ANALYSIS

EMERGING TECHNOLOGY AND PRESIDENTIAL WAR POWERS[1]

Blaine Ravert

Introduction

On September 3, 2025, President Donald Trump ordered a drone strike which killed 11 alleged members of the Trans De Aragua gang using a boat to smuggle drugs into the United States.[2] As of November 11, at least 15 additional boat strikes were conducted, killing over 60 people.[3] On November 3, the Trump Administration declared the strikes did not count as "hostilities" under the 1973 War Powers Resolution (WPR), claiming these actions fell under unilateral presidential authority.[4] Following a build up of military forces in the Caribbean, on January 3, 2026, U.S. military forces captured Venezuela leader Nicolas Maduro. President Trump stated that "We're going to run the country until such time as we can do a safe, proper and judicious transition."[5] These actions have produced mixed reactions. Many commentators argue these strikes lack a sound legal basis.[6] Others, such as the *Wall Street Journal* Editorial Board, argue that Trump is within his constitutional authority to take this

[1] This analysis was in the final stages of editing in December 2025. As such, it does not include any detailed commentary concerning the Trump Administration's January 3, 2026 operation against Venezuela.

[2] Matt Murphy and Joshua Cheetham, "US Strike on Venezuela Drug Boat," *BBC News*, 3 September 2025, https://www.bbc.com/news/articles/cdjzw3gplv7o.

[3] Jeremy Chin and Margaret Chin, "Timeline of Vessel Strikes," *Just Security*, November 6, 2025, https://www.justsecurity.org/124002/timeline-vessel-strikes-related-actions/.

[4] Filip Timotja, "Congressional approval for drug boat strikes not needed, White House says," *The Hill*, November 3, 2025, https://thehill.com/homenews/5587430-white-house-argues-drug-strikes/.

[5] Konstantin Toropin, "A Look at the US military's unusually large force in the Caribbean Sea." Associated Press, October 21, 2025, https://apnews.com/article/us-military-buildup-caribbean-venezuela-ships-troops-810f6181371f53536c723ea562c5277c; Alan McPherson, "Trump's squeeze of Venezuela goes beyond Monroe Doctrine," The Conversation, November 2, 2025, https://theconversation.com/trumps-squeeze-of-venezuela-goes-beyond-monroe-doctrine-in-ideology-intent-and-scale-its-unprecedented-268845; Tiago Rogero, "Pentagon's largest warship sent into Latin America waters as US tensions with Venezuela rise," *The Guardian*, November 11, 2025, https://www.theguardian.com/us-news/2025/nov/11/navy-carrier-trump-drugs-caribbean-latin-america; and, *Associated Press*, "U.S. strikes Venezuela and says leader Maduro has been captured and flown out of the country," January 3, 2026, https://www.pbs.org/newshour/world/us-strikes-venezuela-and-says-its-leader-maduro-has-been-captured-and-flown-out-of-the-country.

[6] Benjamin Wittes, "I Never Signed Up for This Kind of Targeted Killing," *Lawfare*, September 7, 2025, https://www.lawfaremedia.org/article/i-never-signed-up-for-this-kind-of-targeted-killing; and, Blaine Ravert, "Strikes on drug boats raise troubling constitutional issues," *St. Louis Post-Dispatch*, September 18, 2025, https://www.stltoday.com/opinion/column/article_37c59673-c784-44db-915b-72b7ee6781af.html.

unilateral action.[7] Congressional efforts to limit Trump's ability to conduct these strikes have so far failed.[8]

These boat strikes are not the first time Trump has courted controversy regarding war powers. In June, President Trump ordered a major bombing strike against three Iranian nuclear facilities.[9] From March to May, Trump ordered a series of strikes against Houthi rebels in Yemen.[10] These strikes each raise the issue of the degree of unilateral authority the president has in order to use force. In the age of great power competition, including the possibility of China invading Taiwan, this issue is likely to become increasingly important.[11] These strikes are connected by another factor: they each used technologies frequently employed in modern warfare, including drone and missile strikes, supported by cyber operations. This fact highlights another issue: the current legal frameworks regarding the balance of war powers between the executive and legislative branches were not designed to take these technologies into account.

These technologies are connected by several common features that make congressional oversight of their usage by presidents more challenging. Expansive presidential unilateral war powers generate several concerns, including increased escalation risk, lack of long-term strategic planning, and decreased accountability to Congress. This analysis utilizes case studies of congressional oversight of drone strikes by the Obama Administration and the Department of Defense's 2018 offensive cyber strategy shift to explore these issues. These challenges are likely to impact congressional oversight of the second Trump Administration, 2025 to 2029.

The War Powers Struggle

The proper balance of war powers between the president and Congress is a consistent area of contestation between the executive and legislative branches, centering around three core

---

[7] The Editorial Board, "The War Powers Irresolution," *The Wall Street Journal*, November 4, 2025, https://www.wsj.com/opinion/donald-trump-war-powers-senate-congress-venezuela-e801f43a?gaa_at=eafs&gaa_n=AWEtsqesTPrqRwdRIIRCIFP0kH2KwVRmW5B_uwd1EdCJ0r9yX4w95EJldJGKr4tXLhY%3D&gaa_ts=6914d32d&gaa_sig=M1nvyIQWRqykBAU_7XRRB7_3LFYDlmU6U6f2yXk7-Q_7d8dn1yl6ZKxfVf27FMWKFnr-MN_ZS9XS_LwxO9Vd0g%3D%3D.

[8] Frank Thorp V, "Senate rejects bipartisan resolution that would block Trump military action against Venezuela," *NBC News*, November 6, 2025, https://www.nbcnews.com/politics/congress/senate-rejects-resolution-block-trump-military-action-venezuela-rcna242485.

[9] Peppino DeBiaso, "Striking Iranian Nuclear Facilities: A vital U.S. Interest, not Altruism," *Information Series*, No. 631 (Fairfax, VA: National Institute Press, August 1, 2025), https://nipp.org/wp-content/uploads/2025/07/IS-631.pdf, pp. 1-4.

[10] Heather Mongilio, "Operation Rough Rider," *USNI News*, April 29, 2025, https://news.usni.org/2025/04/29/operation-rough-rider.

[11] Keith B. Payne and Matthew R. Costlow, "Victory Denial: Deterrence in Support of Taiwan," *Occasional Paper*, Vol. 2, No. 3 (Fairfax, VA: National Institute Press, March 2022), https://nipp.org/wp-content/uploads/2022/03/OP-Vol.-2-No-3.pdf, pp. 9-27; and, Keith B. Payne and David J. Trachtenberg, "Deterrence in the Emerging Threat Environment," *Occasional Paper*, Vol. 2, No. 8 (Fairfax, VA: National Institute Press, August 2022), https://nipp.org/wp-content/uploads/2022/08/OP-Vol.-2-No.-8.pdf, pp. 20-40.

sources of war powers authority: The Constitution, the 1973 WPR, and the 2001 and 2002 Authorizations for Use of Military Force (AUMFs).

