of the more pertinent, and challenging, domestic and international law issues implicated by gray-zone cyber operations.

A. Domestic Legal Framework

1. The Roles of the President and Congress

[98] Cover involves "measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information." DOD DICTIONARY, *supra* note 2, at 55.

[99] *See generally,* Schmitt, *Grey Zones*, *supra* note 11 (discussing legal gray zones in international law).

[100] *See* Report of the Group of Governmental Experts on Developments In the Field of Information & Telecommunications in the Context of International Security, U.N. DOC. A/70/174, ¶ 27 (July 22, 2015). Even these tepid statements have moved in the wrong direction, with the 2017 round of the UNGGE failing to achieve a consensus report specifically due to disagreements about international law. *See* Arun Mohan Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, LAWFARE (Jul. 4, 2017), https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

[101] *Cf.* DOD LAW OF WAR MANUAL, *supra* note 8, at 994 & n. 1 (discussing applicability of existing international law frameworks to cyber operations).

It is a basic tenet of military operational law that DoD forces only conduct operations when affirmatively authorized or directed to do so by competent authority within the chain of command, which ultimately traces to the President. This principle is grounded in the limited powers of the Federal government and the separation of powers among the three branches.[102] The Constitution confers broad, but not unfettered, authority on the President to direct military action "for the purpose of protecting American lives or property or American interests."[103] The Constitution also confers significant powers on Congress in the area of national defense and security, not the least of which is the power to declare war and authorize the use of funds which it appropriates.[104]

The exact contours of presidential power conferred indemarcation line between Article I and Article II powers and the contours of presidential authority has have long been, and remains, a contested questions beyond the scope of this chapter.[105] As Commander in Chief of the Armed Forces,[106] the President certainly has broad authority to direct the conduct of military operations, including the use of cyber capabilities, to defend the Nation against imminent or actual attack, or as part of on-going, congressionally authorized hostilities.[107] But the question of whether the President possesses authority to unilaterally initiate hostilities or "use force in the pursuit of national interests, but in the absence of an urgent defensive need or congressional approval—remains highly charged and unanswered."[108] For military cyber operations conducted outside of ongoing hostilities and below the threshold of war, at least as that term is used in the context of Congress' constitutional authority to declare war,[109] the scope of the President's authority is

---

[102] *See* INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., U.S. ARMY, OPERATIONAL LAW HANDBOOK 1 (2015) ("Any decision to employ force must rest upon the existence of a viable legal basis in international law as well as in domestic law . . . .") [hereinafter OPERATIONAL LAW HANDBOOK]; Richard M. Whitaker, *Intelligence Law*, *in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 519-20 (2016) (describing intelligence law as "quasi-restrictive" and discussing the need to trace intelligence operations to an affirmative legal authority) [hereinafter Whitaker]; JP 3-12, *supra* note 6, at II-2.

[103] Memorandum from Jack L. Goldsmith, III, Assistant Attorney General, Office of Legal Counsel, to the Counsel to the President, subject: Deployment of United States Armed Forces to Haiti, 31 (Mar. 17, 2004) (quoting Training of British Flying Students in the United States, 40 Op. Att'y Gen. 58, 62 (1941)), https://www.justice.gov/file/18876/download [hereinafter Haiti Memo]. See also United States v. Verdugo-Urquidez, 494 U.S. 259, 273 (1990) (noting that "[t]he United States frequently employs Armed Forces outside this country . . . for the protection of American citizens or national security."); Memorandum from Caroline D. Krass, Principal Deputy Assistant Attorney Gen., Office of Legal Counsel, to Eric Holder, Attorney Gen., subject: Authority to Use Military Force in Libya, 6 (Apr. 1, 2011) (stating that the President can direct military action "for the purpose of protecting important national interests."), https://www.justice.gov/olc/opinion/authority-use-military-force-libya, [hereinafter Krass Memo]; Adams, *supra* note 17, at 410-11.

[104] U.S. CONST. art. I, § 9, cl. 7.

[105] *See generally* GEOFFREY CORN ET AL., NATIONAL SECURITY LAW AND THE CONSTITUTION 205-64 (2017) [hereinafter NATIONAL SECURITY LAW AND THE CONSTITUTION].

[106] U.S. CONST. art. II.

[107] *See* Robert M. Chesney, *Computer Network Operations and U.S. Domestic Law: An Overview*, 89 INT'L L. STUD. 218, 225-228 (2013) (noting that separation-of-powers concerns "drop out to the extent that a given [computer operation] falls within the scope of a statutory authorization for use of military force" or is taken "in circumstances genuinely involving national self-defense.").

[108] CORN ET AL., *supra* note 105, at 45. While most experts agree that the President has no authority to initiate non-defensive hostilities contrary to an express statutory prohibition, if and when the President may do so in the absence of such affirmative congressional action is unclear. What is clear is that presidents have and almost certainly will interpret congressional inaction as tacit endorsement of such actions.

[109] U.S. CONST. art. I, § 8.

more nuanced as it implicates the full range of Article II authority, not just the commander-in-chief power, and is further complicated by the novelty and uncertainties surrounding the use of cyber operations as a tool of national power. [110] Ultimately, any assessment of the President's authority to direct the conduct of a particular gray-zone cyber operation is necessarily fact dependent.[111]

It is axiomatic that "[t]he President's authority to act, as with the exercise of any governmental power, 'must stem either from an act of Congress or from the Constitution itself.'"[112] However, discerning whether the President has the authority to act in a particular circumstance, and if so, just where the President's authority lies along the delicate distribution of powers among the co-equal branches of government, is less obvious. Executive action, especially in the realm of foreign affairs and national security, is not susceptible to neat categorization, but rather falls "at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition."[113] Justice Jackson's familiar tripartite framework from *Youngstown Sheet & Tube Co. v. Sawyer*[114] provides the generally-accepted structure for analyzing claims of Presidential power along this spectrum, dividing presidential action into one of three categories.[115] When Presidents act, they do so either in the absence of a congressional grant or denial of authority, with the express or implied authorization of Congress, or contrary to the express or implied will of Congress.[116]

Within the *Youngstown* framework, Presidential power is understood to be at its zenith when exercised pursuant to an express or implied authorization of Congress, for in those instances the exercise "includes all that [the President] possesses in his own right plus all that Congress can delegate."[117] Absent either a congressional grant or denial of authority, the President "can only rely upon his own independent powers," or upon powers resident in a constitutional "zone of twilight" in which the distribution between the President and Congress is either concurrent or uncertain, but where "congressional inertia, indifference or quiescence" invite the exercise of "independent presidential responsibility."[118] Finally, when "the President takes measures incompatible with the expressed or implied will of Congress his power is at its lowest ebb, for

[110] For example, non-armed conflict uses of cyber capabilities also implicate the President's unique role and authority in foreign affairs and may be best be viewed as actions of military diplomacy. *See* U.S. CONST. art. II, § 2, cl. 2. *See also* United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936) (noting the President's "very delicate, plenary and exclusive power . . . as the sole organ of the federal government in the field of international relations . . . .").

[111] *See* Dames & Moore v. Regan, 453 U.S. 654, 669 (1981) ("[E]xecutive action in any particular instance falls . . . at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition[,]" especially in cases "involving responses to international crises the nature of which Congress can hardly have been expected to anticipate in any detail.").

[112] Medellín v. Texas, 552 U.S. 491 (2008) (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U. S. 579, 582 (1952)).

[113] Dames & Moore, 453 U.S. at 669 (Particularly in cases "involving responses to international crises the nature of which Congress can hardly have been expected to anticipate in any detail.").

[114] Youngstown Sheet & Tube Co. v. Sawyer, 343 U. S. 579 (1952).

[115] *See, e.g.*, Zivotofsky v. Kerry, 135 S. Ct. 2076, 2083-84 (2015) (citing Youngstown, 343 U. S. at 635–638 (Jackson, J., concurring)) ("The [Jackson tripartite] framework divides exercises of Presidential power into three categories . . . .").

[116] *See id*.

[117] Youngstown, 343 U.S. at 635 (Jackson, J., concurring).

[118] *Id.* at 637.

then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."[119]

2. Authorities for Military Cyber Operations

a. Congressional Authorizations? Section 954 of the 2012 NDAA and 10 U.S.C. § 130g

In recognition of the growing cyber threat to U.S. national security, members of Congress have grown increasingly vocal in their view that more active measures are needed to counter and deter cyber threats.[120] Although this growing chorus has manifested more in admonishments of the Executive Branch and calls on it to develop a strategy to deter and respond to cyber threats,[121] Congress has passed a number of cyber-related provisions relevant to assessing the President's authority to direct the military to conduct gray-zone cyber operations. Two in particular warrant discussion: Section 954 of the 2012 National Defense Authorization Act (NDAA),[122] and 10 U.S.C. § 130g.[123]

On its face, Section 954, entitled "Military Activities in Cyberspace," seems no more than a simple affirmation "that the [DoD] has the capability . . . to conduct offensive operations in cyberspace to defend the United States, our allies and interests," and may do so "upon direction by the President."[124] Clearly, Section 954 does not authorize any specific cyber operations. In fact, Congress' apparent purpose in passing this provision, evident only from the legislative history, was primarily to address a narrower question of whether cyber operations can qualify as traditional military activities (TMA) under the Covert Action Statute,[125] a question addressed below.[126] But the accompanying conference report also notes that "in certain instances, the most effective way to deal with threats and protect U.S. and coalition forces is to undertake offensive military cyber activities . . . ."[127] Based on the language and history of Section 954, it is reasonable to read it at least as an affirmation of the President's inherent authority to conduct a broad range of cyber operations outside of armed conflict (or at least do not trigger the

[119] *Id.*
[120] *See, e.g.*, Morgan Chalfant, *Senators Press Trump for Cyber Deterrence, Response Strategy*, THE HILL (May 10, 2017), http://thehill.com/policy/cybersecurity/332759-senators-press-for-cyber-deterrence-response-strategy.
[121] *See e.g.*, National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328 (Dec. 23, 2016), § 1654 (requiring the Secretary of Defense and the President to submit reports to Congress on deterrence of adversaries in cyberspace).
[122] National Defense Authorization Act for Fiscal Year 2012, Public Law 112–81 (Dec. 31, 2011), sec. 954.
[123] 10 U.S.C. § 130g (2015). Congress' recent direction to elevate U.S. Cyber Command to full combatant command status and to infuse it with substantial force-development authorities serves as additional evidence of its expectation that DoD conduct cyber operations to protect and advance U.S. interests. *See id.*, § 923 ("Establishment of a unified combatant command for cyber operations). *See also* Charley Snyder & Michael Sulmeyer, *Decoding the 2017 NDAA's Provisions on DoD Cyber Operations*, LAWFARE (Jan. 30, 2017), https://www.lawfareblog.com/decoding-2017-ndaas-provisions-dod-cyber-operations (discussing Section 923 and other cyber related provisions of the 2017 NDAA).
[124] National Defense Authorization Act for Fiscal Year 2012, Public Law 112–81 (Dec. 31, 2011), sec. 954. Attached to this affirmation are two stipulations. Offensive cyber operations are subject to: 1) the policy principles and legal regimes that DoD follows for kinetic capabilities, including the law of armed conflict (LOAC); and 2) the War Powers Resolution. *Id.* The War Powers Resolution is codified at 50 U.S.C. § 1541 et seq. (1994).
[125] 50 U.S.C. § 3093 (2012).
[126] *See infra* notes 178-188 and accompanying text.
[127] H.R. REP. NO. 112-329, at 686 (2011) (Conf. Rep.).

provisions of the War Powers Resolution), or perhaps even as an express or implied authorization to the President to do so.[128]

Subsequently, on the heels of the Sony Hack,[129] Congress added Section 130g to Title 10 of the U.S. Code in 2015 as part of the 2016 NDAA.[130] Section 130g provides:

> The Secretary of Defense shall develop, prepare, and coordinate; make ready all armed forces for purposes of; and, when appropriately authorized to do so, conduct, a military cyber operation in response to malicious cyber activity carried out against the United States or a United States person by a foreign power (as such terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)).[131]

Section 130g was a late add to the Senate version of the NDAA, to which the House receded in conference with one minor but significant change.[132] Whereas the Senate version allowed for the conduct of military cyber operations "when authorized by the President," the final version clarified "that the authority to conduct cyber operations shall be exercised when *appropriately* authorized."[133]

At first blush this change might be seen as walking back from Section 954's tacit recognition of broad, standing (or congressionally conferred) presidential authority to conduct offensive cyber operations to protect national interests. If such is the case, it stands to reason that in the view of Congress, the President's authority to direct military cyber operations to counter the full range of all malicious cyber activity is not as robust, absent congressional action, as his or her independent authority to "defend the United States, our allies, and interests" against more substantial threats.[134]

However, Section 130g is directed at the Secretary of Defense, not the President, and the conferees noted that nothing in the provision "shall be construed to limit existing presidential or congressional power to authorize action."[135] Moreover, the Senate added Section 130g within the self-established guideline for the 2016 NDAA of improving "the ability of the armed forces to counter emerging and nontraditional threats, focusing on [inter alia], cyber warfare . . . ."[136] As noted in the Senate Armed Services Committee's report accompanying the 2106 NDAA, it added Section 130g out of its concern over "the growing number and severity of malicious cyber

---

[128] *But see,* Chesney, *Computer Network Operations*, *supra* note 107, at 228-29 (discussing whether Section 954 should be read to authorize computer operations in circumstances beyond what would be covered under a congressional use-of-force authorization or by a plausible claim of inherent presidential authority, or whether instead Section 954 "merely confirms existing authority for clarity's sake").

[129] The Senate described the Sony Hack as "the most destructive cyberattack ever on U.S. territory." S. REP. NO. 114-49, at 2 (2015).

[130] National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 1642 (2015).

[131] 10 U.S.C. § 130g.

[132] H.R. 1735, 114th Cong. (2015).

[133] *See* H.R. REP. NO. 114-270, at 820 (2015) (Conf. Rep.) ("The House recedes with an amendment that would clarify that the authority to conduct cyber operations shall be exercised when appropriately authorized.").

[134] Public Law 112–81 (Dec. 31, 2011), § 954.

[135] H.R. REP. NO. 114-270, at 820.

[136] S. REP. NO. 114-49, at 3-4 (2015).

activities being carried out against the United States and its interests" and that "failing to impose meaningful consequences on those seeking to harm the United States through the cyber domain will embolden our adversaries and lead to more severe attacks in the future."[137] As such, Section 130g appears to reflect Congress' policy preference for, and view of the appropriateness of, assigning the DoD the broad mission of countering any and all adversary (foreign power) "malicious cyber activity"—an undefined term encompassing threats that might otherwise be viewed as falling below traditional thresholds for a military response.

Suffice to say that Congress' forays into this area have not provided a clear picture on the state of existing cyber authorities. Absent a more specific congressional authorization, the President would likely have to rely, at least in part, on his or her independent Article II authority to conduct gray-zone cyber operations.

b. The President's Authority under Article II

In the realm of foreign affairs and national security, it is generally recognized that Article II of the Constitution confers extensive, independent powers on the President, to include the authority to direct the deployment and employment of military forces and capabilities to defend and advance important national interests.[138] The President's independent authority in the realm of national security and foreign affairs stems in large measure from the recognition that the President alone is in a unique position to quickly access and assess threat information and to direct immediate actions in the face of "imminent national security threats and rapidly evolving military and diplomatic circumstances. . . ."[139] These imperatives underpin a history "replete with instances of presidential uses of military force abroad in the absence of prior congressional approval" that includes numerous examples of the employment of military force to protect national interests outside of situations of armed conflict.[140]

The President's broad Article II power certainly includes the authority to direct military activities to repel actual or imminent aggressive acts against the United States, and the discretion to determine the nature and level of responsive force.[141] This power logically extends to directing military cyber operations to counter or deter adversary actions, including malicious cyber activities, that pose an imminent threat to or actually harm important U.S. national interests.

---

[137] *Id.* at 264.

[138] Am. Ins. Ass'n v. Garamendi, 539 U.S. 396, 414, 429 (2003) (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U. S. 579 (1952) and Haig v. Agee, 453 U.S. 280, 291 (1981) (Under "the historical gloss on the 'executive Power' vested in Article II," the President holds significant "independent authority 'in the areas of foreign policy and national security.'"). *See also,* Krass Memo, *supra* note 103, at 6-9 (discussing President's authority to order military operations in Libya in 2011 in the absence of congressional authorization).

[139] Krass Memo, *supra* note 103, at 7 (quoting *Presidential Power to Use the Armed Forces Abroad Without Statutory Authorization*, 4A Op. O.L.C. 185, 187 (1980), and citing Haig v. Agee, 453 U.S. 280, 292 (1981)).

[140] Krass Memo, *supra* note 103 (citations omitted). *See also* BARBARA SALAZAR TORREON, INSTANCES OF USE OF UNITED STATES ARMED FORCES ABROAD, 1798-2016, CONG. RES. SERVICE (Oct. 7, 2016) (providing an extensive list of "instances in which the United States has used its Armed Forces abroad in situations of military conflict or potential conflict or for other than normal peacetime purposes").

[141] *See* Campbell v. Clinton, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J. concurring) ("[T]he President has independent authority to repel aggressive acts by third parties even without specific Congressional authorization, and courts may not review the level of force selected."). *See also*, Prize Cases, 67 U.S. 635, 670 (1863) (President may employ the military to protect the national interests of the United States).

Based on countless examples throughout the Nation's history, the President's substantial Article II powers also extend to directing military operations, to include the use of force, as an affirmative means of protecting and advancing U.S. interests, such as in the case of on-going freedom of navigation operations, hostage rescue operations, and even combat operations to enforce security council resolutions as was the case in Libya in 2011.[142]

While considerable, the President's authority under the Constitution to marshal military force is not unlimited, and sweeping generalizations are of course of limited value. Any particular employment of the military necessarily requires a fact-specific assessment of multiple factors to include the "anticipated nature, scope, and duration" of the planned military operation, which is often a complex assessment in its own right, rendered all the more so by the novel and evolving nature of cyber operations.[143] However, buttressed by Congress' actions and pronouncements to date,[144] the President would likely be on solid footing were he or she to direct the conduct of gray-zone military cyber operations. That is, unless the planned measures, under the *Youngstown* framework, would otherwise be "incompatible with the expressed or implied will of Congress."[145]

3. The Implication of Non-cyber Congressional Limitations on the President's Authority

a. The War Powers Resolution

Passed in 1973 in the wake of failed efforts to halt the Vietnam War, the War Powers Resolution (WPR)[146] was intended to restore Congress' role in the war-making process by constraining the President's ability to unilaterally enmesh the United States in "hostilities."[147] The WPR reflects Congress' view that the President is constitutionally permitted to introduce U.S. Armed Forces into hostilities only under finite circumstances.[148] It seeks to protect Congress' constitutional

[142] *See* Krass Memo, *supra* note 103, at 8 ("But the historical practice of presidential military action without congressional approval precludes any suggestion that Congress' authority to declare war covers every military engagement, however limited, that the President initiates.")
[143] *Id.* (quoting Deployment of United States Armed Forces into Haiti, 18 Op. O.L.C. 173, 179 (1994)).
[144] *See* Section IV(A)(3) *infra*.
[145] Youngstown Sheet & Tube Co. v. Sawyer, 343 U. S. 579, 637 (1952).
[146] War Powers Resolution of 1973, Pub. L. No. 93-148 §8, 87 STAT. 559 (codified as 50 U.S.C. §§ 1541–1548 (2012)).
[147] *See* 50 U.S.C. § 1541(a) (setting out the purpose of the War Powers Resolution). The WPR does not define the term "hostilities." Some argue that it was substituted for the term "armed conflict," contained in earlier versions of the legislation, to broaden the WPR's scope. *See* Allison Arnold, *Cyber "Hostilities" and the War Powers Resolution*, 217 MIL. L. REV. 174, 180-81 (2013) (citing *Libya and War Powers: Hearing Before the Comm. Of Foreign Relations*, 112th Cong. 24-25 (2011) (statement of Sen. Corker)); *Libya and War Powers*, *supra*, at 31 (prepared statement of Hon Harold Koh, Legal Adviser, U.S. Dep't of State, Wash., D.C.)). A contrary view holds that the change was meant to avoid confusion by infusing the international law meaning of "armed conflict" and to preserve the President's flexibility in making determinations as to the WPR's applicability. Arnold, *supra* (citing *War Powers: Hearings Before the Subcomm. on National Security Policy and Scientific Developments of the H. Comm. on Foreign Affairs*, 93d Cong. 22 (1973) (statement of Hon. Jacob K. Javits, U.S. Senator from the State of N.Y.)).
[148] The War Powers Resolution (WPR) sets out three circumstances: pursuant to a declaration of war; pursuant to some other form of express statutory authority; or where the President is responding to an actual or imminent attack on the United States or its armed forces. 50 U.S.C. § 1541(c). *See also* GEOFFREY CORN ET AL., NATIONAL

prerogatives by requiring the President to provide timely notice of the introduction of U.S. forces into actual or anticipated hostilities, and providing for the automatic termination of any continued use of the Armed Forces absent congressional authorization.[149]

As noted earlier, Section 954 of the 2012 NDAA evidences Congress' view that at least some offensive cyber operations would be subject to the WPR.[150] However, neither Section 954 nor its legislative history offer any guidance on the types of cyber operations that would in fact trigger the WPR's substantive and procedural requirements. A review of the history of the Executive Branch's interpretation of the WPR indicates that it is unlikely to consider stand-alone gray-zone cyber operations as falling within the scope of the law's provisions.

