Cyber Diplomacy as a Tool for International Peace: A Case Study of Donald J. Trump Approach toward Cyberspace

NUST Journal of International Peace & Stability
2026, Vol. 9(2) Pages 70-83
njips.nust.edu.pk
DOI: http://doi.org/10.37540/njips.v9i2.223

***Mujeeb Ullah Mujaddidi[1] & Tahir Jamil[2]**

Abstract
Cyber diplomacy emerges as a relatively novel and seldom examined concept within the domain of Cyber Politics. The research delineates the American approach to cyber diplomacy and discusses Donald J. Trump's stance in the context of emerging threats and the progression of Cyber Politics. The study emphasizes the efforts of the Trump administration to foster peace and stability within cyberspace. It further explores an emerging concept, particularly salient during this period, situated at the confluence of technology and international relations. The analysis of cyber diplomacy is supported by the theoretical framework of Technological Politics, along with the application of a Neoliberal perspective to the policies enacted by the Trump administration. The research adopts a descriptive and qualitative methodology, focusing on primary and secondary sources. The study contends that Donald J. Trump's Cyber Politics policies were antagonistic to his broader policy agenda, including the travel ban, trade and tariffs conflicts, anti-climate initiatives, and NATO funding. The paper demonstrates that Trump's approach to cyber diplomacy is comprehensive, aimed at promoting stability in cyberspace.

Keywords
United States, cyber-politics, cyber diplomacy, Donald J. Trump, international peace

Introduction
Politics is, as many political scientists define it, the determination of human interactions of 'who gets what, when, and how.' This is a general scholarly understanding of politics.

[1] *Corresponding Author: *Mujeeb Ullah Mujaddidi is* an M.Phil. Scholar in American Studies at Area Study Centre for Africa, North and South America at Quaid-i-Azam University, Islamabad, Pakistan
E-mail: mujeebhidayat@gmail.com
[2] Tahir Jamil is an Assistant Professor in the Area Study Center for African, North and South America at Quaid-i-Azam University, Islamabad, Pakistan.

Received 12 September 2024; **Revised** 15 April 2026; **Accepted** 1 June 2026; **Published online** 30 June 2026

By contrast, the virtual world or cyberspace has its own realities and dynamics. The convergence of politics and cyber has given rise to a new reality or knowledge known as Cyber-Politics (Choucri, 2000). Cyber-Politics is the sphere where cyber and politics intermingle, producing new terms and concepts in the realm of politics.

Over the past two decades, the term 'cyber' has been attached to a wide range of concepts, giving rise to expressions such as cyber-terrorism, cyber-attacks, cyber warfare, cyber defence, and even cyber society. All of these terms revolve around the broader idea of cyberspace, which serves as the underlying environment in which digital interactions and activities occur. Historically, the roots of the term can be traced to the work of Norbert Wiener, who introduced the concept of cybernetics in his 1948 book Cybernetics: Or Control and Communication in the Animal and the Machine. Wiener's work emphasized the evolving relationship between humans and machines, arguing that systems of communication would gradually result in a new interactive environment. Consequently, that idea was later closely interlinked with what is now understood as cyberspace, the domain of Cyber-Politics (Wiener, 1961).

Cyberspace and human society are closely interconnected, since people remain the primary unit in shaping the digital atmosphere. In fact, the physical and software systems that structure cyberspace are designed, developed, and maintained by human beings. Therefore, humans also generate, exchange, and interpret information in line with their knowledge, interests, and objectives. In this context, cyberspace relies on and evolves through human interactions. Initially, as cyber took shape, it remained closely within a technical frame, and its relevance gradually expanded into the realm of politics and economics. What was once largely treated as an issue of *Low Politics* has increasingly acquired the significance of *High Politics* (Craig, 2010). The nature of Cyber-Politics shows a dual character. On one side, cyberspace supports global connectivity, innovation, and economic growth (Mbanaso & Dandaura, 2015). On the other side, it also creates opportunities for cyber threats, conflict, and the disruption of critical infrastructure. Due to this character, cyberspace is now seen as a distinct and important domain in global politics and modern warfare (Khan,2025)

Cyber diplomacy, compared to traditional approaches in political affairs, is a fairly recent development in International Relations (IR) (Sharma et al.,2026). As cyberspace has grown and cyber issues have become more relevant to international politics, diplomatic practices have gradually adapted to this digital environment. In this sense, Cyber-Politics can be described as 'who gets what, when, and how' in cyberspace. Understanding this requires looking at its origins and evolution and how it has become part of the modern global political sphere. At the same time, the rapid expansion of cyberspace has created new cyber threats with serious geopolitical and strategic impacts (Khan,2025). For this reason, cyber diplomacy has emerged as an important tool for states to manage threats, build cooperation, and adopt stable governance models in the digital arena.

