Polish Journal of Political Science

Volume 12 Issue 2 (2026)

V.12

Polish Journal of Political Science
Volume 12 Issue 2

V.12

The journal is published by the Interdisciplinary Research Center
of the University of Warsaw "Identity – Dialogue – Security"
(Interdyscyplinarne Centrum Badawcze Uniwersytetu Warszawskiego
„Tożsamość – Dialog – Bezpieczeństwo")

Editorial address
Polish Journal of Political Science

Interdisciplinary Research Center of the University of Warsaw
"Identity – Dialogue – Security"
Prosta 69, 00-838 Warsaw
email: centrum.tozsamosc@uw.edu.pl

Warsaw 2026

eISSN 2391-3991
Original version: e-book
Submit your paper: pjps@uw.edu.pl

Polish Journal of Political Science is included in:

PBN Polska Bibliografia Naukowa
Biblioteka Nauki
ERIHPLUS European Reference Index for the Humanities and Social Sciences
Central and Eastern European Online Library
BAZEKON

Volume 12 Issue 2 (2026)

Table of Contents

Articles

Book review

Javidan Guliyev*

* University of Warsaw, e-mail: j.guliyev27@gmail.com

Volume 12 Issue 2 (2026)

United States Cybersecurity Policy and the Continuing Threat of Cyberwarfare in the Period from 2009 to 2023

DOI: 10.58183/pjps.03022026

Abstract

This study explores the evolution of cybersecurity and cyberwarfare policy in the United States from 2009 to 2023, situating national developments within the broader context of international legal fragmentation. The central research question guiding this analysis is: How does the legal framework for cybersecurity impact the evolving cyberwarfare threat in the United States? In addressing this question, the article evaluates major strategic, legislative, and institutional initiatives implemented under the administrations of Barack Obama, Donald Trump, and Joseph Biden. Rather than treating these periods as isolated policy cycles, the study examines them as stages in the consolidation of an increasingly sophisticated national cyber regime development. The core hypothesis advanced in this research is that, even with advanced national cybersecurity frameworks, the United States remains vulnerable to cyberwarfare because of the structural weaknesses of international legal regulation. While domestic laws enhance resilience, they do not eliminate the incentives for hostile cyber activity originating beyond national jurisdiction. The study also incorporates three case analyses of major state-sponsored cyber

incidents that exposed gaps in international law and demonstrated the constraints of unilateral legal solutions. The findings suggest that cybersecurity cannot be fully secured through national policy alone. Although the United States has developed one of the most comprehensive cyber governance frameworks globally, enduring instability in cyberspace persists due to insufficient international coordination. Strengthening global cooperation, therefore, emerges as a necessary step toward mitigating cyberwarfare risks in the digital age.

Keywords
cyberwarfare, cybersecurity, cyberattack, international law

Introduction

The relevance of cyberwarfare in a globalized world cannot be ignored, as it has a huge impact on government stability and the protection of human rights. The United States, one of the world's leading global powers in cybersecurity development, faces new challenges in the cyber realm, including cyberterrorism, cyberwarfare, and cyberespionage, which threaten national sovereignty and vital infrastructure. The country's fundamental infrastructure is embedded in cyberspace, making it the most severely impacted on the world stage. The current international and regional legal framework of the US offers guidelines for nations to deal with cyber risks while promoting collaboration and unity. The main question is whether the United States can cope on its own with cyber-attacks and how important the world community is in eliminating cyber problems. Given the global reach of computer technologies and the Internet, which affects factories, hospitals, and infrastructure, it presents a serious risk. By threatening the stability of governments, cyberattacks of warfare can ruin vital infrastructure, expose confidential government data, and weaken the democratization processes. Furthermore, by negatively impacting people's rights to privacy, freedom of expression, and information access, cyberattacks can violate human rights. For instance, state-sponsored cyber "espionage"[1] and monitoring may violate citizens' rights, and cyberattacks may directly impact people's rights to life and security in services like healthcare or education. Cyberwarfare's significance in the modern world is directly related to its capacity to harm, which strengthens the argument that even with contemporary regional legal frameworks for cybersecu-

1. Espionage – a practice implemented by governments to create a group of spies to obtain information.

rity, which are mainly developed in the US, there is a threat of cyberwarfare and cyberattacks because of the weakness of international legal norms, which should strengthen the security of human rights and government stability. This study explores the impact of the US frameworks against cyberattacks established under Barack Obama, Donald Trump, and Joe Biden administrations, and analyzing outcomes of the Stuxnet, SolarWinds, and Equifax cyberattacks will demonstrate the current legal norms vulnerabilities.

Theoretical and Definitional Approaches

Taking into account the concept of "cyberwar," it is necessary to outline that unlike any other conventional armed conflict-related terminology, cyberwar occupies not only the scope of technological development, but also geopolitical implementation and law enforcement. Based on the existing literature, cyberwar's technical operational side can be explained as an advanced technological system that has the capacity to disrupt an adversary's information infrastructure.[2] Often openly ignoring an illegal threshold, it exists under the so-called capability factors. In contrast, legal interpretations focus on whether cyber operations meet the criteria of "use of force" under international law. The Tallinn Manual 2.0 represents a leading effort in this regard, suggesting that only operations producing effects of a physical disruption qualify as attacks.[3] However, most cyber activities are deliberately designed to remain below this threshold. On the other hand, an approach that was advanced by scholars such as Thomas Rid states that, due to a broader strategic perspective, cyberwar is a low-intensity competition where states pursue political objectives without triggering open conflict.[4] This study adopts a wider lens, treating cyberwar as the use of cyber capabilities by entities to achieve strategic goals regardless of legal classification. Due to this wide range of influence, it is necessary to analyze case studies with completely different severity levels, all of which have a single classified topic behind, which is a cyberattack. The paper presented by Al Zaidy mentions the concept overview of cyber-threats and cyber-attacks. He describes that digital systems, networks, as well as portable devices, are susceptible to cyber-attacks, which enable the intrusion, exploitation, and destruction of the internet system. For US cyber security research, the source provides an analytical framework that is useful as background. It defines core technical terms and also threat categories, which are necessary for investigating the US approach to cyber defense and national cyber resilience.[5] Examples of Stuxnet, the SolarWinds hack, and the Equifax breach each sit at a different spot on that range of severity. Stuxnet was interpreted as an actual act of war because it broke Iranian centrifuges, whereas scholars like Samuli Haataja and Afshin Akhtar-Khavari have gone back and forth to identify whether it was legally an act of war under international law.[6] SolarWinds, on

