Page 09 - 29 **DOI:** *https://doij.org/10.10000/IJLMH.118491*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 6

2024

Sovereignty in the Digital Age: Examining Foreign Interference in U.S. Elections through the Lens of International and Domestic Law

ZINAMI IWARISO FYNEROAD[1] AND OYEPHO AKEUSEPH[2]

ABSTRACT

State sovereignty as the cornerstone of international law and relations, faces unprecedented challenges in the digital age. This article examines the evolving nature of sovereignty through the lens of foreign interference in U.S. elections, with a particular focus on alleged Russian and Chinese activities. By analyzing the intersection of international law, domestic legislation, and emerging cyber norms, this study critically assesses the adequacy of existing legal frameworks in addressing modern threats to electoral integrity. It then explores the specific legal aspect of election interference, comparing and contrasting the approaches reportedly taken by Russia and China. The study delves into the challenges cyber operations pose to traditional notions of territorial sovereignty. Furthermore, this article evaluates international and U.S. domestic legal responses to election interference, highlighting progress and limitations in current approaches. The paper argues that while existing laws provide some tools to combat foreign meddling, they are often insufficient in the face of rapidly evolving cyber threats. The research proposes that a multi-faceted approach, combining legal, technological, and diplomatic strategies, is necessary to safeguard electoral processes in the digital era. Ultimately, this study contends that sovereignty must evolve to meet 21st-century challenges. It advocates for developing clearer international norms governing cyber operations, enhanced cooperation in attributing and responding to election interference, and the cultivation of public resilience against disinformation campaigns. By examining these issues, the article contributes to ongoing discussions on the future of democracy, national security, and international law in an interconnected world.

***Keywords**: Sovereignty, Election Interference, Cybersecurity, International Law, U.S.A Elections, Russia, China, Digital Age.*

[1] Author is a Research Candidate at Rivers State University & Legal Practitioner, Nigeria.
[2] Author is a Research Candidate at Rivers State University & Legal Practitioner, Nigeria.

 [ISSN 2581-5369]

I. INTRODUCTION

The integrity of national elections is the foundation of democratic governance, inextricably linked to the fundamental concept of state sovereignty. The sovereign right to conduct free and fair elections, immune from external manipulation and or interference, has long been considered an inviolable aspect of a nation's self-determination. However, in our interconnected global environment, the sanctity of this democratic process faces novel challenges from alleged foreign interference. The United States, as a prominent global power and one of the world's oldest democracies, has found itself at the epicenter of this emerging threat, with allegations of electoral interference by nations such as Russia and China bringing the issue into sharp focus.[3] Thereby generating national and international debates, compelling us to re-evaluate our understanding of sovereignty in the digital age. They raise vital questions about the nature and limits of state power, the adequacy of existing legal frameworks, and the foundations of democratic governance in an era where information flows freely across borders and cyber operations can have far-reaching consequences.[4] By conducting a thorough analysis of the legal implications stemming from alleged interference by Russia and China, the article aims to provide a critical assessment of the current state of sovereignty. Digital evolution has reshaped the landscape of international relations, introducing new vectors for influence and conflict that transcend traditional geopolitical boundaries.[5] This paper's analysis extends beyond mere legal ramifications to encompass the broader geopolitical context and the rapidly evolving technological environment that enables such interference. Moreover, the challenges posed by foreign election interference intertwine with a host of other pressing issues in international law and relations. These include the regulation of cyberspace, the balance between national security and individual privacy rights, the role of non-state actors in international affairs, and the tension between state sovereignty and global governance structures.[6] By examining election interference through these perspectives, we can gain valuable insights into the changing nature of power and influence in the 21st century. We must find ways to protect the integrity of democratic processes and uphold the principle of non-intervention or interference, while also preserving the open and interconnected nature of the internet that has driven unprecedented

[3] Jens David Ohlin, 'Election Interference: The Real Harm and The Only Solution' (2018) Cornell Legal Studies Research Paper No. 18-50 <https://ssrn.com/abstract=3276940> accessed 7 September 2024

[4] Joseph S Nye Jr, 'The Regime Complex for Managing Global Cyber Activities' (2014) Global Commission on Internet Governance Paper Series No 1 <https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf> accessed 7 September 2024

[5] Laura DeNardis, The Global War for Internet Governance (Yale University Press 2014) 15-16

[6] Harold Hongju Koh, 'The Trump Administration and International Law' (2017) (56) *Washburn Law Journal* 413.

