PRINCIPLES, NORMS AND STRATEGIES OF THE US GLOBAL CYBERSPACE GOVERNANCE

Nageen Ashraf and Muhammad Nadeem Mirza [*]

Abstract

This study examines the United States' (US) approach to global cyber governance, including the principles, strategies, and norms the US intends to promote in cyberspace. This also discusses why the US is unwilling to share cyberspace governance with other great powers. While utilizing the official policies and strategies of the US as primary sources, this study identifies that the core principles of US cyber governance encompass a free and open internet, a multi-stakeholder approach, collaboration with allies, and maintaining a stable and secure digital landscape. However, it is criticised for its approach to data privacy, the Internet Corporation for Assigned Names and Numbers (ICANN) control, mass surveillance programs against foes and allies, and its disagreement with other states on cyberspace governance.

Keywords: Cyber World Order, Cyber Governance, Cyber Norms, Cyber Deterrence, Cyber Offence, Surveillance Programmes, Data Privacy.

Introduction

Since its advent, the internet has been mainly under the influence and control of the US. Long before the development of the Internet Corporation for Assigned Names and Numbers (ICANN) and the Advanced Research Projects Agency Network (ARPANET) – the predecessors of the modern internet – the role of assigning names and numbers to the internet was performed by John Postel, an American. However, as the internet began to proliferate, it became increasingly complex for an individual to accomplish this task.[1] He later played a role in the development of ARPANET. The predecessor and successor of the modern internet were, thus, developed by the US. Later, international pressure and the proliferation of the internet started debate about the governance of the internet, especially after the Snowden leaks.[2]

Since the internet is not unified and contains a complex web of networks connecting millions of computers worldwide, its governance becomes more intricate and debatable. This raises questions of the US approach to cyber governance amidst criticism regarding manipulation through ICANN and mass surveillance programmes against foes and allies alike. In this regard, this research paper delves into the early

[*]Nageen Ashraf is a Researcher at the Islamabad Policy Research Institute (IPRI), Islamabad. Her ORCID is 0009-0003-5255-9519. Dr Muhammad Nadeem Mirza is Faculty Member at the School of Politics and International Relations (SPIR), Quaid-i-Azam University, Islamabad. His ORCID is 0000-0002-2196-9174. The author(s) can be reached at nageenashraf13@gmail.com.

cybersecurity policies and strategies of the US that indicate the US views, perceptions, and norms about cyberspace that, in turn, shape its approach towards cyber governance at the international level.

On the other hand, China has consistently challenged the American preponderant position in cyberspace management. Competition has thus ensued, in which both the great powers are vying to promote their version of the cyber world order based on their interests, norms, and ideologies. Several issues have been at the core of their competition and debate, such as cyberterrorism, consumer protection laws which are inadequately defined, computer viruses and cyberattacks, allegation of technology theft through cyber means, spamming, domain name disputes, trademark violations, copyright infringements, privacy incursions, identity theft, online fraud, and the list goes on.[3] These issues have converged on one key question: how to manage cyberspace and whose version of the cyber world order should dominate.

While limiting its scope, this study details US perceptions of the cyber world order and global cyberspace governance. It raises the following questions. What are the contours of an American-supported global cyberspace governance model? What principles, strategies, and norms does the US intend to promote in the cyberspace domain? And why is the US not willing to share cyberspace governance with other great powers? This exploratory study employs a qualitative content analysis methodology to answer the questions using US documents, including national and international cyber policies, as well as other relevant sources.

US Cyber Security Policies and Strategies - International Strategy for Cyberspace 2011 and National Cyber Security Strategy 2023

International Strategy for Cyberspace, released in 2011, denotes the US commitment to pursue international collaboration. It maintains that in cyberspace, international collaboration is more than the best practice; it is a first principle.[4] It also maintains that an effective response to cyber incidents is possible only through collaboration between the private and public sectors, as well as cooperation between states at the international level. Further underscoring the significance of collaboration, the strategy highlights the importance of cyber diplomacy and strengthening partnerships between states, which is also crucial for developing cyber norms among states. The development of cyberspace will ensure responsible state behaviour.[5] Similarly, the US National Cybersecurity Strategy 2023 reiterates the norms that the US promotes internationally regarding internet governance.[6]

Free and Open Internet

The strategy emphasizes the promotion of an "open, interoperable, secure, and reliable" communication network, stating that the free flow of information can only be made possible through interoperability, a principle acknowledged by 174 states in the Tunis Commitment of the World Summit on the Information Society.[7] The

strategy also highlights key constituents of internet governance, including the promotion of an innovative and open internet, the maintenance of a stable and secure cyber environment, the adoption of a multi-stakeholder approach in governing the internet, and the enhancement of innovative capabilities in cyberspace.[8] Similarly, the Cyber Security Strategy of 2023 greatly emphasises the internet's openness; the word "open" has been associated with the internet 10 times in the official document, calling for an "open, free, global, interoperable, reliable, and secure Internet."[9] It is also noteworthy that the US considers opaque internet practices a threat to a stable cyber environment and a breach of individual rights.