2. M.C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation 2009, pp. 106–109.

3. M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press 2017, pp. 382–383.

4. T. Rid, *Cyber War Will Not Take Place*, "Journal of Strategic Studies", 2012, Vol. 35, Issue 1, pp. 5–32, DOI: 10.1080/01402390.2011.608939.

5. A. Al Zaidy, *What are Cyber-Threats, Cyber-Attacks and How to Defend our Systems*, Research Proposal Paper: Final Term Project Paper, Strayer University 2014, pp. 2–4, DOI: 10.13140/RG.2.2.30414.59208.

6. S. Haataja, A. Akhtar-Khavari, *Stuxnet and International Law on the Use of Force: An Informational Approach*, "Cambridge International Law Journal", 2018, Vol. 7, Issue 1, pp. 99–121, DOI: 10.4337/cilj.2018.01.05.

the other hand, was a hugely wide-reaching, very well-planned spying operation. While it fell short of being classified as war, it severely weakened confidence in companies used by the government, as Antonio Coco, Talita Dias, and Tsvetelina van Benthem pointed out in 2022.[7] Lastly, another prominent example of Equifax, according to Jason Thomas, was an instance of a government-related cyber incident. The public exposure of sensitive private information on such a scale showed that cyber harm can have social and legal consequences, even when there is no physical violence, use of force, or military objective.[8] By taking a sufficiently broad definitional framework, adopting a comparative perspective enables an analysis of how the law is supposed to deal with all three cases, but seldom does so in a legally coherent manner.

Theoretical debate on cybersecurity governance can be understood with reference to the realist versus liberal-institutionalist point of view. Based on the research of Yavuz Akdag, the realist perspectives posit that states operate in a competitive hierarchical international system where power, security, and strategic advantage are the main objectives. In this regard, in the cyber domain, more major powers have often resisted binding regulatory arrangements that could constrain the development of cyber offensive or strategic digital capabilities. Instead, they prefer to benefit from the legal and normative ambiguity that still characterizes cyberspace.[9] On the other hand, liberal-institutionalist approaches argue that uncertainty and shared threats can be mitigated through international rules, organizations, confidence-building, and multilateral cooperation. This view is echoed in the repeated effort of the United States, particularly under the Obama and Biden administrations, to push cyber norms and bolster cooperation with allies and international institutions while fitting cybersecurity into a broader rules-based framework of international governance.[10] By combining both theoretical perceptions towards cyberwarfare, it would add clarity on how power has driven the US cybersecurity strategy, while acknowledging the often-ineffective efforts of international institutions to establish governing norms.

Research Review

Scholarly engagement on US cybersecurity policy has multiplied considerably since the early 2010s, yet most existing studies have focused either on the technical or the legal dimension in isolation. The concept of cyberwar itself has been the subject of conceptual groundwork by Rid, Libicki, and others, while Kello asserted that cyberspace has resulted in an extended condition of "unpeace," defined as sustained strategic disruption that lies beneath the threshold of war but beyond the reach of existing legal categories.[11] Ben Buchanan likewise demonstrated that cyber op-

7. A. Coco, T. Dias, T. van Benthem, *Illegal: The SolarWinds Hack under International Law*, "European Journal of International Law", 2022, Vol. 33, Issue 4, pp. 1275–1286, DOI: 10.1093/ejil/chac063.

8. J. Thomas, *A Case Study Analysis of the Equifax Data Breach*, Research paper, 2019, pp. 2–3, DOI: 10.13140/RG.2.2.16468.76161.

9. Y. Akdag, *Great Power Cyberpolitics and Global Cyberhegemony*, "Perspectives on Politics", 2025, pp. 4–5, DOI: 10.1017/S1537592725000040.

10. D.P. Fidler, *America's Place in Cyberspace: The Biden Administration's Cyber Strategy Takes Shape*, Council on Foreign Relations 2021, https://www.cfr.org/articles/americas-place-cyberspace-biden-administrations-cyber-strategy-takes-shape, (access 15.01.2026); M. Nuruzzaman, *Liberal Institutionalism and International Cooperation after 11 September 2001*, "International Studies", 2008, Vol. 45, Issue 3, pp. 193–213, DOI: 10.1177/002088170904500302.

11. L. Kello, *The Virtual Weapon and International Order*, Yale University Press 2017, pp. 8–16; T. Rid, *Cyber War Will...*, op. cit., pp. 5–32; M.C. Libicki, *Cyberdeterrence and Cyberwar*, op. cit., pp. 106–109.

erations are used more as instruments of persistent statecraft than as single acts of war. This suggests the need to assess US policy on a longer strategic continuum rather than on sole incidents.[12] Legal research, such as the Tallinn Manual 2, has added to the debate on when cyber operations can be classified as an armed attack.[13] However, such legal research typically remains normative and does not anchor claims in policy outcomes. Case studies such as those of Jason Thomas deliver empirical depth on the sole incidents but do not engage in the much-needed cross-administration comparison that would reveal structural patterns.[14] This gap is addressed in the article by integrating legal and strategic analysis across three administrations and three typologically different incidents.