The underlying constitutionality of the WPR is a matter of continued debate. It was passed over President Nixon's veto,[151] and since its passage Presidents have filed numerous reports "consistent with" the resolution's provisions without once acknowledging its constitutional validity.[152] These debates aside, whether military cyber operations in principle are "subject to" the WPR is a distinct question from whether and how its provisions might apply to specific cyber operations.[153] The answer to this baseline question of applicability turns primarily on whether cyber operations constitute the *introduction* of U.S. Armed Forces into *hostilities*, as those terms are used in the WPR—a matter which is unclear at best.

In addition to directing Presidents to consult with Congress "in every possible instance . . . before introducing United States Armed Forces into hostilities . . . ," the WPR requires the President to file a report with Congress in any case in which the United States Armed Forces are introduced "into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances."[154] The WPR then requires the President to "terminate any use of

---

SECURITY LAW: PRINCIPLES AND POLICY 68 (2015) [hereinafter NATIONAL SECURITY LAW: PRINCIPLES AND POLICY].

[149] *See* 50 U.S.C. §§ 1543(a) (reporting requirements), 1544(b)(termination provision); NATIONAL SECURITY LAW: PRINCIPLES AND POLICY, *supra* note 148, at 66-84.

[150] § 954, 125 Stat. at 1551.

[151] *See* Veto of the War Powers Resolution, 5 Pub. Papers 893 (Oct. 24, 1973).

[152] *See War Powers,* LIB. OF CONG. https://www.loc.gov/law/help/war-powers.php (last visited Dec. 4, 2017). On the question of the constitutionality of the WPR, see generally Geoffrey S. Corn, *Triggering Congressional War Powers Notification: A Proposal to Reconcile Constitutional Practice with Operational Reality*, 14 LEWIS & CLARK L. REV. 687 (2010); Geoffrey S. Corn, *Clinton, Kosovo, and the Final Destruction of the War Powers Resolution*, 42 WM. & MARY L. REV. 1149 (2001); Michael J. Glennon, *Too Far Apart: Repeal the War Powers Resolution*, 50 U. MIAMI L. REV. 17 (1995); Robert F. Turner, *The War Powers Resolution: Unconstitutional, Unnecessary, and Unhelpful*, 17 LOY. L.A. L. REV. 683 (1984).

[153] Eric Talbot Jensen, *Future War and the War Powers Resolution*, 29 EMORY INT'L L. REV. 500, 538 (2015) (("Of course, being "subject to" the WPR does not mean it applies. It simply means that when it applies, the Executive Branch will comply with its requirements.").

[154] 50 U.S.C. §§ 1542, 1543(a)(1). In the absence of a declaration of war, Section 1543(a) of the WPR requires the President to file a report with Congress in any case in which the United States Armed Forces are introduced:

> (1) into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances;
> (2) into the territory, airspace or waters of a foreign nation, while equipped for combat, except for deployments which relate solely to supply, replacement, repair, or training of such forces; or

United States Armed Forces with respect to which such report was submitted (or required to be submitted) . . .” sixty days thereafter unless Congress takes measures to authorize the President’s actions or to extend the sixty-day period.[155] Debates over the constitutionality of the WPR have focused primarily on this mandatory termination provision.[156] Valid or not, the issue of what constitutes “terminat[ion] of any use of the Armed Forces” raises unique interpretive issues, discussed below, when applied to military cyber operations. Of course, those issues are only raised if military cyber operations themselves trigger the WPR reporting requirements in the first instance.

Absent a declaration of war, Section 1543(a) of the WPR mandates congressional notification within 48 hours of United States Armed Forces being introduced:

> “(1) into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances; (2) into the territory, airspace or waters of a foreign nation, while equipped for combat, except for deployments which relate solely to supply, replacement, repair, or training of such forces; or (3) in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation.”[157]

When cyber operations are conducted as a component of larger military operations, the WPR reporting implications are subsumed in the broader analysis.[158] Standing alone, it is unlikely that a military cyber operation would constitute either the introduction of armed forces into hostilities or a combat-equipped deployment as those terms are used in the WPR.

While only subsection (2) of Section 1543(a) includes a geographic component, the Executive Branch has generally taken the position that subsection (1) is triggered only by the actual, physical “introduction” of members of the Armed Forces into a geographic area of operations under circumstances that place them at a certain level of risk, a requirement unlikely to be triggered by remote cyber operations where the forces conducting the operation remain in the United States or at least distant from the point of delivery of the cyber effect.[159] Relatedly, the meaning generally accorded the term “hostilities” as used in the narrow context of the WPR

> (3) in numbers which substantially enlarge United States Armed Forces equipped for combat already located in a foreign nation . . . .

The termination provision of 50 U.S.C. § 1544(b) applies only to § 1543(a)(1).

[155] *Id.* § 1544(b).

[156] *Id.* Some have argued that this provision is virtually a dead letter in light of the D.C. Circuit’s decision in *Clinton v. Campbell*. Campbell v. Clinton, 52 F. Supp. 2d 34, 35 (D.D.C. 1999), *aff’d* 203 F.2d 19 (D.C. Cir. 2000). *See* Jensen, *supra* note 153, at 525 (citing *Clinton, Kosovo, and the Final Destruction of the War Powers Resolution, supra* note 152, at 1190).

[157] 50 U.S.C. § 1543(a).

[158] *See* U.S. DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011 9 (2011) [hereinafter CYBERSPACE POLICY REPORT].

[159] *See id.* (“Cyber operations might not include the introduction of armed forces personnel into the area of hostilities.”). *See also* NATIONAL SECURITY LAW: PRINCIPLES AND POLICY, *supra* note 148, at 85-86 (discussing Executive Branch’s “Boots-on-the-Ground” approach); Arnold, *supra* note 147, at 185-87 (discussing Executive Branch’s approach to WPR applicability).

seems to require a substantial level of armed force, again tied to actual risk to US forces, which would not be met by most cyber operations standing alone, especially sub-use-of-force gray-zone cyber operations.[160] Finally, an assessment under subsection (2) is unlikely to yield a different result based on the territorial component of the provision, and the Executive Branch's view that "equipped for combat" refers only to the deployment of forces armed with crew-served weapons.[161] However, as the DoD has noted in response to inquiries from Congress, while cyber operations *per se* "might not include the introduction of armed forces personnel into the area of hostilities . . . the Department will continue to assess each of its actions in cyberspace to determine when the requirements of the War Powers Resolution may apply to those actions."[162]

Even under circumstances triggering a WPR report, substantial uncertainty remains not only as to the enforceability of the WPR's termination provision generally, but also as to what constitutes the termination "of any use of U.S. Armed Forces" for purposes of the WPR and its applicability to cyber operations. First, leaving the larger constitutional questions aside, the WPR's termination provision has been understood to require the physical withdrawal of armed forces from areas of active or imminent hostilities, not necessarily the cessation of all operational activity.[163] Under a narrow view of the purpose of the WPR—one linked to actual risk of harm to forces—this interpretation makes sense. Second, for many of the reasons cyber operations are unlikely to qualify as hostilities under that term's WPR meaning, they are unlikely to fall subject to the law's termination requirement. The Executive Branch has consistently emphasized "the distinction between full military encounters and more constrained operations, stating that 'intermittent military engagements' do not require withdrawal of forces under the resolution's 60-day rule."[164] That is, cyber operations alone are likely to be viewed as the type of limited military means unregulated by the WPR, "not the kind of full military engagements with which the [WPR] is primarily concerned."[165]

Should cyber operations increase in scale and frequency, as they likely will in the face of growing cyber threats and gray-zone challenges, arguments for a broader reading of the WPR or

---

[160] *See* Chesney, *Law of the Title 10/Title 50 Debate*, *supra* note 46, at 588 ("What the WPR does not do is impose any form of constraint – substantive, procedural, or informational – on military activity that does not implicate the WPR hostilities triggers . . . . And thus the WPR ha[s] nothing to say about . . . at least some forms of low-intensity military activity."); Arnold, *supra* note 147, at 191 ("[I]t seems unlikely that a stand-alone military cyber operation would ever reach the threshold of "hostilities" sufficient to trigger the statute because its mission, military means, and exposure to U.S. forces would always appear extremely limited in comparison to a full military engagement or conventional kinetic military action."). The Executive Branch has long interpreted the term "hostilities" in the WPR to involve the actual presence of U.S. ground troops in an area of active combat, and/or sustained fighting or active exchanges of fire with hostile forces. *See*, *e.g.*, *Libya and War Powers*, *supra* note 147) (prepared statement of Hon Harold Koh, Legal Adviser, U.S. Dep't of State, Wash., D.C.).

[161] *See*, Jonathan Howard, *Equipped for Combat: Jumping the Gun on Reporting under Section 4(a)(2) of the War Powers Resolution*, ARMY LAW. 44, 46 (2017).

[162] CYBERSPACE POLICY REPORT, *supra* note 158, at 9.

[163] *Cf. Libya and War Powers*, *supra* note 147, at 14 (prepared statement of Hon Harold Koh, Legal Adviser, U.S. Dep't of State, Wash., D.C.) (arguing that U.S operations not involving sustained fighting or active exchanges of fire with hostile forces, or presence of ground troops, do not trigger the WPR); NATIONAL SECURITY LAW: PRINCIPLES AND POLICY, *supra* note 148, at 85-86.

[164] *See Libya and War Powers*, *supra* note 147, at 14 (quoting Letter from Assistant Secretary of State for Legislative Affairs Wendy R. Sherman to Representative Benjamin Gilman, *reprinted in* 139 CONG. REC. H7095 (daily ed. Sept. 28, 1993)).

[165] *Id.* at 9.

for amendments designed to protect Congress' constitutionally assigned prerogatives will persist. For now, given the Executive Branch's narrow interpretation of the WPR and Congress' general acquiescence in that interpretation, the WPR "is unlikely to prove much of a constraint on presidential actions."[166]

b. The Covert Action Statute

After decades of less-than-effective efforts by Congress to assert oversight over the Executive Branch's conduct of covert activities,[167] in 1991 President George H.W. Bush signed into law Section 503 of the National Security Act of 1947, known as the Covert Action Statute (CAS).[168] The CAS requires specified presidential findings and congressional notifications prior to any department, agency, or entity of the U.S. government conducting any "activity or activities . . . to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will not be apparent or acknowledged publically."[169] On its face, Section 3093 is more of a procedural than a substantive statute, and leaves to the President's discretion the decision as to which department or agency will conduct a particular covert action.[170] So long as the President determines in a written finding noticed to Congress that a cyber operation is necessary to support identifiable foreign policy objectives of the United States, is important to the national security of the United States, and does not violate the Constitution or any Statute of the United States, Section 3093 would appear to present no bar to the President directing the military to conduct the operation covertly.[171]

As a matter of policy, however, covert action is, in effect, the sole province of the Central Intelligence Agency (CIA),[172] and Section 3093's requirements are often framed in substantive terms as demarcating the boundaries of institutional roles and authorities. That is, absent specific direction from the President in accordance with the statute's provisions, DoD may not conduct covert action. As we have seen, owing to the nature of the cyberspace environment, some degree of concealment to avoid detection is critical to the success of most military cyber operations. So, to the extent cyber operations are conducted in a manner that conceals the sponsorship of the United States, application of and compliance with Section 3093 are squarely at issue.

---

[166] Jensen, *supra* note 153, at 539.

[167] The DoD defines a covert operation as one "that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor." DOD DICTIONARY, *supra* note 2, at 58.

[168] Intelligence Authorization Act for Fiscal Year 1991, Pub. L. No. 102-88, 10 STAT. 429, *codified at* 50 U.S.C. § 3093 (2012). For a history of the Covert Action Statute, *see* Chesney, *Law of the Title 10/Title 50 Debate*, *supra* note 46, at 586-601; MARSHALL CURTIS ERWIN, CONG. RESEARCH SERV., COVERT ACTION: LEGISLATIVE BACKGROUND AND POSSIBLE POLICY QUESTIONS 1 (2013).

[169] 50 U.S.C. § 3093(e).

[170] *Id.* § 3093(a).

[171] It is important to note that the statute prohibits any covert action "which is intended to influence United States political processes, public opinion, policies, or media." *Id.* § 3093(f).

[172] No "agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective." Exec. Order No. 12,333, § 1.7(a)(4), 3 C.F.R. 200 (1981) [hereinafter EO 12,333], *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53593 (Aug. 27, 2004); and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008). *See also* 50 U.S.C. § 3093(a)(3).

As a threshold matter, concealment alone of an operation does not necessarily mean concealment of the sponsorship of the operation. Department of Defense doctrine distinguishes between the former situation, a "clandestine" operation, and the latter, a covert operation. According to the DoD, a clandestine operation is one "sponsored or conducted . . . in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor."[173] But one may perhaps wonder whether this is a distinction without a difference.

On its face, Section 3093 applies only to a narrow class of activities—those for which "it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[174] For example, U.S. forces wearing standard U.S. uniforms infiltrating foreign territory under cover of darkness and employing standard means of concealing their movements and location to maintain secrecy, should not be considered to be operating covertly. Should the same forces conduct the same operation in non-standard uniforms bearing no markings identifiable to the U.S., the question becomes more nuanced, and may turn on the degree to which the U.S. has issued statements about, or acknowledged publicly the fact that it is conducting, operations more broadly. That is, the CAS is not triggered solely by the fact that operations are conducted utilizing cover and concealment to maintain security or achieve surprise, or are difficult to detect simply by virtue of the operational environment. The statute's applicability turns first on a factual determination of the degree to which the overall role of the United States is apparent or publicly acknowledged. Even where operational security measures are employed, the CAS is triggered only where the intent of utilizing those measures is to conceal the sponsorship of the United States.

However, the subtle distinctions between covert and clandestine activities are often ignored, and covert action "is frequently [albeit incorrectly] used to describe any activity the government wants concealed from the public."[175] The DoD's tendency to consider only intelligence activities as clandestine furthers confusion.[176] Thus, where U.S. military forces are conducting operations in a concealed, unattributed, or undetectable manner, compliance with Section 3093 is implicated. This is especially true for cyber operations, where concealment is an operational imperative and standard uniforms or marked tail fin analogies simply do not hold.[177]

To further complicate matters, not all operations conducted covertly fall within the ambit of the CAS. Specifically excluded from the statute's definition of covert action, and thus its procedural requirements, are a series of exceptions. The most relevant to military cyber operations are: activities the primary purpose of which is to acquire intelligence; traditional counterintelligence

---

[173] DOD DICTIONARY, *supra* note 2, at 33.
[174] 50 U.S.C. § 3093(e).
[175] Jeff Mustin and Harvey Rishikof, *Projecting Force in the 21st Century—Legitimacy and the Rule of Law: Title 50, Title 10, Title 18, and Art. 75*, 63 RUTGERS L. REV. 1235, 1240 (Summer 2011).
[176] *See* Joseph B. Berger, III, *Covert Action: Title 10, Title 50, and the Chain of Command* 67 JOINT FORCES Q. 32, 34 (2012) (citing RICHARD A. BEST, JR., CONGRESSIONAL RESEARCH SERVICE, COVERT ACTION: LEGISLATIVE BACKGROUND AND POSSIBLE POLICY QUESTIONS (2011)).
[177] Chesney, *Law of the Title 10/Title 50 Debate*, *supra* note 46, at 580 ("[t]raditional categorical distinctions among intelligence collection, covert action, and military activity are hard to bring to bear on [cyber operations] . . . .").

activities; and traditional military activities (TMA).[178] Thus, technically, and notwithstanding the less-than-helpful DoD definitions of covert and clandestine, DoD forces may conduct cyber operations to influence political, economic, or military conditions abroad, even where it is intended that the role of the U.S. Government will not be apparent or acknowledged publicly, so long as the activities qualify under one of the relevant exceptions.

While the intelligence-related exceptions are fairly straight forward, the meaning of TMA is less so, and unfortunately the statute offers no definition of the term. This creates difficulty in application, and friction both within the Executive Branch over which agencies may conduct certain activities, as well as between the Executive Branch and Congress over the jurisdiction of the various oversight committees. Understanding the meaning and scope of TMA is therefore key to assessing DoD's authority to conduct concealed or undetectable cyber operations, especially outside of the context of armed conflict.

Although the statute does not define TMA, it is generally accepted that those military operations or activities satisfying certain criteria set forth in the statute's legislative history qualify. According to the Conference Report accompanying Section 3093:

> It is the intent of the conferees that traditional military activities include activities by military personnel *under the direction and control of a United States military commander* (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) *preceding and related to hostilities which are either anticipated* (meaning approval has been given by the National Command Authorities for the activities and for operational planning for hostilities) to involve U.S. military forces, or *where such hostilities* involving United States military forces *are ongoing*, and, where the *fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.* In this regard, the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander. Activities that are not under the direction and control of a military commander should not be considered as traditional military activities.[179]

[178] The specific exceptions are to the definition of covert action itself, which is defined as *not* including:

> (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
> (2) traditional diplomatic or military activities or routine support to such activities;
> (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
> (4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.

50 U.S.C. § 3093(e).

[179] U.S. Congress, House of Representatives, Committee of Conference, Conference Report on H.R. 1455 ("Intelligence Authorization Act, Fiscal Year 1991"), 102nd Cong., 1st sess., July 25, 1991, 5905-5906 (emphasis added).

Some point to the legislative history as evincing a straight-forward, objective definition of TMA that maps neatly to cyber operations.[180] So long as the operation is commanded and executed by military personnel, and takes place in a context where overt hostilities are either underway or anticipated (as evidenced by National Command Authority direction to plan for hostilities), the cyber operation constitutes a TMA.[181] Others disagree, advocating a historical approach to the CAS that looks to whether the activity in question is one the military *traditionally* conducted covertly prior to 1991, the year of the statute's passage. Others take this historical approach a step further, advocating that technologies and capabilities that post-date 1991 simply cannot qualify as "traditional."[182]

This third, overly-narrow historical approach places too much emphasis on the specific means of conducting an operation as opposed to focusing on the purpose— for example disrupting enemy communications regardless of the means used—and thus leads to absurd results. Clearly, Congress could not have intended to forever constrain the military's authority to cover and conceal its operations just because it procures and employs new technologies. And while historical analogies to longstanding military practice can aid in applying the TMA exception to current and future military activities, determining the proper demarcation line between covert action and TMA must account for the constantly evolving nature of military doctrine and operations as well as new technologies. In fact, Congress has indicated as much with respect to cyber operations.

This takes us back to Section 954 of the 2012 NDAA discussed earlier. Recall that on its face, Section 954 is silent as to whether and how cyber operations might qualify as TMA. However, the legislative history speaks directly to Congress' view of the issue. The explanatory statement accompanying Section 954 states that "[t]he conferees recognize that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes traditional military activities in relation to cyber operations and that it is necessary to affirm that such operations may be conducted pursuant to the same policy, principles, and legal regimes that pertain to kinetic capabilities."[183] The conferees also recognized that conducting OCO may at times be the most effective way to deal with threats and to protect U.S. and coalition forces, "including where the role of the United States Government is not apparent or to be acknowledged."[184]

Plainly, Congress does not sanction the "new-technology" argument against considering cyber operations as TMA. It is strong evidence of Congress' sense that the focus of any TMA analysis should be on the proposed activity, not the technology that will be employed to achieve it. In this sense, cyber operations are no more than traditional operations executed in a non-traditional domain. For example, disrupting an adversary's command and control systems leading up to or during armed conflict has always been a means of waging war. Cyber simply offers a new technology and method to achieve this traditional military effect. Language in subsequent

[180] *See* Chesney, *Computer Network Operations*, *supra* note 107, at 221.
[181] *Id.*
[182] *Id.*
[183] U.S. Congress, House of Representatives, Committee of Conference, Conference Report on Report on H.R. 1540 ("National Defense Authorization Act for Fiscal Year 2012"), 112th Cong., December 12, 1991, 8356-8726.
[184] *Id.*

NDAAs, while not exactly on point, provides additional evidence of Congress' approval of the necessity and validity of DoD conducting secret, non-attributable cyber operations under certain conditions.[185]

Albeit helpful, Section 954 will not completely resolve the TMA debate. First, Section 954 does not address the TMA question directly. The specific language addressing TMA found in the Conference Report was originally contained in the proposed House bill, but was stripped in the Senate version, limiting its interpretive value. Second, like covert action, Section 954 arguably subjects OCO to a specific presidential-approval requirement—a restraint not applicable to other means and methods of warfare. Finally, even if Section 954 and its accompanying conference report put the "new-technology" arguments to bed, the timing and nature of each proposed cyber operation will still have to be assessed against the broader TMA criteria of being under the direction and control of a military commander, that it be conducted preceding and related to hostilities which are either anticipated or on-going, and that the overall role of the U.S. in those hostilities is or will be apparent or acknowledged publicly.