Constitution

The Constitution divides war powers between the president and Congress. Article I, Section 8, grants Congress the power to declare war, grant letters of marquee, fund the military, and regulate land and naval forces.[12] An initial draft of the Constitution granted Congress the power to "make war," eventually changed to "declare war" to enable presidents to respond to sudden attacks.[13] The presidents' war powers are more ambiguous. Article II, Section 1 vests the president with the "executive power."[14] While Congress can declare war, the president is Commander-in-Chief, the highest-ranking military officer. Broadly, the system of war powers between the branches is designed to prevent either branch from acting unilaterally.

WPR

The 1973 WPR was passed by Congress in response to the Vietnam War.[15] No president has accepted the WPR as constitutional.[16] Section 2 declares the president can only enter into "hostilities" with respect to at least one of three conditions: one, when war has been declared; two, "specific statutory authorization"; or three, a national emergency.[17] Section 3 requires presidents to consult with Congress "in every possible instance" prior to entering into "hostilities."[18] Section 5 creates a 60-day clock during which the president can use force unilaterally. This window can be extended another 30 days if the president certifies in writing to Congress that necessity requires U.S. forces remain engaged in "hostilities." After this window closes, the president is required to withdraw forces if Congress has not affirmatively authorized this action.[19] Theoretically, the WPR mandates substantial congressional involvement in the decision to use force.

---

[12] National Archives, "The Constitution of the United States: A Transcription," https://www.archives.gov/founding-docs/constitution-transcript, Article I, Section 8.

[13] Stephen P. Mulligan, "The Declare War Clause, Part 1: Overview and Introduction," Congressional Research Service, September 30, 2024, https://crsreports.congress.gov/product/pdf/LSB/LSB11230, p. 2.

[14] Ibid, Article II, Section 1.

[15] Peter E. Quint, "The Separation of Powers Under Nixon: Reflections on Constitutional Liberties and the Rule of Law," *Duke Law Journal*, 1981, No. 2 (February 1981). https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2763&context=dlj, pp. 6-9.

[16] Scott R. Anderson, "The Underappreciated Significance of the War Powers Resolution," *Lawfare*, November 9, 2023, https://www.lawfaremedia.org/article/the-underappreciated-legacy-of-the-war-powers-resolution.

[17] The War Powers Resolution, H.R. 542, 93rd Congress (1973), https://www.congress.gov/93/statute/STATUTE-87/STATUTE-87-Pg555.pdf, Section 2.

[18] Ibid., Section 3.

[19] Ibid, Section 5. Geoffrey Corn offers an excellent description of this section, highlighting its role as a fail-safe measure to retain congressional control over war powers. Geoffrey Corn, "Trump's Latest Military Campaign Tests limits of

AUMFs

The 2001 AUMF was passed on September 18, 2001. The act authorizes the president to use "all necessary and appropriate force," against "nations, persons, or organizations," involved in the September 11, 2001 attacks, granting sweeping authority to presidents.[20] The 2002 AUMF authorizes the president to use all measures necessary to defend the United States against Iraq.[21] More than 20 years after they were enacted, both AUMFs remain in effect (although at the time of this writing the Fiscal Year 2026 National Defense Authorization Act (NDAA) would repeal the latter) and have been used to justify a wide variety of presidential actions.[22]

The Proper War Powers Balance

As these debates and tensions show, the relevant authorities leave a large amount of room for debate regarding the best allocation of war powers. Some policymakers and scholars claim the president should possess primary influence over war powers. A common argument for this position is that the president is best equipped to take rapid and decisive action to defend national security while maintaining operational secrecy.[23] Others argue that Congress should possess primary authority, providing necessary deliberation to ensure uses of force are fully considered.[24] Additionally, the drafters of the Constitution were concerned that presidents, driven by a desire for fame, would use force purely to win public support.[25]

Presidential War Powers," *The Cipher Brief*, November 4, 2025, https://www.thecipherbrief.com/war-powers-caribbean-counternarcotics.

[20] To Authorize the use of United States Armed Force against those responsible for the attacks against the United States, Pub. Law. 107-140, 107th Congress (September 2001), https://www.congress.gov/107/plaws/publ40/PLAW-107publ40.pdf#page73, pp. 1-2.

[21] To Authorize the use of Armed Force against Iraq. Pub. Law, 114, 107th Congress (October 2002), https://www.congress.gov/107/statute/STATUTE-116/STATUTE-116-Pg1498.pdf#page73, pp. 1-4.

[22] Tim Kaine and Todd Young, "War, Diplomacy, and Congressional Involvement," *Harvard Journal of Legislation*, 58, No. 1 (June 2021), https://journals.law.harvard.edu/jol/wp-content/uploads/sites/86/2021/06/201_Kaine-Young.pdf, pp. 198-200; Patrick Hulme, "Repealing the 2002 Zombie AUMF(s)," *Lawfare*, July 15, 2021, https://www.lawfaremedia.org/article/repealing-zombie-iraq-aumfs-clear-win-constitutional-hygiene-unlikely-end-forever-wars; and, Matthew C. Waxman, "War Powers Reform: A Skeptical View," *Yale Law Journal Forum*, March 8, 2024, https://www.yalelawjournal.org/pdf/WaxmanYLJForumEssay_uop6awkf.pdf, p. 683.

[23] Alexander Hamilton, "Federalist 70," March 17, 1788, https://avalon.law.yale.edu/18th_century/fed70.asp; and, Richard Cheney, "Address," *Washington University Law Quarterly*, 68, No. 3 (Fall 1990), https://journals.library.wustl.edu/lawreview/article/4984/galley/21817/view/, p. 528; and, David J. Trachtenberg, "Clarifying the Issue of Nuclear Weapons Release Authority," *Information Series*, No. 503 (Fairfax, VA: National Institute Press, September 2021), https://nipp.org/information_series/david-j-trachtenberg-clarifying-the-issue-of-nuclear-weapons-release-authority-no-503-september-22-2021/, pp. 1-5.

[24] Jack Goldsmith and Matthew C. Waxman, "The Legal Legacy of Light Footprint Warfare," *The Washington Quarterly*, 39, No. 2 (Summer 2016), https://law.yale.edu/sites/default/files/goldsmith_and_waxman.pdf, pp. 10-11.

[25] William Michael Treanor, "Fame, The Founders, and The Power to Declare War," *Cornell Law Review,* 82, No. 1 (May 1997), https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2685&context=clr, pp. 771-772.

Congressional involvement in war powers is required to ensure this desire does not lead to unwise military action.

The Rise of Drones and Cyber Operations

In recent years, a variety of emerging technologies, including drones and cyber operations, have played an increasingly important role in warfare. Unmanned aerial vehicles, known as drones, have played an increasing role in warfare since the War on Terror began. The United States has used drones since the Vietnam War. In 2000, a drone captured an image of Osama Bin Laden, prior to the September 11, 2001 terrorist attacks.[26] After those attacks, drones emerged as a key tool of counterterrorism operations.

