From Reactive to Proactive Cyber State

1 MARCH 2025

Vittoria Giudice



Cyberspace is an "ecosystem" comprising digital technologies where different actors engage in other behaviours and activities (Berg & Kuipers, 2022, p. 2). At first, cyberspace was interpreted as a libertarian space, a utopian realm of freedom and decentralisation from government control (Barlow, 1996). However, in recent decades, it has become a militarised domain where States pursue their national interest. Notably, great powers are using it to consolidate or rebalance their power; states have recognised the significance of this new domain as a new area for state competition and strategic gains. This transformation has led to the concept of cyberspace as

a new realm that transcends the physical domain, fundamentally altering the dynamics of global power and security dynamics.

Examining the Defend Forward strategy is particularly relevant in today's geopolitical landscape, especially given the likelihood of a new Trump administration, which has already signalled a more aggressive and decisive approach to domestic and foreign policy. If further consolidated, the U.S. offence-first approach to cyberspace could increase global tensions, cyber arms races, and escalation risks. Offensive cyber strategies are proactive, preemptive, or retaliatory actions to disrupt, degrade, or destroy adversary cyber capabilities, networks, or infrastructure. While adopting these strategies is justified by their alleged efficacy in deterring threats and safeguarding national interests, they pose significant risks of unintended consequences and geopolitical instability.

Understanding the U.S. shift toward offensive cyber operations is crucial for evaluating its broader implications for international security and global stability. In a rapidly evolving international landscape, where cyber norms and governance remain underdeveloped, decisions made in cyberspace have direct consequences for the physical world. As cyberspace increasingly becomes an arena of perpetual conflict, this article underscores the need to critically assess whether persistent engagement enhances security or exacerbates global instability.

The evolution of cyberspace has resulted in its transformation from a mere communication network into a critical battleground for geopolitical competition. States and non-state actors increasingly exploit its interconnected nature to conduct various cyber operations, from espionage and disruption to full-scale cyber warfare. This section commences with a concise overview of the cyberspace environment, emphasising the pivotal characteristics that have influenced the evolution of diverse state cyber strategies. It then delves into the pivotal role of interconnectedness in the digital domain, showing its vulnerabilities and strategic opportunities and how cyberspace has become a weaponised domain incentivising the adoption of offensive strategies by the state.

Cyber capabilities are increasingly integrated into national and foreign strategies. Nowadays, cyberspace results in a global theatre where actors operate without physical constraints (Atrews, 2020; Betz & Stevens, 2011; Kello, 2013). This shift has redefined spatial and temporal limitations in operation and conflict, allowing a "multiple actors" assemblage (Betz & Stevens, 2011) to influence governance dynamics and establish great powers (Choucri & Clark, 2019).

In this context, states are competitive with diverse actors, including relatively resource-poor entities, non-state actors, and individuals who leverage cyberspace (Kello, 2013). To ensure the security of their critical infrastructure, information systems and data, states must address the threat of cyber-attacks. Such threats may originate from various sources, including foreign governments, criminal organisations and rogue individuals (Choucri

& Clark, 2019). Concurrently, cyberspace enables advanced states to sustain their dominance through their capacity to innovate and integrate cyber capabilities into comprehensive military strategies (Gray, 2013), thereby exacerbating disparities in power and influence (Calderaro & Craig, 2020). In this context, cyber power can be regarded as a mere manifestation of power rather than a distinct form, thereby sustaining the continuity of power dynamics and hierarchies. The intricacy of weaponising cyber tools, as illustrated by the Stuxnet case, frequently reinforces the influence of more powerful states rather than creating asymmetric advantages for states that are less so (Atrews, 2020; Lindsay, 2013).