Operations conducted as part of on-going hostilities tend not to generate significant TMA debate, at least to the extent they are confined to active areas of hostilities, a limitation of questionable practical application in the case of cyberspace.[186] Gray-zone cyber operations, on the other hand, would undoubtedly raise more challenging questions. Prominent among them would be whether the particular operation is of a nature appropriately—or "traditionally"—assigned to the military. Examples of the U.S. military being employed to protect or advance national interests outside of armed conflict are legion, to include low-visibility or secret operations.[187] Ultimately, absent greater clarity from Congress, the likelihood is that the further left of the proverbial boom a particular operation is, the harder it will be to resolve the TMA question (or routine support

---

[185] *See, e.g.,* 10 U.S.C. § 130g; National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 923, 130 Stat. 2000, 2357(2016) (codified at 10 U.S.C. § 167b) (directing the establishment of U.S. Cyber Command to a Unified Combatant Command); U.S. Congress, House of Representatives, Committee on Armed Services, Committee Report on H.R. 4909 ("National Defense Authorization Act for Fiscal Year 2017"), 114th Cong., May 4, 2016, 8 (noting the committee's view that:

> the cyber domain of modern warfare continues to grow in scope and sophistication. H.R. 4909 fully funds the budget request for cyber operations and prioritizes the readiness of the cyber mission forces. The bill provides special procurement authority to facilitate recovery from a cyber attack, as well as increases resiliency for Department of Defense networks, weapon systems, and capabilities. As part of its reform proposals, H.R. 4909 would elevate U.S. Cyber Command to a unified command to provide greater military readiness and preparedness to carry out assigned missions.).

[186] *See* Chesney, *Computer Network Operations*, *supra* note 107, at 221-22 ("Most obviously, any [cyber operation] linked to overt combat operations . . . should qualify [as TMA] without controversy . . . .").

[187] *See* BARBARA SALAZAR TORREON, INSTANCES OF USE OF UNITED STATES ARMED FORCES ABROAD, 1798-2016, CONG. RES. SERVICE (Oct. 7, 2016) (Providing an extensive list of "instances in which the United States has used its Armed Forces abroad in situations of military conflict or potential conflict or for other than normal peacetime purposes"). For example, hostage rescue operations are often conducted employing operational security measures. *See* Karen DeYoung and Greg Jaffe, *Navy SEALs Rescue Kidnapped Aid Workers Jessica Buchanan and Poul Hagen Thisted in Somalia*, WASH. POST (Jan. 25, 2015), https://www.washingtonpost.com/world/national-security/us-forces-rescue-kidnapped-aid-workers-jessica-buchanan-and-poul-hagen-thisted-in-somalia/2012/01/25/gIQA7WopPQ_story.html?utm_term=.d1d58b9c2d91.

thereto, another ill-defined exception to covert action[188]) solely on the basis that the operation will be executed in anticipation of hostilities by military personnel under military command and control. At the same time, while analogies to historical examples will be helpful, the analysis should not be so unyielding as to ignore the distinctive, non-traditional aspects of the cyber domain.

c. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) addresses the problem of computer hacking, i.e., gaining unauthorized access and causing harm to computers and networks. Congress first sought to address the hacking problem when it included in the Comprehensive Crime Control Act of 1984 stand-alone provisions making it a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer, and a felony to access classified information in a computer without authorization.[189] Codified at 18 U.S.C. § 1030, Congress amended and expanded the statute two years later with passage of the CFAA.[190] The CFAA criminalizes seven specific types of activity that fall into two broad areas: the sending of code or commands with the intent to damage or impair the operation of a protected computer without authorization; and the accessing of a protected computer without authority or by exceeding authorized access and thereby obtaining information or causing damage, impairment, or loss.[191] Conspiracy to commit and attempts to commit these crimes are also crimes.[192] Unlike the Electronic Communications Privacy Act (ECPA), the CFAA has explicit, broad extraterritorial scope.[193]

On its face, the CFAA would seem to bring within its scope many of the activities conducted during the course of military cyber operations, although each operation would require fact-specific analysis to determine whether it implicates any of the seven enumerated crimes in the statute. However, applying accepted canons of statutory interpretation and recognized public authority principles, it is apparent that such activities are exempted from the CFAA's criminal proscriptions.

Applying the CFAA to bar otherwise lawfully approved military cyber operations would plainly be contrary to basic public authority principles. The public authority doctrine, usually applied as a justification in criminal law, "holds that acts committed by a public official 'which otherwise would be criminal, such as taking or destroying property, taking hold of a person by force and against his will, placing him in confinement, or even taking his life, are not crimes if done with

[188] 50 U.S.C. § 3093(e)(4).
[189] The Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976.
[190] The Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213.
[191] 18 U.S.C. § 1030(a)(1)-(7). For purposes of the CFAA, a protected computer includes a computer "used in or affecting interstate or foreign commerce or communication . . . ." *Id.* § 1030(e)(2)(b). *See also* COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, CRIM. DIV., DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 1-3 (2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (describing background and scope of the CFAA) [hereinafter PROSECUTING COMPUTER CRIMES].
[192] 18 U.S.C. § 1030(b).
[193] *Id.* § 1030(e)(2)(B); PROSECUTING COMPUTER CRIMES, *supra* note 191, at 116.

proper public authority.'"[194] This basic principle has also been applied as a matter of statutory interpretation to Federal criminal statutes.[195] It is a recognition that "it would not make sense to attribute to Congress the intent with respect to each of its criminal statutes to prohibit all covered activities undertaken by public officials in the legitimate exercise of their otherwise lawful authorities, even if Congress has clearly intended to make those same actions a crime when committed by persons who are not acting pursuant to such public authority."[196]

Congress considered the public authority principle when it passed the CFAA and included an express exception for certain governmental activities which provides that it "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State or political subdivision of a State, or of any intelligence agency of the United States."[197] At first blush, the absence of any reference to non-IC military forces in Section 1030(f) might, applying the interpretive canon *expressio unius est exclusio alterius* (expressing one item of an associated group or series excludes another left unmentioned), undermine claims to a public authority exception.[198] This interpretive canon applies, however, "only when 'circumstances support[ ] a sensible inference that the term left out must have been meant to be excluded.'"[199] No such inference can reasonably be drawn that Congress intentionally excluded military forces from Section 1030(f)'s ambit.

Congress' intent in passing the CFAA was plainly to address the rising problem of computer hacking by private individuals for criminal purposes and to provide law enforcement with clearer guidance and tools to address illicit uses of ITT, not to restrain the President in the use of cyber capabilities for national security purposes.[200] The notion that Congress would provide greater latitude to States or their political subdivisions to conduct hacking for public safety purposes than it would to the U.S. military to protect national security is incongruous. Congress' inclusion of what appears to be almost boilerplate public-authority-exception language predates the true advent of military cyber operations.[201] Further, Section 1030(f) does not exist in isolation. It must be read in the context of Congress' subsequent and repeated recognition and tacit, if not explicit, approval of the DoD conducting offensive cyber operations, such as in Section 954 and

---

[194] Colonel Gary P. Corn, *Should the Best Offense Ever Be a Good Defense? The Public Authority to Use Force in Military Operations: Recalibrating the Use of Force Rules in the Standing Rules of Engagement*, 49 VAND. J. TRANSNAT'L. L. 1, 28 (2016) (describing the public authority doctrine and quoting ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 1093 (1982)).

[195] *See* Nardone v. United States, 302 U.S. 379, 384 (1937) (federal criminal statutes should be construed to exclude authorized conduct of public officers where such a reading "would include such officers would work obvious absurdity as, for example, the application of a speed law to a policeman pursuing a criminal or the driver of a fire engine responding to an alarm.").

[196] Memorandum from the Dep't of Justice, Office of Legal Counsel for the Attorney General, subject: Applicability of Federal Criminal Laws and the Constitution to Contemplated Lethal Operations Against Shaykh Anwar al-Aulaqi 16 (Jul. 16, 2010), https://www.justice.gov/sites/default/files/olc/pages/attachments/2015/04/02/2010-07-16_-_olc_aaga_barron_-_al-aulaqi.pdf.

[197] *Id.* § 1030(f).

[198] *See* National Labor Relations Board v. SW General, Inc., 137 S. Ct. 929, 933 (2017) (citations omitted).

[199] *Id.* (citations omitted).

[200] *See* H.R. REP. NO. 99-612, at 4-6 (1986); S. REP. NO. 99-432, at 2 (1986); PROSECUTING COMPUTER CRIMES, *supra* note 191, at 1.

[201] *See, e.g.,* 18 U.S.C. § 1028(e) (2012) (using identical language with respect to the Federal fraud and false statements statute).

10 U.S.C. § 130g. These later-in-time provisions are relevant to interpreting the CFAA, and demonstrate the incompatibility of reading it to proscribe appropriately authorized military cyber operations.[202]

In addition to subsequent legislation, funding, and repeated statements in support of DoD building and employing offensive cyber capabilities, Congress is routinely informed, both formally and informally, of DoD's cyber activities. Routine briefings are provided to the House and Senate committees of jurisdiction, senior DoD officials frequently testify before these committees and make public statements about DoD activities, and members of Congress have often acknowledged the conduct of military cyber operations in official statements.[203] This serves as further evidence that Congress does not consider these operations to be proscribed by the CFAA, or at least that Congress has acquiesced to the President's exercise of Article II authority in this regard.[204]

4. The Implications of Information Collection Authorities on Cyber Operations

With the exception of some scattered provisions such as Section 954 and 10 U.S.C. § 130g, discussed above, Congress has not passed any legislation specifically addressing military cyber operations per se. More importantly, from the perspective of a *Youngstown* analysis, Congress has passed no law specifically proscribing or circumscribing military cyber operations. To the contrary, Congress has generally expressed its support of military cyber operations, as well as its expectation that the military should play an active role in defending and advancing national security interests in and through cyberspace, as evidenced most recently by Congress' direction that U.S. Cyber Command be elevated to a full unified combatant command.[205] However, there are a number of federal statutes governing aspects of information collection, electronic surveillance, and computer "hacking," to name a few, relevant to assessing the legality of military cyber operations. Most of these laws were not drafted with the military in mind, raising interpretive questions of legislative intent. A comprehensive review of all of these laws would be a substantial endeavor. Rather, this Section provides a more focused discussion of some of the more pertinent frameworks.

a. Information Collection and Military Operations

---

[202] *See* Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 143 (2000) (citations omitted) ("The 'classic judicial task of reconciling many laws enacted over time, and getting them to 'make sense' in combination, necessarily assumes that the implications of a statute may be altered by the implications of a later statute.'")

[203] *See* 10 U.S.C. § 484 (2012) (requiring the Secretary of Defense to provide quarterly briefings to the Armed Services committees on all offensive and significant defensive military operations in cyberspace); Cheryl Pellerin, *U.S. Cyber Command Chief Testifies on Challenges, Security Initiatives*, DOD NEWS, DEFENSE MEDIA ACTIVITY (Apr. 6, 2016), https://www.defense.gov/News/Article/Article/713755/us-cyber-command-chief-testifies-on-challenges-security-initiatives (reporting on congressional testimony); Ian Duncan, *Maryland Senators Introduce Measure to Elevate Status of Cyber Command*, THE BALTIMORE SUN (May 25, 2016), http://www.baltimoresun.com/news/maryland/bs-md-cybercom-amendment-20160525-story.html (public statement of Senator Barbara Mikulski).

[204] *Cf.* Dames & Moore v. Regan, 453 U.S. 654, 657-58 (1981) (discussing congressional acquiescence to presidential action).

[205] *See* National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 923, 130 Stat. 2000, 2357(2016) (codified at 10 U.S.C. § 167b).

The President's basic power to authorize the collection of "information relating to capabilities, intentions, and activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities"[206] is firmly rooted in Article II of the Constitution and encompasses collection against strategic priorities as well as in support of military operational requirements.[207] Prior to the 1970's, the courts and Congress accorded substantial deference to the President in this arena. The collection of information for national security purposes was practically unfettered. However, owing to the discovery of several abuses of this power, the development of new and more intrusive collection technologies, and evolving understandings of the Fourth Amendment, both Congress and the Executive have since developed a robust but complex statutory and regulatory regime to govern the conduct of certain information-collection activities, especially with respect to electronic surveillance[208] and activities conducted by elements of the Intelligence Community (IC).[209] How these regimes apply to the collection of operationally relevant information as part of and in support of cyber operations is complex and legally nuanced.

To be operationally effective, military commanders require deep knowledge and understanding of both the adversary they are charged with influencing or defeating, as well as the complex and

[206] Falling broadly under the heading of "foreign intelligence." DOD DICTIONARY, *supra* note 2, at 92.
[207] *See, e.g.*, EO 12,333, *supra* note 172, □ 2.1 ("Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations.").
[208] In broad terms relevant to cyber operations, the interception of computer data transmissions. Complicating analysis is the fact that electronic surveillance is also a regulatory and statutory term of art with similar but distinct meanings that focus as much on the target and location of the surveillance as on the technique employed. *See infra* notes 255-257 and accompanying text.
[209] The Intelligence Community is a defined set of federal departments and agencies and specific elements thereof. It refers to:

> (A) The Office of the Director of National Intelligence.
> (B) The Central Intelligence Agency.
> (C) The National Security Agency.
> (D) The Defense Intelligence Agency.
> (E) The National Geospatial-Intelligence Agency.
> (F) The National Reconnaissance Office.
> (G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
> (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy.
> (I) The Bureau of Intelligence and Research of the Department of State.
> (J) The Office of Intelligence and Analysis of the Department of the Treasury.
> (K) The Office of Intelligence and Analysis of the Department of Homeland Security.
> (L) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

50 U.S.C. § 3003(4)(2012). *Accord* EO 12,333, *supra* note 172, □ 3.5(h).

dynamic environments within which they are to operate.[210] The operations process—the planning, preparation, execution, and continuous assessment of actions and outcomes—is heavily dependent on the "aggressive and continuous" collection, and when necessary, processing, exploitation, dissemination, and analysis of information not only about the adversary's capabilities, situation, and intentions, but a host of other variables within the operational environment.[211] Although often referred to generically as intelligence, the information that feeds the commander's operations process and decision making can be collected through a variety of means, not all of which constitute intelligence in the technical, and potentially legally relevant, meaning of the term.[212] For example, during traditional military operations, non-intelligence maneuver units are routinely tasked to collect and report against the commander's established information requirements.[213] The information collected may be fed into formal intelligence processes for analysis and fusion with other information, but it may also be provided directly to planners and the commander for evaluation and action. These are not distinctions without a difference. The rules and oversight structures governing intelligence and non-intelligence operations can be quite dissimilar.[214] Yet the line between intelligence and non-intelligence information collection, and the corresponding legal frameworks governing each activity, can be murky, especially in the realm of cyber operations.

The need for information and the operational processes governing its collection, processing, and management are mirrored in the case of military cyber operations, albeit with challenges uniquely related to the nature of the cyber domain, the composition of the forces conducting cyber operations, and the tools and TTPs they employ. Information relevant to planning and executing cyber operations can come from sources external to cyberspace, such as from traditional non-cyber intelligence and open-source collection.[215] But a substantial amount must be collected in and through cyberspace, including data both in transit and at rest,[216] in order to

---

[210] *See*, *e.g.*, JP 3-0, *supra* note 69, at II-9 to II-10 & III-23 to III-26 (discussing the operational assessment process and the joint intelligence function, respectively, and noting that understanding of the operational environment is fundamental to joint operations).

[211] *See* U.S. DEP'T OF THE ARMY, ARMY DOCTRINE REFERENCE PUBLICATION (ADRP) 5-0, THE OPERATIONS PROCESS □□ 1-13, 3-6 (May, 2012) (describing the operations process and noting that "[i]nformation collection (to include reconnaissance and surveillance) is indispensable to building and improving the commander's understanding."); U.S. DEP'T OF THE ARMY ARMY DOCTRINE PUBLICATION (ADP) 2-0, INTELLIGENCE □□ 1-3 (Aug. 2012) (describing the purpose of intelligence) [hereinafter ADP 2-0].

[212] Information and intelligence are not synonymous. Intelligence is "[t]he product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations," as well as "[t]he activities that result in the product." DOD DICTIONARY, *supra* note 2, at 114. That is, unless collected by an intelligence organization or under specific intelligence authorities, information alone does not constitute intelligence.

[213] Intelligence operations are just "one of the four primary means for information collection. The other three are reconnaissance, surveillance, and security operations." ADP 2-0, *supra* note 211, at 6.

[214] *See* Whitaker, *supra* note 102, 512-13, & n. 8 (noting that intelligence authorities and restrictions are "prescribed and levied based on the prerequisite requirement of [intelligence community] membership.").

[215] The traditional intelligence disciplines are: Human Intelligence (HUMINT); Signals Intelligence (SIGINT); Imagery Intelligence (IMINT); Measurement and Signature Intelligence (MASINT); Open-source Intelligence (OSINT); Technical Intelligence (TECINT); and Counterintelligence (CI). *See* Whitaker, *supra* note 102, at 531.

[216] As the terms imply, data at rest "is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way," while data in transit "is data actively moving from one location to another such as across the internet or through a private network." Nate Lord, *Data Protection: Data in Transit vs. Data at Rest*, DIGITAL GUARDIAN (updated Jul. 27, 2017) https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest.

identify, characterize, and pair effects tools against cyber targets consistent with the commander's operational scheme.[217] As illustrated earlier, cyber operations intended to collect data can be nearly indistinguishable from those intended to deliver a cyberspace effect, and may frequently be executed by the same maneuver forces along a continuum of operational activity.[218] The same forces may conduct operations across all five phases of a tactical cyber action described above,[219] including reconnaissance. This raises nuanced questions as to whether and how existing domestic legal frameworks governing information collection, especially the robust oversight processes and procedures applicable to intelligence activities, apply to cyber data-collection operations, especially those conducted by non-intelligence personnel.[220]

b. Information Collection Authorities and the Fourth Amendment

Any discussion about the legality of information-collection activities by federal forces necessarily starts with the Fourth Amendment to the Constitution.[221] The late 1960s and early 1970s saw the Supreme Court fundamentally redefine the Fourth Amendment's role in regulating the government's collection of information for national security purposes. In 1967, the Court issued its watershed decision in *Katz v. United States,*[222] where it applied the Fourth Amendment to a non-trespassory wiretap, expanding the concept of a search under the Fourth Amendment to encompass all areas where a person with standing has a reasonable expectation of privacy.[223] Although *Katz* did not directly overrule *Olmstead v. United States*,[224] the then-controlling case on wiretaps, it effectively supplanted it and established the reasonable expectation of privacy test as the touchstone for determining the permissible scope of wiretapping under the Constitution.[225] Taking its cues from *Katz* and another case decided the same term, *Berger v. New York*,[226]

---

[217] *See* JP 3-12, *supra* note 6, at II-8.

[218] *See* DOD CYBER STRATEGY, *supra* note 7, at 6 (describing the establishment and functions of the Cyber Mission Force). *See generally* JP 3-12, *supra* note 6 (describing the spectrum of cyber operations).

[219] *Supra* Section III(B).

[220] *C.f.*, H.R. No. 114-537, at 310-11 (2016) (Discussing the dual-hat arrangement between US Cyber Command and the National Security Agency (NSA), and noting the House Armed Services Committee's concern "that proper internal and external oversight of the two organizations' roles and responsibilities will become increasingly difficult to distinguish and manage the more cyber is operationalized, especially as it pertains to NSA's collection and other activities in support of national and Departmental priorities for foreign intelligence and counterintelligence, and CYBERCOM's intelligence activities to support cyber operations.")

[221] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

[222] Katz v. United States, 389 U.S. 347 (1967).

[223] *Id.* at 361 (Harlan, J. concurring).

[224] Olmstead v. United States, 277 U.S. 438 (1928).

[225] *See* HOWARD J. KAPLAN, ET. AL, THE HISTORY AND LAW OF WIRETAPPING 3 (2012), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf.

[226] Berger v. New York, 388 U.S. 41 (1967).

Congress passed the federal Wire Tap Act,[227] which in its present, expanded form—the ECPA[228]—regulates, *inter alia*, the interception of both stored and in-transit electronic communications.[229]

However, *Katz* involved domestic law enforcement, and left open the question of whether there existed a national-security exception to the Fourth Amendment.[230] The Court returned to this question five years later, specifically addressing whether the warrant requirement applied to cases of domestic surveillance for national security purposes in *United States v. United States District Court*,[231] commonly referred to as the *"Keith"* case.