 [ISSN 2581-5369]

global communication and innovation.[7]

II. THE CONCEPT OF SOVEREIGNTY IN INTERNATIONAL LAW

(A) Historical Development of Sovereignty

The concept of sovereignty, the bedrock of international relations and law, has undergone a major evolution since its formal inception in the 1648 Peace of Westphalia.[8] Originally conceptualized as the absolute authority of monarchs within their territories, sovereignty has transformed into a principle of international law recognizing the equality and independence of states.[9] This evolution mirrors the changing dynamics of global politics and the international order over centuries. The Westphalian model, emphasizing non-intervention in states' internal affairs, has long been fundamental to international relations.[10] However, this traditional conception faces challenges from globalization, the proliferation of international institutions, and state interdependence.[11] The 20th century, in particular, saw major shifts in sovereignty's interpretation and application. The aftermath of World War II marked a pivotal moment, with the establishment of the United Nations and the codification of sovereign equality in its Charter.[12] Decolonization movements in the mid-20th century further reshaped sovereignty, as newly independent states asserted their right to self-determination.[13] The Cold War era saw sovereignty leveraged as a shield against external interference, particularly by smaller states navigating superpower politics.[14] Recently, concepts like 'shared sovereignty' and 'pooled sovereignty' have emerged, particularly in the context of regional integration efforts like the European Union.[15] These ideas challenge the traditional notion of indivisible state sovereignty. The digital age presents new challenges to sovereignty, with cyberspace defying traditional territorial boundaries.[16] Issues of data sovereignty, cyber operations, and digital jurisdiction are

[7] Milton Mueller, *Will the Internet Fragment?: ´Sovereignty, Globalization and Cyberspace* (Polity Press 2017) 41-66.
[8] Derek Croxton, 'The Peace of Westphalia of 1648 and the Origins of Sovereignty' (1999) (21) (3) *The International History Review* 569.
[9] Stephen D Krasner, Sovereignty: Organized Hypocrisy (Princeton University Press 1999) 3-4.
[10] Andreas Osiander, 'Sovereignty, International Relations, and the Westphalian Myth' (2001) 55(2) *International Organization* 251.
[11] Saskia Sassen, Losing Control?: Sovereignty in the Age of Globalization (Columbia University Press 1996) 1-32.
[12] Charter of the United Nations (24 October 1945) 1 UNTS XVI, art 2(1).
[13] Robert H Jackson, *Quasi-states: Sovereignty, International Relations and the Third* World (Cambridge University Press (1990).
[14] Mohammed Ayoob, 'The Third World in the System of States: Acute Schizophrenia or Growing Pains?' (1989) 33(1) *International Studies Quarterly* 67
[15] Neil Walker, 'Late Sovereignty in the European Union' in Neil Walker (ed), Sovereignty in Transition (Hart Publishing 2003).
[16] Milton L Mueller, *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* (Polity Press 2017) 41-66

forcing a re-evaluation of how sovereignty applies in this borderless domain. This evolving concept of sovereignty continues to be central to debates on international law, global governance, and the future of the nation-state system in a progressively interrelated world.[17]

(B) Modern Understanding of Sovereignty

Sovereignty as enshrined in the United Nations Charter, declares that the organization is "based on the principle of the sovereign equality of all its Members"[18] This principle encompasses the concepts of territorial integrity, political independence, and non-intervention in domestic affairs.[19] The International Court of Justice (ICJ) has in several cases upheld the principle of non-intervention. In the landmark Nicaragua case, the Court affirmed that this principle "forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States".[20] This prohibition extends to methods of interference that do not involve the use of force, reflecting the broad scope of sovereign protection under international law. However, the absolute nature of sovereignty has faced growing scrutiny in the contemporary era. The rise of human rights law has given birth to the concept of 'conditional sovereignty', suggesting that a state's sovereign rights must be balanced against its responsibilities to its citizens.[21] This idea challenges the traditional view of sovereignty as an inviolable right, instead framing it as contingent upon the fulfilment of certain obligations. The Responsibility to Protect (R2P) doctrine, endorsed by all UN member states in 2005, further challenges conventional notions of sovereignty.[22] R2P asserts that the international community has a responsibility to intervene in cases of severe human rights abuses, potentially overriding the principle of non-intervention in extreme circumstances. Moreover, the processes of globalization and rising global interdependence have led to what some scholars term the 'disaggregation of sovereignty'.[23] This refers to the distribution of traditionally sovereign powers among various national, subnational, and supranational actors. The European Union, for instance, exemplifies a system where member states voluntarily pool aspects of their sovereignty for mutual benefit.[24] Environmental issues, particularly climate change, have also reshaped our understanding of sovereignty. Recognizing that environmental problems do not respect national borders has led to calls for