In recent years, cyber operations have posed increasing concerns. Cyberspace consists of multiple systems involved in maintaining the upkeep of computer networks and connections.[27] Offensive Cyber Operations (OCOs) are "any cyber activity which can have an effect on a computer system or network."[28] OCOs seek to degrade or manipulate computers and computer networks while cyber espionage operations seek to gain action about adversary systems and intentions.[29]

Three Factors

These technologies share three factors that make congressional influence over their usage particularly challenging.

First Factor: Speed of Action

Simply put, it takes time for Congress to effectively exercise war powers.[30] Additionally, under the WPR, the president can deploy forces and engage in "hostilities" for up to 90 days without needing express congressional approval. Due to the speed with which drone strikes and cyber operations can be conducted, a lot can happen in 90 days.

Second Factor: Legal Constraints

Most drone strikes and cyber operations do not rise to the level of "war," which requires congressional authorization. For example, in 2011, the Office of Legal Council, a branch of

[26] John W. Rollins, "Armed Drones: Evolution as a Counterterrorism Tool," Congressional Research Service, November 7, 2023, https://crsreports.congress.gov/product/pdf/IF/IF12342, p. 2.

[27] National Institute of Science and Technology, "Cyberspace," https://csrc.nist.gov/glossary/term/cyberspace.

[28] Juliet Skingsley, "Offensive Cyber Operations," Chatham House, September 19, 2023, https://www.chathamhouse.org/2023/09/offensive-cyber-operations/01-introduction.

[29] Ibid.

[30] Ida A. Brudnick, "The Congressional Research Service and the American Legislative Process," Congressional Research Service, April 12, 2011, https://crsreports.congress.gov/product/pdf/RL/RL33471, pp. 7-9.

the Justice Department dedicated to providing the president legal advice, argued the Obama Administration's support of a no-fly zone in Libya did not constitute a war because it was not a "prolonged and substantial military engagement" which exposed U.S. military personnel to "significant risk."[31] The Obama Administration further argued this engagement did not rise to the level of "hostilities," meaning the WPR did not apply.[32] This episode highlights the growing tension between the use of technology in modern warfare and existing authorities designed to regulate war powers.[33]

Third Factor: Issue Placement in Congress

An additional challenge created by these ambiguities is what elements of Congress are best suited to conduct oversight of these operations. There is extensive debate regarding whether the Senate and House military or intelligence committees should be tasked with overseeing presidential actions. This challenge is intensified due to issues related to information sharing between committees, creating a patchwork of oversight authorities.[34]

This analysis considers two case studies, the first dealing with congressional involvement in drone strikes conducted by the Obama Administration, 2009 to 2017, and the second addressing congressional oversight of presidential cyber policy during the first Trump Administration, 2017 to 2021, focusing particularly on the Department of Defense's (DOD's) shift toward a more offensive cyber strategy.

Drone Case Study

The Obama Administration made extensive use of drone strikes. While the exact number of strikes conducted by the administration is unclear, the number is likely around 500.[35] President Obama's strikes expanded outward from the prior Bush Administration's focus on Pakistan to include Yemen, Somalia, Afghanistan, and Iraq.[36] One drone strike drew particular focus. In September 2011, President Obama ordered a drone strike against Al-Qaeda cleric Anwar Al-Awlaki. The Obama Administration stated there was clear evidence

---

[31] United States Department of Justice, "Authority to Use Military Force in Libya," April 14, 2011, https://www.justice.gov/sites/default/files/olc/opinions/2011/04/31/authority-military-use-in-libya.pdf, p. 8.

[32] "*The Law:* Military Operations in Syria: No War? No Hostilities," *Presidential Studies Quarterly*, 42, No. 1 (February 2012), https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1741-5705.2012.03947., pp. 181-182.

[33] Eric Talbot Jensen, "War Powers Resolution and Future War," *Emory International Law Journal*, 29, No. 3 (December 2014), https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1240&context=faculty_scholarship, pp. 534-543.

[34] Oona A. Hathaway et al, "Congressional Oversight of Modern Warfare: History, Pathologies, and Prospects for Reform," *William and Mary Law Review*, 63, No. 4 (October 2021), https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3914&context=wmlr, pp. 150-160.

[35] Micah Zenko, "Obama's Final Drone Strike Data," Council on Foreign Relations, January 20, 2017, https://www.cfr.org/blog/obamas-final-drone-strike-data.

[36] Anna Holyan and Tobias T. Gibson, "Under Fire: Targeted Killings, UAVs, and Three American Presidents," in *Contextualizing Security: A Reader*, ed Tobias T. Gibson and Kurt W. Jefferson (Atlanta: University of Georgia Press, 2022), p. 122.

that Al-Awlaki (a U.S. citizen) was inspiring attacks against the United States.[37] The strike led to intense controversy regarding the scope of presidential authority to conduct lethal drone operations, highlighting the limited role congressional engagement played in this decision.[38]

On November 15, 2011, the Department of Justice produced a white paper which argued that a U.S. citizen could be targeted under three conditions. First, the individual had to pose an "imminent threat." Second, the individual could not feasibly be captured. Finally, the strike had to be consistent with the law of war.[39] The memo defined "imminent threat" broadly, including the chance that a target was currently plotting lethal attacks.[40] This loose definition raised questions about when and how these guidelines were applied.[41] In 2013, President Obama stated "his [Al-Awlaki's] citizenship should no more serve as a shield than a sniper shooting down on an innocent crowd should be protected from a SWAT team."[42] On July 1, 2016, Obama issued an executive order mandating the government publish a yearly report detailing the number of drone strikes and associated civilian casualties.[43]

Congressional Responses

This section describes three ways Congress responded to the Obama Administration's use of drones. First, multiple members of Congress pressured the Obama Administration to be more transparent regarding drone strikes. During a House Judiciary Committee hearing, ranking member John Conyers (D-MI) stated committee members had sent President Obama letters requesting memos which formed the basis of the 2011 Justice Department white paper regarding the targeting of Al-Awlaki, but that these requests had been denied.[44]

At the start of a Senate Judiciary hearing on drones, held April 23, 2013, former committee chairman Dick Durban (D-IL) stated the committee had received these memos.[45] In March 2013, Senator Rand Paul (R-KY) filibustered the confirmation hearing

---

[37] *BBC*, "Islamist cleric Anwar Al-Awlaki killed in Yemen," September 30, 2011, https://www.bbc.com/news/world-middle-east-15121879.

[38] Tobias T. Gibson, "Bring Back The Drone Debate, Sen. Paul," *The Hill,* April 21, 2015, https://thehill.com/blogs/pundits-blog/defense/239483-bring-back-the-drone-debate-sen-paul/.

[39] United States Department of Justice, "Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who is a Senior Operational Leader of Al-Qaeda or an associated force," November 15, 2011, https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/dept-white-paper.pdf, p. 7.

[40] *Justice*, "Lawfulness," op. cit., pp. 7-8.

[41] Holyan and Gibson, "Under Fire," op. cit., p. 124.

[42] The White House, "Remarks by the President at the National Defense University," May 23, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university.

[43] United States White House, "Executive Order-United States Policy on Pre- and Post-Measures to Address Civilian Casualties In U.S. Operations Involving The Use of Force," July 1, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/01/executive-order-united-states-policy-pre-and-post-strike-measures.