The U.S. has played a key role in shaping diplomatic practices, and the cyber domain is no exception. Cyberspace is a strategic asset in today's security and warfare. The United States has recognised the need to actively engage with and manage this fast-changing space. As one of the world's most technologically advanced and networked nations, it integrates cyberspace into its foreign policy and national security strategies (Willers & Gjesvik, 2026). This reflects the close link between technological development, diplomacy, and strategic stability. Recently, during Donald J. Trump's administration, the U.S. made its approach to cyberspace more transparent, emphasizing cyber diplomacy as a tool to promote global cooperation, develop norms,

and secure national interests. In the Trump administration, the U.S. has adopted diplomatic initiatives intended to support stability in cyberspace, reduce cyber threats and the risk of disruption, and reinforce its leadership in shaping the governance and security of the cyber arena (Ashraf & Mirza, 2025).

Methodology

This research article adopts a qualitative, descriptive design grounded in a case study methodology. This approach provides an in-depth examination of the U.S.'s cyber diplomacy under the Donald J. Trump administration and incorporates both primary and secondary sources. Primary sources include official documents such as executive orders, legislation, gazettes, and publications from United States officials, while secondary sources consist of books, journal articles, reports, and academic theses.

A review of the existing literature on cyber diplomacy regarding the Trump administration reveals a gap. While American foreign policy under the Trump regime has been widely studied and an abundance of literature is available, research on cyber diplomacy remains limited. This study addresses that gap by exploring strategies, initiatives, and diplomatic efforts in cyberspace. It clarifies policy choices and highlights the evolving role of the United States under the Trump administration. The study focuses on two main research questions: how the U.S. approach to cyber diplomacy has changed over time, and what strategies the Trump administration used during its tenure. The goal is to analyze how effective U.S. policies have been in managing cyber threats, promoting international cooperation, and maintaining stability in cyberspace.

Theoretical Framework

The research study incorporated two major primary theoretical frameworks, neoliberalism and the theory of Technological Politics. These political theories provide an analytical foundation for exploring the interconnection between the Trump administration's policies and the technological aspects of cyberspace.

To contextualize the theoretical framework within the study, neoliberalism seeks to maintain international politics through peaceful and diplomatic efforts, leading to a world where state actors are interdependent. This approach aims to create a structure in which every state is better off, based on relative gains, through negotiations, consultation, and communication. It is therefore viewed that diplomacy is the best approach to maintaining peace and order in global politics. Similarly, cyber diplomacy is a nascent approach to bringing norms and stability to cyberspace.

The approach of the 45th president of the U.S., Donald J. Trump, reflected a clear neoliberal perspective on cyberspace. During his presidency, the administration emphasized the importance of cybersecurity, norms, and Cyber-Politics by strengthening U.S. infrastructure and engaging international actors, including the EU and global agencies. It also worked with the American legislative bodies to pass laws promoting cyber diplomacy, international cooperation, and the development of norms and legal frameworks in Cyber-Politics.

The Theory of Technological Politics was developed in the 1980s by Langdon Winner. In his seminal essay, Do Artifacts Have Politics? published by MIT Press in 1980, he argued that technological artifacts embody political dimensions. Winner's work highlights the intrinsic interconnection between technology and politics, asserting that neither can be fully understood in isolation from the other (Winner, 1980).

The Theory of Technological Politics involves three major dimensions: (1) Technological artefacts encompass a political function because political narratives and ideas can be projected through inscribed devices. This projection can work through a technological medium. A much more suitable example is the United States presidential campaign in 2015 and the use of Facebook (Meta) as a source to spread political ideas and narratives. 92) Technology artefacts embody a political function that further enhances the effectiveness of tech politics, either intentionally or unintentionally. The unintended consequences can be even more sophisticated, as they unfold meanings for the human imagination that were not even considered. (3) Hence, Winner's theory engages in the democratic process of shaping technological change.

The theory of technological politics, applied in this study, explains the intrinsic link between technology and politics, arguing that neither can be understood in isolation, especially in the digital era. Although cyberspace is technical in nature, it is central to contemporary politics. Within this framework, cyber diplomacy reflects the convergence of technological and political mechanisms in the evolving realm of Cyber-Politics.

Cyber threats and cyberspace are purely technical phenomena; however, politics operates on multiple layers, including war and geopolitics. The study seeks to encapsulate the theory of technological politics because cybersecurity, cyberspace, and politics cannot be considered separately. Similarly, the political realm, due to cyber warfare, can lead to enmity between states. It is therefore important to bring diplomacy to such an important domain as technology and politics. The notion of cyber diplomacy seeks to provide a comprehensive theoretical approach for peaceful coexistence between nations. Cyber diplomacy seeks to mitigate the technological threats posed by individuals or states by sharing knowledge and experience among states to avoid conflict and enmity. Cyber diplomacy seeks to bridge the technical and political domains for better cooperation among states.