[17] Martti Koskenniemi, 'What Use for Sovereignty Today?' (2011) 1(1) *Asian Journal of International Law* 61
[18] Charter of the United Nations (24 October 1945) 1 UNTS XVI, art 2(1).
[19] James Crawford, *Brownlie's Principles of Public International Law* (9th edn, OUP 2019) 447-448.
[20] Military and Paramilitary Activities in and against Nicaragua *(Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, para 205
[21] Anne Peters, 'Humanity as the A and Ω of Sovereignty' (2009) 20(3) *European Journal of International Law* 513
[22] UN General Assembly, '2005 World Summit Outcome' (24 October 2005) UN Doc A/RES/60/
[23] Anne-Marie Slaughter, A New World Order (Princeton University Press 2004) 266-271
[24] Neil Walker, 'Late Sovereignty in the European Union' in Neil Walker (ed), Sovereignty in Transition (Hart Publishing (2003)

'ecological sovereignty', emphasizing states' responsibilities to the global environment.[25] Lastly, the COVID-19 pandemic has highlighted the enduring importance of state sovereignty in crisis management and the limitations of purely national responses to global challenges. The pandemic has underscored the tension between national sovereignty and the need for international cooperation in addressing transnational threats.[26] While the principle of sovereignty remains central to international law and relations, its modern understanding is characterized by increasing complexity and nuances.

(C) Sovereignty in the Digital Age

The advent of the digital age has profoundly complicated traditional understandings of sovereignty. As Schmitt and Vihul astutely observe, cyberspace presents novel challenges to the application of sovereignty, particularly when the effects of cyber operations transcend physical borders.[27] This reality calls for a reconceptualization of sovereignty within the context of cyberspace. The inherently borderless nature of cyberspace raises serious and difficult questions about the applicability of territorial-based concepts of sovereignty. Scholars are advocating for a new understanding of "digital sovereignty" that incorporates the unique characteristics of the online world.[28] This evolving concept encompasses not only control over digital infrastructure within a state's territory but also the ability to regulate and govern the digital activities of its citizens and the data they generate.[29] The Tallinn Manual 2.0, an influential, albeit non-binding study, on the application of international law to cyber operations, posits that states enjoy sovereignty over cyber infrastructure, persons, and cyber activities located within their territory.[30] However, the precise boundaries of this sovereignty in cyberspace remain a subject of debate among legal scholars and policymakers. The concept of data sovereignty has gained notable traction, with states asserting the right to regulate and control data generated within their borders.[31] This trend has led to concerns between states and multinational tech companies, as well as between differing national legal regimes, particularly in areas such as data protection and privacy.[32] China's "Great Firewall" represents perhaps the

[25] Mueller, (n 14) 41-66
[26] Armin von Bogdandy and Pedro A Villarreal, 'International Law on Pandemic Response: A First Stocktaking in Light of the Coronavirus Crisis' (2020) Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2020-07
[27] Michael N Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 *Texas Law Review* 1639
[28] Laura DeNardis, The Global War for Internet Governance (Yale University Press 2014) 15-16
[29] Mueller (n 15)
[30] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) Rule 1
[31] Anupam Chander and Uyên P Lê, 'Data Nationalism' (2015) 64 *Emory Law Journal* 677.
[32] Paul de Hert and Vagelis Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9(2) I/S: *A Journal of Law and Policy for the Information Society* 271

most comprehensive attempt to exert sovereign control over the internet within national borders.[33] The European Union's General Data Protection Regulation (GDPR) exemplifies a regional approach to data sovereignty, imposing strict rules on data handling that apply even to companies outside the EU.[34] Challenges to digital sovereignty are numerous. The distributed nature of cloud computing, for instance, complicates efforts to localize data within national borders.[35] The prevalence of virtual private networks (VPNs) and encryption technologies enables users to circumvent national digital borders, challenging state control.[36] Moreover, the global nature of cyber threats necessitates international cooperation, potentially conflicting with strict notions of digital sovereignty. The 2021 Colonial Pipeline ransomware attack in the U.S. highlighted how cyber incidents can have far-reaching consequences beyond national borders.[37] The concept of "splinternet" - the fragmentation of the global internet into national or regional networks - has emerged as a potential consequence of assertive digital sovereignty policies.[38] This trend raises concerns about the future of the open, global internet and its implications for innovation, free expression, and global commerce. As states face these challenges, the international community faces the task of developing new norms and legal frameworks that balance national sovereignty with the need for a free and open global internet. It is axiomatic that the principles of sovereignty apply in cyberspace, just as it does in the physical space. It animates several obligations for all states. Territorial Sovereignty is a rule under International law.[39] However, International Law provides for exceptions to the general rule of territorial sovereignty to wit, actions : (i) authorized by the United Nations Security Council ; (ii) taken in self-defense concerning an armed attack (iii) consented by the affected state; or (iv) that constitute countermeasure. These exceptions apply in the digital world. Every state is obligated to protect the territorial integrity of every other state. The sovereignty states enjoy over another territory include infrastructure located within their territory and activities associated with them,