In *Keith*, the Court unanimously rejected the Government's claim to such an exception, at least in the context of domestic surveillance, but emphasized the narrow scope of its decision which did not reach "the President's surveillance power with respect to the activities of foreign powers [or their agents], within or without this country."[232] In addition, in deference to the Government's arguments regarding the unique nature of non-criminal, domestic national-security investigations, the Court held that the standards and procedures for conducting surveillance for national-security purposes need not mirror those applicable to criminal investigations, and implicitly invited Congress to enact a special legal framework to govern such activities.[233] Congress took up the invitation in 1978 and passed the Foreign Intelligence Surveillance Act (FISA)*,*[234]discussed below.

---

[227] The Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90–351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2510 *et seq.*).
[228] 18 U.S.C. § 2510 *et seq.*
[229] *Id.* § 2511. For purposes of ECPA, electronic communication "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." *Id.* § 2510(12). The ECPA provides for a number of exceptions to section 2511's general prohibition against intercepting electronic communications; chief among them being a "Title III" authorization as part of a Federal law enforcement investigation. *See id.* §§ 2516, 2517.
[230] Katz v. United States, 389 U.S. 347, 353 (1967). Hence, as originally passed, the Wire Tap Act excluded wiretaps for national security purposes, providing:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities . . . .

18 U.S.C. § 2511(3) (1970 ed.).
[231] United States v. United States District Court, 407 U.S. 297 (1972) ("The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval.").
[232] *Id.* at 308; *see also id.* at 321-22 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.")
[233] *Id.* at 321-24.
[234] Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783 (Oct. 25, 1978), 50 U.S.C. §§ 1801 *et seq.*

Before turning to ECPA and FISA, however, a note on the extraterritorial applicability of the Fourth Amendment is in order. It is well settled that absent a "substantial" or "sufficient connection" to the United States, a nonresident alien abroad enjoys no protection under the Fourth Amendment.[235] On the other hand, it is equally well-settled that at least the reasonableness clause of the Fourth Amendment applies to the conduct of U.S. agents directed against U.S. citizens, and likely lawful permanent residents (LPR), wherever they or their property are located.[236] And although the *Keith* Court refused to recognize a blanket exception to the warrant requirement for domestic surveillance, and the Supreme Court has never ruled on the issue of whether a foreign search of a U.S. citizen or LPR must be supported by a warrant or probable cause, a number of lower-court decisions have made clear that the warrant clause has no extraterritorial applicability.[237] Therefore, it is reasonable to conclude that government searches of U.S. citizens (and likely LPRs) or their property abroad must still satisfy the reasonableness standard of the Fourth Amendment, but do not require prior judicial approval. It is also well recognized that searches, in the form of electronic surveillance or otherwise, of non-U.S. citizens abroad who lack sufficient connections to the United States, are subject only to restraints that the Executive or Congress may, at their discretion, proscribe. The Executive and Congress have done so only for a narrow set of circumstances through EO 12,333 and Section 702 of FISA Amendments Act of 2008,[238]respectively.

c. Electronic Communications Privacy Act

As noted, Congress passed the Wire Tap Act in 1968 as "a comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both activities in general terms but that also permitted federal and state law enforcement officers to use them under strict limitations designed to" conform to the Supreme Courts guidance in *Berger*.[239] The evolution of digital ITT quickly outstripped the Wire Tap Act's usefulness, prompting Congress to enact ECPA in 1986 "to both protect the privacy of an individual's electronic communications and provide the government with a means for accessing these communications and related records."[240] ECPA has been interpreted over time to cover a broad range of data both in transit and at rest, including the content of emails, private instant messages, YouTube and similar videos, as well as some non-

[235] *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).
[236] *See*, *e.g.,* United States v. Odeh (In re Terrorist Bombings of U.S. Embassies in E. Afr. (Fourth Amendment Challenges), 552 F.3d 157, 167 (2nd Cir. 2008) (holding that searches conducted abroad by U.S. agents of U.S. citizens must satisfy the Fourth Amendment's requirement of reasonableness). *But see* United States v. Barona, 56 F.3d 1087, 1094 (9th Cir. 1995) (noting, but declining to answer, whether a resident alien has undertaken sufficient obligations of citizenship or developed a sufficient connection with the United States to be considered protected by the Fourth Amendment even when abroad).
[237] United States v. Stokes, No. 11-2734 (7th Cir. 2013); In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157 (2nd Cir. 2008); *see also* Verdugo-Urquidez, 494 U.S. at 278 (Kennedy, J. concurring) (" The absence of local judges or magistrates avail- able to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials all indicate that the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country."); *id.* at 279 (Steven's J., concurring); *id.* at 279 (Blackmun, J., dissenting).
[238] FISA Amendments Act of 2008, P.L. 110-261, § 101, 122 Stat. 2436 (2008) (codified at 50 U.S.C. §§ 1881-1881g).
[239] CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 5 (Oct. 9, 2012).
[240] RICHARD M. THOMPSON II & JARED P. COLE, CONGRESSIONAL RESEARCH SERVICE, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) Summary (2015).

content metadata. With respect to data at rest, ECPA's coverage extends only to electronic communications held by "electronic communication service" (ECS) providers and "remote computing service" (RCS) providers; in essence, internet service providers (ISP).[241]

Now codified in Title I of the ECPA, the Wire Tap Act regulates the interception of data in transit, and specifically excludes from its scope: 1) interceptions authorized pursuant to FISA;[242] and 2) interceptions by federal agents of "foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal Law involving a foreign electronic communications system, utilizing a means other than" FISA electronic surveillance.[243] That is, the Wire Tap Act contains a public authority exception to its general proscription of electronic eavesdropping (data interception), but limits the procedural constraints attached to that exception to "the interception of *domestic* wire, oral, and electronic communications" for law enforcement purposes.[244] Thus, ECPA's Title I procedures are the exclusive means by which the government can conduct *domestic* interceptions of electronic communications, other than FISA electronic surveillance.[245] Because law and policy place significant restrictions on the use of the military for law enforcement activities within the United States and generally limit the military to conducting cyber operations extraterritorially, and because the information targeted during those operations constitutes foreign intelligence information, military cyber-data collection operations fall outside the scope of Title I of ECPA.[246]

As for data at rest, at least regarding communications content stored with an ISP, the analysis is not as straight forward. When it passed ECPA, Congress sought to extend privacy protections similar to Title I to electronic communications stored with an ISP.[247] Title II of ECPA, the Stored Communications Act (SCA),[248] makes it a crime to intentionally obtain, alter, or prevent authorized access to stored electronic communications by means of accessing without

---

[241] Electronic communication service "means any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). A remote computing service means "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). Essentially, internet service providers. *See* Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 206-7 (2nd Cir. 2016).

[242] 18 U.S.C. § 2511(e) ("Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.").

[243] 18 U.S.C. § 2511(2)(f).

[244] *Id.* The authority to submit an application to a Federal judge of competent jurisdiction is limited to specified officials of the Department of Justice, to obtain an interception authorization for the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of, one of the predicate criminal offenses defined in the statute. *See id*. §§ 2516, 2518.

[245] *Id.*

[246] *See* 18 U.S.C. § 1385 (2012) (Posse Comitatus Act); 10 U.S.C. § 371, *et seq.* (2012); U.S. DEP'T OF DEF., INSTRUCTION 3025.18, DEFENSE SUPPORT OF CIVIL AUTHORITIES (DSCA) (Dec. 29, 2010, incorporating Change 1, Sep. 21, 2012).

[247] Microsoft Corp., 829 F.3d at 201 ("When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider.").

[248] 18 U.S.C. § 2701 (2012), *et. seq.*

authorization or in excess of authorization a facility through which an ECS or RCS is provided.[249] Leaving difficult interpretive questions aside regarding the scope of protected data and ITT systems, on its face the SCA appears to reach a broad range of activity that might encompass some extraterritorial cyber data-collection, which would not, at first glance, seem to fall within the SCA's three enumerated exceptions.[250] As an initial matter, it is unclear whether the SCA's criminal provisions have extraterritorial reach. Applying traditional rules of statutory interpretation, the better read is that they do not. The Second Circuit recently held that the SCA's warrant provisions do not apply overseas, as the statute has no "clear indication of extraterritorial application."[251] There is nothing to indicate that the presumption against extraterritorial effect does not apply equally to the SCA as a whole.[252] Regardless, Congress has extended to the SCA the same public authority exception applicable in the Title I context for the collection of foreign intelligence information. Section 2511(f) of ECPA specifically cross-references chapter 121 of Title 18—the SCA.[253]

Therefore, military cyber data-collection operations conducted outside the United States fall outside the scope of ECPA. They may trigger FISA, however, depending on the target and location of the collection.

d. Foreign Intelligence Surveillance Act

Congress originally enacted FISA to provide the Executive Branch the authority, within defined parameters, to use electronic surveillance to collect foreign intelligence.[254] FISA provided a statutory framework by which the Executive Branch could conduct specific types of electronic surveillance against foreign powers or their agents, to include United States persons, within the

[249] *Id.* § 2701(a). An ECS means "any service which provides to users thereof the ability to send or receive wire or electronic communications;" telephone and electronic mail companies generally, but not exclusively. *See* 18 U.S.C. § 2510(15) (defining ECS).

[250] Section 2701(c) provides three statutory exceptions to a violation of the SCA. Specifically, the SCA does not apply to conduct authorized: "(1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user; or (3) in section 2703, 2704 or 2518 of this title." 18 U.S.C. § 2701(c)(1)-(3). Of these, only one addresses activities by government agents, excluding conduct authorized pursuant to the law-enforcement subpoena and warrant provisions of sections 2703 and 2704 of the SCA, or section 2518 of Title I. *Id.* § 2701(c)(3).

[251] Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 209, 222 (2nd Cir. 2016).

[252] When interpreting federal statutes, courts presume Congress intended them to "apply only within the territorial jurisdiction of the United States," unless a contrary intent clearly appears. Morrison v. National Australian Bank Ltd., 561 U.S. 247, 255 (2010); *see also* RJR Nabisco, Inc. v. European Cmty., 579 U.S. __, __ (2016), 2016 WL 3369423, at *7 (June 20, 2016). To overcome this presumption, "the statutory provision must contain a 'clear indication of an extraterritorial application'; otherwise, 'it has none.'" Microsoft Corp. 829 F.3d at 209 (quoting Morrison, 561 U.S. at 255). *But see* United States v. MacAllister, 160 F.3d 1304, 1307-08 (11th Cir. 1998) (citing United States v. Bowman, 260 U.S. 94 (1922), and holding Congress "need not expressly provide for extraterritorial application of a criminal statute if the nature of the offense is such that it may be inferred").

[253] 18 U.S.C. § 2511(f).

[254] *See*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, THE FISA AMENDMENTS ACT: Q&A (2017), https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf [hereinafter FISA AMENDMENTS ACT: Q&A]; NATIONAL SECURITY LAW: PRINCIPLES AND POLICY, *supra* note 148, at 197 (discussing the purposes of the FISA; JIMMY GURULE´& GEOFFREY S. CORN, PRINCIPLES OF COUNTER-TERRORISM LAW 205 (2011) [hereinafter GURULE´& CORN].

United States.[255] Although the FISA has been amended several times since 1978 to expand its scope,[256] the core focus of the statute, captured in Title I, remains the regulation of "electronic surveillance"—a specific statutory definition that depends as much on the target (foreign powers or their agents) and location of the collection (inside the United States) as it does on the technical means used.[257] With respect to covered surveillance activities, the FISA sets out a complex and extensive set of procedural and oversight requirements, and with limited exception requires prior judicial approval by the Foreign Intelligence Surveillance Court (FISC) based on probable cause to believe both that the proposed target is a foreign power or an agent of a foreign power and that the facility to be surveilled (e.g., telephone number, email address, or other ITT) is or is about to be used by that target.[258]

---

[255] *See* FISA AMENDMENTS ACT: Q&A, *supra* note 254, at 1-2; *see also* 50 U.S.C. § 1801(b)(2) (defining agent of a foreign power as "any person"); *id*. § 1801(f) (defining electronic surveillance as including surveillance against a U.S. person); GURULÉ & CORN, *supra* note 254, at 207-09. For purposes of FISA, a United States person means:

> a citizen of the United States, an alien lawfully admitted for permanent residence . . ., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power . . . .

50 U.S.C. § 1801(i).

[256] Title III, governing physical searches within the United States, was added by amendment in 1994. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443 (1995) (codified as amended at 50 U.S.C. §§ 1821-29 (2012)). Title IV, added in 1998, covers the use of pen registers and trap and trace devices. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105- 271, § 601(2), 112 Stat. 2396, 2405 (codified as amended at 50 U.S.C. §§ 1841-46 (2012). Title V, added in 2001, provides for access to certain business records for foreign intelligence purposes. *See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified at 50 U.S.C. § 1861). Titles I and III of FISA, which apply, respectively, to electronic surveillance and physical searches inside the United States for foreign intelligence purposes, are considered "Traditional FISA." *See* FISA AMENDMENTS ACT: Q&A, *supra* note 254, at 1-2.

[257] For purposes of FISA, "electronic surveillance" means:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f).

[258] *See* FISA AMENDMENTS ACT: Q&A, *supra* note 254, at 1-2.

Title I FISA applies only to electronic surveillance conducted in the United States. When originally enacted, it was Congress' specific intent to exclude from FISA's ambit extraterritorial collection of foreign intelligence which, when conducted by elements of the IC, was governed by EO 12,333.[259] However, this original construct failed to keep pace with the evolution of ITT and the fact that a substantial amount of internet traffic now traverses ISP infrastructure in the United States, including communications between and among foreign persons abroad.[260] Congress passed the FISA Amendments Act (FAA) in 2008 to address this reality, providing procedures for domestic collection targeting certain persons outside of the United States for purposes of foreign intelligence.[261]

The FAA, codified in Title VII of FISA, addresses three distinct situations. First, Section 702 of the FAA permits the Attorney General (AG) and the Director of National Intelligence (DNI) to jointly authorize collection within the United States that targets foreign persons located outside the United States, based either on an order from the FISC or a determination that exigent circumstances exist risking loss of "intelligence important to the national security of the United States" and time does not permit seeking an order from the FISC.[262] Section 702 collection is based not an individual court order, but rather on annual certifications the AG and DNI submit to the FISC specifying the categories of intelligence authorized for collection, as well as targeting and minimization procedures designed to ensure only foreign persons outside of the United States are targeted, and to protect any incidentally collected U.S. person information.[263] Second, Section 703 provides for FISC authorization to target "a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data . . . ."[264] Third, Section 704 of the FAA prohibits any "element of the intelligence community" from targeting a U.S. person reasonably believed to be outside the United States to acquire foreign intelligence under circumstances where the targeted individual has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States.[265]

A complete review of the procedural requirements of the FISA, to include the FAA, and the myriad legal issues related to its application are beyond the scope of this chapter and have received considerable attention elsewhere.[266] Understanding the baseline issue of whether FISA applies to military forces collecting operationally relevant information in and through cyberspace is, however, critical, for at least two reasons. First, FISA provides for the exclusive means by which electronic surveillance, as defined in Section 1801(f), may be conducted,[267] and anyone who engages in electronic surveillance except as authorized by FISA is subject to criminal and

[259] *Id.* at 2; *see infra* Section IV(A)(4)(e) discussing EO 12,333.
[260] See i*d.*; NATIONAL SECURITY LAW: PRINCIPLES AND POLICY, *supra* note 148, at 219.
[261] FISA Amendments Act of 2008, P.L. No. 110-261, 122 Stat. 2436.
[262] 50 U.S.C. § 1881a.
[263] *Id.*; FISA AMENDMENTS ACT: Q&A, *supra* note 254, at 3.
[264] 50 U.S.C. § 1881b.
[265] *Id.* § 1881c.
[266] *See, e.g.*, NATIONAL SECURITY LAW: PRINCIPLES AND POLICY, *supra* note 148, ch. 7.
[267] 18 U.S.C. § 2511(f); 50 U.S.C. § 1812.

civil sanction.[268] Second, as a basic matter of mission authorities within the DoD, "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communications"[269] aligns with the definition of Signals Intelligence (SIGINT).[270] Within the IC, the Director of the National Security Agency is designated as the Functional Manager for SIGINT, and within the DoD "no other department or agency may engage in SIGINT activities except pursuant to a delegation by the Secretary of Defense, after coordination with the DNI."[271]

Thus, Title I FISA electronic surveillance is the sole province of the NSA, unless properly delegated as a SIGINT activity in accordance with EO 12,333, in which case it is still subject to the procedures governing DoD intelligence activities as well as those promulgated by the DIRNSA.[272] The same holds true for electronic surveillance conducted under Sections 702 and 703 of the FAA. In contrast, FAA Section 704's scope is specifically limited to elements of the IC.[273] In other words, FISA governs *any* collection of foreign intelligence within the United States by means of electronic surveillance (or the other techniques addressed in the statute). Where the point of collection is overseas, DoD elements of the IC must obtain authorization from the FISC to target U.S. persons abroad; otherwise intelligence activities targeting foreign persons abroad are governed by EO 12,333 and DoD intelligence oversight regulations. For non-IC elements of the DoD, i.e., operational maneuver forces, cyber data collection is governed only by the reasonableness clause of the Fourth Amendment when applicable, as well as any mission-specific constraints or restraints.

e. Executive Order 12333

In the early 1970s, both the Senate and the House of Representatives conducted several investigations into allegations of civil-rights abuses by several Federal agencies, including the DoD.[274] As a result, in an effort to stave off statutory intervention, President Ford issued an executive order establishing a basic charter for the IC and placing significant controls on the conduct of all intelligence activities.[275] The present version of this order, EO 12,333, "establishes the Executive Branch framework for the country's national intelligence efforts, and for protecting privacy and civil liberties in the conduct of intelligence activities . . . ."[276] As one author notes, intelligence activities (that is, activities conducted by elements of the IC) fall within

---

[268] 50 U.S.C. § 1809.
[269] 50 U.S.C. § 1801(f).
[270] Signals Intelligence is "[a] category of intelligence comprising, either individually or in combination, all communications intelligence, electronic intelligence, and foreign instrumentation signal intelligence, however transmitted." U.S. DEP'T OF DEF., INSTRUCTION O-3115.7, SIGNALS INTELLIGENCE (SIGINT) Glossary (Sep. 15, 2008, incorporating Change 1, Nov. 19, 2010) [hereinafter DoDI O-3115.7].
[271] *Id.* at 4; *see also* EO 12,333*, supra* note 172, § 1.7(c) (establishing responsibilities and authorities of the National Security Agency).
[272] EO 12,333, *supra* note 172, § 1.7(c); DoDI O-3115.7, *supra* note 270, 4; *see also* DEP'T OF DEF. MANUAL 5240.1, PROCEDURES GOVERNING DOD INTELLIGENCE ACTIVITIES (Aug. 8, 2016) [hereinafter DoD Manual 5240.1].
[273] 50 U.S.C. § 1881(c) ("No element of the intelligence community may . . . .").
[274] *See* Whitaker, *supra* note 102, at 542-43; U.S. DEP'T OF DEF. SENIOR INTELLIGENCE OVERSIGHT OFFICIAL, HISTORY OF THE DEPARTMENT OF DEFENSE INTELLIGENCE OVERSIGHT PROGRAM, http://dodsioo.defense.gov/About-DOD-SIOO/History (last visited Dec. 5, 2017).
[275] Exec. Order No. 11,905, 41 Fed. Reg. 7703 (Feb. 19, 1976).
[276] STATUS OF ATTORNEY GENERAL APPROVED U.S. PERSON PROCEDURES UNDER E.O. 12333 May 16, 2017, https://www.dni.gov/files/CLPT/documents/Chart-of-EO-12333-AG-approved-Guidelines_May-2017.pdf.

a "'quasi-restrictive' area of law, which means that every intelligence activity or operation must be tied to an [affirmative] authority that can be traced to" the Commander in Chief.[277] EO 12,333 provides that positive authority for the IC elements. It also sets out a series of restrictive oversight rules designed to ensure intelligence collection efforts are consistent with the Constitution and individual civil liberties, primarily the Fourth Amendment. It is the President's foundational authorizing document for the IC and establishes the basic oversight procedures governing the collection, retention, and dissemination of information concerning United States persons—a legal term of art[278]—by the IC elements, to include by means of electronic surveillance.[279]

f. DoD Implementation of Intelligence Oversight

The DoD implements EO 12,333 and the FISA through *DoD Manual 5240.1, Procedures Governing the Conduct of DoD Intelligence Activities*[280] and its classified annexes, which govern "the conduct of Defense Intelligence Components and non-intelligence components or elements, or anyone acting on behalf of those components or elements, when conducting intelligence activities under DoD's authorities."[281] In broad terms, it establishes the procedures through which the Defense Intelligence Components and those other personnel within the manual's scope are authorized to collect, retain, and disseminate U.S. person information generally, with specific procedures governing the use of certain collection techniques to obtain information for foreign intelligence and counter-intelligence purposes. Procedure 5 of the manual implements both EO 12,333's electronic surveillance provisions, as well as the FISA.[282] As the manual notes, "[t]he legal framework for conducting electronic surveillance is dependent upon the Defense Intelligence Component's mission, the U.S. person status and location of the target, the methods used to conduct the electronic surveillance, and the type of communication sought."[283]

The complexity of the statutory and regulatory framework governing data collection in and through cyberspace should be apparent. The rule sets are labyrinth like, and do not map neatly to the realities of the cyber domain as they turn on concepts of geography and the ability to affiliate

[277] Whitaker, *supra* note 102, at 520.
[278] For purposes of EO 12,333, United States person "means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." Exec. Ord. No. 12,333, *supra* note 172, § 3.5(k). FISA defines United States person slightly differently, as "a citizen of the United States, an alien lawfully admitted for permanent residence . . . , an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3)" of the statute. 50 U.S.C. § 1801(i).
[279] EO 12,333 defines electronic surveillance as the "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter." Exec. Ord. No. 12,333, *supra* note 172, § 3.5(c).
[280] DEP'T OF DEF. MANUAL 5240.1, PROCEDURES GOVERNING DOD INTELLIGENCE ACTIVITIES (Aug. 8, 2016) [hereinafter DoD Manual 5240.1].
[281] *Id.* at § 1-1.
[282] *Id*. at § 3-5.
[283] *Id.*

data or information to specific individuals. Nevertheless, each operation intended or reasonably anticipated to collect operationally relevant information must be carefully constructed, managed, and overseen to ensure compliance with these interrelated legal frameworks.