12. B. Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press 2020, pp. 107–109.

13. M.N. Schmitt (ed.), *Tallinn Manual 2.0...*, op. cit., pp. 380–396.

14. J. Thomas, *A Case Study...*, op. cit., pp. 2–3.

Research Methods

This article employs qualitative research methods, including an analysis of strategic documents, a legal and regulatory analysis, and a comparative case study. The research protocol consists of an analytical examination of US government policy documents from 2009 to 2023. Specifically, these documents were examined to assess the recurring legal, strategic, and institutional priorities in the governance of cybersecurity. Using predetermined analytical categories such as regulatory scope, these documents were categorized and compared in three case studies. In conjunction with established normative frameworks such as the Tallinn Manual 2.0, this study examines legal and strategic texts to evaluate the limits of international regulation and the ways domestic policies respond to cyber threats. The three case studies, Stuxnet, Equifax, and SolarWinds, were chosen because of their different places on the cyber threat spectrum, allowing systematic comparison across the three threat typologies. This methodology empowers the cases to serve as analytical tools, backed by empirical evidence. This helps to interrogate the foundational hypothesis that domestic legal adequacy can only compensate for the functional gap of international regulation.

US Cyberwarfare under Barack Obama

Starting with the Obama administration, the extensive realignment became the catalyst for an overhaul of US security strategy. Although the "fight terrorism"[15] strategy remained at the center of the Obama administration's military security agenda, his understanding of security policies, particularly in the area of cybersecurity, gradually shifted for a variety of reasons, including the domestic elite's desire for a change in direction and the evolving international landscape brought about by the emergence of new threats. As noted by Clorinda Trujillo, Obama's initial stance on the relationship between cyberspace and national security in 2009 stressed that US digital infrastructure is a strategic

15. In this context, the "fight terrorism" is a multifaceted approach that includes, among other things: the use of US military forces, but not in the format of a full-fledged ground war (development of cybersecurity); training to fight terrorism; strengthening international counterterrorism cooperation; transitioning from a military to a political solution to the Middle East crisis.

national asset. The new administration's cybersecurity strategies have become more successful due to military cyber deterrence.[16]

The way the US dealt with cybersecurity has really changed in terms of how the government used its power. As Francesco Amoretti and Domenico Fracchiolla said, the American method went from a "distributive" style to a "Constituent Policy." That change is best seen using the ideas of Theodore Lowi, who in 1972 explained Constituent Policy as the government trying to make new political organizations and share power differently between institutions. Based on the US cyber policy style of "distributive" approach, resources were dispensed in a fragmented manner, focusing on isolated infrastructure grants without a cohesive general rule.[17] But the Obama government recognized cyberspace as a "strategic national asset" and deliberately began to build up the state around it. By setting up new "areas of authority," like the Cyber Coordinator in the White House and the Cyber Threat Intelligence Integration Center, the US tried to build a "Cyber Westphalia"[18] structure, putting state control back over what had been classified as digital chaos. This move to a territorial way of thinking shows that, even though the network is global, full control over it by countries is still the main area of global political desire struggles.[19]

Although it has moved toward a Constituent Policy, the US system has faced internal institutional fragmentation and a lack of a coherent overarching strategy. A strong Constituent Policy needs a clear area of authority, but the US system had a danger of breaking up because of the number of government departments. The main split was over who was responsible between the Department of Homeland Security (DHS) and the Department of Defense (DoD). Eric Talbot Jensen claimed in 2011 that the US government's choice to make DHS the main agency for cybersecurity was "limited," as DHS was, at its heart, a law-and-order organization to protect buildings and services. While it had operational capabilities to secure civilian networks, it lacked the "enforcement abilities" necessary to compel security standards across the private sector.[20]

In general, the Obama administration brought about a dramatic change in American cybersecurity laws by emphasizing privacy and openness. To address privacy concerns, President Obama anchored the White House's strategy with transformative reforms. Amoretti and Fracchiolla state that an important step forward was the creation of the Comprehensive National Cyber Security Initiative (CNCSI), which combined military intelligence, counterintelligence, and law enforcement resources with cyber defense to combat various threats. The CNCSI established the government's offensive and defensive

16. C. Trujillo, *The Limits of Cyberspace Deterrence*, "Joint Force Quarterly", 2014, Vol. 75, No. 4, pp. 44–45.

17. F. Amoretti, D. Fracchiolla, *The Cyber Security Policy of the USA under the Obama Administration: A Case Study of a Constituent Policy*, SSRN Scholarly Paper No. 3490189, 2018, pp. 4–8.

18. Cyber Westphalia – a term that describes the digital activity control of a country with the establishment of digital borders and national oversight.

19. J. Goldsmith, T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press 2006, pp. 6–16.

20. E.T. Jensen, *President Obama and the Changing Cyber Paradigm*, Brigham Young University Law School 2011, Vol. 37, No. 1, pp. 3–4.

cyber objectives, resulting in the establishment of an office for cybersecurity coordination under the leadership of the White House. The creation and alteration of several organizations, such as the Cyber Coordinator office and other departments, also led to changes in the structural makeup of cybersecurity policy.[21]

Another very important initiative was the International Cyber Security Strategy (ICSS) of 2011, which contained the concept of unity that President Obama wanted to strengthen. ICSS laid out the President's vision for the future of the Internet and set an agenda for partnering with other nations and peoples to achieve that vision. The agenda mentioned that the international environment, proper cooperation, technology development, and the rule of law will lead this strategy to effectively fight against threats.[22] The cybersecurity sphere drastically changed under Obama's administration. Both national and international policies were seen as leading irregular warfare, which should represent the US as a main actor of influence worldwide. But the world generally had trouble deciding when a cyberattack was bad enough to be classified as a "threat attempt." Traditional international law, as grounded in the United Nations (UN) Charter, has historically focused on the use of material damage. This creates a significant legal grey zone in which the applicability of existing rules to cyber operations remains uncertain. Actions that may produce severe economic consequences, as seen in examples such as undermining confidence in financial markets or deliberately manipulating data, do not constitute "armed force" in the traditional sense, as they lack a direct physical dimension.[23]

The US has usually supported the idea of cyberspace as a "world common," something for everyone, but other countries wanted a "cyber-sovereignty," where the country had total control over what happens in its digital areas.[24] This fight between the "open" internet and the notion of "Cyber Westphalia," which emphasizes state-centric control, constrains the development of coherent and universally accepted international regulatory frameworks. This "breaking up" of power shows a broader systemic issue in which both historical and emerging state strategies reflect a persistent pursuit of control across strategic domains.