Multi-Stakeholder Governance

While asserting a need to keep the digital landscape secure and stable, the strategy highlights that it can be best ensured by acknowledging the role of diverse stakeholders.[10] It adds that the multi-stakeholder organisations have played a crucial role in making the internet a landmark success; therefore, the US will continue to support forums that acknowledge the role of multiple stakeholders and public-private partnerships in governing the internet and cyberspace.[11] These principles align with the US idea of cyber governance at the international level.

The idea of a public-private partnership and a multi-stakeholder approach has also been emphasized in the 2023 strategy document. It states that the defence of the digital ecosystem can only be ensured if the industry collaborates with the government to overcome cyber threats and cyber incidents. Deep and enduring collaboration between stakeholders across our digital ecosystem will be the foundation upon which we make it more inherently defensible, resilient, and aligned with US values.[12] In an attempt to enhance collaboration, the strategy states five essential steps which include: (1) the defence of critical infrastructure, (2) disruption of threat actors, (3) shaping market forces to drive resilience and security, (4) forging international partnerships to pursue shared goals, (5) investing in a resilient future.[13] The document also acknowledges that the US will collaborate with various stakeholders, including consumer groups, professional societies, academic institutions, international allies, and industry leaders, to ensure the security of modern technologies and protect national security.

International Collaboration

Regarding collaboration with allies, the 2023 strategy emphasizes that the US has worked with allies and partners from around the globe to mitigate cyber threats and incidents, and it will continue to do so in the future to enhance capacity building in the digital space. The document noted that the objectives of such a collaboration are: (1) to build a resilient digital ecosystem, (2) to strengthen cyber norms, (3) to hold states accountable for irresponsible behaviour in the digital domain, (4) and the disruption of networks that criminals use for cyber-attacks throughout the globe.[14]

Interestingly, while the strategy advocates for collaboration at both the domestic and international levels, it also maintains that the norms and actions of China, Russia, Iran, and North Korea pose a serious threat to the principles of internet governance promoted by the US. The strategy refers to them as malicious actors.[15]

In addition to the US 2011 and 2023 cyber strategy documents, the US State Department's Cyberspace and Digital Economy Policy and the US Department of Homeland Security's International Engagement Strategy are other related policies.[16]

Principles of the US Cyber Governance Model

Based on the above strategy documents and other available reports, the following five principles of US cyber governance can be discerned:

- **Internet Freedom**—Internet freedom (free, open, and accessible to all) is one of the key constituents of US 21st-century foreign policy doctrines.[17]
- **Human Rights Protection in Cyberspace** - The US considers cyberspace abuse a threat to the civil liberty of its citizens and encourages efforts to mitigate such abuse.[18]
- **Multi-stakeholder Internet Governance**—A multi-stakeholder approach is necessary for the US because it ensures an open, secure, and resilient internet, broadening its horizons by involving governments, technical experts, and civil society.[19]
- **Collaboration with Partners**—The US believes states should adopt information-sharing practices to develop cyber norms for cooperation in internet governance. Information-sharing agreements and Memoranda of Understanding can enhance cyber collaboration. By sharing information, states can improve their cybersecurity and more effectively mitigate cyber threats.[20]
- **Digital Security and Stability** - According to the US, network stability is essential for global prosperity, and the security of critical networks is key to economic, political, and social well-being. Therefore, the US aims to foster digital stability by propagating cyber norms.

US Cyber Deterrence and Cyber Offence Capabilities

The US is promoting cyber governance norms at both the domestic and international levels, preparing for cyber offense and cyber deterrence, and strengthening its capabilities for both cyberattack and cyber defense. As far as deterrence is concerned, scholars have identified three stages of deterrence thinking. First, in the times of conventional weapons, second, during the era of nuclear weapons, and third, in the era of cyber weapons.[21] The strategies of deterrence and preemption have proven significant for the US during the Cold War and post-9/11 era.