The foregoing represents an incomplete but significant sampling of the domestic law issues implicated by the evolving use of cyber capabilities as a means of military operations, especially outside the context of armed conflict. We now turn to the even more ambiguous realm of international law and its application to gray-zone cyber activities.

B. International Legal Framework

This Part discusses the principles and provisions of international law that lawyers should be mindful of in advising on military cyber operations that occur within the gray zone between peace and armed conflict.

That U.S. military operations must comply with applicable international law is a non-controversial proposition.[284] The same holds true for cyber operations—what some describe as traditional military operations conducted in a non-traditional domain.[285] The U.S. has consistently stated its view that international law applies to state conducted or sponsored activities in cyberspace, and considers the acceptance and advancement of this baseline premise to be a cornerstone of its strategic framework for achieving international cyber stability.[286] The international community is, by and large, in accord with this view.[287] Unfortunately, as of yet recognition of this basic premise has not reduced to any significant degree the substantial

[284] DOD LAW OF WAR MANUAL, *supra* note 8, ¶ 16.3.2 ("International law and long-standing international norms are applicable to State behavior in cyberspace."); JP 3-12, *supra* note 6, at III-10 ("DOD must conduct CO consistent with US domestic law, applicable international law, and relevant USG and DOD policies.").

[285] Joseph McGee, Deputy Commander for Operations, United States Army Cyber Command, Remarks Delivered to The Judge Advocate General of the Army's World Wide Continuing Legal Education Conference. Although helpful in some regards, the analogy should not be overstated. Many aspects of cyberspace and cyber operations differ substantially from more traditional domains and operations, creating special challenges. *See Military Cyberspace Operations*, *supra* note 46, at 130.

[286] *See* Brian J. Egan, Legal Adviser, Dep't of State, Remarks Delivered at Berkeley Law School: Remarks on International Law and Stability in Cyberspace (Nov. 10, 2016), *available at* https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf; INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 16, at 8-10.

[287] Schmitt, *Peacetime Cyber Responses*, *supra* note 4, at 242. The degree of consensus on this point took an unfortunate set back in 2017 when the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (commonly referred to at the UN GGE) seemingly reversed the consensus view adopted in 2013 and reiterated in 2015 that international law applies to states' activities in cyberspace. Cuba, Russia, and China reportedly refused to agree that international humanitarian law, the right of self-defense, or the right to otherwise respond to internationally wrongful acts (countermeasures) apply. *See* Arun Mohan Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, LAWFARE (Jul. 4, 2017), https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well; Adam Segal, *The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?*, COUNCIL ON FOREIGN RELATIONS (Jun. 29, 2017) https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what; Michele G. Markoff, Deputy Coordinator for Cyber Issues, U.S. Dep't of State, Remarks as Prepared for The Chairman, UN GGE: Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (Jun. 23, 2017), https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

normative uncertainties surrounding cyberspace, or the willingness of states to exploit them. Ambiguity persists because the question of *whether* international law applies to cyberspace—by now relatively well settled—is overshadowed by the far more difficult question of precisely *how* particular rules of international law apply to cyber activities; a question that continues to generate significant debates.[288]

It is a fair question whether these uncertainties represent true lacuna in the law, or simply stem from a lack of states' willingness to publicly acknowledge cyber operations or their views on the legal bases supporting them. Regardless, it is evident that the advent of cyberspace has created very real challenges to the existing framework of international peace and security, starting with the international legal structure undergirding it. As we have seen, legal ambiguity is a defining characteristic of the gray zone between war and peace, a zone ripe for exploitation by revisionist states.[289] Yet achieving greater clarity is hindered by the novel, rapidly evolving nature of cyberspace on the one hand, and the slow, iterative process of transposing extant international law principles and norms on the other. For those charged with advising senior policy and decision makers, applying existing international law "to new cyber-circumstances [and threats]," in ways that remain "faithful to enduring principles, while accounting for changing times and technologies" can be exceptionally difficult.[290] However, interpretive challenges do not relieve legal advisors of their duty to assist policymakers and commanders with assessing cyber threats and fashioning responses consistent with the United States' obligations under international law. What follows is a review of some of the more salient aspects of the international legal framework applicable to military cyber operations, with a particular focus on areas of gray zone ambiguity.

1. The Law of State Responsibility

Whether advising on the proper legal characterization of malicious cyber activity directed against the United States and available response options, or reviewing a proposal to conduct a cyber operation as a matter of first resort, the starting point for analysis is the baseline principle in the customary laws of state responsibility that states are legally responsible only for acts or omissions that are attributable to them and which constitute a breach of an international obligation of the responsible state.[291] In other words, states are obligated to conform their

---

[288] *See* Schmitt, *Peacetime Cyber Responses, supra* note 4, at 242 ("While there is no longer any serious debate as to whether international law applies to transborder cyber operations, the international community has been unable to achieve consensus on the precise application of many international law principles and rules that govern them.").

[289] *See supra* notes 7 and accompanying text; s*ee also*, Schmitt, *Grey Zones*, *supra* note 11, at 1-3 (discussing Russia's "hack" of the Democratic National Committee and noting that "[s]uch normative uncertainty provided fertile ground upon which the Russians could conduct their operations.").

[290] Harold Hongju Koh, Legal Adviser, U.S. Dep't. of State, Keynote Address to the USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), *reprinted in* 54 HARV. INT'L L. J. ONLINE 4 (2012).

[291] *See* Draft Articles on Responsibility of States for Internationally Wrongful Acts, art. 2, adopted by the Commission at its fifty-third session in 2001 (Final Outcome) (International Law Commission [ILC]) UN Doc. A/56/10, 43, UN Doc. A/RES/56/83, Annex, UN Doc. A/CN.4/L.602/Rev.1, GAOR 56th Session Supp. 10, 43 [hereinafter Draft Articles on Responsibility of States]. Although not a treaty, the UN General Assembly commended the Articles to governments by General Assembly resolution, and many aspects of the Articles are

activities to the terms of applicable primary rules of international law, whether based in custom or treaty, and can be held legally accountable for breaches of those obligations when sufficient evidence exists to attribute violations to them. Yet despite the proliferation of state conducted or sponsored malicious cyber activity since at least 2012, establishing either of these constituent elements of state responsibility has proved extremely difficult.

The rapid development of cyberspace and the employment of cyber operations as a method of statecraft, as well as the nature of cyber technology itself, have created significant challenges to assessing the potential international wrongfulness of cyber operations. First, with perhaps one very limited exception, states have not enacted any treaties regulating cyberspace or cyber operations per se.[292] Nor have any cyber-specific customary international law norms clearly formed.[293] Therefore, questions persist regarding the nature, scope, and applicability of existing rules of international law to state cyber activities. Second, the technological difficulty of identifying the sponsors of malicious cyber actions has generated substantial questions, and confusion, regarding the role attribution plays as a secondary norm of international law. Each of these issues will be addressed in turn.

2. International Obligations

Logically, the question of whether an act breaches an international obligation turns first on whether an obligation exists *vel non*. That is, does international law regulate the activity at issue? When states "engage in acts that are . . . unregulated by international law," state responsibility is simply not implicated.[294] Thus, even where cyber actions by one state are objectionable, or even prejudicial to another state, unless they constitute a breach of an international obligation they are matters relegated to diplomatic responses, possibly including acts of retorsion, but do not involve legal responsibility.[295]

International legal obligations can be based in either treaty or customary law, or both, and can be breached by either action or omission.[296] Based on the nature of cyberspace, cyber operations have the potential to cut across all operational domains and thereby implicate numerous international law regimes, such as international human rights law, the law of the sea, and even

considered as reflective of customary international law. G.A. Res. 56/83, UN Doc. A/RES/56/83 (Dec. 12, 2001). *See also* JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 43 (2013) (The Draft Articles "are considered by courts and commentators to be in whole or in large part an accurate codification of the customary international law of state responsibility."); TALLINN 2.0, *supra* note 23, at 79 & n. 112.

[292] *See* Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

[293] Again, consider the breakdown in the UN GGE process and the inability of the participating states to achieve meaningful consensus on even baseline rules of international law applicable to cyberspace.

[294] TALLIN 2.0, *supra* note 23, at 85.

[295] *See id.* Retorsions are acts that may be considered "unfriendly," such as sanctions, but are not unlawful. *Id.* at 112 (citing Articles on State Responsibility, *supra* note 291, commentary to pt. 3, ch. II, □ 3).

[296] Schmitt, *Grey Zones*, *supra* note 11, at 256.

space law.[297] As such, each proposed operation must be subjected to an exacting review to assess consistency with potentially applicable international obligations; a review further complicated by the fact that the actual content of each state's international obligations can vary from one state to another.[298]

The advent of new technologies, especially those with military application, invariably generates questions as to whether existing legal frameworks are adequate to cover the employment of those technologies, or instead they fall outside the scope of existing rules altogether. But the law generally abhors a vacuum, and more often than not states tend to apply existing frameworks, at least conceptually, to new technologies. They do so through what Professor Harold Koh refers to as a "translation exercise"—looking to the "spirit" of existing law to adapt it to the "present-day situation."[299] Engaging in this translation exercise to determine whether a particular cyber action or operation would constitute a breach of an international obligation must be done mindful of the unique aspects of the domain, the central, near exclusive role states play in the making of international law, and the generally permissive structure of international law itself, reflected in the so-called *Lotus* principle.

Derived from the Permanent Court of International Justice's (PCIJ) 1927 judgment in *The SS Lotus* case,[300] the *Lotus* principle has long been understood to stand for the proposition that states are free to act on the international plane except to the extent that their actions are proscribed by treaty or customary international law.[301] The case arose out of an at-sea collision between a French steamship and a Turkish collier resulting in the death of eight Turkish nationals.[302] In rejecting France's claim before the PCIJ that Turkey had violated international law by asserting criminal jurisdiction over the French officer in charge of the S.S. Lotus, the court noted that:

> [i]nternational law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. *Restrictions upon the independence of States cannot therefore be presumed*.[303]

---

[297] *Id.* For a comprehensive compilation and analysis of the relevant international law frameworks, see TALLINN MANUAL 2.0, *supra* note 23.
[298] James R. Crawford, State Responsibility, OXFORD PUBLIC INTERNATIONAL LAW, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1093.
[299] Harold Hongju Koh, Keynote Address to The Emory Law School 2016 Randolph W. Thrower Symposium, Redefined National Security Threats—Tensions and Legal Implications: The Emerging Law of 21st Century War (Feb. 11, 2016), http://law.emory.edu/elj/_documents/volumes/66/3/koh.pdf.
[300] The S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7) [hereinafter *Lotus*].
[301] Gary P. Corn & Robert Taylor, *Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Sovereignty in the Cyber Age*, 111 AM. J. INT'L L. UNBOUND 207, 209 (2017).
[302] *Lotus*, 1927 P.C.I.J. (ser. A) No. 10, at 10-13.
[303] *Id.* at 18.

Although not expressly stated, the core issue at play in *Lotus,* and at the heart of the international law principle drawn from the cited passage, is the question of state sovereignty and the normative role it plays in international law, perhaps the most contentious aspect of international law as applied to cyberspace.[304] The gravamen of France's claim in the case was that Turkey had over-asserted its sovereignty to the detriment of France's competing sovereign prerogative to exercise exclusive proscriptive jurisdiction over its own nationals. Faced with this clash of external and internal sovereign interests, the court declined to restrict Turkey's exercise of jurisdiction absent clear evidence of an established rule of international law circumscribing its freedom to do so. The PCIJ's positivist approach has shaped international law to this day.[305]

This is not to say that states enjoy unfettered freedom of action vis a vis one another. States have agreed to numerous limitations on their "free will," surrendering aspects of their sovereignty and subscribing to myriad proscriptive rules. Of greatest relevance to cyber operations, states have established through both custom and treaty clear prohibitions against unlawful uses of force and against certain interventions in the internal affairs of other states. While difficult questions remain as to the specific scope and scale of cyber-generated effects that would violate these binding norms, "the rules provide a reasonably clear framework for assessing the legality of state activities in cyberspace above these thresholds . . . ."[306] It is below these thresholds where the legal analysis gets murkier.

Before discussing the aspects of international law that may directly apply to cyber operations in the gray zone, specifically the principles of non-intervention and sovereignty, it is necessary to discuss how the *jus ad bellum* prohibition against the use of force may apply in the context of cyber operations.

a. The Prohibition against the Use of Force

When it comes to cyber operations, perhaps the most frequently posed question by policy and lawmakers alike is what constitutes a cyber "act of war?[307] The question is understandable given

[304] Significant debate exists as to whether the principle of sovereignty, territorial sovereignty to be exact, operates as a primary rule of international law regulating states' actions in cyberspace, or is more accurately understood as a general principle lacking normative force but undergirding the development of binding norms such as the prohibition on the use of force. Whether territorial sovereignty is a binding rule of international law, and if so, what the contours of the rule are, are significant questions in the realm of gray-zone cyber operations. As stated, cyber operations that do not contravene an established rule of international law may be "unfriendly," but are not internationally wrongful. As such, they are available to states as legitimate means and methods of pursuing their objectives. Inversely, they can only be countered through lawful means. The normative status of the principle of sovereignty is addressed *infra* Section IV(B)(2)(c).

[305] *See* Hugh Handeyside, *The Lotus Principle in ICJ Jurisprudence: Was the Ship Ever Afloat?*, 29 MICH. J. OF INT'L L. 71, 72, 77-80 (2007).

[306] Corn & Taylor, *supra* note 301, at 207.

[307] For example, Senator Mike Rounds of Nevada introduced a bill in 2016, titled "Cyber Act of War Act of 2016," which would have directed the President to, among other things, "develop a policy for determining when an action carried out in cyberspace constitutes a use of force against the United States . . . ." H.R. 5220; *see also* Bryant Jordan, *US Still Has No Definition for Cyber Act of War*, MILITARY.COM (Jun. 22, 2016), http://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html; Ellen

the steady increase in state-sponsored and state-conducted malicious cyber activity, the growing recognition of the threat these activities pose, and the difficulty of characterizing them beyond rhetorical generalities. Many view the ability to set red lines and deter cyber threats as dependent on clearly defining the line between war and peace in cyberspace, and there is little question that states are seizing on this ambiguity to push boundaries.[308] Certainly, greater clarity in this area would aid efforts to regulate behavior and deter destabilizing activity in cyberspace.[309] However, to date no state has asserted that any of these activities, in and of themselves, have crossed the threshold of war.[310] Fortunately, international law does not leave states powerless to defend against and respond to gray-zone cyber threats.[311] Before turning to the array of options available to states, proper framing of the "act of war" question is in order.

Properly characterizing cyber operations and threats is no doubt important, as "[a]ny decision to employ force [or other measures to address cyber threats] must rest upon the existence of a viable legal basis in *international law* . . . ."[312] Nevertheless, as typically framed, the question of what constitutes a cyber act of war is somewhat of a distraction. It is legally vague and essentially unanswerable in that, just as in the physical domains, determining what constitute legitimate casus belli is a fact specific inquiry that "involves, and should involve, strategic and political factors that render attempts to produce unambiguous definitions futile."[313] Determining what actions cross the threshold between peace and war, irrespective of modality, "has always been complex."[314]

Further contributing to confusion is the recurrent use of the inexact term "attack" to refer to all manner of malicious or unauthorized cyber activity, regardless of the perpetrator, purpose, or

---

Nakashima, *When Is a Cyberattack an Act of War?*, WASH. POST (Oct. 26, 2012), https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html?utm_term=.79f2f366be90.

[308] *See* Mike Rounds, *Defining a Cyber Act of War: The Rules Regarding This Dangerous Threat Aren't Clear—Some Concision Is Urgently Needed,* WALL ST. J. (May 8, 2016), https://www.wsj.com/articles/defining-a-cyber-act-of-war-1462738124.

[309] For example, consider reports of the European Union's decision to formally declare for deterrent purposes that under the right circumstances, member states could consider malicious cyber operations as acts of war and respond with kinetic force. James Crisp, *EU Governments to Warn Cyber Attacks Can Be an Act of War*, THE TELEGRAPH (Oct. 31, 2017), http://www.telegraph.co.uk/news/2017/10/29/eu-governments-warn-cyber-attacks-can-act-war.

[310] Some academics point to a handful of examples, such as the reported use of a cyber operation to cause Iranian centrifuges to function improperly, as examples of a cyber use of force. *See* TALLIN 2.0, *supra* note 23, at 342.

[311] Cyber operations conducted below the threshold of war may nevertheless violate international law and thereby give rise to self-help measures below the use of force, to include certain measures, to include countermeasures, that would otherwise be internationally wrongful. *See* TALLINN 2.0, *supra* note 23, at 330.

[312] OPERATIONAL LAW HANDBOOK, *supra* note 102, at 1 (emphasis in original).

[313] Net Politics and Digital and Cyberspace Policy Program, *The Cyber Act of War Act: A Proposal for a Problem the Law Can't Fix*, COUNCIL ON FOREIGN RELATIONS (May 12, 2016), https://www.cfr.org/blog/cyber-act-war-act-proposal-problem-law-cant-fix.

[314] *See* Geoffrey Corn, *The Jus ad Bellum, in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 94 (Geoffrey S. Corn et al., eds.) (2016) ("However, a threat to international peace and security triggering the individual and collective right of self-defense has always been complex.").

level of harm or effect caused.[315] The ubiquitous and legally imprecise use of this term clouds policy discussions and decisions about how to characterize state-conducted or state-sponsored cyber operations and to fashion appropriate responses. Such imprecision serves only to exacerbate uncertainty in an already uncertain environment. This inaccuracy in lexicon is all-the-more unfortunate because attack and armed attack are legally operative terms of art employed in the *jus in bello* and the *jus ad bellum*, respectively, neither of which are implicated by the vast majority of cyber activities, even harmful or prejudicial ones.[316]

The term attack is at the heart of many of the *jus in bello* rules regulating the conduct of hostilities, or armed conflict, such as the prohibitions on attacking civilians or civilian objects, the ban on indiscriminate attacks, and the rules of precaution and proportionality in the conduct of attacks. With respect to these rules, the generally accepted definition of attack is found in Additional Protocol I to the Geneva Conventions, where attacks are defined as "acts of violence against the adversary, whether in the offense or in the defence."[317] Beyond regulating the employment of cyber capabilities as a means or method of warfare, however, this definition is only indirectly relevant to informing the issue of whether a cyber operation executed outside of or unrelated to an existing armed conflict breaches an international obligation owed by the executing state to an affected state.

Certainly, where a cyber operation generates an effect amounting to physical damage to objects or death or injury to individuals, AP I's definition of "attack" is triggered, assuming the operation is conducted as part of, or itself constitutes the initiation of, armed conflict.[318] However, where the effects of an *in bello* cyber operation fall below this bright line, significant questions linger as to whether some lesser impact on the functionality of a targeted system is sufficient to satisfy the attack definition and thereby trigger the various targeting rules of the LOAC, or whether cyber operations directed against data, no matter the impact on that data, can

---

[315] DOD LAW OF WAR MANUAL, *supra* note 8, at 996 ("The term 'attack' often has been used in a colloquial sense in discussing cyber operations to refer to many different types of hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services.").