The distinctive attributes of the cyber domain, encompassing land, sea, air, and space, have been identified as the principal catalysts for these advancements (Betz & Stevens, 2011; Kello, 2013): Cyberspace transcends conventional military operations (Choucri & Clark, 2019; Kello, 2013), facilitating simultaneous global operations for political and social influence without spatial and temporal limitations (Betz & Stevens, 2011; Kello, 2013), as demonstrated by the sophisticated cyber-influence campaigns that Russia has perpetrated to target public opinion across multiple nations, including the U.S. (Microsoft, 2022). The borderless nature of cyberspace challenges traditional notions of sovereignty, as attested by the lack of clarity and attribution in international law (Kello, 2013), by introducing "grey zones" that are exploited by different states, especially those with authoritarian or non-liberal governance systems (Schmitt, 2017a) and hindering the effectiveness of retaliation and accountability. These complexities blur the lines between war and peace (Kello, 2013), incentivising offensive actions through low operational costs and high deniability). In light of these developments, states are adopting this offensive strategy, with the U.S. serving as a prime example, as outlined in the 'defend forward' theory (Taillat, 2019), fuelled by anonymity and ubiquity (Arquilla & Ronfeldt). The following section will delve into the core principles of one of the leading theories of offensive cyber strategies, examining its advantages in modern conflict dynamics.

This section explores the theory of cyber persistence, a foundational concept that forms the basis for analysing the Defend Forward strategy. This theory has reshaped traditional notions of offensive strategy by building on an understanding of cyberspace as a weaponised domain. It introduces two concepts representing how states exploit operations based on the persistence theory: the cyber fait accomplishes and the direct cyber engagement. These concept enables us to understand the approach of the U.S. from a theoretical foundation perspective.

In contrast to conventional military operations, which rely on episodic engagements, cyber persistence posits that states must engage in persistent and continuous offensive cyber operations to maintain a strategic advantage in cyberspace (Devanny, 2022; Smeets, 2020). It conceptualises it as a dynamic and contested environment, necessitating continuous

engagement to shape security conditions and deter adversaries (Healey, 2019a). Rather than relying solely on blunt instruments of deterrence, the strategy involves tailored, graduated responses to keep adversaries off balance without unnecessary escalation (Fischerkeller et al., 2022). While advocating for a sustained and measured offensive posture that aligns with broader national security objectives while remaining subject to interagency oversight and legal constraints (Healey, 2019a), this method reflects a clear departure from traditional reactive models, suggesting cyberspace should be understood as the environment of explosion rather than coercion.

Cyber persistence theory contends that the inherent characteristics of the cyber strategic environment do not naturally encourage coercive escalation but rather encourage fast, decisive actions to reshape the environment in one's favour. This idea is strictly related to two concepts proposed by Fischerkeller et al. (2022): cyber "faits accomplish" and "direct cyber engagements" (Fischerkeller et al., 2022). The "faits accomplish" refers to the achievement of rapid, unilateral advantages incentivised by the structure of the cyber strategic environment (Altman, 2017). This concept in cyberspace can be understood as achieving an advantage within the cyber domain through direct engagement or manipulation, which is quickly consolidated before the adversary can recognise or respond to the change in conditions (Fischerkeller et al., 2022). In contrast, "direct cyber engagements" convey the target targeted, exploitative cyber operations that fall short of triggering an armed attack. Instead of causing physical damage or kinetic effects, these actions target and manipulate critical cyber infrastructure (command and control systems or vital components of an adversary's strategic operations) recognised as essential by states to to their security and operational effectiveness (Fischerkeller et al., 2022). Unlike cyber faits accomplis, direct cyber engagements occur within active competition. Both sides seek control over crucial cyberspace terrain, and each actor's actions can influence the other's strategy. The aim is to reshape the cyber environment in one's favour, disrupting or neutralising an adversary's ability to project power or execute operations while still adhering to a threshold that avoids a kinetic conflict.

Following the persistence theory, these types of engagements are distinct from traditional armed attacks because they leverage cyber tools and tactics for strategic gain rather than direct physical harm in a way that avoids full-scale escalation.

Visualisation. Timeline main events and policy

After establishing the foundational understanding of the cyber domain and the theory of persistent engagement, this section examines the strategic transformation of American cyber policy following 2018. It explores how the U.S. moved from a primarily deterrence-based approach toward a more proactive strategy focused on continuous, real-time cyber operations.

