Boston College Law Review

Volume 63
Issue 9 *Electronic Supplement*

Article 1

10-13-2021

Staccato Warfare

Matthew H. Ormsbee
United States Air Force Judge Advocate General's Corps

STACCATO WARFARE

MATTHEW H. ORMSBEE*

Abstract: "Staccato warfare" describes the prevailing characteristic of modern American warfare, which features military operations that are increasingly characterized by frequent, disconnected offensives in the battlefield of cyberspace rather than a physical battlefield. Stakeholders in political and military circles will benefit from a better understanding of the President's cyberattack arsenal as the executive branch gradually turns to cyber operations over traditional kinetic options. Historically, the President's legal advisers have construed the unilateral war powers of the executive branch very broadly, foregoing robust and traditional notions of congressional scrutiny and public review. Nevertheless, staccato warfare remains a powerful and lawful tool at the President's disposal. This Article argues that staccato warfare protects the American homeland and is justifiable under the President's noncombat military powers and intelligence activities. Staccato warfare achieves vital national security objectives while minimizing the risk of spilling American blood and wasting scarce resources.

INTRODUCTION

American warfare is now marked by brief, spotty conflicts falling below the threshold of war in the constitutional sense. Conflicts take place primarily via cyberattacks, unmanned aircraft strikes, and precision special operations. This Article focuses on cyberattacks to build on constitutional law principles and further the law of war for all stakeholders in contemporary warfare. Military commanders will find ample room within the existing statutory and regulatory framework for a robust but lawful cyberattack arsenal.

President Biden stands to be the latest in a long line of American Presidents who construe the unilateral war powers of the executive branch broadly, aggressively, and with few meaningful checks. Yet, his administration heralds the chance to clarify at least one aspect of presidential war powers: unilateral use of cyberattacks by the executive branch to defend vital national interests. Cyberattacks, as opposed to traditional use of force, offer perhaps the most precise and bespoke tools in the President's defense toolkit. Still, such attacks

* Captain Matthew H. Ormsbee is a commissioned officer in the United States Air Force Judge Advocate General's Corps, currently serving as the Area Defense Counsel at Misawa Air Base, Japan; J.D., Benjamin N. Cardozo School of Law; B.A., Hendrix College. Opinions, conclusions, and recommendations expressed are solely those of the author and do not necessarily represent the views of the U.S. Government, the Department of Defense, or any of its components.

are not without risks, especially as they largely evade congressional review and public scrutiny.

This Article argues that modern warfare has evolved to favor short and discrete unilateral attacks, "staccato warfare," rather than lengthy, all-out wars pitting army against army. Staccato warfare aptly describes the nature of contemporary conflicts, especially in cyberspace where states and non-state parties pursue brief and distinct (though never-ending) operations that are unlikely to escalate to actual armed conflict. Although largely invisible, staccato warfare is preferable to traditional war because it risks less bloodshed, defends American interests, and comports with constitutional parameters on presidential warfighting.

I. CYBERATTACKS

The U.S. Department of Defense (DoD) Joint Publication 3-12 defines a cyberspace attack in terms of impact: "Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains."[1] The DoD's definition of a cyberattack expressly excludes cyber operations that merely seek to gather information or surveille foreign cyber networks. Instead, "denial effects" in the real world are a prerequisite. Because the DoD executes cyberattacks but also conducts substantial cyber offensives for information gathering, this Article includes in its scope virtually every American cyber activity.

Though the definition of a cyberattack is straightforward, the scope of cyberattacks is incredibly vast and diverse. One end of the spectrum features routine attacks that tamper with adversaries' data, for example, while the other end of the spectrum includes multistate attacks that can cripple banking or telecommunications networks with devastating real-world impact. A survey of the past few years provides numerous examples of global ransomware attacks that have imposed exacting tolls around the world, such as the SolarWinds and Microsoft Exchange incidents.[2] In addition, the United States will feel the effects of the 2021 ransomware cyberattack on Colonial Pipeline for years to come.[3]

---

[1] JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS II-7 (2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf [https://perma.cc/7CSS-C8JV].

[2] Danny Steed, *The United Kingdom's New Vision of Cyber Power*, WAR ON THE ROCKS (May 3, 2021), https://warontherocks.com/2021/05/the-united-kingdoms-vision-of-cyber-power [https://perma.cc/N2TG-6DJZ].