[316] *Id.* ("Operations described as 'cyber attacks' or 'computer network attacks,' therefore, are not necessarily 'attacks' for the purposes of applying rules on conducting attacks during the conduct of hostilities. Similarly, operations described as 'cyber attacks' or 'computer network attacks' are not necessarily 'armed attacks' for the purposes of triggering a State's inherent right of self- defense under *jus ad bellum*.") (internal citations omitted).

[317] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 49(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

[318] *See* TALLIN 2.0, *supra* note 23, at 415. As discussed *infra*, the level of harm or effect involved can be relevant to assessing whether the operation constitutes a prohibited use of force and/or triggers Article 2 Common to the Geneva Conventions. *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2, Aug. 12, 1949, 75 U.N.T.S. 31 ("[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 of the High Contracting Parties . . . .); Geneva Convention for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members, art. 2, Aug. 12, 1949, 75 U.N.T.S. 85 (same); Geneva Convention, Relative to the Treatment of Prisoners of War, art. 2, Aug. 12, 1949, 75 U.N.T.S. 135 (same); Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 2, Aug. 12, 1949, 75 U.N.T.S. 287 (same).

ever constitute an *in bello* attack.[319] As it is the policy of the Department of Defense to apply the Law of War in all military operations, these uncertainties are significant, especially when considering cyber operations conducted during armed hostilities.[320] They also factor into the review process of any pre- or extra-hostilities cyber operation that might, alone or in conjunction with other activities, cross the *jus ad bellum* use-of-force threshold. As a strict matter of law, however, the LOAC, to include its concept and definition of attack, is inapplicable to gray-zone cyber operations conducted outside of armed conflict. More relevant are the meanings ascribed to the *ad bellum* concepts of "use of force" and "armed attack" included in Articles 2(4) and 51 of the U.N. Charter.

International law substantially circumscribes states' authority to use force against one another to protect or advance their interests; limitations widely understood to apply equally to cyber operations.[321] In general terms, the *jus ad bellum*—the body of international law governing the conditions under which states may resort to the use of force—is reflected in the UN Charter, which provides only three exceptions to the baseline prohibition in Article 2(4) against states threatening or using force in a manner inconsistent with the purposes of the Charter, namely against the territorial integrity or political independence of any other state.[322] First, actions conducted with the consent of the affected state do not violate Article 2(4).[323] Second, states can lawfully use force pursuant to a Chapter VII enforcement action authorized by the Security Council.[324] Finally, as set forth in Article 51 of the Charter, states are permitted to use force in the face of an "armed attack" as an exercise of their inherent right of individual or collective self-defense.[325] Once triggered, even if by a cyber operation, the right of self-defense permits the victim state to respond with any and all lawful means available, subject to the principles of necessity and proportionality.[326] Seemingly straight forward on its face, the *ad bellum*

---

[319] *See, e.g.,* Schmitt, *Grey Zones*, *supra* note 11, at 17-19; TALLINN 2.0, *supra* note 23, at 437 (taking the position that data does not constitute a tangible object that can be attacked within the meaning of article 49(1) of AP I).
[320] DEP'T OF DEF. DIRECTIVE 2311.01E, DOD LAW OF WAR PROGRAM, ¶ 4.1 (May 9, 2006) (certified current as of Feb. 22, 2011).
[321] DOD LAW OF WAR MANUAL, *supra* note 8, at 998-9 ("Cyber operations that constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law must have a proper legal basis in order not to violate *jus ad bellum* prohibitions on the resort to force."). *Accord* Schmitt, *Grey Zones*, supra note 11, at 13 (citing TALLINN 2.0, *supra* note 23, at 329).
[322] Article 2(4) of the UN Charter provides: "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."
[323] *See* Draft Articles on the Responsibility of States, *supra* note 291, art. 20 ("Valid consent by a State to the commission of a given act by another State precludes the wrongfulness of that act in relation to the former State to the extent that the act remains within the limits of that consent.").
[324] TALLINN 2.0, *supra* note 23, at 329 ("[T]he lack of agreed-upon definitions, criteria, and thresholds for application creates uncertainty when applying the *jus ad bellum* to the rapidly changing realities of cyberspace.").
[325] Article 51 of the Charter provides: "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 measures necessary to maintain international peace and security." Several states, to include the United States, consider Article 51 as reflective of customary international law.
[326] DOD LAW OF WAR MANUAL, *supra* note 8, at 999-1000 ("As a matter of national policy, the United States has expressed the view that when warranted, it will respond to hostile acts in cyberspace as it would to any other threat to the country.").

framework of the Charter and customary international law is in fact rife with interpretive ambiguities. These ambiguities are exacerbated when attempting to map the *jus ad bellum* rules onto the cyber domain.[327]

Neither the term "use of force" nor "armed attack" are defined in the Charter, and international consensus is lacking on the precise contours of these terms, making it even more difficult to apply them neatly to cyber operations. A number of states and legal scholars take the view that the two standards should be analyzed separately, and indeed that the thresholds for meeting each standard are different. These states and scholars take the view that the different terms in the Charter reflect "distinct levels of activity, each with different legal results."[328] The term "armed attack" is used in Article 51 of the Charter to denote the triggering condition justifying a state's resort to force in self-defense, whereas the "use of force" standard is intended to delineate a proscription on state actions.[329] Most agree that an action causing death or injury to persons or

[327] U.N. Charter, art. 39; *see also* TALLINN 2.0, *supra* note 23, at 357 (Rule 76).

[328] Brown et al., *Military Cyberspace Operations*, *supra* note 46, at 135. These states and scholars base this view primarily on the ICJ's distinction in its *Nicaragua* decision between "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms." Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), 1986 I.C.J. 14, □ 191 (June 27) [hereinafter *Nicaragua* Judgment]. Under this approach, all armed attacks constitute uses of force, but the inverse is not necessarily the case. *See* TALLINN 2.0, *supra* note 23, at 332-33. The distinction is potentially significant. Under the "force-gap" approach, states' lawful response options to uses of force not amounting to an armed attack are far more limited in scale and scope than would be permitted in the exercise of self-defense. *Id.* at 337 ("This distinction is critical in that the mere fact that a use of force has occurred does not alone justify a use of force in response."). For example, response options would be limited to countermeasures or actions consistent with the pleas of necessity. *Id.* The United States' rejects this so-called "response gap" between a use of force and an armed attack. *See* OPERATIONAL LAW HANDBOOK, *supra* note 102, at 4. The United States has long taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. DOD LAW OF WAR MANUAL, *supra* note 8, at 1000 (citing Harold Hongju Koh, Keynote Address at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace, (Sept. 18, 2012)). *See also* OPERATIONAL LAW HANDBOOK, *supra* note 102, at 4.

[329] TALLINN 2.0, *supra* note 23, at 337. Whether the use of force/armed attack distinction is significant in practice is unclear. Some view the gap as "so narrow as to be insignificant or non-existent." TALLINN 2.0, *supra* note 23, at 332; OPERATIONAL LAW HANDBOOK, *supra* note 102, at 4 (noting the size of the gap is unclear and referencing Yoram Dinstein's description of the gap as "but a hiatus" in his book WAR, AGGRESSION, AND SELF-DEFENSE). With respect to each standard, the analysis is understood to be principally concerned with the anticipated consequences of the action. Under this view, the analysis must the "scale and effects" of an operation in light of a non-exhaustive list of factors such as the prevailing political circumstances at the time of the operation, the identity of the perpetrator, the nature of the objects or systems targeted, and the assessed intent behind the operation. DOD LAW OF WAR MANUAL, *supra* note 8, at 999 & n. 22. The relevance of assessing the scale and effects of a cyber operation is drawn from the ICJ's use of that approach in its *Nicaragua* judgment for determining whether particular actions involve sufficient gravity to qualify as an armed attack. *See Nicaragua* Judgment, *supra* note 328, para. 195 (distinguishing between armed attacks and "mere frontier incidents" based on the "scale and effects" of the former). The *Tallinn Manual 2.0* adopts the same standard for assessing uses of force. *See* TALLINN 2.0, *supra* note 23, at 330-31.

By no means conclusive on the issue, the United Nations definition of aggression contained in General Assembly Resolution 3314 is instructive on the types of actions that would presumptively constitute acts of aggression, and by extension, uses of force. *See* ELIZABETH WILMSHURST, DEFINITION OF AGGRESSION 2 (2008), *available at* http://legal.un.org/avl/pdf/ha/da/da_e.pdf ("The Definition begins with a broad definition of aggression, drawn largely from Article 2, paragraph 4, of the Charter (though omitting reference to threats) and then enumerates specific examples of acts of aggression."); *Nicaragua* Judgment, *supra* note 328, at para. 195 (referring to the Definition of Aggression in determining what constitutes an armed attack for purposes of Article 51). The non-exhaustive list of examples includes actions such as the invasion or attack by the armed forces of a state of the

physical damage or destruction to objects, regardless of the modality employed, qualifies as an unlawful use of force.[330] For the United States, cyber operations causing the same or similar effects as those that would be considered a use of force if caused through traditional physical means would be treated equally under the *jus ad bellum*.[331]

Consensus among states concerning how the use of force and armed attack prohibitions apply in the context of cyber operations is sorely lacking. It is relatively clear that most non-destructive actions are unlikely to be viewed as crossing the use-of-force threshold, even if coercive in nature.[332] With that said, nothing in the *jus ad bellum* requires that death, injury, or destruction be the proximate result of a hostile operation to qualify it as a use of force, and some argue that the overall impairment of state functions and stability is the proper focus of inquiry.[333] The most oft-cited example of where states might deem such cyber operations a use of force is the case of causing substantial or economically "crippling" interference or degradation to a state's financial systems or critical infrastructure.[334] Not all agree, however, and beyond general statements in support of a non-destructive-or-injurious use of force approach, there is little agreement as to the circumstances under which such operations, cyber or otherwise, would cross the use-of-force and armed attack thresholds.[335] Related questions linger as well, such as whether in the aggregate a series of cyber operations that alone would not amount to a use of force can cross the threshold.[336] The importance of these questions should not be understated. As states and other hostile actors continue to push boundaries with malicious cyber operations, pressure will mount on victim states to respond. Imprecision in framing the *jus ad bellum* implications of cyber operations risks continued uncertainty and risks unnecessary escalation. In addition, when

territory of another state, military occupation, bombardments or the use of any weapons against the territory of another state, blockades, attacks on the armed forces of another state, and the use of armed proxies to commit the same acts. *See* G.A. Res. 3314 (XXIX), annex, art. 3, U.N. DOC. A/9631 (Dec. 14, 1974).

[329] Schmitt, *Grey Zones*, supra note 11, at 14; Brown et al., *Military Cyberspace Operations*, supra note 46, at 135. *See also* TALLINN 2.0, *supra* note 23, at 328 (quoting Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 1996 I.C.J. 226, □ 39 (July 1996) (The *jus ad bellum* applies to "any use of force, regardless of the weapons employed.").

[330] Schmitt, *Grey Zones*, supra note 11, at 14; Brown et al., *Military Cyberspace Operations*, supra note 46, at 135; *see also* TALLINN 2.0, *supra* note 23, at 328 (quoting Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 1996 I.C.J. 226, □ 39 (July 1996) (The *jus ad bellum* applies to "any use of force, regardless of the weapons employed.")).

[331] DOD LAW OF WAR MANUAL, *supra* note 8, at 1000. The *Department of Defense Law of War Manual* lists examples of cyber operations that would presumptively cross the threshold of a use of force—those that trigger a nuclear plant meltdown; open a dam above a populated area, causing destruction; disable air traffic control services, resulting in airplane crashes; or cripple a military's logistics systems—but emphasizes the context specific nature of the inquiry. *Id.* at 998-99. In addition to the nature of the effects, other factors such as the perpetrator, the target location, and the intent of the cyber operation would be relevant.

[332] Actions such as economic coercion, for example through sanctions, or the mere funding of armed groups conducting operations against another state, would not qualify. *See* UN GAOR Special Comm. on Friendly Relations, UN DOC. A/AC.125/SR.110 to 114 (1970); *Nicaragua* Judgment, *supra* note 328, □ 228.

[333] *See* TALLINN 2.0, *supra* note 23, at 342 (Some experts take the view that it is not the injurious or destructive nature of the consequences that matters, "but rather the extent of the ensuing effects.")

[334] *See* TALLINN 2.0, *supra* note 23, at 337, 342-43 (discussing differing views of the *Tallinn 2.0* contributors).

[335] For example, arming and training guerilla forces to fight against another state. Schmitt, *Grey Zones*, *supra* note 11, at 15.

[336] TALLINN 2.0, *supra* note 23, at 342.

considering appropriate response strategies and options, states should not ignore the international law rules and remedies available below the Article 2(4) demarcation line.

b. The Principle of Non-intervention

Apart from the *jus ad bellum*, states have evolved the customary international law principle of non-intervention as an additional protection against impairments of their sovereignty below the threshold of a use of force.[337] The principle, considered a "a corollary of every state's right to sovereignty, territorial integrity and political independence,"[338] and especially sovereign equality, comprises the "right of every sovereign State to conduct its [internal and external] affairs without outside interference . . . ."[339] Although the precise content and scope of the non-intervention principle are unclear, certain core aspects of the rule are firmly established. First, to be internationally wrongful, an intervention must bear "on matters in which each State is permitted, by the principle of State sovereignty, to decide freely."[340] This zone of protected interests is relatively narrow, covering only matters falling within what is commonly referred to as the domaine réservé of a state.[341] Although malleable as a concept and subject to evolution over time, the domaine réservé is generally understood to refer to those matters reserved in international law to the sole prerogative of states, matters such as the right to choose a political, economic, social, and cultural system, and to formulate and execute foreign policy.[342] A frequently cited example of an activity falling within the scope of the rule's protection is a state's right to hold elections without outside intervention. Conversely, purely commercial activities fall outside the scope of the protection, as do matters otherwise subject to international legal regulation.[343] That is, the concept of sovereign prerogative is not without limits, and those "domains or activities" not strictly reserved to the state are potentially subject to foreign action.[344] Ultimately, like many aspects of international law, whether a matter falls within the domaine réservé of a state is a fact-specific inquiry, considering state practice and *opinio juris* prevalent at the time.[345]

---

[337] The customary international law nature of the non-intervention principle is well settled. *See Nicaragua* Judgment, *supra* note 328, □ 202; TALLINN 2.0, *supra* note 23, at 312; *see also* U.N. Charter, art. 2(7) (prohibiting the United Nations from intervening in "matters which are essentially within the domestic jurisdiction of any state . . . .").

[338] *See* CHATHAM HOUSE, THE PRINCIPLE OF NON-INTERVENTION IN CONTEMPORARY INTERNATIONAL LAW: NON-INTERFERENCE IN A STATE'S INTERNAL AFFAIRS USED TO BE A RULE OF INTERNATIONAL LAW: IS IT STILL? 2 (2007) (quoting 1 LASSA OPPENHEIM, OPPENHEIM'S INTERNATIONAL LAW 432 (Sir Robert Jennings & Sir Arthur Watts, eds., 9th ed. 1992).) [hereinafter CHATHAM HOUSE].

[339] *Nicaragua* Judgment, *supra* note 328, □ 202.

[340] *Id.*, □ 205.

[341] *See* Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1587-1588 (2017) (discussing the concept of domaine réservé).

[342] Schmitt, *Grey Zones, supra* note 11, at 7; TALLINN 2.0, *supra* note 23, at 315; CHATHAM HOUSE, *supra* note 338, at 2; *Nicaragua* Judgment, *supra* note 328, □ 205. Some point to the UN General Assembly's *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance With the Charter of the United Nations* as setting forth authoritative examples of prohibited intervention.

[343] Schmitt, *Grey Zones, supra* note 11, at 7; TALLINN 2.0, *supra* note 23, at 315.

[344] Ohlin, *supra* note 341, at 1588.

[345] *See* TALLINN 2.0, *supra* note 23, at 314.

Second, even with regard to matters squarely falling within a state's domaine réservé, interference alone is not enough. Although intervention and interference are frequently used interchangeably, international law only proscribes the former as wrongful; "[i]nterference pure and simple is not intervention."[346] The touchstone of the non-intervention principle is "[t]he element of coercion, which defines, and indeed forms [its] very essence . . . ."[347] To be internationally wrongful, the intervention "must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question."[348] That is, only actions that deprive or substantially impair a state's freedom of choice over a protected matter in a way that forces it to take or refrain from taking an action against its will are prohibited.[349]

As with the domaine reserve element, international law offers little interpretive guidance on the key element of coercion. In the *Nicaragua* judgment, the ICJ described as a particularly obvious case "an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."[350] Equally obvious is that neither propaganda nor aggressive diplomacy qualifies as prohibited interventions.[351] Between these extremes, the standard lacks clarity, making it difficult to easily map to the cyber domain.

Some point to the *Nicaragua* judgment's description as implying that to constitute coercion, there must be a threat against the affected state, and the threatened consequence of non-compliance must itself be unlawful.[352] But there is nothing in the *Nicaragua* judgement or international law more broadly explicitly limiting the threatened consequence to one of unlawful action. The threatened consequence must be judged contextually to determine whether it crosses the line between prohibited coercion and lawful, albeit "corrosive," pressure.[353] Furthermore, it is worth also noting that the prohibition of nonintervention is not limited to threats of force. As evidenced by the facts of the *Nicaragua* judgment, the nonintervention prohibition can be violated by "forcible or dictatorial, or otherwise coercive," actions that prevent a state from freely exercising its sovereign prerogatives.[354] While such forcible actions might also cross the use-of-force threshold, rendering the intervention question somewhat moot, it may not always be so. Considering the full context of an action or set of actions and their full impact on the affected

---

[346] 1 LASSA OPPENHEIM, OPPENHEIM'S INTERNATIONAL LAW 432 (Sir Robert Jennings & Sir Arthur Watts, eds., 9th ed. 1992) [hereinafter OPPENHEIM].
[347] *Nicaragua* Judgment, *supra* note 328, ¶ 205.
[348] OPPENHEIM, *supra* note 346, at 432.
[349] Schmitt, *Grey Zones, supra* note 11, at 7; TALLINN 2.0, *supra* note 23, at 315-17.
[350] *Nicaragua* Judgment, *supra* note 328, ¶ 205. These actions would also constitute prohibited uses of force in violation of Article 2(4) of the Charter, triggering the victim state's inherent right of self defense under the U.S. view of the *jus ad bellum*. *See id.* and *supra* note 328 and accompanying text. Some argue that, implicit in the *Nicaragua* judgment's description is the notion that to constitute coercion, the threatened consequence must itself be unlawful.
[351] Schmitt, *Grey Zones, supra* note 11, at 7.
[352] *See* Ohlin, *supra* note 341, at 1589.
[353] *See id.*
[354] OPPENHEIM, *supra* note 346, at 432.

state, non-use-of-force actions that would not otherwise qualify as coercive could rise to the level of an unlawful intervention.[355]

Debates over whether Russia's reported hack into the Democratic National Committee's (DNC) servers and subsequent "meddling" in the 2016 presidential election constituted a prohibited intervention are a case in point. Some argue that, in the aggregate, Russia's actions sufficiently manipulated the election process to qualify, while others view them as espionage and propaganda, which are not violations of international law by themselves.[356] As the DNC hack demonstrates, cyberspace affords revisionist states an unprecedented and powerful space in which to interfere in the internal affairs of their adversaries. Cyber operations such as the DNC hack and the DPRK's operations against Sony International Pictures will undoubtedly increase pressure on states to clarify the scope and application of the non-intervention principle, and potentially draw within its ambit a wider array of prejudicial activities.[357] In the meantime, outside of obvious cases, the precise contours of the prohibition remain "unclear in light of ever evolving and increasingly intertwined international relations."[358]

Interpretive uncertainties notwithstanding, the *jus ad bellum* and the principle of nonintervention are universally accepted as primary rules of international law binding on states, with consensus building that they apply with full force to states' activities in cyberspace. As important as these frameworks are, in the realm of cyber operations their value in regulating state behavior is limited, as the vast majority of cyber operations conducted outside of situations of armed conflict fall well below the use-of-force threshold and do not fit squarely within the traditionally recognized elements of the nonintervention rule. Whether, and if so, how, "extant international law regulates this less-intrusive class of cyber activities is therefore a critical question."[359]

c. The Role of Sovereignty

The *jus ad bellum* and the principle of nonintervention are grounded in and designed to protect sovereignty—the most fundamental interest of states and a foundational pillar of the international order.[360] But as much as sovereignty involves freedom from certain outside interference, it also

[355] *See* TALLINN 2.0, *supra* note 23, at 319 (noting the view of some experts that actions can rise to the level of an intervention based on the context and consequences).
[356] *See, e.g.,* Schmitt, *Grey Zones, supra* note 11, at 7; Ohlin, *supra* note 341, at 1579-80; Steven J. Barela, *Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion*, JUST SECURITY (Jan. 12, 2017), https://www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion.
[357] *See* CHATHAM HOUSE, *supra* note 338, at 2 ("Since the reach of international law is constantly changing, so too is the line between what is, and what is not, covered by the principle of non-intervention."). *See also* Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law*, 40 N.C. J. INT'L L. & COM. REG. 443, 473-74 (2015) (arguing that economic espionage should be brought within the scope of the non-intervention rule).
[358] TALLINN 2.0, *supra* note 23, at 314.
[359] Corn & Taylor, *supra* note 301, at 207.
[360] TALLINN 2.0, *supra* note 23, at 11 ("Sovereignty is a foundational principal of international law); Schmitt, *Grey Zones, supra* note 11, at 4 (same).

means freedom of action on the international plane.[361] In broad terms, it refers to "the collection of rights held by a state, first in its capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane, representing that territory and its people."[362] It is understood as encompassing "the whole body of rights and attributes which a state possesses in its territory, to the exclusion of all other states, and also in its relation with other states."[363] The importance of sovereignty as a "basic constitutional doctrine of the law of nations" cannot be overstated.[364] Nevertheless, the exact meaning of the term is susceptible to many uses, and "its exact contours are frustratingly indeterminate."[365]

As we have seen, the basic structure of cyberspace does not adhere neatly to traditional, geography-based Westphalian concepts, and states' increasing use of cyber operations as a means and method of statecraft has called into direct question the precise meaning, and perhaps more importantly, the normative character, of the principle of sovereignty. Not surprisingly, questions about the content and consequence of the principle are highly contested among international lawyers.[366] With respect to cyber operations, the debate proceeds along two general lines. First, there is an open question as to whether sovereignty constitutes a primary rule of international law susceptible to breach and state responsibility, or instead exists as a baseline principle undergirding specific primary norms such as Article 2(4) of the Charter. This debate is far from settled, certainly with respect to cyberspace.[367] Second, even among those international lawyers who assert sovereignty as a primary rule, there is little consensus as to the types of cyber operations and level of effects that would constitute violations of the purported rule.[368]

DRAFT

---

[361] James Crawford, *Sovereignty as a Legal Value*, *in* THE CAMBRIDGE COMPANION TO INTERNATIONAL LAW, 118 (James Crawford & Martti Koskenniemi eds. 2012) ([International law] regards each state as sovereign, in the sense that it is presumed to have full authority to act not only internally but at the international level, to make (or not to make) treaties and other commitments, to relate (or not to relate) to other states in a wide variety of ways, to consent (or not to consent) to resolve international disputes.") [hereinafter Crawford, *Sovereignty as a Legal Value*].