Introduction to Cyber Diplomacy

Cyber diplomacy has emerged as a significant concept as major powers adapt their foreign policies to the realities of cyberspace. Recognising its growing importance, the United States of America incorporated cyber diplomacy into its public diplomacy framework in 2009 to safeguard and advance national interests in the digital domain (Andreas, 2015). In 2015, the European Council also emphasised its relevance in global politics (Draft Council Conclusions on Cyber Diplomacy, 2015). Over time, terms such as e-diplomacy, digital diplomacy, mass diplomacy, and Diplomacy 2.0 have often been used interchangeably with cyber diplomacy, which has generated conceptual ambiguity despite all referring to the same evolving practice.

Cyber diplomacy is defined by scholars Andre Barrinha and Thomas Renard as the use of diplomatic tools and functions to advance national interests in cyberspace, shaped by public diplomacy and broader geopolitical implications (Barrinha & Renard, 2017). In the present, the scope of cyber diplomacy has expanded to include influential private actors. For example, Tom Fletcher, a former British Ambassador, remarked on the power of influential individuals across a wide range of disciplines. He noted that Eric Schmidt, an American businessman, software engineer, and former CEO of Google, has a 'pulling power' that is complex and difficult for any state representative to match, and he considered such figures the 'new emperors.' This evolution highlights that cyber diplomacy is no longer only the domain of states. It now requires coordinated efforts from governments, international organizations, and influential private actors

(Spence, 2017). The term 'cyber diplomacy' was formally introduced by the European Union in its Strategic Framework for Cyberspace in 2015.

U.S. Approach Towards Cyberspace: Prior to 2016 Analysis

The United States' approach to cybersecurity has evolved over the past two decades. During the George W. Bush administration, cyberspace was largely in its embryonic stage. Nevertheless, Bush Jr. signed a National Security Presidential Directive authorising the use of America's cyber offensive capabilities against Iraq in 2002 (Graham, 2003). These cyber-based operations targeted Saddam Hussein's regime, and until then the United States had not fully leveraged its cyber potential against other major powers. As cybersecurity advisor to George Bush, Richard A. Clarke and Knake (2010) reflected at the end of his tenure: we have capabilities, we have organizations; we do not yet have an elaborated strategy, doctrine, [or] procedures. Compared with Bush, the Obama administration adopted an organised and forward-looking approach, placing cyberspace at the centre of the policy agenda and structuring cyber policy around five pillars: protection of cyberspace, threat identification and response, international engagement, critical infrastructure security, and public–private collaboration.

To further enhance his vision, the Obama administration introduced the 2009 *Cyberspace Policy Review*, aiming to strengthen leadership, reassess legal frameworks, and improve strategic competitiveness (White House, 2013). This approach was later followed by an Executive Order establishing the Cybersecurity Framework for Critical Infrastructure in 2013, which also focused on international cooperation and collaboration. These policies marked the first formal expression of U.S. engagement in cyberspace for peace and security (White House, 2013). However, despite national and international efforts, their full implementation remained limited (Malik, 2023). Beyond the 2015 U.S.–China cyber diplomacy initiatives, global engagement was relatively restrained (Rosenfeld, 2015). Even so, the Obama administration played a key role in bringing cybersecurity into mainstream foreign policy. This was done through executive orders, congressional actions, and public awareness campaigns, laying the groundwork for later administrations.

U.S. Cyber Diplomacy under the Donald J. Trump Administration

Donald J. Trump took office as the 45th President of the United States on January 20, 2017. His presidency is widely regarded as controversial, marked by persistent allegations of election hacking and foreign interference. These events, however, played a significant role in shaping the discourse around cyberspace and the emerging practice of cyber diplomacy. Despite the political turbulence, the Trump administration undertook significant measures to address the enigma of cyberspace through Executive Orders, Congressional legislation, and engagement with the international community for peaceful purposes, while simultaneously adopting certain offensive measures to advance American hegemony in the cyber realm and protect the U.S. economy and political system from further vulnerabilities.

Donald Trump's Executive Orders

On April 29, 2017, Donald Trump completed his first 100 days in the Oval Office as the President of the U.S. His administration has been the main focus of American media and public discourse across the globe, owing to policies that differed from those in American presidential history. The Trump withdrawal from the Trans-Pacific

Partnership, the nomination of a conservative judge to the Supreme Court, and the ban on entry from certain countries to the United States (Qiu, 2017) were notable developments. However, the realm of cyber and digital has been a focus for Trump from the very beginning. Furthermore, Trump appointed technocrats to shape cyberspace policy (Kurbalija, 2025). Doyle (2017) reported that President Trump remarked:

> Whether it is our government, organizations, associations, or businesses, we need to aggressively combat and stop cyberattacks. I will appoint a team to give me a plan within 90 days of taking office. The methods, tools, and tactics we use to keep America safe should not be a public discussion that will benefit those who seek to do us harm.