Likewise, the US is pursuing both these strategies to win a cyber war. However, considering the nature of cyberspace, it is pertinent to note that deterrence alone is insufficient to prevent a disruptive cyberattack from an adversary; instead, deterrence accompanied by preemption can help mitigate the growing cyber threats.[22] In contemporary times, cyber deterrence can have different meanings: (1) to deter a military attack using military cyber means, (2) to deter a military cyberattack using military means, (3) to deter a military cyberattack using military cyber means.[23]

Additionally, the types of cyber deterrence are similar to traditional deterrence, which include deterrence through denial, deterrence through punishment, deterrence through de-legitimization, and deterrence through entanglement. However, some scholars have argued that concepts such as deterrence, in the form of mutual assured destruction, are outdated and require modification when applied to cyberspace, considering this arena's unique contingencies.[24] The United States has been promoting its cyber norms related to 'responsible state behaviour in cyberspace.' It has also been actively engaged in cyber deterrence against the states showing irresponsible behaviour, as defined by the US.

The US acknowledges the role of cyberspace and cyber warfare in the military domain. One government agency that the US thinks should have control of the internet is its military. Therefore, military doctrines have developed, including the National Military Strategy for Cyberspace Operations (NMS-CO), the DoD Cyber Strategy, and the Cyberspace Operations Concept Capability Plan 2016-2028.[25] These strategies outline key principles for navigating cyberspace in the military context.

Cyber Offence through Persistent Engagement

The US Department of Defence has released documents calling for strengthening cyber deterrence and capacity building. These documents include the DoD Cyber Strategy,[26] National Strategy to Secure Cyberspace,[27] National Strategy for Homeland Security,[28] and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.[29] Regarding cyber deterrence, it has adopted the "persistent engagement", thus shifting the US cyber posture from reactive to proactive.[30] In 2018, the US Cyber Command released a vision document, "Achieve and Maintain Cyberspace Superiority," which states that persistent engagement requires consistent defensive and offensive cyber operations.[31]

The primary goal of persistent engagement is to deter adversaries from launching cyberattacks against the US, highlighting the costs they would face. It can also be regarded as a preventive defence in cyberspace.[32] The roots of this concept can be traced back to the idea of "offence-persistent strategic environment" opined by Richard Harknett and Emily Goldman.[33] To strengthen cyber deterrence, the US has established a team of cyber warriors to counter cyberattacks directed at the US. As highlighted by one of the authors, this team is not a defensive team at all. Instead, this

warrior team is an offensive defence team that the state uses in case of a cyberattack from an adversary.[34]

Cyber Capabilities

Considering the importance of cyber warfare, the US has encouraged the development of cyber weapons for defensive and offensive purposes. The Department of Defence Cyber Strategy of 2015 explicitly states that the state can control or block the escalation of any conflict through network strategies.[35] Later that year, the US also displayed ambitions to conduct network attacks against its alleged targets as a right to self-defence. In this regard, it retaliated against Chinese network attacks by breaching China's firewall through complex network operations.[36] The International Strategy for Cyberspace also regards the "Right of Self-Defence" as a basis of cyber norms. According to this right, states have an inherent right to self-defence in response to acts in cyberspace that trigger aggression and violence.[37] The US has adopted integrated deterrence to deter attacks from opponents in all domains, including cyberspace.[38] Analogous to the Nuclear Posture Review (NPR) of the Trump Administration, Biden's NPR also emphasises the precarious and destructive nature of cyberattacks, which can undermine the US national security. Moreover, it has developed various viruses and worms that can be used as powerful cyberweapons against adversaries.[39] The US is believed to have already been using such attacks against its potential adversaries.[40]

In the National Security Strategy 2022, Biden Administration pointed out that since advanced technologies are changing the nature and dynamics of warfare, the US is "investing in a range of advanced technologies including applications in the cyber and space domains, missile defeat capabilities, trusted artificial intelligence, and quantum systems, while deploying new capabilities to the battlefield in a timely manner".[41] This indicates the US focus on incorporating cyber technologies in the military domain. Additionally, the 2023 Cyber strategy also asserts "to make sure we have the right cyber capabilities, cyber security, and cyber resilience to help deter conflict and to fight and win if deterrence fails". [42]