[3] David E. Sanger, Clifford Krauss, & Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html [https://perma.cc/M2YJ-UBDD] ("One of the nation's largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks.").

With the constant threat of cyberattacks from abroad, the United States relies on its flagship cyberattack program Defend Forward to execute diverse low-level cyberattacks on a daily basis.[4] Notably, Defend Forward also possesses capabilities for more aggressive cyberattacks with lasting effects, though such capabilities are used far less frequently.[5] Opposed to the all-or-nothing nature of most military intervention, Defend Forward involves a perpetual level of conflict, in which the United States must maintain continual vigilance for attacks on the U.S. Cyber Command's leader described the use of Defend Forward as follows:

> Cyber Command implements this defend forward strategy through the doctrine of persistent engagement. . . .
>
> This doctrine of persistent engagement reflects the fact that one-off cyber operations are unlikely to defeat adversaries. Instead, U.S. forces must compete with adversaries on a recurring basis, making it far more difficult for them to advance their goals over time.[6]

Near-peer competitors will strive for small strategic gains over time through staccato warfare campaigns in cyberspace, where ongoing targeted campaigns remain below the level of warfare and fall well short of catastrophic damage. Instead, discrete attacks on a daily basis seek out chinks in American cyber armor that can be exploited. Defending against endless malicious cyber activity is a consistent theme across the National Defense Strategy, the National Military Strategy, and the 2018 DoD Cyber Strategy.[7]

---

[4] Erica D. Borghard, *Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior*, LAWFARE (Mar. 12, 2020), https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior [https://perma.cc/3ZCE-JEGS] ("Defend forward . . . entails the proactive observing, pursuing, and countering of adversary operations and imposing costs in day-to-day competition to disrupt and defeat ongoing malicious adversary cyber campaigns, deter future campaigns, and reinforce favorable international norms of behavior, using all the instruments of national power."); *see also* Eric Talbot Jensen & Sean Watts, *Due Diligence and the U.S. Defend Forward Cyber Strategy*, LAWFARE (Oct. 20, 2020), https://www.lawfareblog.com/due-diligence-and-us-defend-forward-cyber-strategy [https://perma.cc/J4SE-RR9T] (explaining the primarily preemptive nature of the American "Defend Forward" approach to cyber warfare).

[5] *See* Borghard, *supra* note 4.

[6] Paul M. Nakasone & Michael Sulmeyer, *How to Compete in Cyberspace: Cyber Command's New Approach*, FOREIGN AFFS. (Aug. 25, 2020), https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity [https://perma.cc/Z3ZS-UWVX]; *see also* Matthew C. Waxman, *Cyberattacks and the Constitution* 13 (Hoover Inst., Aegis Series Paper No. 2007, 2020), https://www.hoover.org/research/cyberattacks-and-the-constitution [https://perma.cc/L7CL-MBED] (quoting Nakasone & Sulmeyer, *supra*).

[7] Emily O. Goldman, *From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy*, TEX. NAT'L SEC. REV., Fall 2020, at 84, 86, https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy [https://perma.cc/7B8B-LAUF].

II. LEGAL AUTHORITY

At the heart of any war powers discussion is the division of authority between the President and Congress. The authorization of cyberattacks is no different. Although numerous historical arguments exist regarding the constitutional mandate for each political branch to direct military force, these arguments often assume that cyberattacks amount to "war powers."[8] Admittedly, as the expected damage of an American cyberattack increases, the likelihood that observers will label the cyberattack an exercise of war powers also increases.[9] In addition to the aforementioned constitutional questions, this debate also raises statutory questions. In particular, the drafters of the 1973 War Powers Resolution (WPR), enacted to rein in lengthy military operations without congressional approval, could not foresee cyberattacks, and the WPR does not address them as a possibility. Absent congressional action in the form of an amendment, the WPR is not directly applicable to cyberattacks, though it may be a persuasive authority.[10]

The overwhelming majority of cyberattacks carried out by the United States are so insignificant that they could not credibly be construed as an exercise of war powers under the Constitution. Defend Forward, for its part, employs primarily micro-operations that do not implicate a war powers analysis under constitutional law, and generally do not qualify as "use of force" under international law. Thus, a war powers analysis of cyberattacks—at least garden-variety attacks carried out by the United States on a daily basis—is inappropriate because the war powers framework is ultimately inapplicable.

---

[8] Waxman, *supra* note 6, at 1 (offering an alternative view that the deployment of cyberattacks should not automatically be deemed a "war powers issue" (internal quotations omitted)).