[44] Drones And The War On Terror: When Can the U.S. Target American Citizens Overseas, House Committee on Oversight and Reform, 113th Congress (2013), https://www.congress.gov/113/chrg/CHRG-113hhrg79585/CHRG-113hhrg79585.pdf, pp. 2-3.

[45] Ibid, p. 2.

of Central Intelligence Agency director John Brennan for 13 hours, vowing to keep talking until the Obama Administration confirmed whether it had the legal authority to kill a U.S. citizen on American soil.[46]

Congress members proposed a variety of bills restricting various aspects of the Obama Administration's drone program. The first group of bills prevented the administration from targeting U.S. citizens.[47] The second group of bills focused on limiting the ability of the Central Intelligence Agency and Department of Homeland Security to conduct drone strikes.[48] None of these bills succeeded. While certain Congress members sought tighter restrictions on drone policy during Obama's eight years in office, Congress did not support these efforts.

Between 2008 and 2017, Congress held four hearings regarding drone strikes. The House Committee on Oversight and Government Reform held the first two hearings in Spring 2010.[49] The Senate and House Judiciary Committees each held one hearing in 2013.[50] These hearings highlighted concerns related to the degree to which the 2001 AUMF applied to drone strikes, the degree of transparency regarding these strikes, and strategic concerns related to the effectiveness of these strikes in eliminating terrorist threats.[51] However, in spite of Congress discussing these issues, no legislation directly resulted from these hearings, meaning they were ultimately of limited importance.[52]

On balance, congressional responses to Obama era drone policy were lacking. While there were multiple attempts to pass legislation limiting drone strike authorities, none of these efforts were successful. Even though the Congress repeatedly pressured the Obama Administration to release more specific details regarding various drone policies, transparency concerns remained throughout the remainder of Obama's time in office. While the four congressional hearings held in 2010 and 2013 raised many of these concerns, they were only marginally useful.

This case study reveals multiple challenges relating to the scope of the 2001 AUMF. Much of the debate and discussion throughout the four congressional hearings centered on

---

[46] Carrie Johnson, "When Rand Paul Ended Filibuster, He Left Drones On Center Stage," *NPR*, March 8, 2013, https://www.npr.org/2013/03/10/173864536/when-rand-paul-ended-filibuster-he-left-drones-on-national-stage.

[47] To prohibit the use of drones to kill citizens of the United States within the United States, S. R. 505, 113th Congress (2013), https://www.congress.gov/113/bills/s505/BILLS-113s505pcs.pdf, pp. 1-4. To prohibit the use of drones to kill citizens within the United States, H.R. 1242, 113 Congress (2013), https://www.congress.gov/113/bills/hr1242/BILLS-113hr1242ih.pdf, pp. 1-2.

[48] Drone Accountability Act, H.R. 1283, 113th Congress (2015), https://www.congress.gov/113/bills/hr2183/BILLS-113hr2183ih.pdf, pp. 1-4.

[49] Rise of The Drones: Unmanned Systems And The Future Of War, House Committee on Oversight and Reform, 111th Congress (2010), https://irp.fas.org/congress/2010_hr/drones1.pdf. 7, p. 7. Rise Of the Drones Part II: The Legality of Unmanned Killing, House Committee on Oversight and Reform, 111th Congress (2010), https://www.congress.gov/111/chrg/CHRG-111hhrg64922/CHRG-111hhrg64922.pdf, pp. 7-20.

[50] Drones and the, p. 113; and, *Drone Wars: The Constitutional and Ethical Implications of Targeted Killing, Senate Committee on the Judiciary*, 113th Congress (2013), https://www.govinfo.gov/content/pkg/CHRG-113shrg26147/pdf/CHRG-113shrg26147.pdf, pp. 8-16.

[51] Pages 40-45 of my thesis describe these hearings in more detail.

[52] This lack of action highlights the fact that mere oversight is not enough to produce effective changes.

whether the 2001 AUMF authorized drone strikes against terrorist targets outside of countries (such as Afghanistan) where the United States was actively engaged in armed conflict. This issue ties into the question of what counts as "hostilities" under the WPR, because drones enable uses of force without requiring troop presence in a given area. The scope and application of the 2001 AUMF and WPR to drone warfare remains highly contested.

A central theme throughout proposed legislation and congressional hearings was whether the DOD should exclusively conduct drone strikes. This issue hints at the broader question of what congressional committees should deal with drone related issues. If drone strikes are best considered covert action, it could make sense for the Senate and House Intelligence Committees to have primary oversight responsibility. However, if these strikes are best considered as military action, the Senate and House Armed Services Committees (SASC and HASC) could have a better oversight claim. Daniel E. Rosenthal, former director of Counterterrorism at the National Security Council, writes "while the DOD may go to extraordinary lengths to ensure that the armed services committee receives … information… the DOD may completely ignore … requests by the intelligence committees."[53] Additionally, because information regarding drone programs is stovepiped, no single committee has access to all relevant information.[54] Overall, the second and third factors, as previously noted, appear to have played a substantial role in undermining congressional efforts to influence drone policy throughout Obama's two terms.

Persistent Engagement and Defend Forward Case Study

In 2018, under the first Trump Administration, the DOD adopted a new, assertive posture in cyberspace, Persistent Engagement via Defending Forward. Defend Forward focuses on increased offensive action in cyberspace.[55] This engagement seeks to force attackers to pour more resources into defensive actions.[56] President Trump reportedly signed a presidential directive granting the DOD increased authority to conduct OCOs to enable this posture.[57] Defend Forward is part of the broader concept of Persistent Engagement, which seeks to

[53] Rosenthal, "Congress Perhaps."

[54] Ibid.

[55] United States Department of Defense, "2018 Cyber Strategy," 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf, pp. 6-7; and, United States Cyber Command, "Achieve and Maintain Cyber Superiority," March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, p. 6.

[56] United States Cyber Command, "Achieve and Maintain Cyber Superiority," March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, p. 6.

[57] Mark Pomerleau, "Two years in, how has a new cyber strategy changed cyber operations," *C4ISRNET*, November 11, 2019, https://www.c4isrnet.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/.

engage adversaries proactively and consistently.[58] This overarching concept was maintained under the Biden Administration.[59]

The classical deterrence framework (via punishment and denial) does not clearly apply to cyberspace for multiple reasons.[60] First, due to the number of possible attack surfaces in cyberspace, under most circumstances, if an adversary is determined enough to attack a given target, the attack will eventually succeed.[61] Second, attribution is a famous challenge in cyberspace. If the United States is unable to effectively attribute an attack to a given actor, the credibility of deterrence by punishment will be severely degraded.[62] Third, many cyberattacks do not rise to the level of impact that would credibly entail a kinetic response, while it is extremely challenging to figure out appropriate counter responses in cyberspace to a given attack. As a result, it is hard to create red lines which advesaries know not to cross if they wish to avoid escalation.[63] Persistent Engagement and Defend Forward are based on the view that these challenges mean that relying on traditional deterrence in cyberspace will be ineffective at preventing attack.[64] A new framework is needed to effectively advance U.S. security in cyberspace.