The first year of the Trump administration largely maintained the cybersecurity policies of his predecessor, Obama, continuing a broad approach to

deterrence (Shively, 2021). Initially, Trump framed cybersecurity primarily as a domestic risk management issue, as attested by the release of Executive Order 13800 in 2017 (CISA, n.d.). The objective was to secure critical infrastructure, assess vulnerabilities through technical updates and personnel training, and improve cyber resilience (Shively, 2021). Despite ongoing cyber threats, the shift has been delayed, and 2018 saw a significant departure from previous strategies, with the "defend Forward" doctrine (Devanny, 2022; Fidler, 2020; Rosenzweig et al., 2017) marking the new offensive-first approach of the U.S.(Boussios, 2021). The goal of this strategy is well expressed in the words of Paul Nakasone, head of the U.S. Cyber Command and the National Security Agency: "Before, during and after, we have taken action and imposed costs with many elements of our government" (Barnes, 2021). This

Trump's strategy took a pre-empting approach to "preserving peace through strength" (The White House, 2018, p. 20), . It emphasised the need to operate persistently in cyberspace to counter adversaries before they could carry out harmful actions against U.S. interests (Devanny, 2022), aligning with the main principle of persistent engagement theory. The 2018 Dod-based American action thought 1) proactive intelligence collection to monitor and penetrate adversary networks and 2) integrating cyber operations with traditional military forces (Summary, 2018).

Several measures accompanied this strategy. From an operational perspective, Trump promoted a collaborative approach between the federal government and the private sector for managing critical infrastructure alongside the repeal of Presidential Policy Directive-20 (PPD-20). Most notably, he granted U.S. Cyber Command (CYBERCOM) and other agencies greater autonomy to conduct offensive cyber operations without the extensive bureaucratic approvals previously required under the Obama administration (Shively, 2022). Ultimately, the Trump administration's approach integrated cyber operations into a broader strategy of maximum pressure on its adversaries, Russia, Iran, China, and North Korea (The White House, 2018), , including sanctions, diplomatic isolation and cyberattacks to force adversaries to change their behaviour (Shively, 2021). Cyber capabilities were not the administration's central priority but rather an integration into a broader national security framework, prioritising the traditional and geopolitical threats and employing military (traditional) responses (Shively, 2021).

As we previously discussed, the logic of persistence engagement suggests consistently engaging with adversaries and exploiting vulnerabilities for immediate strategic gains, and Russia was the first target. Trump administration seized the opportunity to demonstrate its capabilities and willingness to act decisively in cyberspace with the launch of an operation against the St Petersburg-based Internet Research Agency (IRA), a 'troll farm' responsible for disinformation campaigns during the 2016 presidential election (Sanger & Perlroth, 2019; Shively, 2021) in October 2018. In June 2019, to further

demonstrate its aggressive and proactive stance in cyberspace, the U.S. launched a cyberattack on Iranian military and intelligence targets while the CYBERCOM gradually increased its authority to conduct digital attacks (Farrell et al., 2019; Shively, 2022).

These cases reflect the concept of faits accomplis, where initial gains alter the adversary's ability to act. CYBERCOM took the initiative to exploit the vulnerabilities of the IRA and gain strategic gains. This operation not only conferred an immediate advantage by neutralising potential interference but also forced the Russian cyber apparatus to divert time, talent, and resources to assess and counter American exploitation (Fischerkeller et al., 2022).

In 2020, the Trump administration transitioned to the Biden administration. As is widely known, the election process was not without contention, surrounded by the unique circumstances of the ongoing pandemic and Trump's attempts to overturn the results. Despite this, cybersecurity remained a top national security priority, necessitating immediate and strategic policy interventions. This section examines how Biden's policy remained rooted in persistent engagement, ensuring that cyber operations remained continuous, proactive, and adaptive.

The handling of the SolarWinds cyberattack immediately marked Biden's inauguration. This sophisticated and impactful supply chain breach infiltrated the Orion software platform by inserting malicious code into its updates, enabling the creation of a backdoor called "Sunburst", which was distributed to approximately 18,000 organisations worldwide (Tidy, 2020). This allowed attackers to access sensitive data and systems across various sectors and affected several organisations (Heckman, 2021), including U.S. government departments such as the Treasury and Commerce (Tidy, 2020). The incident exploited the vulnerabilities in the software supply chain, serving as a critical catalyst for recalibrating the federal cybersecurity posture and underscoring the necessity of continuous cyber operations, reinforcing the need for persistent engagement to counter adversarial cyber activities before they could escalate.