[9] *See, e.g.*, Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SEC. L. & POL'Y 155, 169 (2010) (describing the risk of "inadvertent escalation" from cyberattacks); Jason Healey & A.J. Wilson, *Cyber Conflict and the War Powers Resolution: Congressional Oversight of Hostilities in the Fifth Domain*, GEO. J. INT'L AFF. 59, 62 (noting that the government's narrow definition of "hostilities" may not appropriately account for cyber activities as "remote war-fighting technology becomes ever more capable, reliable, and ubiquitous"); Tyler K. Lowe, Note, *Mapping the Matrix: Defining the Balance Between Executive Action and Legislative Regulation in the New Battlefield of Cyberspace*, 17 SCHOLAR: ST. MARY'S L. REV. ON RACE & SOC. JUST. 63, 74 (2015) (delineating between the executive authority to use "offensive cyber operations" and "the traditional rules of armed conflict"); Lyle Denniston, *Constitution Check: Is the War Powers Clause a Dead Letter in the Cyberspace Age?*, YAHOO! NEWS (Feb. 5, 2013), https://news.yahoo.com/constitution-check-war-powers-clause-dead-letter-cyberspace-113217808.html [https://perma.cc/Y9YT-L5W2] (highlighting the stark contrast of traditional warfare, as understood by the founders and the modern reality of cyber warfare).

[10] *See, e.g.*, Eric Talbot Jenson, *Future War and the War Powers Resolution*, 29 EMORY INT'L L. REV. 499, 503 (2015). *See generally* Oona A. Hathaway, *How to Revive Congress' War Powers*, TEX. NAT'L SEC. REV. 41 (Nov. 14, 2019), https://tnsr.org/roundtable/policy-roundtable-the-war-powers-resolution/ [https://perma.cc/8XZ4-8KB4] (appearing in *Policy Roundtable: The War Powers Resolution*, a group of legal scholars and practioners gathered to "discuss the War Powers Resolution and what should, or should not, be done to improve it").

Executive action for cyberattacks below the war threshold can find more ample doctrinal support from other sources of law, such as the President's non-combat military powers and intelligence powers. To alleviate concerns about unchecked executive power, Congress has played an active role in developing U.S. cyber strategy. Members of Congress actively greenlight cyber defense measures and more aggressive uses of military cyber operations for certain adversarial states.[11] In short, the legislative and executive branches have demonstrated a successful collaboration to orchestrate cyber military engagements.[12]

III. Eschewing Traditional War Powers

The Founders' delegation of power to Congress to declare war seems uncomplicated, yet the question soon arose as to whether Congress has *full* discretion to decide when the country goes to war. There are certainly reasons to argue that Congress does have this authority. In particular, this would ensure thorough deliberation over such heavy determinations, preventing rash decisions and ensuring that a single person does not wield war declaration powers. Over time, stakeholders formed a consensus around the idea that Congress alone should decide when to move the country from peacetime to war.

Despite this understanding, Presidents have gradually asserted far greater authority to employ military force without congressional approval. At times, this evolution has occurred with the implied blessing of Congress and the courts. "Modern executive-branch legal precedent and practice generally hold that the president has broad authority to launch military strikes"—even without Congress's approval, so long the action defends American interests.[13] Proponents of unilateral executive action in cyber operations draw parallels to the President's well-established powers to use kinetic military force. Indeed, in 2020, the DoD's General Counsel, Paul Ney, argued that the legal analysis for cyberattacks mirrors the analysis for kinetic military attacks:

---

[11] Robert Chesney, *The Domestic Legal Framework for US Military Cyber Operations* 3 (Hoover Inst., Aegis Series Paper No. 2003, 2020), https://www.hoover.org/research/domestic-legal-framework-us-military-cyber-operations [https://perma.cc/R3WB-S43D].

[12] *Id.* at 1 ("Congress and the executive branch have cooperated effectively over the past decade to build a legal architecture for military cyber operations.").

[13] Waxman, *supra* note 6, at 3; *see, e.g.*, Memorandum Opinion from Steven A. Engel, Assistant Att'y Gen., Office of Legal Couns., to the Couns. to the President, April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities 3 (May 31, 2018), https://www.justice.gov/olc/opinion/file/1067551/download [https://perma.cc/8HMJ-QXJD]; Memorandum Opinion from Caroline D. Krass, Principal Deputy Assistant Att'y Gen., Office of Legal Couns., to the Att'y Gen., Authority to Use Military Force in Libya 6 (Apr. 1, 2011), https://www.justice.gov/olc/file/2011-04-01-libya-deployment/download [https://perma.cc/65QK-P3RM].