[33] Ronald Deibert, 'The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace' in Andrew Chadwick and Philip N Howard (eds), *Routledge Handbook of Internet Politics* (Routledge 2009) 323-336.
[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1
[35] W Kuan Hon and Christopher Millard, 'Data Localization Laws and Policy' (Edward Elgar Publishing 2017).
[36] Milton Mueller and Karl Grindal, 'Is It "Sovereignty" or "Autonomy"? Clarifying Regulatory Objectives for the Internet' (2018) Internet Governance Project
[37] William Turton and Kartikay Mehrotra, 'Hackers Breached Colonial Pipeline Using Compromised Password' Bloomberg (4 June 2021) <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password> accessed 10 September 2024
[38] Jack Goldsmith and Tim Wu, Who Controls the Internet?: Illusions of a Borderless World (Oxford University Press (2006)
[39] Government of Canada, ´International Law applicable in Cyberspace´,https://international.gc.ca/world-monde/issues-development –enjeux-development /peace-security-paix-security/cyberspace-law > accessed 10 September 2024

an infringement upon the affected state's territorial integrity, or interference with or usurpation of inherently governmental functions of the affected state, would constitute a violation of territorial sovereignty. An example of an infraction of governmental function is a malicious cyber activity that hacks and disables a state election commission´s cyber infrastructure, days before the election, preventing a major number of citizens from voting and ultimately influencing the outcome of the election. This example also constitutes a violation of international human rights law particularly, Articles 13(1) 21 and 25 of the African Charter.[40] Universal Declaration of Human Rights[41] and the International Covenant on Civil and Political Rights respectively. [42] In Assessing the possible infringement of states' territorial sovereignty in the digital age or cyberspace, several key factors must be considered. The scope, scale, impact, or severity of the disruption caused including the disruption to economic and social activities, essential services, governmental function, and public safety must be assessed to determine whether the violation of the territorial sovereignty of the affected state has taken place. In general, the severity of the cyber effects will be evaluated in the same manner as physical activities, cyber or digital activities that rise above a level of negligible or de miniminis effects causing significant harmful effects within the territory of another state without the state consent could amount to a violation of the rule of territorial sovereignty. It is important to reemphasize that cyber activities conducted remotely without physical presence do not inherently violate a state's territorial sovereignty. However, unauthorized actions targeting or interfering with cyberinfrastructure within another state's territory can constitute a breach of sovereignty, even without physical effects. While some cyber activities, such as espionage, exist in a legal gray area and are not explicitly prohibited by international law, they may still be regarded as internationally wrongful acts if they significantly interfere with governmental functions or disrupt critical infrastructure. The absence of physical presence does not exempt a state from responsibility under international law if the cyber operation infringes upon another state's sovereignty.[43] Some states prohibit espionage in their laws. In Canada, for example, economic espionage is a violation of section 19 of the Security of Information Act and offenders upon conviction are liable to imprisonment for a term not more than 10 years.[44] The ongoing debate over digital sovereignty will likely shape the future of international relations, global governance, and the very nature of state power in the 21st century.

[40] African Charter on Human and Peoples Right 1981 arts 13(1) ,21,25
[41] 1948 Art 21
[42] 1966 art 25
[43] Schmitt (n) rule 19 para 7-9
[44] Security of Information Act 1985 , s. 19

 [ISSN 2581-5369]

III. U.S. DOMESTIC AND ELECTORAL SOVEREIGNTY

The concept of electoral sovereignty in the United States is rooted in the nation's constitutional framework and federal structure. The U.S. Constitution grants states primary authority over the administration of elections, including federal ones, while simultaneously empowering Congress to regulate certain aspects of federal elections.[45] This delicate balance reflects the broader relationship between state and federal powers that characterizes the American political system. The elections clause of the U.S. Constitution (Article I, Section 4, Clause 1) establishes that states have the primary responsibility for regulating the "Times, Places and Manner" of holding elections for Senators and Representatives.[46] However, it also grants Congress the authority to "at any time by Law make or alter such Regulations," creating a system of shared sovereignty over election administration.[47] This constitutional arrangement has led to a complex geopolitical space of election laws and practices that vary significantly from state to state. Several federal laws aim to protect the integrity of elections and, by extension, U.S. electoral sovereignty. The Federal Election Campaign Act of 1971 (FECA), as amended, regulates campaign financing and prohibits foreign nationals from making contributions or expenditures in connection with U.S. elections.[48] The Foreign Agents Registration Act (FARA) requires persons acting as agents of foreign principals to disclose their relationship with the foreign principal and their activities.[49] The Help America Vote Act of 2002 (HAVA) established minimum standards for states to follow in several key areas of election administration.[50] The Bipartisan Campaign Reform Act of 2002 (BCRA) further regulates campaign finance, including restrictions on foreign national involvement in U.S. elections.[51] While federal laws provide an overarching framework, state laws play an important role in determining the specifics of election administration. This includes everything from voter registration procedures to the type of voting machines used.[52] The diversity of state election systems can be both a strength and a weakness in terms of election security. While it makes it more difficult for a single attack to compromise the entire system, it also leads to inconsistencies in security measures and complicates coordinated responses to threats.[53] Some of the US domestic laws are