Cyber Diplomacy and Norms

Cyber diplomacy refers to the application of diplomatic tools in the digital domain to promote a broader diplomatic agenda, managing and mitigating problems, issues, and threats related to cyberspace.[43] Some scholars also employ digital diplomacy; however, the two terms differ in their definitions. Riordan clarifies that digital diplomacy refers to the use of digital techniques and tools in diplomacy, whereas cyber diplomacy involves the application of diplomatic tools to resolve issues in cyberspace.[44] There are several key components of cyber diplomacy; these elements include (1) engaging with other states at a multilateral level to build strategic partnerships in cyberspace, (2) enhancing cooperation, capacity building, incident response, and collective action in cyberspace through collaboration, (3) building consensus for the stability of cyberspace at international level and advancing strategic

policy and (4) cyber deterrence.[45] Through its policies and strategies, the US has been pursuing cyber diplomacy and enhancing international collaboration.

US Engagement at the International Level

The US has signed multiple cyber agreements to promote digital cooperation and to encourage collaboration. From the beginning of the 21st century, it maintained a collaborative approach in cyberspace. In this regard, successive administrations made efforts to enhance cyber diplomacy. The National Strategy to Secure Cyberspace in 2003 identified three core strategic objectives of the US: (1) to protect critical infrastructures of the US from potential cyberattacks, (2) to minimise the recovery time and damage done by cyberattacks, (3) and to reduce the vulnerability to cyberattacks at the national level.[46] The US prioritized establishing National Security and International Cyberspace Security Cooperation to meet these motives and improve international response and management of cyber incidents.[47]

Advocacy for Cyber Norms

The US has repeatedly called for the establishment of "cyber-norms". The 2011 International Strategy for Cyberspace asserts that developing cyber norms is crucial for effective internet governance. This is because norms shape the behaviour of states in times of peace and conflict.[48] Norms have played a vital role in promoting shared understanding and stability in other international domains. Likewise, norms are essential for the digital domain. In this regard, the document asserts that developing cyber norms does not necessitate the creation of new international laws in cyberspace; instead, the same norms that states have been following in their interactions with each other also apply to the cyber domain.[49] The 2023 National Cybersecurity Strategy also calls for collaboration between states to develop cyber norms that govern responsible state behaviour.[50] One of the significant reasons for promoting cyber norms is to ensure the stability of the digital ecosystem, as the International Strategy for Cyberspace asserts that states have tried to exercise national power through cyberspace. Therefore, norms will help guide states' behaviour in cyberspace, thus ensuring a stable and secure digital environment.

Protection of Critical Infrastructure (CI)

Protecting critical infrastructure is an integral part of any state's national security. ICT control of critical infrastructure may be compromised, allowing hackers to access personal data, financial assets, or intellectual property.[51] Important sectors that form the backbone of a state's economy include health, finance, energy, defense, telecommunications, and others. In today's world, infrastructures in one state are also interconnected, which means that if one sector is attacked, it may trigger a chain of issues in other sectors of infrastructure.[52] The US raised the issue of interconnectedness and its consequences in 1988 through Presidential Decision Directive No. 63. The directive clearly stated that the economic and national security

of US citizens depended on critical infrastructures and the information systems responsible for their proper operation.[53] It highlights that at the domestic level, the US is committed to protecting its critical infrastructure. Through this step, the US acknowledges the role of public and private actors in cyberspace and develops the norm of protecting such infrastructures. The US national cybersecurity strategy puts the defence of critical infrastructures as one of the key pillars of digital cooperation.

The US has made many efforts to protect its CI. Some of these efforts include the establishment of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to address the resilience and protection of various sectors. Furthermore, establishing the Protected Critical Infrastructure Information (PCII) program also signifies its commitment to protecting its critical infrastructures.[54] In the National Security Strategy, the US maintains that its infrastructure is highly dependent on cyberspace. Russia and some other states have attempted to conduct disruptive cyberattacks against the US critical infrastructures. The US has made efforts to secure these CIs by expanding law enforcement cooperation, launching innovative partnerships with allies and partners, countering illegal use of cryptocurrency for cybercrimes, and denying sanctuary to cybercriminals.[55]

Protecting critical infrastructure is also crucial for the US to ensure economic and national stability. It underscores US advocacy for multi-stakeholders in governance, where the US calls for cooperation and collaboration to protect cyberspace. Providing the resilience and protection of critical infrastructures in the US calls for a stable cyber environment and a stable cyber world where transparency, security, safety, and openness prevail. Thus, protecting critical infrastructure is the cornerstone of the United States' internet governance, emphasizing inclusivity, security, and collaboration as significant constituents in shaping the cyber world order.