> The domestic legal authority for the DoD to conduct cyber operations is included in the broader authorities of the President and the Secretary of Defense to conduct military operations in defense of the nation. We assess whether a proposed cyber operation has been properly authorized using the analysis we apply to all other operations, including those that constitute use of force.[14]

When the executive branch utilizes "military operations in defense of the nation" they broach broad and unsettled constitutional boundaries.[15] Such operations tend not to be implicated by the war powers clause. Ney went on to explain the legal framework as it applied to the department's cyber capabilities:

> The President has authority under Article II of the U.S. Constitution to direct the use of the Armed Forces to serve important national interests, and it is the longstanding view of the Executive Branch that this authority may include the use of armed force when the anticipated nature, scope, and duration of the operations do not rise to the level of "war" under the Constitution, triggering Congress's power to declare war. Furthermore, the Supreme Court has long affirmed the President's power to use force in defense of the nation and federal persons, property, and instrumentalities.[16]

Ney concluded that "the President has constitutional authority to order military cyber operations even if they amount to use of force" to protect the nation.[17] There is an argument that a cyberattack becomes an exercise of war powers when U.S. Cyber Command executes it, the resulting damages are on par with a kinetic strike, and the United States can reasonably expect it to incite armed retaliation.[18] But there are more persuasive reasons *not* to classify cyberattacks as uses of war powers, since such powers were originally intended to address physical violence rather than cyber violence. The exercise of war powers is apt partly because of the risk of American bloodshed, but cyberat-

---

[14] *See* Waxman, *supra* note 6, at 4 (quoting Hon. Paul C. Ney, Jr., Dep't of Def. Gen. Couns., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference [https://perma.cc/J479-GBUG]).

[15] *Id.* (quoting Hon. Paul C. Ney, Jr., *supra* note 14).

[16] *Id.* (quoting Hon. Paul C. Ney, Jr., *supra* note 14).

[17] *Id*. (quoting Hon. Paul C. Ney, Jr., *supra* note 14).

[18] *Id.* ("Viewing some cyberattacks as the exercise of war powers may seem sensible for several reasons. If they are carried out by US Cyber Command, the organization of the armed forces tasked with conducting offensive cyber operations, the agent is the same one that conducts kinetic attacks.").

tacks hardly risk American lives. Extreme human remoteness in cyber conflicts helps to justify unilateral presidential action.[19]

War powers are unique because they require careful consideration for the risk of conflict escalation. Thoughtful inter-branch deliberation is vital if actions are likely to induce militaristic responses. "In recent decades, executive-branch practice and legal justifications have acknowledged this factor, too, in assessing whether a military intervention rises to the level of 'war' perhaps requiring congressional authorization."[20] In 2018, the Justice Department's Office of Legal Counsel issued an opinion which justified President Trump's use of air power against Syria. The report noted that the military took measures to reduce the likelihood of military reprisals, thereby strengthening the argument that the strikes were within presidential authority.[21] On the other hand, if cyberattacks create a substantial risk of provoking retaliatory violence, then perhaps congressional approval should be required.

Additionally, cyberattacks, much like kinetic attacks, can have unintended consequences and risk escalation or retaliation.[22] It is very unlikely, however, that cyberattacks—barring those with catastrophic impact—would risk provoking an armed military response. More probable reactions to cyberattacks include diplomatic censure, economic sanctions, or counter-cyberattacks. A very small percentage of cyberattacks justifiably invoke constitutional war powers, even when the recipient state regards the acting state's cyberattack as a hostile military action under international law.

For those cyberattacks that may qualify as uses of force or armed attacks, under the United Nations Charter, the United States has reserved the right to

---

[19] *See, e.g.*, Engel, *supra* note 13, at 2–3 (emphasizing that the President selected strike targets in Syria that would "minimize collateral damage" (citations omitted)); Memorandum Opinion from Caroline D. Krass, *supra* note 13, at 25 (explaining that the strike zones in Libya specifically targeted enemy air bases away from civilian settlements);

[20] Waxman, *supra* note 6, at 5.

[21] *Id.*; *see also* Engel, *supra* note 13, at 21.