In 2017, a significant phase emerged when President Donald J. Trump issued the first Executive Order widely regarded as a firm approach to cybersecurity. While some cybersecurity pundits viewed it as a continuation of President Obama's cyber policy, others emphasised its statutory importance, noting that it addressed minor details and addressed shortcomings in previous frameworks. Consequently, on May 13, 2017, President Donald J. Trump signed Executive Order No. 13800 to quell cyber-attacks against the United States (Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 2017).

Executive Order 13800 set out strategies and guidelines to reduce cyber-attacks while promoting the development and coordination of information technology across federal agencies and private entities. The executive order involved multiple stakeholders and was structured into four major sections to address the complexities of cyberspace. The executive branch assumed responsibility for the protection of federal data, and agency heads were responsible for mitigating cyber risks. Agencies were also required to submit a risk management report within 90 days, and core officials, including the Secretary of Homeland Security and the Director of the Office of Management and Budget, were tasked with presenting a comprehensive cybersecurity plan within 60 days.

The order also highlighted the importance of securing reliable internet access, seen as essential for national social and economic development, and called for international collaboration in cybersecurity. To ensure implementation, the executive order defined key terms such as 'appropriate stakeholders,' 'information technology,' and 'network architecture' (Mitchell, 2020). Political pundits and analysts expected more traditional policies focused on geopolitics rather than a cyber-focused approach from the Trump administration; however, the executive order came unexpectedly within the first 100 days. The early introduction marked the Trump administration's recognition of cybersecurity as a central theme in American policy. Often regarded as one of the most comprehensive cybersecurity initiatives following the Obama framework, EO 13800 reflected the Trump administration's emphasis on homeland protection under the 'America First' vision. The order sought to address vulnerabilities that could be exploited through cyberattacks while requiring timely submission of reports and strategic roadmaps. Although primarily focused on domestic protection, it also underscored the importance of international engagement, framing cyber diplomacy as a key mechanism for collaboration, knowledge-sharing, and improved internet governance with the global community.

The executive order also emphasized a reliable and secure internet as a tool for social and economic prosperity and called for international collaboration in

cybersecurity. Furthermore, to implement the executive order effectively, it defined key terms such as 'appropriate stakeholders,' 'information technology,' and 'network architecture' (Mitchell, 2020). The executive order was introduced unexpectedly within Trump's first 100 days, as political pundits had expected the administration to prioritize traditional geopolitical priorities rather than a cyber-focused policy. Therefore, its early introduction highlighted Trump's recognition of cyberspace as a central policy concern. The executive order is often considered by analysts to be a more comprehensive initiative than the Obama framework. Executive Order 13800 reflected the Trump administration's emphasis on homeland protection under the 'America First' vision. It focused on addressing vulnerabilities that could be exploited through cyberattacks while requiring the timely submission of reports and strategic roadmaps. Although primarily focused on domestic protection, it also underscored the importance of international engagement, framing cyber diplomacy as a key mechanism for collaboration, knowledge-sharing, and improved internet governance with the global community.

President Trump issued Executive Order 13870 in 2019, titled 'America's Cybersecurity Workforce,' aimed at strengthening the country's cyber capabilities. The executive order highlighted the administration's consistent focus on cybersecurity, big data, and internet governance, as set out in earlier directives and the Presidential Management Agenda (The American Presidency Project, 2019). The rapid adaptation of executive orders reflected the administration's serious approach to Cyber-Politics and the protection of U.S. interests in cyberspace. Moreover, Executive Order 13870 framed the cybersecurity workforce as a strategic national asset, emphasising the need to bring experts capable of designing, operating, and managing cybersecurity structures to safeguard critical data networks and infrastructure. The executive order also introduced the 'President's Cup Cybersecurity' to encourage mobility among technocrats and specialists at the national level. This will also reinforce accountability to the executive branch, improve coordination, and enhance institutional capacity.

The Trump administration placed strong emphasis on expanding federal cybersecurity capabilities. It sought to improve coordination among government agencies and to increase public awareness. At the same time, it worked to strengthen partnerships with the private sector. The policy gave clear importance to protecting physical-cyber infrastructure, especially defence-related systems. In this way, the physical side of cyberspace was brought into more serious policy discussions. Within this framework, EO 13870 focused mainly on strengthening domestic capacity. In contrast, EO 13800 placed more emphasis on international cooperation and the peaceful use of cyberspace.