Persistent Engagement and Defend Forward offer this new framework. In addition to seeking to deter cyberattacks which rise to the level of a kinetic use of force, cyber operators should constantly engage adversarial networks, seeking to undermine these actors, along with gaining intelligence which can be used to limit the effectiveness of adversary attacks.[65]

---

[58] Paul M. Nakasone and Michael Sulmeyer, "How to compete in cyberspace," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

[59] United States Department of Defense, "2023 Cyber Strategy," 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF, pp. 7-8.

[60] Payne offers a description of the fundamental concepts inherent in deterrence. "the basic principle of deterrence as applied to international relations in general is *not* complicated: a latent threat is posed with the expectation that an opponent may decide, via its calculation of cost, benefit, and risk, not to take an action for fear of that latent threat." Keith B. Payne, "Deterrence is Not Rocket Science: It is more Difficult," *Information Series*, No. 527 (Fairfax, VA: National Institute Press, July 6, 2022), https://nipp.org/wp-content/uploads/2022/07/IS-527.pdf, p. 2.

[61] Martin C. Libicki, "Cyberdeterrence and Cyberwar," RAND Cooperation, 2009, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf, pp. 13-24.

[62] Jon R. Lindsey, "Tipping the Scales: The attribution problem and the feasibility of deterrence against cyber attacks," *Journal of Cyberpolicy*, 1, No. 1 (September 2015), https://academic.oup.com/cybersecurity/article/1/1/53/2354517#37861698, pp. 61-66; Timothy M. McKenzie, "Is Cyber Deterrence Possible," *Fundamentals of Cyber Power*, 2017, https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF, pp. 8-9; and, William Banks, "Cyber Attribution and State Responsibility," *International Law Studies*, 97, 2021, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2980&context=ils, pp. 1046-1048.

[63] Thomas Van de Velde, "Cyber Deterrence is Dead. Long Live Integrated Deterrence," *Joint Forces Quarterly*, 109, No. 3 (Fall 2023), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-109/jfq-109_41-50_Van-de-Velde.pdf, pp. 47-48.

[64] Thomas F. Lynch, "Forward Persistence in Cyber Great Power Competition," *Cyber Defense Review*, Fall 2024, https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Lynch_CDRV9N3-Fall-2024.pdf, pp. 87-90.

[65] There is a clear tension between Persistent Engagement and Defend Forward and traditional understandings of deterrence. The exact contours of how this tension should be resolved in strategic discussions has been lacking in DOD public discussion. As Jon Lindsey and Eric Gartze write "cyber warriors find themselves in the awkward position of explaining how cyber contributes to "integrated deterrence." Erik Gartze and Jon Lindsey, "The U.S. Department of Deterrence," *War on the Rocks*, July 22, 2024, https://warontherocks.com/2024/07/the-u-s-department-of-deterrence/.

Over time, the intensity of cyber conflict will be reduced, as adversaries have to spend more time defending their own networks, rather than attacking the United States, hopefully leading to a more stable equilibrium of conflict intensity.[66] While the logic of Defend Forward is plausible, this strategy has several possible downsides.

The first, and perhaps most obvious risk associated with Persistent Engagement via Defend Forward is unintended escalation.[67] Just because a cyber attack is perceived by the United States to be mildly escalatory does not mean that an adversary will perceive this action similarly. One pair of scholars, Jason Healy and Robert Jervis, argue that increased offensive action in cyberspace could generate intense and perhaps unintended escalation, especially when combined with existing geopolitical tension. They ask, "states are getting closer to crossing the threshold of death and major destruction outside of wartime. How long until one state, through mistake, miscalculation, or maliciousness crosses that line?"[68] To be clear, the risk of escalation must be balanced against the potential benefits of a given cyber operation.[69] The second concern regards the impact of Persistent Engagement via Defending Forward on allies. Without close and clear lines of communication, allies could feel they are being entangled in U.S. cyber operations, leading to increased friction.[70] The final, and perhaps most basic concern, is how will Defend Forward's success or failure be measured? In order to determine if a strategy is working, one has to have metrics for success. Jason Healey worries this lack of metrics could lead to "some future cyber general [echoing] what seems a constant refrain in other US … wars: We're turning the corner in Iraq/Afghanistan/cyberspace … we just need more resources and fewer constraints."[71]

Overall, Persistent Engagement, driven by Defending Forward, is a logical and coherent cyber strategy, with several possible downsides, including unintended escalation, allied friction, and lack of metrics. Each of these downsides offers support for Congress to be involved with overseeing this strategy. The 2018 through 2020 NDAAs offer more insight into how Congress sought to influence cyber policy.

---

[66] Jason Healey, "The implications and logic of persistent (and permanent) engagement in cyberspace," *Journal of Cybersecurity*, 5, No. 1 (2019), https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878, pp. 6-8.

[67] There is a rich discussion of escalation and cyberspace. For a few examples, Rebecca Hersman, "Wormhole Escalation In The New Nuclear Age," *Texas National Security Review*, 3, No. 3 (Summer 2020), https://tnsr.org/2020/07/wormhole-escalation-in-the-new-nuclear-age/, pp. 94-100; Martin C. Libicki and Oles Tkacheva, "Cyberspace Escalation: Ladders or Latices," NATO Defense Center For Cyber Excellence, https://ccdcoe.org/uploads/2020/12/3-Cyberspace-Escalation-Ladders-or-Lattices_ebook.pdf, pp. 1-13; Jason Healy and Virpantpap Vikram Singh, "Amplifiers and Dampeners of Cyber Escalation, *War on the Rocks*, March 19, 2025, https://ccdcoe.org/uploads/2020/12/3-Cyberspace-Escalation-Ladders-or-Lattices_ebook.pdf.

[68] Jason Healey and Robert Jervis, "The Escalation Inversion And Other Oddities Of Situational Cyber Stability," *Texas National Security Review*, 3 (2020). https://tnsr.org/wp-content/uploads/2020/09/TNSR-Vol3-Iss4-Healey-and-Jervis.pdf, p. 32; and, Bailey, "Offensive," 249.

[69] Thank you to an anonymous reviewer for this point. This balancing act is extremely complex and warrants further discussion which this piece cannot engage with, due to space constraints.

[70] Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," *Lawfare*, May 27, 2019, https://www.lawfaremedia.org/article/cyber-commands-strategy-risks-friction-allies.

[71] Healey, "Implications," 11; Jacquelyn Schneider, "The Cyberspace Solarium Commission," *Lawfare*, April 1, 2020, https://www.lawfaremedia.org/article/persistent-engagement-foundation-evolution-and-evaluation-strategy.

2018 NDAA

Section 1631 modified Title 10 of the U.S. Code to require the Secretary of Defense to submit a report of any "sensitive military cyber operation," conducted within 48 hours to the "congressional defense committees." The provision contained a section stating this requirement did not apply to covert action.[72] Section 1632 included a notification requirement, mandating the Secretary of Defense provide a quarterly briefing to congressional defense committees regarding cyber activities.[73] Section 1633 required the president to send a report to Congress regarding U.S. cyber posture, including efforts to develop offensive cyber capabilities.[74] Overall, the 2018 NDAA demonstrates that Congress sought to enhance oversight of cyber operations.