US Cyberwarfare under Donald Trump

When Trump came to office, the US began to implement self-oriented policies in both the security and military spheres. His central principle was "Make America Great Again," which meant shifting the focus from international cooperation to the United States itself. He possessed leadership attributes strongly related to his personal characteristics and perception of the environment, which

21. F. Amoretti, D. Fracchiolla, *The Cyber Security...*, op. cit., pp. 12–13.

22. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House 2011, pp. 11–22.

23. E.T. Jensen, *President Obama and...*, op. cit., pp. 3–4.

24. A. Segal, *China's Alternative Cyber Governance Regime*, Prepared Statement before the U.S.-China Economic Security Review Commission, Hearing on 'A China Model?' Beijing's Promotion of Alternative Global Norms and Standards, Council on Foreign Relations 2020, pp. 3–4.

contributed to the emergence of a new model of decision-making aimed at ensuring US superiority. This approach showed that this type of security has ontological or existential significance for the US; therefore, it can be characterized as a break from Obama's cyber cooperation approach.[25]

Trump's way of dealing with national safety was formed by doubting international organizations and believing that arrangements with multiple countries often limited the power of the US, which confirms his political stance from the realist perspective. In the realm of cybersecurity, this translated into a reduced emphasis on international cooperation and a greater reliance on military capabilities. Cyberspace was thus framed less as a domain requiring collective governance and more as a competitive arena comparable to traditional types of conflict. The National Cyber Strategy (NCS) of 2018 stated that cyber dangers were threats that threatened the existence of the US's wealth and development capacities. The NCS document stressed that enemies were already constantly doing cyber operations against American strategic targets and that stopping them needed constant involvement, not just a last resort defense interference when a crisis occurs. This was a clear and pragmatic change from the approach of the Obama years, which at that time placed greater emphasis on caution in international engagement and the gradual development of normative standards, which manifests a liberal theory perspective. Trump understood cyber power not only as an instrument of defense, but it was also seen as a strategic tool that could change the digital security framework of the US. This idea was in line with Trump's larger foreign policy strategy, which prioritized relative gains over multilateral cooperation and collective institutional engagement. The result for the US was mostly acting according to what is best for its own safety, where the regulations and law reforms are considered less important than the force power of national security development.[26]

This was one reason why Trump established new Department of Defense (DoD) reforms to strengthen power in cyberwarfare. Specifically, the strategic steps prepared by the DoD under the Trump administration for cybersecurity were: 1. to maintain ready forces and capabilities to conduct cyberspace operations and continue to develop technology to remain at the forefront of dealing with threats by increasing cyber defense capabilities; 2. to build and maintain viable cyber options and plan to use those options to control conflict escalation and shape the conflict environment at all stages, as well as build cyber systems that are sustainable and integrated with the plans of related agencies; and 3. to build cooperation capacity in cybersecurity and defense through engagement with the international cyber world.[27] This meant that the DoD also supported the US National Defense Strategy through technology-based information and data security. So, under Trump, US government

25. *The White House National Cyber Strategy: Continuity with a Hint of Hyperbole*, Council on Foreign Relations 2018, https://www.cfr.org/articles/white-house-national-cyber-strategy-continuity-hint-hyperbole, (access 15.01.2026).

26. *Summary of the 2018 Department of Defense Cyber Strategy*, Washington, DC: U.S. Department of Defense, pp. 3–4.

27. Ibidem, pp. 6–7.

departments started to construct dedicated approaches to manage risk, guidelines to protect vital systems, and enhanced internal reporting systems, all to reduce vulnerability and improve recovery from critical cyberattack scenarios.

However, cybersecurity is and was, at its heart, intentional. Harmful software does not bother itself with boundaries, which means that it often acts from jurisdictions outside the reach of the US's legal authority. Consequently, domestic regulations are insufficient to deter foreign states or non-state actors from engaging in hostile cyber activities. Agreements between regions or states cannot force countries to behave if they do not have the same views on politics and the determination of what is considered a positive strategic outcome. So, while the US's legal systems made the nation counter defense abilities stronger, they did not resolve factors that drive cyberwarfare at its roots. That is why, unlike the law of the seas or the air, international law in cyberspace still does not have a complete and enforceable set of laws, as there is no universally accepted treaty defining what actions are permitted or prohibited for countries. General discussions in the UN have created voluntary rules and ways to build trust, but these initiatives are not binding and are applied inconsistently. It leads to the important questions that have not been answered. When does a cyber operation become an act of war? How much trouble justifies defending yourself? How should countries react to cyber spying, which happens all the time, but isn't usually said to be legal? Without definitive guidelines, potentially harmful activities are permitted to occur. Countries can carry out cyber operations that are not classified as a full-scale war, or threat acts, to avoid legal responsibility. The trouble of finding out where the attack originated also makes it harder to hold cybercrime entities accountable, because those involved can deny participation or blame individual entities rather than disclose any governmental links. That is why Simran Maker calls cyberspace a place of "less-than-war," where countries follow their strategic goals by constantly carrying out small-level operations. This describes the main contradiction of modern cyber conflict: actions that are unfriendly and cause damage, but don't usually cause traditional military reactions.[28]

Trump's cyber strategy quietly accepted this. Instead of trying to solve the legal confusion, it tried to make the most of it by giving the US as much freedom to act as possible. While sensible from a realist point of view, this does not lower the amount of cyber conflict as a whole. His idea was based on the fact that cyber operations are part of a wider competition between countries.[29] These patterns show that cyberwarfare is part of the existing struggles for power. Weak international law does not stop this, because it does not change the reasons why it is attractive to opponents. Trump's focus on

28. S.R. Maker, *New Frontier in Defense: Cyberspace and U.S. Foreign Policy*, National Committee on American Foreign Policy Report 2017, pp. 5–15.