[362] JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 448 (8th ed. 2012).

[363] Corfu Channel (U.K. v. Alb.), Merits, 1949 ICJ REP. 4, 43 (Apr. 9) (individual opinion by Alvarez J.).

[364] CRAWFORD, *supra* note 362, at 447.

[365] Ohlin, *supra* note 341, at 1579. *See also* Crawford, *Sovereignty as a Legal Value*, *supra* note 361, at 118; Matthew C. Waxman, *Cyber Strategy & Policy: International Law Dimensions* 6, Testimony Before the Senate Armed Services Committee, Mar. 2, 2017, https://www.armed-services.senate.gov/imo/media/doc/Waxman_03-02-17.pdf. ("But sovereignty is not absolute and its precise meaning is fuzzy—even in physical space, let alone cyberspace.").

[366] *See* Crawford, *Sovereignty as a Legal Value*, *supra* note 361, at 119; Schmitt, *Grey Zones, supra* note 11, at 4-5.

[367] *See, e.g.,* Schmitt, *Grey Zones, supra* note 11, at 4; *Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0*, AM. J. INT. L. UNBOUND 2017 (containing several scholarly articles debating the normative character of sovereignty), https://www.cambridge.org/core/journals/american-journal-of-international-law/volume/AB96AEDAFFEE503674B493BDBF8E5ACD?sort=canonical.position%3Aasc&pageNum=3&searchWithinIds=AB96AEDAFFEE503674B493BDBF8E5ACD&productType=JOURNAL_ARTICLE&template=cambridge-core%2Fjournal%2Farticle-listings%2Flistings-wrapper&hideArticleJournalMetaData=true&displayNasaAds=false.

[368] *See* TALLINN 2.0, *supra* note 23, at 17-27 (setting out differing views of the Tallinn 2.0 contributors as to the threshold of harm necessary to constitute a violation of sovereignty).

As originally conceived, sovereignty referred only to the supreme and exclusive power within a state, what is today referred to as internal sovereignty.[369] It represents a monopoly over governing authority within the state, and signifies the independent right, in regard to a discrete portion of the globe, "to exercise therein, to the exclusion of any other state, the functions of a state."[370] In addition to encompassing the near-exclusive right over the domaine réservé of the state, internal sovereignty extends to such matters as prescriptive, enforcement, and adjudicative jurisdiction, as well as determinations as to who may enter and reside within the territory of the state, who may qualify for citizenship, and the composition and employment of the state's security and military forces.[371] Thus, internal sovereignty allows a state to assert jurisdiction over individuals, entities, and objects present within its territory, and to prohibit acts within or affecting its territory as an exercise of governmental authority. This undoubtedly encompasses jurisdiction over the physical layer of cyberspace located within a state's territory, as well as components of the logical and social layers as well.[372]

Sovereignty also relates to the recognition in the international order of the absolute equality and independence of all states.[373] This external aspect of sovereignty "forms the unifying principle of international law—that only states have the legal personality necessary to create and be bound by international law."[374] The principle of sovereign equality is at the heart of the *Lotus* principle that "[r]estrictions on the independence of states cannot . . . be presumed,"[375] which means that states are free to act on the international plane, even with respect to cyber operations beyond their borders, except to the extent that their actions are proscribed by treaty or customary international law.[376]

---

[369] *See* Crawford, *Sovereignty as a Legal Value*, *supra* note 361, at 118; TALLINN 2.0, *supra* note 23, at 13-16 (discussing internal sovereignty). The concept of sovereignty is often associated with the Treaty of Westphalia, but it actually traces to pre-Westphalia France, where Jean Bodin is credited with developing the notion of sovereignty to bolster the absolute power of the French king over recalcitrant feudal lords, consolidation of the French state, and the principle that he who makes the laws cannot be bound by the laws (*majestas est summa in cives ac subditos legibusque solute potestas*). *See* SOVEREIGNTY, ENCYCLOPAEDIA BRITANNICA (last visited Nov. 20, 2017), https://www.britannica.com/topic/sovereignty. This conception of unitary sovereignty slowly gave way to broader notions of popular sovereignty through the Enlightenment and institution of constitutional forms of government. *Id.* Externally, sovereigns were viewed as existing in a state of anarchy, as expressed in Thomas Hobbes' *Leviathan,* with unfettered freedom of action vis a vis one another; a view that slowly gave way to international legal regulation. *Id.*

[370] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A 829, 838 (Perm. Ct. Arb. 1928). *See also* Crawford, *Sovereignty as a Legal Value*, *supra* note 361, at 120-21; Samantha Besson, *Sovereignty*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 119 (2011) (noting that sovereignty is generally characterized as the "powers and privileges resting on customary law which are independent of the particular consent of another state").

[371] *See* Crawford, *Sovereignty as a Legal Value*, *supra* note 361, at 121.

[372] TALLINN 2.0, *supra* note 23, at 14-15.

[373] *See* U.N. Charter art. 2(1); TALLINN 2.0, *supra* note 23, at 16.

[374] Corn & Taylor, *supra* note 301, at 209; Crawford, *Sovereignty as a Legal Value*, *supra* note 361, at 118; *Nicaragua* Judgment, *supra* note 328, 135 ("[I]n international law there are no rules other than such rules as may be accepted by the state concerned, by treaty or otherwise . . . .").

[375] *Lotus*, 1927 P.C.I.J. (ser. A) No. 10, at 18.

[376] TALLINN 2.0, *supra* note 23, at 16 ("External sovereignty means that a state is independent in its external relations from other states and is free to engage in cyber activities beyond its territory subject only to international law.").

Since the rise of the modern nation-state, these two aspects of sovereignty have existed in a natural state of tension. The rights inherent in internal sovereignty often clash with the external sovereign rights and interests of other states. This was the situation, for example, in the *Corfu Channel* case*,* where the ICJ had to reconcile competing claims of sovereign rights to jurisdiction over territorial seas on one hand, and the right to maritime transit of straits on the other.[377] In light of this inherent tension, and the import of the *Lotus* rule, at best "assertions in terms of sovereignty are not indefeasible; they are more in the character of presumptions than inflexible rules."[378] Below the thresholds of a use-of-force or a prohibited intervention, there is insufficient evidence of either state practice or opinio juris to support claims that the principle of sovereignty operates as an independent rule of customary international law that regulates states' activities in cyberspace.[379]

A contrary view asserts that sovereignty is more than a foundational principle. In this view, sovereignty is itself a primary rule of international law that can be violated.[380] This view draws from the exclusivity of internal sovereignty and the general mandate that states respect the personality, territorial integrity, and political independence of other states.[381] Frequently stated in terms of violations of a state's "territorial sovereignty,"[382] this view confuses the right of a state to exercise control over and within its territory, inherent in the notion of internal sovereignty, with the more precise concepts of territorial integrity and the inviolability of borders specifically protected through Article 2(4), the UN Charter more broadly, and the customary rule of non-intervention.[383] Those specific proscriptions against violating territorial integrity or borders involve a threshold of harm much higher than the mere conduct of cyber operations limited to affecting ITT infrastructure located inside another state's borders.[384] International law

[377] Corfu Channel (U.K. v. Alb.), *supra* note 363, at 28 ("Unless otherwise prescribed in an international convention, there is no right for a coastal State to prohibit [innocent] passage [of another State's warships] through straits in time of peace."). The subsequent development of the innocent passage regime in the Law of the Sea reflects a clear compromise of these competing sovereign claims. The differences in how sovereignty is reflected in international law with respect to the domains of space, air, and the seas further support the view that sovereignty is a principle, subject to adjustment depending on the domain and the practical imperatives of states rather than a hard and fast rule. The fact that states have developed vastly different regimes to govern these distinct domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace.

[378] Crawford, *Sovereignty as a Legal Value*, *supra* note 361, at 121.

[379] Waxman, *supra* note 365, at 6 (noting the lack of evidence of state practice or a sense of binding legal obligation among states "to conclude that the principle of sovereignty would prohibit cyber-operations just because, for example, some cyber-activities take place within another state, or even have some effects on its cyber-infrastructure, without consent.").

[380] *See*, *e.g.,* Michael Schmitt, *US Transparency Regarding International Law in Cyberspace,* JUST SECURITY (Nov. 15, 2016); TALLINN 2.0, *supra* note 23, at 17.

[381] TALLINN 2.0, *supra* note 23, at 16.

[382] *See, e.g.,* Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1644-45 (2017) (framing the question in terms of territorial sovereignty).

[383] Corn & Taylor, *supra* note 301, at 210.

[384] *See, e.g.*, The Final Act of the Conference on Security and Cooperation in Europe, Aug. 1, 1975, 14 I.L.M. 1292 (Helsinki Declaration). With respect to the inviolability of borders, the Final Act requires the signatory states to refrain from "assaulting" borders or making any "demand for, or act of, seizure and usurpation of part or all of the territory of any participating State." *Id*., § III. With respect to territorial integrity, the Final Act requires the signatories to refrain from any act inconsistent with the principles of the U.N. Charter—specifically Article 2(4)—and to refrain from making "each other's territory the object of military occupation or

simply does not obligate other states to abstain from all non-consensual activities within the territory of another state or that might otherwise infringe on or operate to the prejudice of that state's internal sovereignty.[385]

Even among those who view sovereignty as a stand-alone primary rule of international law, there is little consensus on two critical issues: first, how to square states' ubiquitous conduct of espionage, both in the physical and virtual domains, with the primary rule they proffer; and second, how to define the types of cyber operations covered by the rule and applicable thresholds for assessing compliance.[386]

States routinely engage in espionage, an activity that is clearly prejudicial to and subject to the domestic jurisdiction of the spied-upon state. States frequently acknowledge that they do so, and often have public laws authorizing intelligence collection.[387] These activities often involve undisclosed entry into the territory of other states, as well as actions that alter physical and virtual conditions inside the territory to permit access to and exploitation of information.[388] And while these activities may violate the domestic law of the affected state, it is widely accepted that they are not prohibited by international law.[389] Since the advent of the internet, states have also engaged in espionage at an ever increasing rate in and through cyberspace, and "like traditional espionage, there is no explicit legal prohibition" that attaches to these activities.[390] Unless these operations employ modalities that otherwise constitute a violation of a specific provision of international law, they are subject only to the risk of diplomatic consequences or the exercise of domestic jurisdiction over intelligence operatives if discovered and caught.[391]

---

other direct or indirect measures of force in contravention of international law, or the object of acquisition by means of such measures or the threat of them." *Id.*, § IV.

[385] Some point to cases such as Costa Rica v. Nicaragua (Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicar.) and Construction of a Road in Costa Rica along the San Juan River (Costa Rica v. Nicar.) (Dec. 16, 2015)), Corfu Channel, and Armed Activities on the Territory of the Congo (Armed Activities on the Territory of the Congo (New Application 2002 (Dem. Rep. Congo v. Uganda), 2006 ICJ REP. 6 (Feb. 3)) as support for this position. It is true that the ICJ referred in general terms to violations of sovereignty in those cases. However, in each instance the facts ruled on involved substantial military presence, de facto control of territory, and in some instances, violent operations, all of which implicate higher thresholds than the sovereignty-as-a-rule proponents assert. For example, in Armed Activities on the Territory of the Congo, the ICJ found that Uganda's "unlawful military intervention" inside the territory of the Democratic Republic of the Congo (DRC) constituted a use of force in violation of Article 2(4) and a prohibited intervention, as well as military occupation of some DRC territory, and as such, constituted a violation of the DRC's sovereignty and territorial integrity in the broader sense. *See* CHATHAM HOUSE, *supra* note 338, at 3 (describing both the Corfu Channel and DRC judgments as involving violations of the non-intervention rule).

[386] *See* Schmitt, *Grey Zones, supra* note 11, at 6; TALLINN 2.0, *supra* note 23, at 17-27.

[387] Such as FISA and EO 12,333, discussed *supra. See also* Lotrionte, *supra* note 357, at 473-74; TALLINN 2.0, *supra* note 23, at 169.

[388] Hence, for example, the specific exception to the Computer Fraud and Abuse Act for intelligence collection. *See supra* notes 197 and accompanying text.

[389] TALLINN 2.0, *supra* note 23, at 169 ("The International Group of Experts agreed that customary international law does not prohibit espionage *per se*.").

[390] Lotrionte, *supra* note 357, at 476; *see also* DOD LOW MANUAL, *supra* note 8, at 999 ("[T]o the extent that cyber operations resemble traditional intelligence and counter-intelligence activities . . . such cyber operations would likely be treated similarly under international law.").

[391] TALLINN 2.0, *supra* note 23, at 168-74 (discussing peacetime cyber espionage).

The widespread and consistent conduct of both traditional and cyber-enabled intelligence collection within the territory of unwitting states is fundamentally at odds with the sovereignty-as-a-rule approach. Some argue that espionage constitutes a carve-out from the rule of territorial sovereignty based on longstanding state practice, but offer no evidence of *opinio juris* to substantiate this claim.[392] Others try unpersuasively to reconcile the discordance. The *Tallinn Manual 2.0* seems to adopt the latter approach, noting correctly that while espionage is not prohibited *per se*, the means by which it is conducted may implicate other rules of international law. Simply put, blowing up a bridge to facilitate intelligence collection would not fall outside of the scope of Article 2(4) just because it was done for an intelligence gathering purpose.[393] However, with a degree of circularity, the *Tallinn Manual 2.0* then goes on to state that sovereignty is one of the distinct rules of international law that may render an espionage activity internationally wrongful. Given the broad view adopted by some of the contributors to the *Manual* of those cyber activities that would violate a state's sovereignty, the concession that espionage is not *per se* internationally wrongful is of little value.

Rule 4 of the *Tallinn Manual 2.0* is straight forward but substantively lacking: "A State must not conduct cyber operations that violate the sovereignty of another State."[394] The related commentary to Rule 4 attempts to delineate three basic sub-components to the rule: (1) a prohibition against simple physical trespasses;[395] (2) a prohibition against remote cyber operations that cause some un-defined level of effect on any cyber infrastructure located on the territory of another state;[396] and (3) a prohibition against cyber operations that interfere with or usurp inherently governmental functions.[397] Each of these variants rests on flawed premises and convey as *lex feranda*, not *lex lata*.

As noted above, the first of these three variants of the rule is fundamentally incompatible with the longstanding state practice of espionage and the recognition that it is not *per se* internationally wrongful, as evidenced by the division among the Experts on this aspect of Rule 4.[398] The majority view that tresspassory espionage violates sovereignty is incongruent with reality, and the minority view that it is a carve-out of the broader sovereignty rule is legally unsupported. Non-consensual or surreptitious entry into the territory of another state to conduct espionage is not internationally wrongful, not because it is espionage, but because it does not

[392] *See id.* at 19 (acknowledging the view of some of the experts that state practice has created an exception to the sovereignty rule).
[393] *See id.* at 170. The *Tallinn Manual 2.0* also suggest that cyber espionage might implicate violations of international human right to privacy as well. There are a number of challenges to this assertion, not the least of which is the lack of clarity on the content of the right and the scope of application of human rights law to intelligence collection conducted against non-citizens. *See* Ohlin, *supra* note 341, at 1583-85.
[394] TALLINN 2.0, *supra* note 23, at 17 (Rule 4).
[395] *Id.* at 19 ("The Experts agreed that a violation of sovereignty occurs whenever one State physically crosses into the territory or national airspace of another State without either its consent or another justification in international law . . . .").
[396] *Id.* at 20-21.
[397] *Id.* at 19-20; *see also* Schmitt, *Grey Zones, supra* note 11, at 5-7.
[398] *Id.* at 19.

constitute a prohibited intervention or a use of force, and states have articulated no other rule proscribing it.

The second variant of Rule 4 suffers from some of the same defects as the first. Like physically enabled espionage, remotely-conducted espionage is ubiquitous, involves surreptitious access into targeted systems, and is not prohibited by international law.[399] Again, there is simply no evidence that these activities are unregulated based on an undefined espionage exception to an existing sovereignty rule. Additionally, the distinct lack of consensus as to whether any cyber-generated effect other than one resulting in physical damage or injury (which would likely violate other primary rules such as the prohibition against use of force) would be sufficient to violate the purported rule of sovereignty is illustrative of the lack of evidence of customary international law in this regard. It is generally accepted that international law does not prohibit remote cyber operations *per se*, especially those involving only *de minimis* effects.[400] Whether and where international law draws the line below the rule of non-intervention is unclear, and the view that there is a rule of sovereignty that prohibits cyber espionage is insufficiently supported by evidence of state practice or a sense of binding legal obligation among states.[401]

The final variant of Rule 4—interference with or usurpation of inherently governmental functions—is similarly untethered from state practice or *opinio juris*. The inability of the Experts to even define "inherently governmental functions" or to adequately distinguish this mere-interference rule from the narrower, well-established non-intervention rule illustrates the overly-broad and aspirational character of this concept. While the contours of the non-intervention rule are not static or inflexible,[402] presumably, the scope of protection accorded by the rule is limited by design; states having deliberately excluded non-coercive interference.[403] Arguments for sweeping a greater range of otherwise unregulated sovereign state activities within the ambit of international proscription should proceed with caution, and are better nested within the broadly-recognized non-intervention rule and its attendant parameters.[404] Whole-cloth

[399] *See* Lotrionte, *supra* note 357, at 476.
[400] *See* Egan, *supra* note 286, at 11 (noting the absence of an absolute prohibition on remote cyber operations as a matter of international law, especially with respect to activities in another state's territory that have *de minimis* effects).
[401] *See* Waxman, *supra* note 365, at 6 ("However, it is my view that there is not enough evidence of consistent and general practice among states, or a sense of binding legal obligation among states, to conclude that the principle of sovereignty would prohibit cyber-operations just because, for example, some cyber-activities take place within another state, or even have some effects on its cyber-infrastructure, without consent."). Some of the Tallinn Experts took the view that damage or injury was but one factor for consideration. A majority took the view that causing some loss of functionality would "sometimes" run afoul of the rule, but could reach no consensus "as to the precise threshold at which this is so due to the lack" of *opinio juris,* and no consensus could be reached at all as to "whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty." TALLINN 2.0, *supra* note 23, at 20-21; *see also* Schmitt, *Grey Zones, supra* note 11, at 5-7.
[402] CHATHAM HOUSE, *supra* note 338, at 2 ("Since the reach of international law is constantly changing, so too is the line between what is, and what is not, covered by the principle of non-intervention.").
[403] *See* OPPENHEIM, *supra* note 346, at 432.
[404] *See* Lotrionte, *supra* note 357, at 492-509 (arguing for extending non-intervention to cover economic espionage).

claims to the existence of a distinct, more expansive rule of sovereignty effectively renders the more limited non-intervention rule a nullity.[405]

The ramifications of the growing debate as to whether and how international law regulates state actions in cyberspace below the nonintervention threshold should not be understated. Because of the distributed nature of cyberspace, operations may involve cyber effects directed against adversary-controlled infrastructure on networks or systems located in multiple states. While these "subintervention" cyber activities should consider the sovereignty of the states in whose territory these infrastructures reside, this does not answer the key question of whether or how international law proscribes such cyber activities. Consideration of these third-party states' sovereign interests is an exceptionally important factor in operational planning, but sovereignty does not itself establish a bar against individual or collective state cyber operations against all cyber infrastructure within another state, particularly those controlled by hostile adversaries. In short, sovereignty is a principle, not a rule, and its legal consequences are not fully formed in this area.