All in all, the US commitment to protect its critical infrastructures aligns with its perception of the cyber world order and cyber governance in three ways; (1) because of advocacy for a multi-stakeholder approach in internet governance, (2) through its advocacy for the stable and secure cyber environment, (3) and because of its emphasis on collaboration between multiple actors. Ensuring the security and safety of critical infrastructures also emphasises the importance of these practices and norms at the international level.

Challenges and Criticism

The US Approach to Data Privacy Regulations

The US has been under scrutiny due to concerns about individual privacy. Concerns were further exacerbated in 2016 when a US court ordered Apple to bypass the security features of a mobile phone used by one of the terrorists responsible for the San Bernardino shootings. However, Apple refused to do so as it considered such a breach a violation of an individual's privacy, which can have far-reaching

consequences.[56] Nonetheless, the incident raised serious concerns about privacy and data breaches. This incident also raised concerns about the norm of cyber espionage, which contrasts with the portrayal of "responsible state behaviour" in cyberspace advocated by the US and its allies.[57] The US has used its internet firms to exercise extraterritorial powers in cyberspace and the internet. Microsoft, Facebook, Google, Apple, and Yahoo have helped the US achieve its surveillance objectives through these platforms. As Snowden revealed, the US National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) sought Microsoft's assistance to access encrypted information on email and cloud storage. It was also alleged that the NSA had direct access to the systems of many of these firms, further highlighting the violation of citizens' privacy.[58] A free and open internet, managed by the US, thus remained a tool to access any personal information of anyone living anywhere in the world.

Criticism of the Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN remained a highly criticised institution. The criticism includes the insufficient authority of governments within the organisation, its ineffectiveness in incorporating civil society, questions about the legitimacy of the organisation, sometimes excessive and unnecessary government oversight, the greater influence of the US, and the relationship between ICANN and the US government.[59] Critics also argue that even the development of Internet Governance Forum (IGF) was not an effort to promote multi-stakeholders; instead, its development was just a compromise which resulted from a standoff over governmental and UN calls for the diminishment of certain administrative functions (which the US was carrying out) and the US resistance to these recommendations.

Thus, even though IGF is claimed to be a platform for the dialogue on internet policy, these dialogues are merely deliberations about internet policy and, in practice, do not influence the policy-making in internet governance.[60] Another critic claims that, as an emblem of the multi-stakeholder model, the IGF's hierarchical structure under UN leadership does not strike the correct balance with its democratic ambitions for multi-stakeholders. Moreover, it cannot contribute to the policymaking of internet governance.[61] Hoffman asserts that ICANN's organisational structure has created unintended divisions and biases among the stakeholders by creating different identities. This, in turn, shapes policy developments at ICANN since the Governmental Advisory Committee also struggles to find a standard position on specific political issues.[62]

Inefficiencies of multi-stakeholders

Critics have also highlighted specific issues regarding the model of multi-stakeholders. Brotman argues that, although the model appears attractive and increases the role of civil society in internet governance, there is a high likelihood of its failure.[63] This is because it will weaken legitimacy and allow developed states and

those with a strong IT sector to dominate internet governance. Moreover, due to the involvement of multiple stakeholders, policy processes take longer, resulting in lower participation. He further opined that limiting the control of authorities also raises pertinent questions regarding the problems of accountability, because there will be no 'one' authority to be questioned, unlike the state-led model, which makes the accountability of the government to the citizens much easier. Finnemore and Hollis have also argued that the debate around the multilateral or multi-stakeholder model is trivial because the multi-stakeholder model does not apply to all aspects of cyberspace.[64] This is because internet governance requires tasks to be carried out by different stakeholders,[65] and multi-stakeholders are central to only a few. There are still tasks carried out primarily by states, which reflect state-led control in internet governance.[66]

Controversies Surrounding Mass Surveillance Programmes

The Internet developed and evolved under the US influence; therefore, there have been many instances where it exploited this factor and made use of the internet and cyberspace to conduct massive surveillance programmes against opponents, allies, and even US nationals alike. Internet firms can be a source of extraterritorial power in the international arena, and the US has been using these firms to internationalize its state power.[67] The Snowden Leaks were a pivotal point for states with differing views on internet governance. Snowden Leaks gave China, Russia, and other like-minded states a fair chance to criticise the US for its massive surveillance programme. They proposed the concept of cyber sovereignty as an alternative approach to governing the internet.[68] Literature on Snowden pointed out that ARPANET and the internet were created as a weapon for military surveillance and were dominated by the military-industrial complex for a long time.[69] At the international level, Snowden Leaks also shaped the discussion on the development of norms for political espionage – a proposal that we had negated on the premise that political espionage is not prohibited under international law.[70]