2019 and 2020 NDAAs

Section 1632 of the 2019 NDAA states the Secretary of Defense has authority to conduct cyber operations under the level of "hostilities." Section C states that clandestine military operations in cyberspace count as traditional military activities and that the Secretary of Defense must report these operations to the congressional defense committees.[75] Additional sections mandate enhanced U.S. focus on preventing damaging cyber attacks.[76] The 2020 NDAA modified the notification requirement by mandating that only activities which had a medium to high degree of risk needed to be reported.[77] Because of this activity, much cyber activity was placed outside of the oversight framework established by the 2018 and 2019 NDAAs.

NDAA Critiques

These provisions overall expanded DOD authority to conduct OCOs while limiting oversight via three mechanisms. First, the WPR does not apply to most OCOs, meaning these activities would not be covered under the legislation.[78] Second, the covert action statute, meant to oversee intelligence related activities, does not apply to most cyber activities. The 2019

---

[72] National Defense Authorization for Fiscal Year 2018, Pub. L. No., 2810, 115th Congress (2018), https://www.congress.gov/115/statute/STATUTE-131/STATUTE-131-Pg1283.pdf, Section 1631.

[73] Ibid, Section 1632.

[74] Ibid, Section 1633.

[75] National Defense Authorization for Fiscal Year 2019, Pub. L. No., 5515, 116th Congress (2019), https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf, Section 1636.

[76] Ibid, Section 1636-1642.

[77] National Defense Authorization for Fiscal Year 2020, Pub. L. No. 1790, 117th Congress (2020), https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf, Section 1642. Due to the highly uncertain nature of cyberspace, it can be challenging to determine what counts as a "medium or high risk" operation.

[78] Gaudion, "Answering," p. 155; Jensen, "Future," p. 54; and, Bailey, "Offensive," pp. 259-260; Ashley Deeks, "Will Cyber Autonomy Undermine Democratic Accountability," *International Law Studies*, 96 (2020), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2929&context=ils, pp. 479-485.

NDAA declares that most cyber activities count as traditional military activities, therefore are not subject to the covert action statute.[79] Third, due to the 2020 NDAA notification requirement modification, most cyber activities (those deemed to not be medium or high risk), would not be covered under the 2018 NDAA's 48-hour reporting requirement.[80]

Successive NDAAs lacked provisions enhancing congressional oversight of U.S. cyber policy. Meanwhile, the Biden Administration maintained the concepts of Persistent Engagement and Defend Forward in the 2023 Cyber Strategy,[81] while placing them under the broader umbrella of "integrated deterrence," which "combines every military, economic, and political capability possessed by the United States and its allies in a purposeful way to deter major …threats to the rules-based order."[82] President Trump has not yet revealed whether his administration intends to retain this concept.[83]

Overall, Congress pushed for an assertive cyber strategy, while undermining oversight needed to ensure this strategy is effective. While the 2018 NDAA required briefings regarding relevant cyber activities, successive legislation degraded this requirement. Congressional oversight is needed to ensure strategic effectiveness for several reasons.[84] First, mandating that officials involved in cyber strategy and policy defend the logic of their actions helps ensure that cyber strategy and policy is based on clear and compelling logic.[85] Additionally, oversight can force proponents of Persistent Engagement and Defend Forward to engage critics in public and private settings.[86] Second, Congress can use oversight to determine if the amount of money delegated to DOD cyber operations is sufficient.[87] Third,

---

[79] Deeks, "Will," op. cit., p. 485.

[80] Gaudion, "Answering," op. cit., p. 163.

[81] United States Department of Defense, "Summary of 2023 cyber strategy," 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf, pp. 1-2. Emerson T. Brooking and Erica Lonergan, "Welcome to Cyber Realism," *War on the Rocks*, September 25, 2023. https://warontherocks.com/2023/09/welcome-to-cyber-realism-parsing-the-2023-department-of-defense-cyber-strategy/.

[82] James J. Writs and Jeffrey A. Larson, "Wanted: A strategy to integrate deterrence," *Defense and Security* Analysis, 40 (2024). https://www.tandfonline.com/doi/full/10.1080/14751798.2024.2352943, p. 361; and, United States Department of Defense, "2022 National Defense Strategy," 2022. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf, pp. 8-14.

[83] For discussion on whether integrated deterrence is likely to be retained, see Jeffrey A. Larson and James J. Wirtz, "Obstacles to Integrating Deterrence," *Joint Forces Quarterly*, 117 (2025). https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1239&context=joint-force-quarterly, pp. 14-20.

[84] Thank you to the anonymous reviewer who made me consider this point.

[85] Todd Garvey, Mark J. Oleszek, and Ben Wilhelm, "Congressional Oversight and Investigations," Congressional Research Service, December 3, 2024, https://www.congress.gov/crs_external_products/IF/PDF/IF10015/IF10015.6.pdf, p. 1.

[86] Chuck Grassley, President pro tempore of the Senate, makes this point in a different context. Chuck Grassley, "Chuck Grassley on the importance of Congressional Oversight," June 25, 2018, https://www.judiciary.senate.gov/grassley-on-the-importance-and-responsibility-of-congressional-oversight. Possible critiques of Persistent Engagement and Defend Forward include that it does not effectively explain what role deterrence should play in cyber strategy, risks unintended escalation, and lacks clearly definable goals.

[87] For an in-depth treatment of the complexities raised by the power of the purse in foreign affairs, see Zachary S. Price, "Funding Restrictions and Separation of Powers," *Vanderbilt Law Review*, 71, No. 1 (2018), https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1015&context=vlr, pp. 365-378. For a recent

oversight enables Congress to determine if it needs to mandate additional policies and resources to enhance U.S. security in cyberspace. Overall, while Defend Forward and Persistent Engagement are a sound cyber strategy in theory, the lack of clearly defined measures of success and failure undermines an effective cost/benefit assessment of the strategy. Given the role that the cyber domain is likely to play in future conflicts, this assessment is needed.

It is important to note that OCOs rely on a large degree of secrecy to be effective.[88] For example, if China becomes aware the United States has penetrated a given network, China can increase focus on this network, looking for ways to protect it from intrusion. As such, the more information regarding U.S. offensive capabilities that is released publicly, the more these capabilities could be degraded. As a result, much congressional cyber engagement should be classified, to reduce the harm this information could do to national security. At the same time, due to the importance of U.S. cyber strategy to U.S. citizens, some degree of public transparency should be maintained. The exact place to draw this line between secrecy and accountability is outside the scope of this analysis.

Analysis

There was little direct discussion in materials reviewed regarding speed of action as a major concern in cyber operations. However, the discussion of the 48-hour reporting requirement could raise similar concerns to the 90-day clock contained in the WPR[89] because of how much cyber activity can occur within 48 hours.