29. *Presidential Proclamation on National Cybersecurity Awareness Month, 2019*, The White House 2019, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-proclamation-national-cybersecurity-awareness-month-2019/, (access 15.01.2026).

national strength dealt with the result of the problem, not the reason for it. It made America better at competing, but did not change the conditions that make cyber conflict appealing to enemies.

US Cyberwarfare under Joe Biden

Upon entering the White House in 2021, President Joe Biden faced a growing number of ransomware incidents, extensive spying efforts, and frequent break-ins to vital governmental systems. According to the Biden-Harris Administration's National Cybersecurity Strategy, previous models that placed the burden of cyber defense primarily on small entities were no longer sufficient, prompting the federal government to take a greater role in leading cybersecurity efforts.[30] As a result, the Biden team began to view cybersecurity as something requiring the full attention of the government and of all Americans, stressing the need to rebound from attacks and set a new partnership between the public and private sectors. A central element of the Biden administration's policy is the elevation of cybersecurity to a national security priority, framing cyber threats as equivalent in seriousness to terrorism. The Biden administration's method was based on the idea that weakness in the digital world is a feature of the whole system. Government networks need technologies from the private sector and companies that have the most essential and developed systems. While the Trump administration stressed being prepared for war and attacking in cyberspace, the Biden administration put more importance on being able to recover by cooperating with private companies. Both administrations, however, have worked in the same international environment where there are few legal limits on cyber operations.

The Executive Order on Cybersecurity, enacted in May 2021, mandated the adoption of a "zero-trust architecture,"[31] fortifying federal networks against cyber incidents. It was the primary legal basis for this overhaul. Instead of viewing cybersecurity as something agencies could do, the order put actual, necessary upgrades on federal departments, required secure standards for software coming into use, and quickened the move to zero-trust systems. Cyber defense was no longer framed as a reactive shield but as a regulated condition of participation in the federal digital environment.[32]

However, this also brought to light a key issue: cybersecurity was increasingly governed by domestic law, while aggressive cyberattacks from other countries were not effectively constrained by international rules. This discrepancy between domestic requirements and what is permitted on the international stage creates a fundamental weakness. The Biden administration has not enacted a single law titled "cyberwarfare legislation." Rather than through clear international rules, cyber-

30. *National Cybersecurity Strategy*, The White House 2023, pp. 4–8, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, (access 15.01.2026).

31. ZTA, zero trust architecture – new security strategy to implement developed IT, cloud, and cyber systems. General meaning – never trust, always verify.

32. *Executive Order 14028: Improving the Nation's Cybersecurity*, Information Technology Laboratory, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity, (access 15.01.2026).

warfare has been influenced by national laws controlling information flows, incident reporting, and the security of key systems. The Cyber Incident Reporting for Critical Infrastructure (CIRCIA) Act of 2022 required organizations subject to its rules to report significant cyberattacks and ransom payments within specified timeframes. In legal terms, cyber operations became more formally regulated rather than purely covert. This is significant for cyberwarfare, as identifying perpetrators is essential for diplomatic action. By developing internal capacities to identify where potential cyberattacks were occurring, the US, under the new CIRCIA Act, improved its ability to turn cyberattacks into tools of government. The "Bipartisan Infrastructure Law" prioritizes cybersecurity in modernizing infrastructure, integrating digital safety with power networks and transportation, and expanding broadband availability. Cybersecurity thus becomes an integral part of the country's development plans. While these laws did not limit US cyber-operations in other countries, they improved the government's capacity to participate in cyber-competition. Cyberwarfare under Biden, therefore, became an institutionalized rather than an ad hoc policy implementation.[33]

The 2023 National Cybersecurity Strategy (NCS) significantly reallocated responsibility for cyber risk. The new approach shifted responsibility to technology manufacturers and service providers instead. This shift in responsibility had significant effects on strategy. By requiring the companies that build and maintain digital systems to ensure they are secure, the US sought to limit its exposure to potential cyber threats. This approach could make cyberwarfare more costly, but it also creates a gap in the system. Most rules apply only within the US, leaving companies manufacturing abroad and multinational digital platforms operating in areas where regulations are unclear. Consequently, adversaries can exploit global supply chains even as domestic standards in the US improve.[34]

Under President Biden, cyber conflict was not seen as a series of separate emergencies but rather as a continual state of affairs. Institutions were adapted to accommodate this reality. The Cybersecurity and Infrastructure Security Agency (CISA), in its expanded role, serves as the primary link between federal government departments and the entities that operate private essential services. CISA does not only defend networks; it manages the overall cyber risk landscape. In cyberwarfare terms, this suggests the US views cyber conflict as an enduring reality. The objective became not the eradication of cyber conflict, but its improved management. The strategic shift in cybersecurity was evident in the move away from traditional deterrence toward improving deterrence through the structural conditions of cyberspace. Instead of primarily depending on the ability to retaliate, the United States began to devote increasing resources to altering the cyber environment to make it more

33. *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, America's Cyber Defense Agency, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia, (access 15.01.2026).