[45] U.S. Const. art. I, § 4, cl. 1
[46] *Arizona v Inter Tribal Council of Arizona, Inc.*, 570 U.S. 1 (2013)
[47] U.S. Const. art. I, § 4, cl. 1
[48] Federal Election Campaign Act of 1971, 52 U.S.C.
[49] Foreign Agents Registration Act, 22 U.S.C. § 611 et seq
[50] Help America Vote Act of 2002, 52 U.S.C. §§ 20901-21145.
[51] Bipartisan Campaign Reform Act of 2002, Pub. L. No. 107-155, 116 Stat. 81
[52] National Conference of State Legislatures, 'State Laws Governing Early Voting' (20 August 2023) <https://www.ncsl.org/research/elections-and-campaigns/early-voting-in-state-elections.aspx> accessed 10 September 2024.
[53] Lawrence Norden and Christopher Famighetti, 'America's Voting Machines at Risk' (Brennan Center for Justice,

(A) Alleged Russian and Chinese Interference in U.S. Elections

a. Russian Interference

While both nations have been accused of attempting to influence U.S. electoral processes, their methods, objectives, and the scale of their operations differ considerably. Russian interference has been characterized by its overt and aggressive nature. The U.S. intelligence community, particularly in its assessment of the 2016 presidential election, concluded that Russian President Vladimir Putin ordered a comprehensive influence campaign.[54] This campaign allegedly includes cyber operations targeting election infrastructure, hacking and strategic release of information to sway public opinion, and extensive use of social media platforms to spread disinformation and worsen societal divisions amongst others. The Internet Research Agency, a Russian organization, played a central role in these efforts. It created numerous fake social media accounts, organized events, and disseminated content designed to influence American voters.[55] The operation's scale and sophistication marked a major escalation in foreign interference efforts.

b. Chinese Interference

In contrast, Chinese interference efforts have been described as more subtle and long-term oriented. The Office of the Director of National Intelligence (ODNI) reported that while China "considered" interference in the 2020 U.S. Presidential election, it did not deploy large-scale influence efforts to change the outcome.[56] Chinese activities have reportedly focused on influencing U.S. policy through ostensibly legitimate channels, such as lobbying and public diplomacy. Leveraging economic influence and potential coercion. Conducting cyber espionage targeting political organizations and individuals implementing more nuanced disinformation campaigns on social media platforms. China's approach often operates in a gray area between legitimate influence and unlawful interference. This includes efforts to shape public opinion through state-controlled media outlets operating in the U.S. and the use of social media platforms to amplify pro-China narratives.

---

15 September 2015) <https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf> accessed 10 September 2024

[54] Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections' (6 January 2017) <https://www.dni.gov/files/documents/ICA_2017_01.pdf> accessed 12 September 2024

[55] Robert S Mueller III, 'Report On The Investigation Into Russian Interference In The 2016 Presidential Election' (U.S. Department of Justice, March 2019).

[56] National Intelligence Council, 'Foreign Threats to the 2020 US Federal Elections' (15 March 2021) <https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf> accessed 12 September 2024

c. Comparative Analysis

The contrasting approaches of Russia and China reflect their different strategic objectives and risk tolerances. Russia's more aggressive tactics suggest a willingness to directly challenge U.S. institutions, even at the risk of exposure and retaliation. China's more cautious approach aligns with its long-term strategy of expanding global influence while avoiding confrontation with the U.S. Both nations have leveraged the interconnected nature of the modern information ecosystem, exploiting vulnerabilities in social media platforms, cyberinfrastructure, and public discourse. However, the detection and attribution of Chinese activities have proven more challenging due to their less overt nature.