Fragmentation of the Internet

It has also been alleged that the US and other Western states propagate an open and free internet; however, their policies undermine this principle. This fragmentation on the internet is often termed as "splinternet," indicating the split that exists in the words and actions of the Western world.[71] On the one hand, the US and its allies propagate a free and global internet; on the other hand, they exacerbate internet fragmentation in technical, user experience, and governance domains. Hawkins notes that the extension of national boundaries in cyberspace is not a phenomenon adopted by most states, and most of the internet is still interoperable. Moreover, the US and its allies also adopt regulatory policies regarding the control of information, which suggests that the words and actions of the US and its allies are highly fragmented.[72]

Conclusion

The US aims to collaborate with allies, partners, the public sector, the private sector, and all other stakeholders in the digital domain to promote an internet that is free, transparent, and open to everyone. The multi-stakeholder approach is crucial for the US notion of cyber governance because it ensures that human rights are not infringed upon, freedom of speech and expression is protected, and the privacy of individuals is safeguarded while promoting innovation and prosperity in the digital domain. These ideas are criticised by US adversaries, especially China, which calls for a sovereign cyberspace. This is because, despite advocacy for free cyberspace, Snowden Leaks and WikiLeaks played a crucial role in spotlighting the US exploitation of dominance on the internet, thus raising concerns about cyber governance.

References

[1] Adkinson Jr, William F. "Progress on Point-domain name services: let competition, not ICANN, rule." The Progress & Freedom Foundation. United States of America,

[2] BBC, 'Edward Snowden: Leaks That Exposed US Spy Programme', *British Broadcasting Corporation News*, 17 January 2014, sec. US & Canada, https://www.bbc.com/news/world-us-canada-23123964; Jacob Appelbaum et al., 'NSA Preps American for Future Battle: New Snowden Docs Indicate Scope of NSA Preparations for Cyber Battle', *Der Spiegel*, 17 January 2015, sec. International, https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html; Geo, 'US Hacked NTC to Spy on Pakistan Military, Political Leadership: Snowden Documents', *Geo News*, 20 August 2016, https://www.geo.tv/latest/112040-US-hacked-NTC-to-spy-on-Pakistan-military-political-leadership-Snowden-documents.

[3] David Drissel, "Internet governance in a multipolar world: Challenging American hegemony." *Cambridge Review of International Affairs* 19, no. 1 (2006): 105-120. https://doi.org/10.1080/09557570500501812

[4] US National Security Council. Executive Office of the President. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. [Washington, D.C. 2011]: p. 8.

[5] International Strategy for Cyberspace, 2011, p. 11.

[6] The United States seeks to build and enhance collaboration around five pillars: 1. Defend Critical Infrastructure. 2. Disrupt and Dismantle Threat Actors. 3. Shape Market Forces to Drive Security and Resilience. 4. Invest in Resilient Future. 5. Forge International Partnerships to Pursue Shared Goals. Joseph R Biden and Kamala Haris, 'FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy' (The White House, 2 March 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[7] International Strategy for Cyberspace, 2011, p. 8.

[8] International Strategy for Cyberspace, 2011, p. 22-23.

[9] President, National Cybersecurity Strategy, 23. President. National Security Strategy. Washington, DC: White House, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[10] International Strategy for Cyberspace, 2011, p. 22.

[11] International Strategy for Cyberspace, 2011, p. 12.

[12] National Cybersecurity Strategy, 2023, p. 4.

[13] National Cybersecurity Strategy, 2023, p. 4.

[14] National Cybersecurity Strategy, 2023, pp. 3-14.

[15] National Cybersecurity Strategy, 2023, p. 3.