34. *National Cybersecurity Strategy*, op. cit., pp. 8–10.

resilient and less vulnerable. Cyber policy during the Biden period integrated cyberwarfare with economic policy. Regulations on advanced semiconductors, the screening of investments, and the securing of supply chains all directly affect how cyber capabilities are developed. Cyber strength increasingly depends on having the latest computing technologies, artificial intelligence, and research into quantum physics. By controlling the flow of technology, the US indirectly limited adversaries' ability to develop advanced cyber tools. Instead of direct network attacks, the US targets the technological infrastructure that underpins cyber operations. While this approach could yield long-term strategic advantages, it is complicated by international divisions. Different technology systems could emerge, reducing US power and creating separate cyber spheres governed by different standards.[35]

The Biden administration's approach created several structural opportunities. First, systemic resilience reduces the likelihood that single cyber incidents produce national-level crises. Second, institutionalized information sharing accelerates collective learning and adaptation. Third and last, alliance-based coordination increases political costs for malicious cyber activity through joint attribution and sanctions. These opportunities do not end cyberwarfare, but they can moderate its most destabilizing effects.[36]

Even with these improvements, key problems remained: international law still does not clearly define what constitutes an "act of war" in cyberspace, what constitutes a fair response, and what constitutes a legitimate target. The Biden administration shows that good government structure and cooperation can change the perception of cyber defense, even amidst persistent cyber conflict. This supports the idea that the main reason for cyberwar is not a lack of rules within countries themselves, but the fact that international legal rules are weak.

Case Studies of State--Sponsored Cyberattacks

Besides existing regional frameworks for cybersecurity in the US, state-sponsored cyberattacks have increased due to the lack of a comprehensive international legal framework, posing serious risks to international security. Notably, the Stuxnet, SolarWinds, and Equifax cyberattacks provide strong proof of the consequences of a weakness in global legal standards. Those three case scenarios will be examined, each to illustrate institutional improvisation in the face of legal inadequacy. They reveal a structural cycle that repeated across more than a decade of American cyber governance. In each instance, a hostile state or state-linked actor exploited a normative vacuum in international law, whereas either the operation was calibrated to remain at or beneath the margins of legally actionable

35. V. Mishra, S. Patil, *Decoding the Biden Administration's Cyber Security Policy*, Observer Research Foundation Issue Brief 2024, No. 686, pp. 1–18.

36. *The Biden-Harris Administration's Engagement with International Partners on Responsible State Behavior in Cyberspace*, FPC Briefing, U.S. Department of State 2022, https://2021-2025.state.gov/briefings-foreign-press-centers/responsible-state-behavior-in-cyberspace/, (access 15.01.2026).

thresholds, attribution proved legally inconclusive, or domestic institutional responses were mobilized after the fact but proved incapable of addressing the conditions that had made the attack possible in the first place. The repetition of this cycle in three successive administrations shows that the problem is structural, not a result of the specific decision-making process. The study analyzes each instance along four common analytical dimensions. The first is the challenge of attribution and the legal consequences of that challenge. The second is the threshold implicated, namely, whether the operation came close to, met, or intended to avoid meeting the use-of-force threshold under international law, as well as the relevance of that threshold. The third is the domestic institutional and policy response to the incident generated. The fourth is the specific gap in the international legal framework that the incident exposed. Consistent application of these dimensions in all three cases enables moving the analysis beyond the sequencing of storytelling towards the comparative examination of the structural patterns defining governance deficit in international cyberspace.

Stuxnet

Stuxnet, the first virus to cross the cyberspace-physical border, was discovered in 2010 by security experts from Iran. After years of cooperation between the US and Israeli security agencies, the Stuxnet worm was created in 2009. According to Paul Mueller, the purpose of the Stuxnet worm was to compromise Iran's infrastructure, which included transportation, telecommunications, and nuclear power plants. The early versions of Stuxnet were secretive, but both the US and Israel had access to the source code, which was later used to destabilize foreign sources and gain influence in the regions.[37] Samuli Haataja questions whether the cyber-attack exceeded the use-of-force criterion or not, which is crucial to the judicial proceeding of the Stuxnet case. The Tallinn Manual is a good source to analyze when it comes to a legislative solution to the Stuxnet problem. This document is a study of the views of a team of prominent international lawyers on the applicability of existing international law to military action in cyberspace. The Tallinn Manual as a whole persuasively interprets existing international norms, including humanitarian law and the laws of war, as they apply to military operations in cyberspace. Concerning Article 2(4) of the Tallinn Manual[38] on international law of cyber operations, scholars like David Weissbrodt[39] think that because of the threat to nuclear production it caused, it should be considered an act of force. Another issue was related to the fact that Stuxnet was different from traditional weapons, which makes it a newly established cyber weapon to which arbitration cannot be assigned. This case proves the fact that at the time when Obama signed

37. P. Mueller, *The Stuxnet Worm*, University of Arizona Department of Computer Science 2012, p. 1.

38. M.N. Schmitt (ed.), *Tallinn Manual 2.0...*, op. cit.

39. D. Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, "Minnesota Journal of International Law", 2013, Vol. 22, No. 2, pp. 347–376.

Cybersecurity adjustment reforms, he also planned a foreign influence cyber operation, namely the Stuxnet worm, which severely disrupted Iran's uranium-enrichment process. Weissbrodt's opinion illustrates the uncertainty of the legal proceedings in the Stuxnet case till today, as it is a complex and initially secret cyber operation.[40]