The Biden administration's response included the realisation of Executive Order 14028: "Improving the Nation's Cybersecurity", (Shively, 2022) to enhance federal cyber capabilities, improve defences against supply chain attacks and enhance public-private collaboration (Buresh, 2021; Clarke & Klein, 2022; Heckman, 2021; Shively, 2022). At the same time, allocating valuable investments to the Cybersecurity and Infrastructure Security Agency (CISA) and other federal entities under the Infrastructure Investment and Jobs Act (Clarke & Klein, 2022). Biden administration also strengthened federal oversight by expanding the Cybersecurity and Infrastructure Security Agency (CISA) and launching the Joint Cyber Defense Collaborative (JCDC) to enhance real-time threat intelligence sharing between government agencies and private sector entities (Clarke & Klein, 2022), reflecting a collaborative model that balanced government involve-

ment with industry expertise (Buresh, 2021). Recognising the need for a robust governance framework and the importance of continuous cyber operations, Biden also prioritised expanding cybersecurity leadership roles by integrating thousands of specialists into critical roles, ensuring a coordinated and persistent response to emerging threats (Clarke & Klein, 2022; Shively, 2022) and providing clarity and direction to the government's cyber initiatives.

In contrast to the Trump administration's decentralised, deterrence-centric cyber posture, the Biden administration pursued a centralised and multilateral strategy. It facilitated federal oversight and resource allocation to secure critical infrastructure (Clarke & Klein, 2022; Heckman, 2021; Shively, 2022) and expanded cybersecurity requirements in energy, healthcare, and water systems (Clarke & Klein, 2022). In addition, Biden resumed collaboration with U.S. allies to address international cyber threats, particularly those from Russia and China (Clarke & Klein, 2022).

Despite the shift from Trump's unilateral approach, on March 2, 2023, the Biden administration formally released its National Cybersecurity Strategy (The White House, 2023), which retained elements of Trump's "Defend Forward" doctrine. Biden's cyber strategy moved away from the deterrence-focused conceptual framework that had defined U.S. cybersecurity strategies since President George W. Bush's plan (2008) while recognising cyber warfare as no longer a separate domain but an integral part of modern military strategy (Karazanishvili, 2023). The strategy did not use terms such as deterrence, dissuasion or deter, signalling a shift in the US approach.

Instead, it directed the Department of Defense to continue the "Defend Forward" strategic approach, which is aligned with one of the strategy's core pillars ", disrupting and degrading threat actors", (The White House, 2023) and integrating elements of Trump's Defend Forward doctrine as a proactive focus on enhancing resilience by fostering public-private partnerships (The White House, 2023). One notable example is the "hunt forward" missions conducted by U.S. Cyber Command (USCYBERCOM). These missions involve deploying cyber teams to foreign countries to identify and neutralise malware and other cyber threats before they impact U.S. networks (Matishak, 2022). U.S. officials have described increased cyber incursions into Russia's critical infrastructure, particularly its power grid, as part of a broader strategy to deter malicious cyber activities (Shively, 2022), and CISA has continually pursued actions against Chinese state-sponsored cyber operations, particularly those related to intellectual property theft. The U.S. has taken legal action and imposed sanctions against Chinese hackers involved in cyber-enabled economic espionage (Shively, 2022).

Despite retaining Trump's doctrine, Biden combined substantial refinements to enhance cyber resilience and multilateral cooperation (Boussios, 2021; Current, 2024). He forged international cooperation to contain malicious actors (The White House, 2023, p. 29-30), shape market forces to advance security and resilience (The White House, 2023, p. 19-22) and

invest in a resilient future (The White House, 2023, p. 23-24). In addressing the structural realities of the virtual domain, the strategy emphasised the importance of pre-emptive action to mitigate threats as a strategic defence and resilience (Current, 2024).

Since 2018, following Trump's first administration, the shift in the United States' approach to offensive cyber operations has reflected continuity and refinement in the persistent engagement strategy, primarily through the Defend Forward doctrine. This section assesses the evolution of U.S. offensive cyber operations, evaluating their strategic effectiveness, risks, and broader implications.