[22] *See, e.g.*, Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world [https://perma.cc/H5MH-KSUN]; David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [https://perma.cc/D8JY-PYAC] (relating to Russian-made malware that targeted Ukrainian servers in 2017 and inadvertently spread around the world to devastating effect); Vivian Yeo, *Stuxnet Infections Spread to 115 Countries*, ZDNET (Aug. 9, 2010), https://www.zdnet.com/article/stuxnet-infections-spread-to-115-countries [https://perma.cc/NG33-CSDB] (providing an update regarding the spread of the malicious computer code that targeted Iranian nuclear plant control systems, widely attributed to U.S. operations, which later spread across the globe). *See generally* BEN BUCHANAN, THE CYBERSECURITY DILEMMA: HACKING, TRUST AND FEAR BETWEEN NATIONS (2017) (arguing that cyber operations, regardless of their true intent, are often viewed as threatening and malicious by recipient states, thus destabilizing relations).

respond with kinetic military force.[23] Other states similarly take this stance, drawing a legal analogy between cyberattacks and kinetic attacks.[24] For its part, Defend Forward is based around utilizing cyber operations well below such levels of severity. Thus, it is unclear why kinetic military attacks should be the presumptive analogy for cyberattacks under a constitutional powers analysis. The differences between the two forms of attacks are numerous and substantial. Ultimately, a war powers analysis is a poor fit for considering the lawfulness of cyberattacks. It is unclear whether most cyberattacks should alone be considered "hostilities," thereby implicating the limitations imposed by the War Powers Resolution."[25] Including cyberattacks under the war powers umbrella is a broad and illogical expansion of constitutional doctrine when other constitutional powers are more apt.

IV. DEFEND FORWARD

If the legal community accepts that cyberattacks rarely amount to war powers, then justification for the power must be found elsewhere in the constitution. While a number of constitutional justifications may be applicable, U.S. cyberattacks should most commonly be categorized similarly to noncombat military powers and intelligence powers.[26]

"Defend Forward involves proactively countering malicious adversary cyber campaigns through day-to-day competition. Defend Forward aims to disrupt adversary cyber operations, deter future campaigns."[27] Per the 2018

---

[23] *See Cyber Strategy & Policy: International Law Dimensions: Testimony Before the S. Armed Forces Comm.*, 115th Cong. 3 (2017) (statement of Matthew C. Waxman, Professor of Law, Columbia Law School).

[24] *See, e.g.*, Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 431 (2011); Michael N. Schmitt, *Noteworthy Releases of International Cyber Law Positions—Part I: NATO*, Posting to *Articles of War*, LIEBER INST. W. POINT (Aug. 27, 2020), https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i [https://perma.cc/VL6E-4M5J].

[25] In the 2011 Libya intervention, the Obama Administration argued that "hostilities" did not arise because the exposure of U.S. military forces, risk of escalation, and military means were all limited. *See Libya and War Powers: Hearing Before the S. Comm. on Foreign Relations*, 112th Cong. 58 (2011) (statement of Harold Koh, Legal Adviser, U.S. Dep't of State); *see also* Waxman, *supra* note 24, at 434–35 (reasoning why cyberattacks should not be equated with physical, armed military strikes).

[26] *See* Gary P. Corn, *Cyber National Security: Navigating Gray-Zone Challenges in and Through Cyberspace*, *in* COMPLEX BATTLESPACES: THE LAW OF ARMED CONFLICT AND THE DYNAMICS OF MODERN WARFARE 367 (Christopher M. Ford & Winston S. Williams eds., 2019) (clarifying that for many U.S. cyber operations, "the scope of the president's authority is 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"); *see also* Waxman, *supra* note 6, at 7.

[27] Waxman, *supra* note 6, at 8; *see also* Borghard, *supra* note 4.

DoD Cyber Strategy: the DoD "will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[28]

The vast majority of Defend Forward operations do not meet the threshold necessary to be considered "cyberattacks" under the definition adopted by the DoD. Defend Forward operations include penetrating to foreign networks, collecting data, and creating groundwork for other potential operations. Certainly, some of Defend Forward actions are properly classified as cyberattacks. These might include interrupting communications from an adversary military facility used to infiltrate U.S. military command and control systems, inserting malware that deletes or encrypts data on servers engaged in malign foreign influence campaigns online, or denying service to networks used by adversary intelligence agencies to conduct industrial espionage."[29] Such operations involve combinations of at least two constitutional powers.[30]