(B) U.S. Legal and Policy Responses

The United States has implemented a comprehensive and diverse approach to counter foreign election interference, reflecting the complex nature of the threat and the unique challenges posed by the country's federal system. This response encompasses executive actions, legislative measures, cybersecurity initiatives, interagency coordination, and state and local efforts, demonstrating a whole-of-government strategy to protect the integrity of U.S. elections. At the federal level, executive actions have played a crucial role in setting the tone and direction for the nation's response to election interference. Executive Order 13848, signed in 2018, represents a major step in this direction, authorizing sanctions against foreign entities involved in election interference.[57] This order does not only provides a mechanism for punitive action but also serves as a deterrent against potential foreign actors contemplating interference. The establishment of the Cyber Unified Coordination Group (UCG) further demonstrates the administration's commitment to a coordinated response to cyber threats, allowing for rapid mobilization of resources in the face of election-related cyber incidents.[58] The 2018 National Cyber Strategy provides a broader framework for these efforts, outlining a comprehensive approach to safeguarding American interests in cyberspace, including election infrastructure.[59] Legislative measures have sought to address specific vulnerabilities and threats to the electoral process. The proposed Honest Ads Act, for instance, aims to close a significant loophole in campaign finance law by extending disclosure requirements to online political advertisements.[60] This measure, if passed, could enhance transparency and accountability in digital political advertising, a key

[57] Exec. Order No. 13,848, 83 Fed. Reg. 46,843 (Sept. 12, 2018).
[58] Cybersecurity and Infrastructure Security Agency, 'Cyber Incident Response' <https://www.cisa.gov/cyber-incident-response> accessed 14 September 2024
[59] White House, 'National Cyber Strategy of the United States of America' (September 2018) <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> accessed 14 September 2024.
[60] Honest Ads Act, S. 1989, 115th Cong. (2017)

 [ISSN 2581-5369]

route for foreign influence operations. The DETER Act, enacted in 2019, takes a different approach by targeting individuals involved in election interference, making them inadmissible to the United States.[61] This law adds another layer of deterrence and demonstrates the U.S. government's willingness to use immigration policy as a tool to combat election interference. The Countering America's Adversaries Through Sanctions Act (CAATSA), while broader in scope, includes provisions specifically targeting Russian interference in the 2016 election, illustrating the use of economic sanctions as a response to state-sponsored election meddling.[62] The designation of election infrastructure as critical infrastructure in 2017 marks a key shift in how the U.S. government approaches election security.[63] This designation allows for prioritized cybersecurity assistance to election officials and underlines the importance of secured elections to national security. The establishment of the Cybersecurity and Infrastructure Security Agency (CISA) in 2018 further institutionalizes this approach, creating a dedicated federal agency to coordinate cybersecurity efforts across all levels of government.[64] The creation of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) complements these efforts by facilitating information sharing and analysis among election officials, a vital component in identifying and responding to threats promptly.[65] Interagency coordination has been a key focus in the U.S. response to election interference. The Election Infrastructure Subsector Government Coordinating Council facilitates communication between federal, state, and local partners on critical infrastructure protection, ensuring a unified approach to election security.[66] The FBI's Foreign Influence Task Force plays a crucial role in identifying and counteracting foreign influence operations targeting U.S. democratic institutions and processes, bringing the Bureau's investigative expertise to bear on this complex threat.[67] The establishment of the Office of the Director of National Intelligence (ODNI) Election Threats Executive, further centralizes and coordinates election security activities across the Intelligence Community, enhancing information sharing and strategic planning.[68] At the state and local levels, increased federal

[61] No Defending Elections against Trolls from Enemy Regimes Act, Pub. L. No. 116-33, 133 Stat. 1063 (2019).
[62] Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44, 131 Stat. 886 (2017).
[63] U.S. Department of Homeland Security, 'Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector' (6 January 2017) <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical> accessed 14 September 2024.
[64] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (2018).
[65] Center for Internet Security, 'EI-ISAC' <https://www.cisecurity.org/ei-isac/> accessed 14 September 2023
[66] U.S. Election Assistance Commission, 'Election Infrastructure Subsector Government Coordinating Council Charter'<https://www.eac.gov/sites/default/files/eac_assets/1/6/GCC_Charter_EIS_Approved_Nov_2017_508.pdf> accessed 14 September 2024.
[67] Federal Bureau of Investigation, 'Combating Foreign Influence' <https://www.fbi.gov/investigate/counterintelligence/foreign-influence> accessed 14 September 2024
[68] Office of the Director of National Intelligence, 'Director of National Intelligence Announces Changes to Election Security Threat Updates' (10 August 2020) <https://www.dni.gov/index.php/newsroom/press-releases/item/2135-

funding for election security measures has been key in upgrading voting systems and improving cybersecurity.[69] The provision of training and resources to state and local election officials has helped to build capacity and resilience at the grassroots level.[70] Many states have also taken the initiative to enact their legislation to enhance election security, including mandating post-election audits and improving the security of voter registration databases.[71] These state-level efforts are particularly important given the decentralized nature of U.S. elections and highlight the need for a cooperative approach between federal and state governments in safeguarding the electoral process. While these measures represent a robust and multi-layered approach to countering election interference, challenges remain. The fast-evolving nature of cyber threats requires constant adaptation of security measures. The decentralized nature of U.S. elections, while providing some security benefits, also creates challenges in implementing uniform security standards across the country. Moreover, the balance between enhancing election security and maintaining the accessibility and efficiency of the voting process remains an ongoing concern. As foreign actors continue to develop new methods of interference, the U.S. will need to remain vigilant and adaptive in its approach to protecting the integrity of its democratic processes.