In May 2019, President Donald J. Trump issued Executive Order(EO) 13873, titled 'Securing the Information and Communications Technology and Services Supply Chain.' The order declared a national emergency in response to threats posed by foreign adversaries to the ICT supply chain. It authorised the Secretary of Commerce to block ICT-related transactions that could pose risks to national security. The order also called for the formation of a task force, comprising agency heads, to identify and manage vulnerabilities in critical infrastructure. In addition, the Secretary of Homeland Security was directed to assess entities and emerging technologies that might threaten national security. This included examining potential weaknesses and how such gaps could be exploited. EO 13873 reflected the administration's awareness of the evolving nature of cybersecurity challenges. It aimed to strengthen national resilience by addressing risks

linked to the global ICT supply chain. It also underscored that cyberspace remained a central concern in Trump's overall policy agenda.

In February 2020, President Trump signed Executive Order(EO) 13905, titled '*Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services.*' This order highlighted the importance of PNT services for both national security and critical infrastructure. It focused on addressing vulnerabilities in these systems, while also promoting their responsible use. The order encouraged both interagency coordination and international cooperation. It also required risk assessments and the development of policies to improve resilience (Federal Register, 2020). By combining policy efforts, cooperation, and risk management, EO 13905 underlined the strategic importance of protecting essential services in an increasingly connected world. It also reaffirmed that cyberspace remained a key priority for the administration.

Overall, Trump's executive orders on cybersecurity reflect a structured and balanced approach. They combine domestic capacity-building with the protection of national interests. EO 13800 laid the foundation by assigning accountability for federal-level cybersecurity reporting. This demonstrated an early recognition that cyberspace is now part of mainstream foreign policy. EO 13870 further developed this approach by focusing on the human dimension of cyber capabilities. It treated the cybersecurity workforce as a strategic asset. Programmes such as the 'President's Cup Cybersecurity' and efforts to encourage expert mobility suggest that the administration recognised the need for skilled personnel alongside strong institutions. At the same time, EO 13873 addressed weaknesses in the ICT supply chain. It highlighted that U.S. cybersecurity cannot be ensured in isolation from global networks.

EO 13905 further expanded this framework to include essential services like positioning, navigation, and timing systems. This reflected a broader and more systematic understanding of cyber resilience. The administration combined risk assessment with interagency coordination and also looked toward international cooperation. In this way, cyberspace was treated both as a domestic priority and as an area for strategic engagement at the global level. Taken together, these executive orders show a clear direction. They aimed to strengthen federal infrastructure and workforce, while also reducing risks linked to global ICT systems. At the same time, they reflect a practical and layered approach to cyber politics. Domestic security, technological capacity, and international responsibility were treated as connected parts of a single national strategy.

Congress Legislations Under the Trump Administration

The United States' approach under the Trump administration cannot be fully understood without considering the role of Congress. As Congress plays a vital role and, at times, cyberspace emerged as a central concern in American polity, sustained legislative attention was required. Under the Trump administration, Congress remained active in addressing and engaging with issues related to cyberspace. It is therefore important to examine the congressional approach during this period, as it provides critical, in-depth insight into how the United States shaped its approach to cyber diplomacy and integrated legislative support into its broader strategic framework.

The Cyber Diplomacy Act of 2017

The Cyber Diplomacy Act of 2017 was introduced with bipartisan support, sponsored by House Homeland Security Committee Chairman Mike McCaul (R-Texas), House Foreign Affairs Committee Chairman Ed Royce (R-California), and Ranking Member

Eliot Engel (D-New York) (House Committee on Foreign Affairs, 2025). The bill was formally introduced on September 14, 2017, and later reported out of the House Foreign Affairs Committee by voice vote on November 15, 2017. The bill's introduction highlighted Congress's growing attention to cyberspace as a strategic domain within U.S. foreign policy, signalling a commitment to formalise legislative oversight and engagement in cyber diplomacy.

The Cyber Diplomacy Act's objective was to strengthen American engagement in cyberspace. Through this bill, the U.S. would promote an open, interoperable, secure, and reliable digital environment, supporting global trade, commerce, and communication (Kerry, 2017). Additionally, the Act formally recognized cyberspace as a critical domain for both national security and economic development. It included eleven congressional findings that underscored the growing threat of cyberattacks, the importance of international cooperation, the protection of human rights online, and the need for a coordinated and comprehensive approach to cyber diplomacy. The Act also highlighted the legislation for the U.S. role in shaping international norms and standards for cyberspace. It introduced a reporting mechanism that required annual reports to Congress on emerging cyber threats, opportunities, and relevant executive agreements. This can be seen as a legislative effort to systematically bring cyber issues into broader foreign policy decision-making.