A. Noncombat Military Powers

Cyberattacks and operations carried out by U.S. military agencies should be viewed presumptively as noncombat military activities, thus constitutionally authorized as a power reserved to the executive branch, though falling short of the hostile application of armed force. As the Commander in Chief of the Armed Forces, the President has authority to engage U.S. military forces in training exercises to prepare for conflict.[31] Historically, the executive branch has viewed its authority broadly in this respect, notably ordering American pilots to train British pilots at U.S. facilities in 1941. At that time, the U.S. Attorney General opined:

> [T]he president "has supreme command over the land and naval forces of the country and may order them to perform such military duties as, in his opinion, are necessary or appropriate for the defense of the United States. These powers exist in time of peace as well as in time of war."[32]

---

[28] U.S. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018), https://media.defense.gov/2018/sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf [https://perma.cc/UU7B-7SY7].

[29] Waxman, *supra* note 6, at 8.

[30] *Id*.

[31] *See* W. TAYLOR REVELEY III, WAR POWERS OF THE PRESIDENT AND CONGRESS: WHO HOLDS THE ARROWS AND OLIVE BRANCH? 15–16 (1981) (listing the hypothetical military scenarios that require joint authorization or action from the President and Congress).

[32] Waxman, *supra* note 6, at 8 (quoting Training of British Flying Students in the United States, 40 Op. Att'y Gen. 58, 61 (1941)).

Thus, Defend Forward's use of cyberattacks against foreign systems as a proactive measure to thwart enemy invasions into American intelligence networks resembles the British improving their pilot program to undercut the prowess of Germany's air force in World War II.[33] In both cases, the adversary's capabilities are degraded without kinetic strikes or actual physical destruction. In fact, the vast majority of cyberattacks, even outside the scope of Defend Forward, could be viewed as an exercise of the President's noncombat military powers. A prominent example is the 2019 U.S. cyber operation that destroyed Iranian information systems used to target ships.[34] Such efforts are primarily prophylactic and aimed at general deterrence or thwarting specific future attacks.

Finally, Congress reserves the right to limit executive authority with respect to war powers. The executive branch has broad discretion as Commander in Chief but legally must stay within statutory restrictions. To that point, Congress regulates the extent to which the U.S. military trains and equips foreign forces. Legislative tools such as appropriation of funds, limit the President's authority.[35] Historically, Congress has imposed various limitations on the executive branch deploying troops abroad during peacetime.[36] Yet, while Congress could legislate to restrict military cyber activities, to date it has not done so.

B. Intelligence Activities

Another conduit for cyberattacks via Defend Forward is the President's intelligence powers under the Constitution.[37] National security concerns somewhat cloud this area of constitutional law, regrettably precluding the degree of public analysis of government action that typically accompanies war-

---

[33] *See id.* ("Cyberattacks carried out by the US military inside foreign networks to, for example, prevent or deter adversary efforts to infiltrate US information systems could be understood much like the training of British pilots aimed at undermining German air superiority.").

[34] *See* Julian E. Barnes, *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*, N.Y. TIMES (Aug. 28, 2019), https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html [https://perma.cc/CPY4-L2AY] (explaining that U.S. Cyber Command designed the strike "to stay well below the threshold of war," and merely inhibit the Iranian Revolutionary Guard's capacity to initiate future attacks against American systems).

[35] *See generally* BOLKO J. SKORUPSKI & NINA M. SERAFINO, CONG. RSCH. SERV., R44602, DOD SECURITY COOPERATION: AN OVERVIEW OF AUTHORITIES AND ISSUES (2016) (providing an overview of the authorities Congress grants the DoD in regard to foreign engagements and national security).

[36] *See generally* JENNIFER K. ELSEA, MICHAEL JOHN GARCIA & THOMAS J. NICOLA, CONG. RSCH. SERV., R41989, CONGRESSIONAL AUTHORITY TO LIMIT MILITARY OPERATIONS (2013) (synthesizing the various mechanisms Congress uses to confine the President's use of military power).

[37] *See* Joshua Rovner, *Cyber War as an Intelligence Contest*, WAR ON THE ROCKS (Sept. 16, 2019), https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest [https://perma.cc/38EH-F942].

time action. The President has historically argued for broad discretion under the intelligence powers, citing the President's authority in the realm of foreign relations, in combination with the Commander in Chief's authority. Accordingly, the President has claimed robust intelligence authority to undercut adversaries' militaries and state organs. Cyber efforts to collect information fit cleanly within the President's intelligence powers, while more disruptive offensives require closer analysis.