In the U.S., cybersecurity has a well-established history, with the first national cyber strategy implemented in 2003 under the Bush administration, which aimed to protect critical infrastructure, government operations, and the private sector (The National Strategy to Secure Cyberspace, 2003). The focus on cyberspace intensified under the Obama administration, particularly during his second term when cybersecurity was recognised as a critical national security and economic concern (Shively, 2021, 2022). Obama emphasised the importance of international cooperation and the need for cyber norms, framing deterrence as a strategy to ensure that "the risks associated with attacking or exploiting our networks far outweigh the potential benefits" (Council on Foreign Relations, 2017).

The evolution of U.S. offensive cyber operations after Trump's first administration demonstrates continuity and adaptation within persistent engagement. Trump's presidency introduced Defend Forward, removing bureaucratic constraints and expanding CYBERCOM's authority to conduct pre-emptive cyber operations. Biden's administration built upon this foundation, embedding offensive cyber actions within a broader framework emphasising resilience, multilateral cooperation, and federal oversight. While the fundamental principle of persistent engagement—continuously contesting adversaries in cyberspace—remained unchanged, Biden's strategy emphasised interagency coordination, closer collaboration with the private sector, and stronger international alliances to counter cyber threats.

The effectiveness of persistent engagement is evident in U.S. cyber operations targeting Russian and Chinese adversaries. Under Biden, CYBERCOM launched offensive operations against Russian disinformation networks, disrupting the Internet Research Agency's activities during 2021–2022. In response to Russia's invasion of Ukraine, the U.S. engaged in cyber operations aimed at undermining Russian military infrastructure. Similarly, U.S. cyber efforts against Chinese threats included the 2023 disruption of a large-scale botnet used for espionage and cyber intrusions into U.S. critical infrastructure. Additionally, operations in 2024 targeted Chinese cyber actors attempting to steal military and trade secrets, reinforcing cyber resilience measures to counter ongoing espionage efforts. These operations illustrate how persistent engagement seeks to impose costs on adversaries

and degrade their cyber capabilities before they can inflict harm on U.S. interests.

Despite its strategic advantages, persistent engagement carries inherent risks, particularly concerning cyber escalation. While Obama was known for carefully weighing risks before taking action, as noted by General Joseph Dunford, Chairman of the Joint Chiefs of Staff (Farrell et al., 2019), the Trump administration adopted a less risk-averse approach, demonstrating less concern for potential unintended consequences. This shift in posture may have contributed to a broader proliferation of offensive cyber operations. Critics argue that persistent engagement could escalate cyber conflicts, leading to unintended strategic consequences (Healey, 2019; Smeets, 2020). Rather than deter adversaries, the doctrine may establish a continuous cycle of offensive operations, inadvertently creating greater instability (Healey, 2019; Smeets, 2020), turning cyberspace into a perpetual cycle of offensive operations that may inadvertently lead to greater instability rather than deterrence (Healey, 2019; Rosenzweig et al., 2017).

Beyond operational effectiveness in disrupting adversaries, the U.S. strategy lacks sufficient mechanisms to promote responsible cyber behaviour among other cyber powers. Unlike traditional deterrence strategies, which focus on imposing costs after an attack, persistent engagement assumes that adversaries will divert resources toward cyber defence. However, this assumption lacks empirical validation. Historical evidence suggests that adversaries do not necessarily de-escalate in response to persistent engagement but adapt and intensify their cyber capabilities (Healey, 2019). This dynamic may encourage adversaries to develop more covert and resilient cyber techniques (Jun, 2022; Rosenzweig et al., 2017). increasing the likelihood of a cyber arms race rather than fostering stability (Smeets, 2020). The lack of clarity surrounding intent and decision-making in cyber operations could also lead to accidental escalation, where a limited cyber engagement is misperceived as a more serious threat, prompting a disproportionate response. Additionally, ambiguities in cyber engagement rules and potential misalignment in operational procedures may unintentionally escalate conflicts beyond their original scope. The challenge lies in navigating these risks while maintaining the flexibility to act decisively in cyberspace (Jun, 2022; Rosenzweig et al., 2017).

A failure to communicate intent or an unclear decision-making process could lead to accidental escalation, where a limited cyber engagement is misperceived as a much more serious threat, prompting a disproportionate response. Similarly, ambiguity in cyber engagement rules and the potential for misalignment in operational procedures could unintentionally lead to a broader conflict than initially intended. The issue lies in navigating these risks while maintaining the flexibility to act quickly and decisively in cyberspace (Fischerkeller et al., 2022).