40. S. Haataja, A. Akhtar-Khavari, *Stuxnet and International...*, op. cit., pp. 99–121.

Equifax

The second case relates to the Equifax cyber-attack in 2017, which constituted a significant turning point in the US public awareness of cybersecurity risks. According to the Federal Trade Commission (FTC) of the US, the intrusion resulted in the exfiltration of personal records belonging to approximately 147 million American citizens, including names, Social Security numbers, dates of birth, residential addresses, and, in some cases, driver's license numbers.[41] The breach was limited in geographic scope to US residents, though its scale was such that it exposed a substantial share of the American adult population to financial identity harm. The incident drew widespread attention to the structural vulnerabilities of credit reporting infrastructure and the adequacy of data protection obligations in the financial sector. Josh Fruhlinger mentioned that some responses included hearings and investigations, while others called for stronger regulations to prevent similar breaches in the future. To look at how Equifax handled security practices and responded after being hacked into itself became a subject under scrutiny by both the FTC and the Consumer Financial Protection Bureau (CFPB).[42] In the aftermath, stakeholders increasingly shifted responsibility onto one another while calling for accountability from all parties involved in the incident. While the case was being revealed, the core pathway implementations were made to address its consequences. The company was ultimately required to offer credit monitoring services to affected individuals and was subjected to substantial financial penalties, resulting in one of the largest data breach settlements in US history. The inadequacy of existing enforcement mechanisms was further underscored by difficulties in attributing the intrusion to a specific state actor, a challenge that would recur in subsequent cases. The scale of this attack, which impacted millions of Americans, highlights major gaps in the way we regulate cybersecurity on a national level. Given that technology is constantly changing and becoming more sophisticated with new threats emerging all the time, one needs a unified, stronger, holistic approach to protecting systems against unauthorized access or use.[43]

41. *Equifax Data Breach Settlement*, Federal Trade Commission 2019, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement, (access 15.01.2026).

42. Consumer Financial Protection Bureau – an independent organization that is linked to the FTC and deals with the consumer financial sector.

43. O. Fruhlinger, *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO Online 2020, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html, (access 15.01.2026).

SolarWinds

Going further to the late 2020s, the SolarWinds supply chain breach caused another massive cyberattack that affected over ten thousand organizations, including government agencies within the US. Antonio Coco et al. mention that because of the difficulty of enforcing laws and the lack of regional cybercrime court action in the US, legal consequences are still unclear despite the seriousness of the breach. It happened because the courts faced a challenge in attributing an attack to a specific actor or nation, requiring extensive technical analysis. Meaning that the SolarWinds cyberattack was linked to Russian government cyber tools by US authorities without any legal proof. Brad Smith, the president of Microsoft, has proposed the creation of an international agreement that forbids cyberattacks on critical infrastructure, as well as a federal disclosure law.[44] Based on the outcomes of the SolarWinds case, Google Cloud, during the National Security Council White House summit, established an Open-Source Maintenance Crew. The Linux Foundation and Open-Source Security Foundation established a $150 million plan to improve open-source and supply chain security over the next two years. By its very nature, the remedy advanced in the Open-Source Software Security is very complex, long-term oriented, and involves a huge number of players, who will contribute to the development of cybersecurity. Based on outcomes for an open-source world, the US government and businesses were making some progress. However, it is too early to forget about open-source and supply chain vulnerabilities. As the government and the industry evolve to improve open-source security, the bad actors also evolve in response.[45] This event also emphasized the necessity of international collaboration and highlighted the importance of procedural measures in countering cyber threats in the contemporary world.

Conclusion

To conclude, the presence of cyber warfare in our contemporary world demands attention because cyber threats impact both government stability and the safeguarding of human rights. While US regional legal frameworks provide guidelines, the threat of cyber warfare continues to exist due to the weakness of comprehensive global norms. The significance of US regional frameworks, such as the National Cyber Security Initiative, the Cyber Coordinator Office, the Department of Defense, the US National Defense Strategy, and the Infrastructure Security Agency, in developing global cybersecurity capabilities is evident and can provide opportunities to address cyberattacks. However, state-sponsored cyberattacks, illustrated by cases like Stuxnet, SolarWinds, and Equifax, underscore the need for a comprehensive international legal framework. What distinguishes the three cases

44. A. Coco, T. Dias, T. van Benthem, *Illegal: The SolarWinds...*, op. cit., pp. 1275–1286.

45. *The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II*, The Linux Foundation 2022, https://www.linuxfoundation.org/press/press-release/linux-foundation-openssf-gather-industry-government-leaders-open-source-software-security-summit, (access 15.01.2026).

from one another is the specific dimension of the international legal order each exposed as deficient. Stuxnet tested the outer limits of the use-of-force doctrine, demonstrating that cyber operations capable of causing physical destruction could be conducted by state actors without triggering recognized legal consequences. All of this was partly because attribution was deliberately concealed, and partly because no binding legal instrument existed to adjudicate the claim, even if attribution had been established. The Equifax breach illustrated a different failure, where even after a state actor was eventually identified, the domestic legal architecture of the victim country could not compel accountability from actors operating beyond its jurisdiction, and no internationally coordinated framework existed for the protection of civilian data infrastructure at scale. SolarWinds, the most consequential of the three, demonstrated that the problem had deepened rather than diminished over time. Despite years of policy development across three administrations, it was able to embed itself within US governmental software supply chains for months without detection. The progression from Stuxnet to Equifax to SolarWinds is therefore not only a story of escalating threat but of a widening gap between the sophistication of hostile cyber operations. In all three instances, furthermore, the same underlying cycle recurred with remarkable regularity. In every case, a hostile actor sought to exploit a gap in relevant international law by ensuring that its operation stayed beneath whatever empirical threshold would draw legal responsibility, or by maintaining plausible deniability. After the incident news broke out, domestic institutions were mobilized reactively to come up with a policy response of regulatory reform, but in no case did legal accountability follow for responsible actors. The basis on which the attack was made possible, namely the lack of an enforceable international legal framework to raise the costs of cyber hostility, remained completely unchanged.

Each administration studied here responded to the challenge of its moment with genuine institutional effort. Obama constructed the foundational cyber governance architecture and initiated the first serious attempt to engage international partners. Trump reoriented that architecture toward deterrence and offensive readiness, accepting the normative vacuum in cyberspace as a competitive reality rather than a problem to be resolved diplomatically. Biden embedded cybersecurity in systemic resilience, pairing domestic institutionalization with renewed multilateral engagement that nonetheless stopped short of binding international commitments. Each approach advanced the domestic dimension of the problem with increasing coherence. None could achieve, through national policy alone, the kind of enforceable international framework capable of raising the costs of cyber activity at its source.