The Cyber Diplomacy Act also proposed the creation of a Bureau of International Cyberspace Policy within the Department of State. This bureau was intended to lead U.S. diplomatic efforts and promote global norms in the area of cyber politics. The Act further authorized a Cyber Diplomacy Office, which was responsible for engaging international stakeholders. It also required the President to submit annual reports on cybersecurity capacity-building efforts in developing countries. In addition, the Act allocated 10 million USD for fiscal year 2018, with provisions for further funding in the following years. Overall, the Act served as an important step in bringing cyber politics into mainstream American policymaking. It is widely considered the first U.S. legislation to formally use the term 'Cyber Diplomacy,' reflecting the Trump administration's attempt to integrate cybersecurity into both legislative and diplomatic domains.

The Cyber Diplomacy Act of 2017 represents a deliberate effort by Congress to institutionalize U.S. engagement in cyberspace. Over time, cyber issues had become central to both national security and foreign policy, especially in relation to protecting national interests. The establishment of the Bureau, along with reporting mechanisms and dedicated funding, further strengthened this institutionalization. It helped shift cybersecurity from a technical or temporary issue to a more sustained strategic and policy priority. The Act's focus on shaping international norms, engaging global stakeholders, and supporting capacity-building in developing countries shows that Congress viewed cyberspace as a global common. Moreover, its bipartisan support and the formal use of the term 'Cyber Diplomacy' indicate a clear effort to turn abstract cyber challenges into practical policy frameworks, while also linking executive initiatives with legislative oversight.

Cyber Diplomacy Act of 2019

To counter the rising threats of cyberattacks, the Cyber Diplomacy Act of 2019 was introduced on January 23, 2019. The Act (H.R. 739) was formally introduced by Representative Michael McCaul. The bill proposed creating the Office of International Cyberspace Policy within the Department of State, led by a Senate-confirmed

ambassador, to establish a formal diplomatic structure to manage international cybersecurity challenges (Michael, 2019). In a rapidly evolving digital environment, the bill underscored the urgent need to enhance U.S. diplomatic capacity and position the United States as a proactive leader in shaping international cyber norms. At the same time, by institutionalizing cyber diplomacy at a senior level, the Act signalled that effective engagement in cyberspace requires not only technical expertise but also coordinated policy leadership and international cooperation.

Although the Act was co-sponsored by 29 members of Congress and reported out of the House Foreign Affairs Committee by voice vote in March 2019, it was not considered by the full House before the end of the 116th Congress (Polit, 2021). Despite this, the bill fits within a broader legislative trajectory, especially when viewed alongside earlier efforts and the redrafted 2017 version of the Cyber Diplomacy Act. In this context, the Trump administration played a significant role. President Donald J. Trump elevated cybersecurity to a central concern in both domestic and international policy by combining executive orders with active engagement with Congress. He pushed for greater recognition of cyberspace within legislative discussions and executive initiatives. H.R. 739 reflects both the ambitions and the limitations of U.S. legislative action on cyber diplomacy (Michael, 2019). While the bill received bipartisan support and committee approval, it did not reach the House floor. At the same time, the administration's use of executive orders in parallel suggests a more calculated approach. By shaping policy at the executive level while also encouraging legislative formalization, the administration followed a dual-track strategy in Cyber-Politics.

International Engagement in Cyberspace

In 2020, the Donald J. Trump administration formalized the U.S.-Australia Cyber Cooperation through the signing of a memorandum of understanding. Within the context of bilateral relations, this represented a significant advancement in the field of cyber diplomacy. As the distinctions between traditional borders and cyberspace have become increasingly blurred in modern warfare, both nations acknowledged the importance of collaboration in addressing emerging cyber threats and safeguarding critical infrastructure (U.S. Department of War, 2020). Furthermore, the partnership, supported by government agencies, technocrats, and the private sector, adopted a holistic approach to transnational cyber risks; effective cyber diplomacy, therefore, depends not only on technological measures but also on mutual trust, coordinated governance, and a proactive stance in shaping norms and resilience within the digital domain (Department of Foreign Affairs and Trade, 2020). The core pillars of the America-Australian partnership encompass innovation, norm-building, and cyber collaboration (Williams, 2020). Additionally, as technological advancements proceed rapidly and cyber threats become increasingly lethal, both nations concurred on the necessity of a defense system capable of responding to emerging adversarial tactics.

Under the leadership of Donald J. Trump, a new dimension was introduced into U.S.-UK cyber relations, with the United States achieving its geopolitical objectives through cyber diplomacy. Huawei emerged as a leading developer of 5G infrastructure, which remained a point of contention for American leadership and raised concerns regarding Huawei's alleged connections to Chinese state involvement in espionage and cyber exploitation (Kharpal, 2020). However, mounting geopolitical pressure ultimately compelled London to rescind its understanding with Huawei and mandate the removal of Huawei equipment by 2027 (Sabbagh, 2020). This development underscored the approach of the Trump administration, which utilized assertive cyber

diplomacy complemented by executive actions and legislative measures. Through this approach, the United States maintained its dominance in the cyberspace arena.