The shift from a deterrence-based approach to an active defence strategy defines the Biden administration's cybersecurity policy. Unlike

previous administrations that framed cyber operations around retaliation, Biden's approach prioritises disrupting adversary networks before they strike, strengthening national cyber defences, and fostering international cyber alliances. This represents a shift toward a structured, institutionalised form of persistent engagement, aligning cyber operations with broader national security objectives. However, balancing offensive cyber dominance with strategic stability remains a challenge. While persistent engagement ensures continuous pressure on adversaries, its long-term effectiveness will depend on the U.S.'s ability to prevent escalation, establish international cyber norms, and invest in sustainable cyber resilience. Ultimately, the evolution of U.S. cyber strategy after Trump underscores the growing recognition that cybersecurity requires proactive, continuous engagement rather than reactive deterrence.

This article addressed the research question: How has the United States' approach to offensive cyber operations evolved after Trump's first administration? The analysis demonstrated a shift from deterrence to persistent engagement, mainly through the Defend Forward doctrine. Trump's administration initiated this shift by removing bureaucratic barriers and granting greater autonomy to U.S. Cyber Command (CYBERCOM) for preemptive operations. Biden's administration institutionalised and expanded these efforts, integrating international cooperation, federal oversight, and resilience-building measures into offensive cyber strategy.

Persistent engagement has made U.S. cyber operations more proactive and continuous, targeting Russian disinformation networks, military cyber capabilities, and Chinese cyber intrusions. However, its long-term effectiveness remains uncertain, as adversaries may adapt rather than de-escalate. Additionally, the lack of international norms governing cyber operations raises risks of unintended escalation and diplomatic tensions.

From a policy perspective, persistent engagement must be carefully managed to balance offensive dominance with strategic stability. The U.S. should complement offensive operations with stronger cyber resilience measures, public-private partnerships, and diplomatic initiatives to establish more explicit rules of engagement and promote a cyber domain characterised by shared responsibility and security.

References

Altman, D. (2017). By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries. International Studies Quarterly, 61(4), 881–891. https://doi.org/10.1093/isq/sqx049

Arquilla, J., & Ronfeldt, D. (1993, Spring). Cyberwar is Coming! 12(2), 141–165.

Atrews, R. (2020). Cyberwarfare: Threats, Security, Attacks, and Impact. Journal of Information Warfare, 19(4), 17–28.

Barnes, J. E. (2021, December 5). U.S. Military Has Acted Against Ransomware Groups, General Acknowledges. The New York Times. https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html

Berg, B. van den, & Kuipers, S. (2022). Vulnerabilities and Cyberspace: A New Kind of Crises. In Oxford Research Encyclopedia of Politics. https://doi.org/10.1093/acrefore/9780190228637.013.1604

Betz, D. J., & Stevens, T. (2011). Chapter One: Power and cyberspace. Adelphi Series, 51(424), 35–54. https://doi.org/10.1080/19445571.2011.636954

Boussios, E. G. (2021). Hacking Back: Trump's "Madman Theory" Approach to Cybersecurity. Journal of Applied Security Research, 16(4), 514–525. https://doi.org/10.1080/19361610.2020.1832860

Buresh, D. L. (2021, March). A Comparison of the National Security and the Cybersecurity Approaches of the United States under Presidents Trump and Biden versus the National Security and Cybersecurity Approach of Canada. Journal of Business Management and Economics, 09(3). https://doi.org/10.15520/jbme.v9i03.3265

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. Third World Quarterly, 41(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Choucri, N., & Clark, D. D. (2019). International Relations in the Cyber Age: The Co-Evolution Dilemma. The MIT Press. https://doi.org/10.7551/mitpress/11334.001.0001

Clarke, A., & Klein, T. (2022). 2021 Year in Review: The Biden Administration's Efforts on Cybersecurity. Third Way. https://www.jstor.org/stable/resrep39419

Current, A. C. (2024). Does Academic Theory Sway US Cyber Strategy Implementation? (No. Insight; Sharing Academic Research). National Intelligence University.