The persistence of cyberwarfare as a threat to the US is not a consequence of insufficient domestic governance. US cyber policy is, by comparative standards, among the most developed in the world, and its evolution across the three administrations examined here reflects a sustained institutional learning process. It is, rather, a consequence of a structural asymmetry between the maturity of national legal frameworks and the immaturity of the international legal order governing cyberspace. Future research should examine the international legal framework adaptation process for improved, transparent, and effective government responses. As an example, to encourage a collaborative effort toward prevention in cyberspace, the US must lead the creation of a systematic practice regarding cyber offenses and new, legally binding standards.

Bibliography

Akdag Y., *Great Power Cyberpolitics and Global Cyberhegemony*, "Perspectives on Politics", 2025, pp. 1–22, DOI: 10.1017/S1537592725000040.

Al Zaidy A., *What are Cyber-Threats, Cyber-Attacks and How to Defend our Systems*, Research Proposal Paper: Final Term Project Paper, Strayer University 2014, DOI: 10.13140/RG.2.2.30414.59208.

Amoretti F., Fracchiolla D., *The Cyber Security Policy of the USA under the Obama Administration: A Case Study of a Constituent Policy*, SSRN Scholarly Paper No. 3490189, 2018.

Buchanan B., *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Harvard University Press 2020.

Coco A., Dias T., van Benthem, T., *Illegal: The SolarWinds Hack under International Law*, "European Journal of International Law", 2022, Vol. 33, Issue 4, pp. 1275–1286, DOI: 10.1093/ejil/chac063.

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), America's Cyber Defense Agency, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia, (access 15.01.2026).

Equifax Data Breach Settlement, Federal Trade Commission 2019, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement, (access 15.01.2026).

Executive Order 14028: Improving the Nation's Cybersecurity, Information Technology Laboratory, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity, (access 15.01.2026).

Fidler D.P., *America's Place in Cyberspace: The Biden Administration's Cyber Strategy Takes Shape*, Council on Foreign Relations 2021, https://www.cfr.org/articles/americas-place-cyberspace-biden-administrations-cyber-strategy-takes-shape, (access 15.01.2026).

Fruhlinger O., *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO Online 2020, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html, (access 15.01.2026).

Goldsmith J., Wu T., *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press 2006.

Haataja S., Akhtar-Khavari A., *Stuxnet and International Law on the Use of Force: An Informational Approach*, "Cambridge International Law Journal", 2018, Vol. 7, Issue 1, pp. 99–121, DOI: 10.4337/cilj.2018.01.05.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, The White House 2011.

Jensen E.T., *President Obama and the Changing Cyber Paradigm*, Brigham Young University Law School 2011, Vol. 37, No. 1, pp. 3–4.

Kello L., *The Virtual Weapon and International Order*, Yale University Press 2017.

Libicki M.C., *Cyberdeterrence and Cyberwar*, RAND Corporation 2009.

Maker S.R., *New Frontier in Defense: Cyberspace and U.S. Foreign Policy*, National Committee on American Foreign Policy Report 2017.

Mishra V., Patil S., *Decoding the Biden Administration's Cyber Security Policy*, Observer Research Foundation Issue Brief 2024, No. 686, pp. 1–18.

Mueller P., *The Stuxnet Worm*, University of Arizona Department of Computer Science 2012.

National Cybersecurity Strategy, The White House 2023, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, (access 15.01.2026).

Nuruzzaman M., *Liberal Institutionalism and International Cooperation after 11 September 2001*, "International Studies", 2008, Vol. 45, Issue 3, pp. 193–213, DOI: 10.1177/002088170904500302.

Presidential Proclamation on National Cybersecurity Awareness Month, 2019, The White House 2019, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-proclamation-national-cybersecurity-awareness-month-2019/, (access 15.01.2026).

Rid T., *Cyber War Will Not Take Place*, "Journal of Strategic Studies", 2012, Vol. 35, Issue 1, pp. 5–32, DOI: 10.1080/01402390.2011.608939.

Schmitt M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press 2017.

Segal A., *China's Alternative Cyber Governance Regime*, Prepared Statement before the U.S.-China Economic Security Review Commission, Hearing on 'A China Model?' Beijing's Promotion of Alternative Global Norms and Standards, Council on Foreign Relations 2020.

Summary of the 2018 Department of Defense Cyber Strategy, Washington, DC: U.S. Department of Defense.

The Biden-Harris Administration's Engagement with International Partners on Responsible State Behavior in Cyberspace, FPC Briefing, U.S. Department of State 2022, https://2021-2025.state.gov/briefings-foreign-press-centers/responsible-state-behavior-in-cyberspace/, (access 15.01.2026).

The Linux Foundation and Open Source Software Security Foundation (OpenSSF) Gather Industry and Government Leaders for Open Source Software Security Summit II, The Linux Foundation 2022, https://www.linuxfoundation.org/press/press-release/linux-foundation-openssf-gather-industry-government-leaders-open-source-software-security-summit, (access 15.01.2026).

The White House National Cyber Strategy: Continuity with a Hint of Hyperbole, Council on Foreign Relations 2018, https://www.cfr.org/articles/white-house-national-cyber-strategy-continuity-hint-hyperbole, (access 15.01.2026).

Thomas J., *A Case Study Analysis of the Equifax Data Breach*, Research paper, 2019, DOI: 10.13140/RG.2.2.16468.76161.

Trujillo C., *The Limits of Cyberspace Deterrence*, "Joint Force Quarterly", 2014, Vol. 75, No. 4, pp. 43–52.

Weissbrodt D., *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, "Minnesota Journal of International Law", 2013, Vol. 22, No. 2, pp. 347–387.

Volume 12 Issue 2 (2026)