On occasion, the executive branch has asserted that the President's intelligence powers include control over electronic surveillance, signals intelligence, "quasi-military activities such as paramilitary support to proxy groups or physical sabotage operations, as well as propaganda campaigns and other political manipulation."[38] Further removed activities include propaganda campaigns and other manipulation efforts when the United States government can reasonably deny any responsibility or involvement.[39] It is unclear whether certain intelligence activities, especially when they include physical violence, aptly fall within war powers or another constitutional category.

Congress has played an active role, regulating intelligence activities through procedural and reporting requirements.[40] Oversight statutes can be viewed either as a recognition and limitation on the President's intelligence powers or as an implicit authorization of the President to conduct covert intelligence activities without specific congressional approval. Ultimately, the current framework does not require the President to seek formal approval for each operation, but must meet congressionally imposed limitations.[41]

---

[38] Philip A. Lacovara, *Presidential Power to Gather Intelligence: The Tension Between Article II and Amendment IV*, 40 L. & CONTEMP. PROBS. 106, 106-108 (1976) (describing intelligence gathering and the President's "sweeping" powers with respect to intelligence gathering); Waxman, *supra* note 6, at 10 (citation omitted).

[39] S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK I, S. REP. NO. 94-755, at 475 (1976) (defining "covert action" as it is used in the American intelligence community (citation omitted)); *see Oversight Legislation: Hearing on S. 1721 and S. 1818 Before the S. Select Comm. on Intel.*, 110th Cong. 93 (1987) (statement of Charles J. Cooper, Assistant Att'y Gen., Office of Legal Counsel, United States Department of Justice) (testifying that some degree of secrecy and discretion is imbued in the in the President's constitutional duties); *see also* Richard O.W. Morgan & Jonathan M. Fredman, *The Law of Foreign and National Intelligence*, *in* NATIONAL SECURITY LAW & POLICY 1041, 1048 (John Norton Moore, Guy B. Roberts & Robert F. Turner eds., 3d ed. 2015) (labeling "covert action" a category of the President's Article II intelligence powers).

[40] 50 U.S.C. § 3093 (requiring the President to report to Congress any material information regarding "covert actions").

[41] *See* M.E. Bowman, *Secrets in Plain View: Covert Action the U.S. Way*, 72 INT'L L. STUD. 1, 10 (1998) ("Although the precise authority for covert action is debatable, it is clear that both the Congress and the Executive believe it a necessary option. Both presume that legal authority exists to engage in covert action and each presumes to have a Constitutionally authorized, if not precisely defined, role.").

Cyberattacks pursued under Defend Forward can be constitutionally based in the intelligence powers, since the method of cyberattacks (secret incursion to foreign networks) is primarily an intelligence activity.[42] Even more damaging cyber operations that alter data or input malware are analogous to "black bag jobs" that secretly aid "proxy paramilitary forces," a common tactic deployed by American intelligence groups. This type of attack differs from Stuxnet—a cyber mission that wrought notable, concrete damage to strategically significant military sites—which appears more like an "exercise of war powers."[43] Still, such operations are similar to past operations undertaken pursuant to intelligence powers. Such intelligence operations tend to be treated as a different constitutional category.[44]

CONCLUSION

Military lawyers and commanders must not reflexively categorize cyberattacks as exercises of war powers, except in rare circumstances. More commonly, the American doctrine of "persistent engagement" in cyberspace fits cleanly in the constitutional categories of noncombat military powers and intelligence powers. While the President may wield extraordinary power as the Commander in Chief of U.S. cyber warfare, Congress should maintain its active engagement in shaping U.S. cyber strategy, encouraging assertive cyber operations against certain adversaries.[45] Staccato warfare will continue to characterize modern warfare, requiring constant agility against adversaries as the United States competes at levels just below that of armed conflict and deflects malicious cyberattacks on a daily basis.

Preferred citation: Matthew H. Ormsbee, *Staccato Warfare*, 63 B.C. L. REV. E. SUPP. I.-1 (2022), http://lawdigitalcommons.bc.edu/bclr/vol63/iss9/1/.

---

[42] Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SEC. L. & POL'Y 539, 580 (2012).

[43] Waxman, *supra* note 6, at 10.

[44] *Id.*

[45] Robert Chesney, *supra* note 11, at 3.