[16] It also accentuates the importance of collaboration between the US and other states at international level as it clearly states its mission "to establish international science and technology partnerships to provide an enhanced, cost-effective, cooperative approach to common homeland security problem sets." US Department of Homeland Security, *"International Engagement Strategy",* 2020, pg. 6, https://www.dhs.gov/sites/default/files/publications/ICPO%20International%20Engagement%20Strategy.pdf

[17] The 21st century statecraft agenda was built to address a moment of transition – an era of rapid change at the intersection of technology and foreign policy. US Department of State, *"21st Century Statecraft"* January 20, 2009, https://2009-2017.state.gov/statecraft/overview/index.htm#:~:text= 21st%20century% 20statecraft%20is,and%20forced%20governments%20to%20respond. However, it is argued that where USA promotes free internet on the pretext of human rights, there is also an element of power attached to its advocacy for open and free internet. Madeline Carr. "Internet freedom, human rights and power." *Australian Journal of International Affairs* 67, no. 5 (2013): 621-637. https://doi.org/10.1080/ 10357718.2013.817525

[18] The White House, "*The National Strategy to Secure Cyberspace",* 2003. https://apps.dtic.mil/sti/pdfs/ADA413614.pdf

[19] The United States acknowledges that internet is a global space and no single government, state, or an actor should have the authority to control it. Therefore, it takes into account multiple stake holders in ensuring effective governance of internet. Stuart N. Brotman, "Multi-stakeholder Internet governance: A pathway completed, the road ahead." *Center for Technology Innovation at Brookings,* (2015). https://www.brookings.edu/wpcontent/uploads/2016/06/multistakeholder-1.pdf

[20] Theresa Hitchens and Nilsu Goren. "International Cybersecurity Information Sharing Agreements." Center for International & Security Studies, U. Maryland, 2017. http://www.jstor.org/stable/ resrep20426.

[21] Michael P Fischerkeller, Emily O. Goldman, and Richard J. Harknett. *Cyber persistence theory: Redefining national security in cyberspace*. Oxford University Press, 2022.

[22] Pioneer Press, "Mike McConnell: To win the cyber war, look to the Cold War", *Twin Cities Pioneer Press,* November 11, 2015, https://www.twincities.com/2010/03/07/mike-mcconnell-to-win-the-cyber-war-look-to-the-cold-war-2/

[23] Stefan Soesanto and Max Smeets, "Cyber Deterrence: The Past, Present, and Future" In *Deterrence in the 21st Century—Insights from Theory and Practice* (Ed) Frans Osinga, Tim Sweijs. 2021. Asser Press. https://library.oapen.org/bitstream/handle/20.500.12657/43303/1/

[24] Franz-Stefan Gady, and Greg Austin. "Russia, the United States, and cyber diplomacy." *Opening the Doors, East West Institute, New York* (2010).

[25] The United States Army "*Cyberspace Operations Concept Capability Plan 2016-2028",* February 2010, https://irp.fas.org/doddir/army/pam525-7-8.pdf

[26] US Department of Defence, "Summary 2023 Cyber Strategy", 2023,

[27] The White House, "National Strategy to Secure Cyberspace", 2003, https://www.energy.gov/ceser/articles/national-strategy-secure-cyberspace-february-2003

[28] Homeland/security Council, "*National Strategy for Homeland Security",* October 2007, https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

[29] The White House, "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", February 2003, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

[30] U.S. Cyber Command PAO, *"CYBER 101 - Defend Forward and Persistent Engagement",* US Cyber Command, 25 October, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

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

[32] Sergei Sebekin, "Choosing between persistent engagement and deterrence in the American cybersecurity strategy." *ПРОЦЕССЫ* (2020): 124. ; See also Jason Healey, "The implications of persistent (and permanent) engagement in cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019): tyz008. https://academic.oup.com/cybersecurity/article-pdf/doi/10.1093/cybsec/tyz008/29212814/ tyz008.pdf

[33] Richard J. Harknett, and Emily O. Goldman. "The search for cyber fundamentals." *Journal of Information Warfare* 15, no. 2 (2016): 81-88. https://www.jstor.org/stable/26487534

[34] Gerry Smith, "Security Chief's Cyberwar Testimony Seen As Veiled Threat To Enemies" *The Huff Post*, 14 March (2013) ,

[35] The DOD Cyber Strategy, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.

[36] David Sanger. US decides to retaliate against China's hacking, *The New York Times,* 2015, .

[37] International Strategy for Cyberspace, 2011, p. 10.

[38] The Department of Defense, *"2022 Nuclear Posture Review"*, October 2022, p. 9.https://s3.amazonaws.com/uploads.fas.org/2022/10/27113658/2022-Nuclear-Posture-Review.pdf

[39] Ellen Nakashima, "List of cyber-weapons developed by Pentagon to streamline computer warfare" *The Washington Post* May 31, 2011,

[40] Joel Schectman, Christopher Bing, and Christopher Bing, 'Exclusive: Trump Launched CIA Covert Influence Operation against China', *Reuters*, 14 March 2024, sec. United States, https://www.reuters.com/world/us/trump-launched-cia-covert-influence-operation-against-china-2024-03-14/; BBC, 'Edward Snowden'; Geo, 'US Hacked NTC to Spy on Pakistan Military, Political Leadership'.