Traditional means of regulating military force might not apply to OCOs, as these operations typically do not rise to the level of a use of force.[90] This line blurring contributes to challenges relating to what congressional committees are best suited to oversee military uses of OCOs and other emerging technologies. This tension stands out in the debate over

example, see James Fitzgerald, "Congress ups Pressure to release boat strikes video," *BBC News*, December 9, 2025, https://www.bbc.com/news/articles/c773de38p2go.

[88] For more on the impact of secrecy on deterrence, see Jason Healy and Robert Jervis, "Over classification and Its Impact On Cyber Conflict And Democracy," Modern War Institute, March 22, 2022, https://mwi.westpoint.edu/overclassification-and-its-impact-on-cyber-conflict-and-democracy/; and, Erik Gartze and Jon Lindsay, "The U.S. Department of Deterrence," *War on the Rocks*, July 22, 2024, https://warontherocks.com/2024/07/the-u-s-department-of-deterrence/. For more on challenges related to oversight and classification, see Oona A. Hathaway, "Secrecy's End," *Minnesota Law Review*, 106 (2021). https://minnesotalawreview.org/wp-content/uploads/2021/12/3-Hathaway_MLR.pdf, pp. 691-801. Of course, congressional oversight increases the risk of leaks which can undermine national security. The more congress members and associated staff are read in on a given operation, the greater this risk. While important, this challenge is outside the scope of this piece.

[89] War Powers Resolution, Section 2.

[90] For one prominent U.S. statement of when a cyber attack could count as a use of force, see Harold Koh, "International Law in Cyberspace," United States Department of State, September 18, 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

whether cyber activities are best described as military activity or covert action.[91] On balance, this case study suggests Congress should reevaluate existing mechanisms for overseeing and shaping cyber strategy.

Why Do These Trends Matter?

The prior discussion gives rise to a natural question: Why should Congress seek to become more engaged in war powers? First, as the case studies highlight, there are multiple strategic concerns associated with drone strikes and OCOs. These issues, such as the effectiveness of drone strikes in reducing terrorism versus their potential for generating blowback which could harm U.S. security deserve congressional scrutiny. Second, these technologies have enhanced the ability of presidents to conduct offensive operations without clear paths toward congressional scrutiny and accountability, increasing the risk that injustices occur. Third, due to the lack of clear escalation thresholds in cyberspace, Defend Forward and Persistent Engagement could inadvertently generate aggressive adversarial responses that ultimately undermine U.S. cyber security.[92] This same risk applies to kinetic military action as well. For example, Trump's ongoing strikes against drug boats could spark a response from Venezuela that drags the U.S. into a broader military engagement in Latin America.[93] Escalation risk is not intrinsically harmful, however Congress should play a role in ensuring such risk is justified.[94]

Recommendations

There are four sets of recommendations Congress should consider to address these concerns.

Modify the WPR

The WPR should be modified to effectively encompass the range of technologies used in modern conflict. First, the word "capabilities" should be added to the discussion of armed forces.[95] Second, violations of sovereignty, should be added as a trigger for the WPR's 90-day

---

[91] Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, September 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/#:~:text=The%20cyberspace%20competition%20is%20an,and%20stealing%20information%20from%20rivals.

[92] Healey and Jervis, "The Escalation Inversion," op. cit., pp. 34-43.

[93] Roxanna Vigil, "U.S. Military Boat Strikes Escalate Tension with Venezuela," Council on Foreign Relations, September 9, 2025, https://www.cfr.org/expert-brief/us-militarys-boat-strike-escalates-tensions-venezuela.

[94] Charles Richard and Robert Peters, "Escalation: A Tool to be Considered, not Dismissed," *Information Series*, No. 600 (Fairfax, VA: National Institute Press, October 2, 2024), https://nipp.org/wp-content/uploads/2024/10/IS-600.pdf, pp. 5-7.

[95] The article uses the phrasing "personnel, supplies, or capabilities are introduced or effectuated." Jensen, "Future," op. cit., p. 552.

clock, along with hostilities.[96] A violation of sovereignty should be considered an action intended to produce nonconsensual military relevant impacts in another country's territory.[97] Additionally, this modification should state that sovereignty would only be violated per the WPR if the action was intended to cause an effect, rather than generate information that could be used to cause an effect in the future. This change would help ensure the WPR remained focused on war powers, not intelligence operations.[98] Additionally, Section 2, subsection C of the resolution should be modified to state that the president can undertake unilateral action in cases of imminent threats, where there is "necessity of self-defense, instant, and overwhelming, [which] leav[es] no choice of means and no moment of deliberation."[99] This revision should further state that if a president acts according to this provision Congress must be informed of the evidence supporting this justification within 48 hours of operation commencement.[100] Making this change would grant presidents the authority to act when Congress cannot due to time constraints.

Repeal the 2001 and 2002 AUMFs

The 2001 and 2002 AUMFs have outlived their usefulness.[101] In response, Congress should repeal and replace these authorizations with a narrowly targeted AUMF that authorizes the president to pursue action against specific terrorist groups, in a clearly defined geographic area, for 3 to 5 years, with the option for renewal. Multiple DOD officials have argued against this legislative change.[102] One argument for keeping the 2001 and 2002 AUMFs is that terrorist threats can arise anywhere, anytime, meaning a more limited AUMF could undermine U.S. national security. However, a new AUMF should still be created for three reasons. First, the national security benefits from the current AUMFs might not outweigh the potential harm done to separation of powers from this language being contorted.[103] Second,

---

[96] Ibid, pp. 552-554.

[97] Ibid, p. 554. This wording is intended to give the president freedom of action regarding other tools of statecraft outside military power.

[98] This wording is not perfect, and would likely generate controversy regarding how it should best be applied. This recommendation is intended to improve on the status quo, not be a perfect solution.

[99] Matthew C. Waxman, "The 'Caroline' Affair in the Evolving International Law of Self-Defense," *Lawfare*, August 28, 2018, https://www.lawfaremedia.org/article/caroline-affair. The other modifications described in this section, along with enhanced U.S. congressional oversight, are needed to ensure this clause does not become distorted.

[100] This statement should explain why the relevant (and clearly defined) threat arose so quickly there was not enough time for the U.S. Congress to respond.

[101] Bradley and Goldsmith, "AUMF Legacy," op. cit., pp. 636-638.

[102] Matthew C. Weed, "The 2001 AUMF: Issues Concerning its Continuing Application," Congressional Research Service, April 14, 2015, https://sgp.fas.org/crs/natsec/R43983.pdf, p. 12; and, Terri Moon Cronk, "Mattis: AUMF Authorizations Remain Sound," *DOD News*, October 30, 2017, https://www.war.gov/News/News-Stories/Article/Article/1358069/mattis-military-force-authorizations-remain-sound/.