The U.S. approach to cyber diplomacy under the Trump administration is characterized by an assertive, results-oriented engagement in the international digital sphere. Its policies comprise a combination of multiple executive orders issued in a timely manner, targeted legislative involvement, and strategic partnerships with allied states. Consequently, the Trump administration elevated cyber politics to a central aspect of U.S. foreign policy. These policies do not reflect a mere abstract commitment to multilateralism in cyberspace; rather, they exemplify pragmatic exertion of power aimed at shaping norms, developing standards, and fostering collaboration with allied nations to uphold American supremacy in cyber diplomacy.

Conclusion

Conceptually and analytically, cyber diplomacy remains an embryonic field despite its growing significance. Limited scholarly attention and the absence of a universally accepted definition indicate considerable work still required to understand the nascent stage of cyber diplomacy within Cyber-Politics. Furthermore, current academic and policy discussions tend to emphasise the technical aspects of cyberspace, often neglecting the political, strategic, and diplomatic dimensions essential for comprehensive engagement. This narrow focus fails to address the complexity of state approaches and the rapidly evolving digital landscape. Consequently, there is a notable gap in understanding how cyberspace intersects with broader international political contexts. There is a clear need for integrative approaches that combine technological considerations with political analysis to advance the conceptual development of cyber diplomacy and promote broader application in global peace and stability.

In this context, the Donald J. Trump administration's approach to foreign policy presents a valuable case study, given the developments during his leadership. The Trump administration's stance on Cyber-Politics was markedly antagonistic, characterised by policies such as a trade war with China, controversial approaches to climate change, pressure on allied partners to contribute funding to NATO, and reductions in funding for global initiatives, including the WHO. The administration's interest in cyberspace was evident in the issuance of significant executive orders within the first 100 days of the first term, reflecting an early recognition of cyberspace's importance and its integration into US foreign policy. Subsequent executive orders and congressional engagement helped embed cyber diplomacy within the institutional framework of U.S. foreign policy. Despite broader tensions with European partners, cooperation with NATO members in cyberspace remained a notable area of collaboration.

The Trump administration's cybersecurity strategy aimed to promote stability, security, and resilience within cyberspace. The administration prioritised strengthening American cyber resilience through institutional reforms and emphasised the protection of rights and critical infrastructure, prioritising the American people over technology alone. Given the complex and multidimensional nature of cyber threats, responses needed to be coordinated across institutional, political, and diplomatic spheres. Legislative initiatives during this period reflected a collective effort to formalise cyber diplomacy under Trump's leadership. Nevertheless, divergent interests and rapid technological advancements complicated consensus-building, often preventing the formulation of a coherent policy.

Overall, the Trump administration's approach to cyberspace was characterised by careful policy and strategic planning, despite a broader tendency towards unilateralism in foreign policy. Cyber diplomacy transitioned from a peripheral concern to a core element of U.S. governance and foreign policy, driven by executive orders, legislative actions, and international partnerships. Moreover, Trump sought to elevate cyberspace beyond its technical or peripheral status within foreign policy by establishing norms, fostering strategic competition, and developing standards for cyber governance, aiming to enhance peace and stability through cyber diplomacy.

Conflict of Interest: The author declares no conflict of interest.

Funding: This research received no external funding.

References

Ashraf, N., & Mirza, M. N. (2025). Principles, Norms, and Strategies of the US Global Cyberspace Governance. *Margalla Papers*, *29*(1), 41-54.

The American Presidency Project. (2019). *Executive Order 13870—America's Cybersecurity Workforce*. https://www.presidency.ucsb.edu/documents/executive-order-13870-americas-cybersecurity-workforce

Andreas, S. (2015). *Digital Diplomacy: Conversations on Innovations in Foreign Policy*. Diplo Resource (Maryland: Rowman & Littlefield Publishers, 2015). https://www.diplomacy.edu/resource/digital-diplomacy-conversations-on-innovations-in-foreign-policy/

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The Making of an International Society in the Digital Age. *Global Affairs*, *3*(4-5), 353-364. https://doi.org/10.1080/23340460.2017.1414924

Choucri, N. (2000). Introduction: CyberPolitics in international relations. *International Political Science Review*, *21*(3), 243-263. https://doi.org/10.1177/0192512100213001

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

Craig, D. M. (2010). High Politics and the New Political History. *The Historical Journal*, *53*(2), 453-475.