Both Russian and Chinese activities probably violate the principle of non-intervention in international law. The concept of state sovereignty in cyberspace remains contested. Proving state responsibility for cyber operations remains a difficult hurdle. The anonymity and complexity of cyberspace make it difficult to attribute actions to specific state actors with the level of certainty required under international law.

IV. INTERNATIONAL LEGAL RESPONSES TO ELECTION INTERFERENCE

(A) United Nations Initiatives

The United Nations has been key in developing norms for responsible State behaviour in cyberspace: The Assembly has affirmed that international law applies to state conduct in cyberspace.[72] The United Nations Group of Governmental Experts (UN GGE) has been

director-of-national-intelligence-announces-changes-to-election-security-threat-updates> accessed 14 September 2024.

[69] U.S. Election Assistance Commission, 'EAC Expedites Distribution of $380 Million in Election Security Grants to States' (17 April 2018) <https://www.eac.gov/news/2018/04/17/eac-expedites-distribution-of-380-million-in-election-security-grants-to-states> accessed 14 September 2024.

[70] Cybersecurity and Infrastructure Security Agency, 'Election Security' <https://www.cisa.gov/election-security> accessed 14 September 2024.

[71] National Conference of State Legislatures, 'Election Security: State Policies' (2 August 2023) <https://www.ncsl.org/research/elections-and-campaigns/election-security-state-policies.aspx> accessed 14 September 2024.

[72] UNGA Res 70/237 (30 December 2015) UN Doc A/RES/70/237

instrumental in shaping the international discourse on cybersecurity and the application of international law to state conduct in cyberspace. In its landmark 2015 report, the UN GGE affirmed that international law, particularly the UN Charter, applies to the use of information and communication technologies (ICTs) by states.[73] The report also outlined a set of voluntary, non-binding norms for responsible state actions in cyberspace, including the principle that States should not conduct or knowingly support ICT activities that intentionally damage critical infrastructure.[74] Notably, the GGE emphasized the importance of confidence-building measures and international cooperation in addressing cyber threats, which could encompass issues of election interference.[75] The GGE's work has been instrumental in establishing a framework for understanding how existing international law principles, such as state sovereignty and the prohibition of intervention, apply in the cyber context.[76] However, despite these advancements, challenges remain in achieving consensus on more specific issues, such as how to attribute cyber operations to states and what constitutes a violation of sovereignty in cyberspace.[77] Through its Open-Ended Working Group (OEWG) on developments in information and telecommunications in the context of international security, it established as a more inclusive forum compared to the Group of Governmental Experts (GGE), the OEWG has provided a platform for broader international discussions on cyber norms and the application of international law in cyberspace.[78] The final substantive report of the OEWG, adopted on 12 March 2021, reaffirmed that international law, including the UN Charter, applies to state conduct in cyberspace and emphasized the importance of responsible state behavior. The report also highlighted the need for capacity-building efforts to enhance states' ability to address cybersecurity threats and called for increased cooperation in developing confidence-building measures.[79] While the OEWG process has been instrumental in fostering dialogue and building consensus on certain issues, challenges remain in translating these discussions into binding norms or treaties that effectively address the geographical space of cyber threats, including election interference. The 2021 report of the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security marks an important evolution in the international community's approach to cybersecurity issues. This

[73] UN GGE, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174
[74] ibid.
[75] ibid.
[76] Michael N Schmitt and Liis Vihul (n 26)
[77] Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (2016) 70 *Journal of International Affairs* 75.
[78] UNGA, 'Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (Final Substantive Report, 10 March 2021) UN Doc A/AC.290/2021/CRP.2
[79] ibid.

 [ISSN 2581-5369]

report builds upon previous GGE efforts, reaffirming that international law applies to state use of ICTs while also expanding on norms of responsible state behavior.[80] Notably, the report emphasizes the principle of state sovereignty in the context of ICT activities, asserting that states have the primary responsibility for maintaining a secure ICT environment within their territories. This principle has important implications for addressing issues such as foreign election interference through cyber means. The GGE also highlighted the need for states to take reasonable steps to ensure the integrity of the supply chain for ICT products and services, which is crucial for maintaining the security of election infrastructure.[81] Furthermore, the report underscores the importance of not allowing state territory to be used for internationally wrongful acts using ICTs, a principle that could be applied to combating foreign-based disinformation campaigns aimed at influencing elections. While the report represents progress in developing shared understandings of responsible state conduct in cyberspace, challenges remain in operationalizing these norms and ensuring compliance, particularly in contentious areas such as election interference.[82] The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has made reasonable contributions to understanding how international law applies in cyberspace, mostly through the Tallinn Manual process. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, published in 2017, comprehensively analyzes how existing international law norms apply to cyber activities, Of particular relevance to issues of sovereignty and election interference, the Manual affirms that the principle of state sovereignty applies in cyberspace, asserting that states have the right to exercise control over cyber infrastructure and activities within their territory.[83] It also addresses the prohibition of intervention, stating that cyber operations that have a coercive effect on matters falling within a state's domaine réservé, such as elections, could constitute a violation of this principle.[84] The Manual's treatment of these issues provides valuable guidance for understanding the legal implications of foreign cyber activities aimed at influencing elections.[85] However, it's important to note that while the Tallinn Manual is highly influential, it is not a binding legal document but rather reflects the opinions of international law experts.[86] As such, while it offers insights, state