[103] Gene Healy and John Glaser, "Repeal, Don't replace the 2001 AUMF," *CATO Institute Policy Journal*, July/August 2018, https://www.cato.org/policy-report/july/august-2018/repeal-dont-replace-aumf; Oona A. Hathaway, "Replacing the 2001 AUMF: Opening statement," April 9, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3808779 , pp. 1-3. For a description of this overall debate, see Kenneth Katzman et al, "The Islamic State Crisis and U.S. Policy," Congressional Research Service, February 11, 2015,

the "imminent attack" change to the WPR would cover situations where a terrorist group not covered under the new AUMF had to be quickly targeted, while requiring the president to explain the reasoning behind these strikes to Congress. Third, Congress can add a new group or geographical area to the AUMF if needed. A carefully crafted AUMF could effectively enable the president to defend national security, while maintaining effective congressional engagement in war powers. Congress has taken a preliminary step in this direction by repealing the 2002 AUMF via the 2026 NDAA, though it did not authorize a new AUMF.[104]

Drone Case Study Specific Recommendations

One major challenge identified in the first case study is that drone strikes do not neatly fall under the existing division between intelligence and armed forces oversight in Congress. This issue can undermine the effectiveness of oversight efforts. In response, Congress should consider centralizing authorization to conduct kinetic drone strikes meant to eliminate terrorists and terrorist supporters as part of the War on Terror within the DOD. New SASC and HASC subcommittees should be created to address strategic, legal, and ethical issues related to these targeted killing operations.[105] This division, while not perfect, would likely enable stronger oversight by reducing the challenges related to information stovepiping between defense and intelligence committees, denying any one committee full access to the information needed to effectively conduct oversight. Taken in conjunction with legislation to centralize targeted killing authority within the DOD, this proposal could help center drone oversight efforts more clearly, enhancing overall oversight.[106]

https://www.everycrsreport.com/files/20150211_R43612_c6248653f2c76dd3d7123e4c2d7e770f16e0e11b.pdf, pp. 25-33.

[104] "Kaine & Young Applaud Inclusion of Bipartisan Legislation to Formally End Iraq Wars in FY26 NDAA," *Kaine.senate.gov*, December 8, 2025, https://www.kaine.senate.gov/press-releases/kaine-and-young-applaud-inclusion-of-bipartisan-legislation-to-formally-end-iraq-wars-in-fy26-ndaa.

[105] The language about targeting of individuals is meant to exclude drones which are used for information gathering purposes. More broadly, drones play an increasing role in modern warfare. The drone discussion in this piece is limited to the sort of targeted killing program undertaken by the Obama Administration, not drone usage in an active combat scenario, such as in defense of Taiwan. Thank you to an anonymous reviewer for making me consider this point. For a discussion of drone usage in modern conflict, see Noah Robertson, "Replicator: An Inside Look at the Pentagons ambitious drone program," *Defense News*, December 19, 2023, https://www.defensenews.com/pentagon/2023/12/19/replicator-an-inside-look-at-the-pentagons-ambitious-drone-program/; Stacie Pettyjohn, "Evolution Not Revolution: Drone warfare in Russias 2022 invasion of Ukraine," Center For New American Security, February 2024, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Defense-Ukraine-Drones-Final.pdf, pp. 1-67; and, Stacie Pettyjohn, Hannah Demis, and Molly Campbell, "Swarms over the Strait: Drones in a future fight over Taiwan," Center for New American Security, https://www.cnas.org/publications/reports/swarms-over-the-strait, pp. 1-100.

[106] This proposal seeks to reduce this challenge, rather than solve it. One committee will not be able to cover all aspects of drone warfare. However, this change would remove some complications associated with coordinating between the defense and intelligence committees.

Defend Forward Specific Recommendations

Congress should consider passing legislation mandating that OCOs only be conducted by the DOD. This change would enable oversight authorities regarding cyber operations to be more centralized, enabling the SASC and HASC to gain a better overall picture of the overall state of cyber operations. Following this change, the SASC and HASC subcommittees focused on cyber operations should lead two sets of actions to enhance effective oversight of Defend Forward and Persistent Engagement. First, DOD cyber officials should be pressured to provide clear metrics via which the success or failure of Persistent Engagement via Defending Forward can be measured, in a mix of classified and unclassified settings.[107] Second, Congress should consider requiring a quarterly briefing regarding all OCOs, not just ones deemed to be "medium to high risk."[108] By taking these steps, Congress could more fully assess the risks and benefits of the current U.S. cyber strategy along with generating more insight into the exact scope of cyber operations.

None of these proposed reforms are perfect. Reforming the WPR and repealing and replacing the 2001 and 2002 AUMFs could create multiple interpretative challenges.[109] While increased oversight of presidential war powers could increase congressional knowledge of administration activities, without clear actions by Congress in response, the impact of this increased knowledge could be limited. Still, these combined measures would place Congress in a stronger position to reassert influence regarding war powers.

Conclusion

Emerging technologies, including drones and cyber operations have changed the way in which modern warfare is conducted. The Constitution, the 1973 WPR, and the 2001 and 2002 AUMFs do not effectively address the complex challenges raised by emerging technology. As a result, the ability of Congress to effectively engage in the war powers struggle has been undermined. By pursuing the above sets of policy recommendations, Congress can place itself in a better position to engage with war powers in the current age.

Certain members of Congress want to move in this direction. In March 2023, the Senate voted to repeal the 2002 AUMF, an effort led by a bipartisan pair of senators, Tim Kaine (D-VA) and Todd Young (R-IN).[110] The bipartisan nature of this effort reflects the understanding that war powers engagement can and should transcend partisanship. In September 2025,

---

[107] Possible metrics include the rate and intensity of attacks against U.S. critical infrastructure networks, examples of unintended escalation from U.S. OCOs, and measures of the amount of time and effort that actors spend trying to attack U.S. systems.

[108] The wording "should consider" is used in case the number of OCOs is too large for effective briefing, forcing these briefs to focus on the most important operations.

[109] Any new AUMF should be careful to clarify which groups and geographic regions U.S. presidents can target, within what timeline.

[110] Tim Kaine, "Kaine and Young Applaud passage of Senate 2001 and 1992 AUMF repeal, Formally end Iraq and Gulf Wars," March 29, 2023, https://www.kaine.senate.gov/press-releases/kaine-and-young-applaud-senate-passage-of-their-bill-to-repeal-1991_2002-aumfs-formally-end-gulf--iraq-wars.

the House passed the 2026 NDAA, containing a provision repealing the 2002 AUMF[111] and this repeal was included in the final version of the Fiscal Year 2026 NDAA. The combination of these two votes could soon mean the formal repeal of the 2002 AUMF. While the practical impact of this appeal could be limited, this action would send a clear signal that Congress actively sought to reclaim war powers authority, an act of "constitutional hygiene."[112] However, more work remains to be done to turn this intention signaling into actual, substantive action.

Blaine Ravert is a Spring 2025 graduate of Missouri State University's School of Defense and Strategic Studies. This article is a condensed and somewhat modified version of his Master's thesis.

[111] Ellen Mitchell, "House passes defense policy bill with proposal to repeal Iraq war authorizations," *The Hill*, 10 September 2025, https://thehill.com/policy/defense/5497564-house-passes-defense-bill/.

[112] Hulme, "Repealing," op. cit.