Department of Foreign Affairs and Trade. (2020). *Australia's International Cyber Engagement Strategy 2020*. https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf

Doyle, M. (2017, January 6). *Trump finally says Russia was behind cyberattacks, but also criticizes intelligence agencies*. *Los Angeles Times*. https://www.latimes.com/opinion/opinion-la/la-ol-trump-intelligence-20170106-story.html

Draft Council Conclusions on Cyber Diplomacy. (2015). The Council of European Union. https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Federal Register. (2020, February 18). *Strengthening national resilience through responsible use of positioning, navigation, and timing services*. https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

Graham, B. (2003, February 7). *"Bush Orders Guidelines for Cyber-Warfare,"*. The Washington Post. https://www.washingtonpost.com/archive/politics/2003/02/07/bush-orders-guidelines-for-cyber warfare/dd8b4a18-140c-4690-88a5-0041d4ce1b1c/

House Committee on Foreign Affairs. (2025, May 30). *H.R. 3776, Cyber Diplomacy Act of 2017*. https://foreignaffairs.house.gov/committee-activity/bills/h-r-3776-cyber-diplomacy-act-2017

Kerry, C. F. (2017, December 4). *Cyber Diplomacy Act Gives Cyber the Importance Its Needs at the State Department*. Brookings. https://www.brookings.edu/articles/cyber-diplomacy-act-gives-cyber-the-importance-it-needs-at-the-state-department/

Kharpal, A. (2020, January 28). *Huawei allowed limited access to UK's 5G networks as Britain defies US pressure*. CNBC. https://www.cnbc.com/2020/01/28/huawei-uk-chinese-firm-allowed-limited-access-to-uk-5g-network.html

Khan, Z. F. (2025). Cyber Warfare and International Security: A New Geopolitical Frontier. *The Critical Review of Social Sciences Studies*, *3*(2), 513-527.

Kurbalija, J. (2025, May 15). *Tech continuity in President Trump's first 100 days*. Diplo. https://www.diplomacy.edu/blog/tech-continuity-in-president-trumps-first-100-days/

Malik, M. B. (2023). *Cyber Threats and International Relations Post 9/11: An Analysis of US. -China Cyber Politics.* (Ph.D. Dissertation) Quaid-i-Azam University, Islamabad.

Mbanaso, U. M., & Dandaura, E. S. (2015). The Cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering*, *17*(3), 17-24.

Michael, T. (2019, January 24). *H.R.739 — 116th Congress (2019-2020)*. Congress Gov. https://www.congress.gov/bill/116th-congress/house-bill/739/text

Mitchell, C. (2020). *Cyber in the age of Trump: The unraveling of America's national security policy* (1st ed.). Rowman & Littlefield Publishers.

Polit, K. (2021). *Cyber Diplomacy Act Reintroduced in the House*. Federal Technology News, Research & Events | MeriTalk. https://meritalk.com/articles/cyber-diplomacy-act-reintroduced-in-the-house/

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (2017). The White House. https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

Qiu, L. (2017). Fact-Checking President Trump Through His First 100 Days. *New York Times*. https://www.nytimes.com/2017/04/30/us/politics/fact-check-trump-100-days.html

Rosenfeld, E. (2015, September 25). *US-China agree to not conduct cybertheft of intellectual property*. CNBC. https://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html

Sabbagh, D. (2020, July 13). *What is Huawei and why is its role in UK's 5G so controversial?* The Guardian. https://www.theguardian.com/technology/2020/jul/13/what-is-huawei-and-why-role-in-uk-5g-so-controversial

Spence, J. (2017). Naked diplomacy: Power and statecraft in the digital age and the future of diplomacy. *International Affairs*, *93*(4), 973-975. https://doi.org/10.1093/ia/iix126

Sharma, V., CR, R. K., & Bindu, G. H. (2026). *Cyber Diplomacy: A New Era of International Relations*. Vaagai International Publishing House.

U.S. Department of War. (2020, December 4). *U.S., Australia Sign Agreement to Develop Virtual Training Range*. https://www.war.gov/News/News-Stories/Article/Article/2432955/us-australia-sign-agreement-to-develop-virtual-training-range/

White House. (2013). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (pp. 2-3). Federation of American Scientists. https://irp.fas.org/eprint/cyber-review.pdf

Wiener, N. (1961). *Cybernetics or control and communication in the animal and the machine*. MIT Press. https://mitpress.mit.edu/9780262537841/cybernetics-or-control-and communication-in-the-animal-and-the-machine/

Williams, B. K. (2020, September 16). *An Opportunity for Strengthening U.S.-Australian Cyber Cooperation*. Lawfare. https://www.lawfaremedia.org/article/opportunity-strengthening-us-australian-cyber-cooperation

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121-36. https://www.jstor.org/stable/20024652

Willers, J. O., & Gjesvik, L. (2026). Diplomacy in the age of expertise: The case of cyber diplomacy. *International Affairs*, iiaf271.