Devanny, J. (2022). 'Madman Theory' or 'Persistent Engagement'? The Coherence of US Cyber Strategy under Trump. Journal of Applied Security Research, 17(3), 282–309. https://doi.org/10.1080/19361610.2021.1872359

Farrell, M. B., Starks, T., & Bade, G. (2019, July 12). Trump is rattling sabers in cyberspace—But is the U.S. ready? Politico. https://www.politico.com/story/2019/07/13/trump-cybersecurity-defense-1415650

Fidler, D. P. (2020, February 12). President Trump's Legacy on Cyberspace Policy. Council On Foreign Relations.

Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). Cyber persistence theory: Redefining national security in cyberspace. Oxford University Press.

Gray, C. (2013). Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling. Books, Monographs & Collaborative Studies. https://press.armywarcollege.edu/monographs/529

Healey, J. (2019a). The implications of persistent (and permanent) engagement in cyberspace. Journal of Cybersecurity, 5(1), tyz008. https://doi.org/10.1093/cybsec/tyz008

Healey, J. (2019b). The implications of persistent (and permanent) engagement in cyberspace. Journal of Cybersecurity, 5(1), tyz008. https://doi.org/10.1093/cybsec/tyz008

Heckman, J. (2021, April 3). Biden makes cybersecurity 'top priority' in national security guidance. Federal News Nwtwork. https://federalnewsnetwork.com/cybersecurity/2021/03/biden-makes-cybersecurity-top-priority-in-national-security-guidance/

Jun, J. (2022, March 30). Preparing the next phase of US cyber strategy. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/preparing-the-next-phase-of-us-cyber-strategy/

Karazanishvili, T. (2023). Understanding US Cyber Security Policies During the Donald J. Trump and Biden-Harris Administrations: In N. Chitadze (Ed.), Advances in Digital Crime, Forensics, and Cyber Terrorism (pp. 211–223). IGI Global. https://doi.org/10.4018/978-1-6684-8846-1.ch013

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Matishak, M. (2022, December 23). Biden signs $858 billion defense policy bill into law, expanding gov't cyber operations. The Record Media. https://therecord.media/biden-signs-858-billion-defense-policy-bill-into-law-expanding-govt-cyber-operations

McManus, R. (2025, January 24). The Limits of Madman Theory: How Trump's Unpredictability Could Hurt His Foreign Policy. https://www.foreignaffairs.com/united-states/limits-madman-theory

Microsoft. (2022). Defending Ukraine: Early Lessons from the Cyber War. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

Rosenzweig, P., Bucci, S. P., & Inserra, D. (2017). Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense (No. 3188; Backgrounder). The Heritage Foundation. http://report.heritage.org/bg3188

Sanger, D. E., & Perlroth, N. (2019, February 26). U.S. Cyber Command operation disrupted Internet access of Russian troll farm on day of 2018 midterms. The New York Times. Retrieved. https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html

Schmitt, M. N. (2017). Grey Zones in the International Law of Cyberspace. The Yale Journal of International Law Online, 1–21.

Shively, J. (2021). Cybersecurity policy and the Trump administration. Policy Studies, 42(5–6), 738–754. https://doi.org/10.1080/01442872.2021.1947482

Shively, J. (2022). Cybersecurity Policy, Punctuated Equilibrium Theory, and the Biden Administration. Politics and International Relations. https://doi.org/10.33774/apsa-2022-rcn85

Skingsley, J. (2023). Offensive cyber operations: States' perceptions of their utility and risks. Royal Institute of International Affairs. https://doi.org/10.55317/9781784135850

Smeets, M. (2020). U.S. cyber strategy of persistent engagement & defend forward: Implications for the alliance and intelligence collection. Intelligence and National Security, 35(3), 444–453. https://doi.org/10.1080/02684527.2020.1729316

Summary. (2018). Department of Defense.

Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. Contemporary Security Policy, 40(3), 368–381. https://doi.org/10.1080/13523260.2019.1581458

The White House. (2018). National Cyber Startegy. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The White House. (2023, January 3). National Cyber strategy. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Tidy, J. (2020, December 16). SolarWinds: Why the Sunburst hack is so serious. BBC. https://www.bbc.com/news/technology-55321643