The principle of sovereignty is universal, but its application to the unique particularities of the cyberspace domain remains for states to determine through state practice and the development of treaty rules. Ultimately, whether and precisely when nonconsensual cyber operations below the threshold of a prohibited intervention violate international law is a question that must be resolved through the practice and *opinio juris* of states, developed over time and in response to the need of states effectively to protect themselves from the growing threat of gray-zone cyber operations.[406]

3. The Attribution Problem

Perhaps the most frequently cited problem in relation to cyber security, deterrence, and operations, is the issue of attribution.[407] Upon reflection, it becomes clear that the challenges related to attribution in the cyber domain have less to do with legal ambiguity and more to do with factual uncertainty and confusion over the meaning of the term itself. There is no question that the basic operating construct of cyberspace lends itself to obfuscation and makes technical

[405] In this regard, it is telling that at no point has the UNGGE, the only international body to date charged with the task of examining how international law applies to cyber operations by States, identified sovereignty as a primary rule of international law that would, absent a justification, bar some or any non-consensual cyber operations below the threshold of a prohibited intervention within the territory or on the infrastructure of another state. On the contrary, the 2015 UNGGE adopted only "general and declaratory" language that "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States." Report of the Group of Governmental Experts on Developments In the Field of Information & Telecommunications in the Context of International Security, U.N. DOC. A/70/174, ¶ 27 (July 22, 2015). The 2015 UNGGE then went on to adopt a number of non-binding, voluntary peacetime norms, many, if not all of which would be superfluous under Rule 4 of the *Tallinn Manual 2.0*.

[406] Corn & Taylor, *supra* note 301, at 211.

[407] *See*, *e.g.,* Egan, *supra* note 286, at 17 (discussing the "frequently raised and much debated 'problem of attribution' in cyberspace"); Brown et al., *Military Cyberspace Operations*, *supra* note 46, at 161-62 (discussing the challenges to attributing cyber attacks); Andrea Little Limbago, *The Fog of (Cyber) War: The Attribution Problem and Jus ad Bellum*, ENDGAME (Jan. 1, 2015) (same), https://www.endgame.com/blog/technical-blog/fog-cyber-war-attribution-problem-and-jus-ad-bellum.

(i.e., factual) attribution difficult. From a policy perspective, this renders attribution claims particularly vulnerable to public criticism and second-guessing.[408] But the challenge of adequately identifying the origin and author of hostile or malicious activity, cyber or otherwise, is neither unique to the cyber domain, nor limited to any one means or method of gathering proof. Adversaries routinely operate clandestinely in all domains, especially in the gray zone below open hostilities, in order to maximize strategic effect and operational flexibility, and to maintain plausible deniability. Governments can and do rely on all-source means to gain actionable insight into and develop response options to threat actors. This holds equally true for cyber threats.

As a matter of international law, these factual and policy challenges should be distinguished from the customary international law requirement that a breach of an international obligation must be attributable to a state in order to hold that state legally responsible.[409] Under the customary international law of state responsibility, states "bear responsibility for the internationally wrongful cyber activities of their organs, such as the armed forces, intelligence services, and law enforcement agencies," as well as for the acts of persons or entities exercising "elements of governmental authority."[410] States can also be held accountable under international law for the conduct of non-state actors where "the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[411] It is important to emphasize that in establishing the element of attribution, international law does not set any particular burden of proof. Rather, "international law generally requires [only] that States act reasonably under the circumstances when they gather information and draw conclusions based on that information."[412] In the face of mounting malicious cyber operations emanating from sophisticated and geographically distributed ITT infrastructure, questions are sure to arise regarding the level of attribution necessary to conduct disabling cyber operations against intermediate nodes, where only technical attribution is possible.

With respect to state responsibility for the conduct of non-state actors, there is considerable uncertainty surrounding the meaning of "instructions," "direction," and "control."[413] These uncertainties exist independent of cyber operations, especially with respect to what constitutes sufficient direction and control over an individual or non-state group.[414] These uncertainties will

---

[408] For example, many in the cyber security community openly questioned the U.S. Government's claim that the DPRK was behind the Sony hack. *See, e.g.,* Kim Zetter, *Experts Are Still Divided on Whether North Korea Is Behind Sony Attack*, WIRED (Dec. 23, 2014), https://www.wired.com/2014/12/sony-north-korea-hack-experts-disagree.

[409] Egan, *supra* note 286, at 17.

[410] Schmitt, *Grey Zones, supra* note 11, at 8 (citing Draft Articles on Responsibility of States, *supra* note 291, arts. 4 & 5).

[411] Draft Articles on Responsibility of States, *supra* note 291, art. 8.

[412] Egan, *supra* note 286, at 17.

[413] Schmitt, *Grey Zones, supra* note 11, at 9; TALLINN 2.0, *supra* note 23, at 94-100.

[414] Schmitt, *Grey Zones, supra* note 11, at 9 (discussing the lack of precision and conflicting standards of "overall" verses "effective" control articulated by various international tribunals); Schmitt, *Peacetime Cyber Responses*, *supra* note 4, at 255 (noting the conjunctive understanding of the rule, as opposed to the disjunctive formulation in Article 8 of the Draft Articles). *Contrast Nicaragua* Judgment, *supra* note 328, ¶ 115 (effective control); Application of

obtain increasing relevance as states continue to use loosely affiliated hacker groups as a means of hybrid, gray-zone confrontation.[415]

4. Countermeasures and the International Law of Justification

Another foundational principle of the customary international law of state responsibility is that even if state action violates a rule of international law, wrongfulness may be "precluded" if the action is taken based on a recognized justification, such as national self-defense or as a countermeasure.[416] This customary international law analog to the common law defense of justification, which precludes criminal responsibility, is reflected in Chapter V of the *Articles on the Responsibility of States*. Chapter V lists six specific circumstances precluding the wrongfulness of conduct that would otherwise constitute a breach of an international obligation of the state concerned: consent, self-defense, countermeasures, necessity, *force majeure*, and distress.[417] Of these, countermeasures is the most relevant to cyber operations aimed at countering gray-zone cyber threats and activities.[418] Yet as currently understood, there are substantive aspects of the countermeasure rule that limit its potential effectiveness as a tool in the realm of cyber operations designed to counter gray-zone threats.

The traditional definition of countermeasures includes unlawful actions below the use-of-force threshold that are rendered lawful when taken for the sole purpose of causing another state to desist in its unlawful conduct.[419] Acts of retaliation or retribution do not qualify as countermeasures.[420] Because the purpose of countermeasures is to induce a return to the *status quo ante* between the states involved, the unlawful act triggering the countermeasure must be ongoing or reasonably assessed to be one in a series of wrongful acts, and the countermeasure or measures must be terminated as soon as the responsible state complies with its obligations.[421] When justified, cyber operations that would otherwise be unlawful can be conducted as a countermeasure, but countermeasures are not limited to responses in kind. Non-cyber

---

the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro) (*Bosnian Genocide)*, Judgment, 2007 I.C.J. 43 (Feb. 26) (effective control); *with* Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 137 (Int'l Crim. Trib. For the Former Yugoslavia) (July 15, 1999) (overall control).

[415] *See, e.g.,* Robert Hackett, *Meet 5 of the World's Most Dangerous Hacker Groups*, FORTUNE (June 22, 2017) ("[T]oday the biggest and baddest hacker groups are backed by nation-states."), http://fortune.com/2017/06/22/cybersecurity-5-hacker-groups; SEGAL, *supra* note 4, at 71 (discussing the CyberBerkut, a group headed by "former" Russian and Ukrainian security personnel, conducting cyber operations against NATO websites during Russia's operation in the Crimea in 2013).

[416] TALLINN 2.0, *supra* note 23, at 104-05.

[417] Draft Articles on Responsibility of States, *supra* note 291, arts. 20-26.

[418] *See generally* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 967 (2014) [hereinafter Schmitt, *Countermeasures*].

[419] Schmitt, *Peacetime Cyber Responses*, *supra* note 4, at 253; TALLINN 2.0, *supra* note 23, at 111; Brown et al., *Military Cyberspace Operations*, supra note 46, at 139 & n. 81.

[420] Schmitt, *Peacetime Cyber Responses*, *supra* note 4, at 253.

[421] *Id.;* Draft Articles on Responsibility of States, *supra* note 291, art. 53.

countermeasures can be used to counter internationally wrongful cyber operations, and vice versa, so long as the measures employed adhere to the rule of proportionality.[422]

Countermeasures may only be conducted in response to internationally wrongful acts, and thus require an *ex ante* determination that the act or omission to be countered is both attributable to the state against which the countermeasure will be employed and constitutes a breach of an international obligation of that state.[423] For a number of the reasons already discussed, the various uncertainties involved in properly characterizing particular cyber operations under international law render this baseline determination difficult, as does the need to attribute the cyber operation to the state in question. This requirement also highlights the importance of the sovereignty question, as "violations" of sovereignty below the non-intervention threshold open the door to countermeasures *only* if sovereignty is considered a primary rule of international law. Otherwise, non-coercive operations affecting cyber infrastructure, although prejudicial, are not internationally wrongful and response options are limited to acts of retorsion.[424]

Like self-defense, the concept of countermeasures traces its roots to the historical law of peacetime reprisals.[425] Unlike self-defense, however, countermeasures, the descendant of the non-forcible branch of peacetime reprisals, are bounded by a number of constraints unsuited to the emerging realities of cyber threats.

The first of these conditions is the requirement that the state considering countermeasures must first put the responsible state on notice that it is considered to be in breach of a particular international obligation, and the victim state intends to confront this violation with countermeasures.[426] Although this requirement is not absolute, being subject to a condition of feasibility,[427] the nature of the cyber domain renders it highly impractical. Leaving aside open questions as to what constitutes adequate notice, in the case of countering unlawful cyber operations, for example a coercive DDOS that violates the nonintervention rule, time is likely of critical importance to addressing the harm.[428] Providing prior notice and waiting for the responsible state to voluntarily cease its operation is unrealistic. Further, providing notice may very well enable the responsible state to take steps to defeat the counter-cyber operation and put

[422] That is, the measures must be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question." Draft Articles on Responsibility of States, *supra* note 291, art. 51.
[423] *Id.*
[424] Again, retorsion refers to the taking of measures that are lawful, albeit prejudicial or "unfriendly." *See* Dino Kritsiotis, *International Law and Enforcement*, *in* THE CAMBRIDGE COMPANION TO INTERNATIONAL LAW 251 (James Crawford & Martti Koskenniemi eds., 2012).
[425] Schmitt, *Countermeasures*, *supra* note 418, at 701. Historically, the notion of reprisals encompassed both forceful and non-forceful measures. Forceful reprisals have been subsumed into the *jus ad bellum* as reflected in UN Charter's use of force paradigm. *Id.*
[426] TALLINN 2.0, *supra* note 23, at 120; Draft Articles on Responsibility of States, *supra* note 291, art. 52(1).
[427] TALLINN 2.0, *supra* note 23, at 120; Draft Articles on Responsibility of States, *supra* note 291, art. 52(2); Schmitt, *Peacetime Cyber Responses*, *supra* note 4, at 253.
[428] Egan, *supra* note 286, at 22 ("The sufficiency of a prior demand should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement . . . .").

the victim states sensitive tools and infrastructure at increased risk of compromise. For these reasons, exactly how the notice requirement will play out in the cyber domain remains to be seen.

In contrast to the law of self-defense, with limited exception states cannot engage in collective countermeasures.[429] "Only injured States may engage in countermeasures" and the measures may only be directed against the responsible state.[430] Collateral impacts on third-party states may implicate independent breaches of the executing state's international obligations.[431] Given the trans-border makeup of the global ITT system, to include its basic operating protocols, this limitation can present real challenges to counter-cyber operations. The prohibition on collective action also imposes a questionable barrier to international cooperation and assistance between and among states to counter cyber threats of mutual concern.

Another limitation on countermeasures is that, unlike the case of self-defense, they cannot be taken in anticipation of an actionable harm: "by virtue of their intent to induce a return to lawful relations, countermeasures are reactive, not prospective."[432] As such, they cannot be employed for deterrent purposes.[433] The necessity of anticipatory actions in the face of an imminent threat of unlawful force is well-recognized in international law. But owing to the historically limited nature of countermeasures, no analogous option currently exists. The nature of gray-zone cyber threats is unique, however, and the speed at which sub-use-of-force cyber actions occur will likely bring pressure to adapt the rule and incorporate the *Caroline* standard of imminence and anticipatory self-help measures.[434]

---

[429] Article 48(1) of the Draft Articles on Responsibility of States provides for two exceptions to the prohibition on collective countermeasures:

> [a]ny state other than an injured State is entitled to invoke the responsibility of another State . . . if: (a) [t]he obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or (b) [t]he obligation breached is owed to the international community as a whole.

Draft Articles on Responsibility of States, *supra* note 291, art. 48(1).

[430] Schmitt, *Countermeasures*, *supra* note 418, at 728-29.

[431] *Id.*

[432] *Id.* at 715; *see also* Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 I.C.J. 7, ¶ 83 (Sept. 25) (Countermeasures "must be taken in response to a previous international wrongful act of another State.").

[433] Schmitt, *Countermeasures*, *supra* note 418, at 715.

[434] The *Caroline* standard is the touchstone of the rule of anticipatory self-defense. The *Caroline* incident involved an exchange of diplomatic letters between the United States and Great Britain regarding an attack by the latter against Canadian rebels inside the United States. In 1837, British troops set fire to a steamer, the Caroline, on the U.S. side of the Niagra River, alleging self-defense in that the Caroline had been used to transport Canadian rebels across the border to attack British forces. Then U.S. Secretary of State Daniel Webster filed a strong objection to the British action and justification, stating "[i]t will be for … [Her Majesty's] Government to show a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment of deliberation" and the action must not be "unreasonable or excessive, since the act, justified by the necessity of self-defense, must be limited by that necessity, and kept clearly within it." ELIZBETH WILMHURST ET AL., PRINCIPLES OF INTERNATIONAL LAW ON THE USE OF FORCE BY STATES IN SELF-DEFENCE 7, n. 12 (2005) (quoting letter of Daniel Webster); *see also* Martin A. Rogoff & Edward Collins, Jr., *The Caroline Incident and the Development of International Law,* 16 BROOK. J. OF INT'L L. 493 (1990) (discussing the *Caroline* incident).

Perhaps the most debilitating restraint on countermeasures is the fact that they are only available against states.[435] As such, countermeasures cannot be invoked as a justification for actions taken against non-state actors. Thus, "the international wrongfulness of an injured State's response will not be precluded unless a separate breach by the State to which the injured State's obligations are owed can be identified." The proportionality of the countermeasures taken must be measured against that state's breach, not the actions of the non-state actor.[436]

In this regard, some point to the international obligation of due diligence, which requires states to take feasible or reasonable steps to ensure that harmful or hostile cyber operations, including those by non-state actors, are not conducted from or through their territory.[437] However, as with the principle of sovereignty, the applicability and scope of the due diligence rule to cyberspace is hardly a settled issue, and there are legitimate concerns about mapping it onto the information environment.[438] Even if one accepts that it applies, the obligation is only one of feasibility. Therefore, if it is infeasible for a particular State to identify the source of and take effective action to stop harmful non-state actor cyber activity emanating from within its borders, it has not breached its international obligation, and countermeasures are not available to the victim state. This lacuna in the law is all the more significant if one accepts that conducting a cyber operation against a non-state actor's cyber infrastructure, or any third-party's infrastructure for that matter, would constitute an unlawful violation of the territorial state's sovereignty. Such a gap is untenable, and encourages aggressor states' and malicious cyber actors' use of loosely affiliated proxies and distributed, co-opted cyber infrastructure to operate with impunity.

Countermeasures may ultimately prove to be an effective tool to counter gray-zone cyber threats. But given the current construct of the doctrine and the substantial limitations on its use, "they are not a panacea."[439] As with many aspects of international law, much work remains for states to evolve the law of countermeasures to adapt it to the exigencies of the cyber domain. In the meantime, those advising states on their options for responding to malicious cyber activity directed against them should be mindful of countermeasures and the ambiguities and limitations surrounding them.

V. Conclusion

If 2017 is any indication, the prospect of state-sponsored cyber threats diminishing any time soon is exceedingly poor. For proof, one need look no further than reports of Russia's continued cyber assault on western democratic processes, state sponsored ransomware attacks such as WannaCry, Petya and NotPetya, and China's continued use of cyber as a tool of economic

[435] Schmitt, *Countermeasures*, *supra* note 418, at 730-31.
[436] *Id.*
[437] *See* TALLINN 2.0, *supra* note 23, at 30-43 (discussing the rule of due diligence).
[438] *Id.* (noting the view that the rule has not attained the status of *lex lata*, especially in the context of cyber operations); Michael N. Schmitt, *US Transparency Regarding International Law in Cyberspace*, JUST SECURITY (Nov. 15, 2016) (noting the unsettled nature of the rule), https://www.justsecurity.org/34465/transparency-international-law-cyberspace.
[439] Schmitt, *Countermeasures*, *supra* note 418, at 699.

conflict.[440] Clearly, cyber operations have become a mainstay of international statecraft, and a lucrative, asymmetric tool for revisionist states to pursue their gray-zone strategic objectives. Cyberspace is an offense-dominant environment like no other. Unfortunately, its unique characteristics have lent themselves to a state of persistent confrontation. Further, the line between pure cyber operations and aggressive information warfare is increasingly undiscernible. Unfortunately, recognition of these realities has yet to produce a comprehensive strategy for confronting the growing national-security threat of gray-zone cyber operations. Worthy policy goals aimed at securing a free and open internet and establishing cyberspace as a domain for legitimate, peaceful state and non-state activities will have to be balanced against the pressing need to incorporate traditional deterrence and counter-cyber operations into broader national security strategies.

At the same time, international efforts to bring normative structure and certainty to cyberspace hit rocky shoals with the breakdown of the UN GGE process. The difficult process of adapting and applying existing legal frameworks to the relatively nascent environment of cyberspace has failed to keep pace with the threat, reinforcing the ambiguities that mark the gray zone and make it such an appealing setting for revisionist states. This is not to suggest that cyberspace is, as some have shortsightedly argued, a law-free zone. This important, baseline question has by and large been properly put to rest, and states and the lawyers advising them should not stray from these first principles when approaching the use of cyber operations for state ends to reduce legal uncertainty and achieve greater stability through advancement of the rule of law. However, as demonstrated throughout this Chapter, legal ambiguity predominates in this space, and will take a concerted effort by states to do the difficult work of translating and evolving existing legal frameworks and principles to this new technology and medium of statecraft. These efforts must proceed carefully, mindful not only of the important national security imperatives presented, but also of the unique role states play in the law-making process and the often distorted line between *lex lata* and *lex feranda*.

DRAFT

[440] *See e.g.,* Lily Hay Newman, *The Biggest Cybersecurity Disasters of 2017 So Far*, WIRED (July 1, 2017), https://www.wired.com/story/2017-biggest-hacks-so-far/; Lieutenant Commander Robert Bebber, *China's Cyber-Economic Warfare Threatens U.S.* 143 PROCEEDINGS MAGAZINE 7 (July, 2017), *available at https://www.usni.org/magazines/proceedings/2017-07/chinas-cyber-economic-warfare-threatens-us;* Charles Riley and Samuel Burke, *Intelligence Agencies Link WannaCry Cyberattack to North Korea*, CNNTECH (June 16, 2016), http://money.cnn.com/2017/06/16/technology/wannacry-north-korea-intelligence-link/index.html; *Britain, Germany Brace for Pre-election Cyber Attacks*, THESTRAITSTIMES (May 6, 2017), http://www.straitstimes.com/world/europe/britain-germany-brace-for-pre-election-cyber-attacks.