[41] The White House, *"National Security Strategy",* October 2022, pg. 21, https://www.whitehouse.gov/ wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[42] US Department of Defense, *"DOD Releases 2023 Cyber Strategy Summary",* September 12, 2023, https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/#:~

[43] Amel Attatfa, Karen Renaud, and Stefano De Paoli. "Cyber diplomacy: A systematic literature review." *Procedia computer science* 176 (2020): 60-69.

[44] Shaun Riordan. "Cyber diplomacy vs. digital diplomacy: a terminological distinction." *CPD Blog* (2016).

[45] Chris Painter, The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. *American Foreign Service Association*, (June 2018),

[46] Critical Infrastructure Protection Board, "National strategy to secure cyberspace." *The White House, Washington, DC, USA* (2002).

[47] Michael Zimmer, "The tensions of securing cyberspace: The Internet, state power and The National Strategy to Secure Cyberspace." *First Monday* (2004).

[48] International Strategy for Cyberspace, 2011, p. 9.

[49] International Strategy for Cyberspace.

[50] National Cybersecurity Strategy, 2023, p. 31

[51] Martha Finnemore, and Duncan B. Hollis. "Constructing norms for global cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 425-479. https://doi.org/10.1017/S0002930000016894

[52] Harel Menashri, and Gil Baram. "Critical infrastructures and their interdependence in a cyber-attack–the case of the US." *Military and strategic Affairs* 7, no. 1 (2015): 22. https://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/5_Menashri_Baram.pdf

[53] Menashri and Baram, 2015.

[54] T. M. Ballou, Joseph A. Allen, and K. K. Francis. "US Energy Sector Cybersecurity: Hands-off Approach or Effective Partnership?." *Journal of information warfare* 15, no. 1 (2016): 44-59. https://www.jstor.org/stable/pdf/26487480

[55] National Security Strategy, 2022, p. 34.

[56] Finnemore and Hollis, 2017.

[57] Ilina Georgieva, "The unexpected norm-setters: intelligence agencies in cyberspace." *Contemporary Security Policy* 41, no. 1 (2020): 33-54. https://doi.org/10.1080/13523260.2019.1677389

[58] Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe, "Microsoft handed the NSA access to encrypted messages", *The Guardian,* July 2013,

[59] Mark Raymond, and Laura DeNardis.. "Multi-stakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7 (03): 572–616. 2015, Doi: 10.1017/S1752971915000081.

[60] Raymond, and DeNardis, 2015.

[61] Jeremy Mark Malcolm. *"Multi-stakeholder public policy governance and its application to the Internet Governance Forum."* PhD diss., Murdoch University, 2008. https://researchportal.murdoch.edu.au/esploro/outputs/doctoral/Multi-stakeholder-public-policy-governance-and-its/9910055428114078 91

[62] Hoffman, 2016

[63] Stuart N. Brotman, "Multistakeholder Internet governance: A pathway completed, the road ahead", *Centre for Technology Innovation at Brookings*, July (2015),

[64] Finnemore and Hollis, 2016, p. 461.

[65] Laura DeNardis, *The global war for internet governance*. Yale University Press, 2014.

[66] Finnemore and Hollis, 2016, p. 462.

[67] Madison Cartwright. "Internationalising state power through the internet: Google, Huawei and geopolitical struggle." *Internet Policy Review* 9, no. 3 (2020): 1-18.

[68] Julien Nocetti, Contest and conquest: Russia and global internet governance, *International Affairs*, Volume 91, no. 1, (2015): 111–130, https://doi.org/10.1111/1468-2346.12189

[69] Noel Packard, "Three Kinds of Demand Pull for the ARPANET into the Internet." *Cogent Social Sciences* 6, no. 1 (2020): https://doi.org/10.1080/23311886.2020.1720565

[70] Adriana Erthal Abdenur, and Carlos Frederico Pereira da Silva Gama. "Triggering the norms cascade: Brazil's initiatives for curbing electronic espionage." *Global Governance* 21 (2015): 455. https://heinonline.org/HOL/LandingPage?handle=hein.journals/glogo021&div=35&id=&page=

[71] Zoe Hawkins, "Internet Governance Doublespeak: Western Governments and the Open Internet", *Council on Foreign Relations,* January 4, 2023,

[72] Hawkins, 2023.