[80] UNGA, 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the C context of International Security' (14 July 2021) UN Doc A/76/135.
[81] ibid.
[82] Michael N Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace' (Just Security, 10 June 2021) <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/> accessed 15 September 2024.
[83] *ibid* Rule 1
[84] *ibid* Rule 4
[85] Michael N Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law' (2018) (19) (1) Chicago Journal of International Law 30
[86] Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) (112) (4) *American Journal of International Law* 583.

 [ISSN 2581-5369]

practice, and opinio juris continue to play a vital role in shaping the definitive application of international law to cyber operations, including those related to election interference.[87]

(B) Regional Efforts

The regional efforts to combat election interference, as exemplified by the European Union's General Data Protection Regulation (GDPR), the Council of Europe's Convention on Cybercrime (Budapest Convention), and the Organization for Security and Co-operation in Europe's (OSCE) guidelines, represent progressive steps towards addressing the complex challenges posed by foreign interference in electoral processes. These initiatives demonstrate a growing recognition of the transnational nature of cyber threats and the need for coordinated responses that transcend national boundaries. The GDPR's focus on data protection provides a valuable framework for safeguarding personal information that could be exploited in targeted disinformation campaigns,[88] while the Budapest Convention offers a mechanism for international cooperation in investigating and prosecuting cybercrime related to election interference.[89] The OSCE's work in developing guidelines for election observation in the context of new voting technologies acknowledges the evolving nature of electoral processes and the need for updated monitoring practices.[90] However, these regional efforts, while commendable, also point to the fragmented nature of the global response to election interference. The effectiveness of these measures is limited by their geographical scope and the varying levels of implementation and enforcement across different jurisdictions. Moreover, the evolving nature of cyber threats and interference techniques poses a constant challenge to the relevance and efficacy of these legal and policy frameworks. There is also a gap in addressing the specific challenges posed by state-sponsored disinformation campaigns and cyber operations aimed at influencing elections, which often operate in a gray area of international law.[91] As such, while these regional initiatives provide valuable tools and frameworks, they also underline the need for more comprehensive, globally coordinated efforts to safeguard electoral integrity in an interconnected digital landscape. Similarly, Non-binding initiatives like the Paris Call for Trust and Security in Cyberspace and the Christchurch Call represent important steps

[87] Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers' (2017) (30) (4) *Leiden Journal of International Law* 877

[88] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

[89] Council of Europe, Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS 185.

[90] OSCE Office for Democratic Institutions and Human Rights, 'ODIHR and Election Observation' <https://www.osce.org/odihr/elections> accessed 13 September 2024

[91] Michael N Schmitt, (n 81)

in addressing cyber threats and election interference through multi-stakeholder cooperation.[92] These initiatives demonstrate a growing recognition of the need for global collaboration in tackling digital challenges that transcend national borders. However, their non-binding nature limits their enforceability, and their effectiveness largely depends on voluntary compliance by signatories.[93] While they provide valuable frameworks for dialogue and cooperation, their impact on preventing concrete instances of election interference remains to be fully realized.

V. CHALLENGES TO SOVEREIGNTY IN THE DIGITAL AGE

The digital revolution has presented tough challenges to how nations assert and maintain their authority in cyberspace. These challenges stem from the inherently borderless nature of the internet and the rapid pace of technological advancement, which often outstrips the development of legal and regulatory frameworks. Prosecuting foreign state actors presents jurisdictional challenges. While the U.S. has indicted Russian individuals and entities, most remain outside U.S. jurisdiction.[94] One of the conspicuous problems in the digital age is the difficulty of attributing cyber activities to specific actors, particularly nation-states. This "attribution problem" complicates efforts to hold states accountable for malicious cyber activities, including election interference.[95] The key issues include but are not limited to the technical complexity of tracing cyber-attacks to their source, the use of proxy actors and "patriotic hackers" by states to maintain plausible deniability, time-consuming nature of forensic analysis, often allowing perpetrators to escape consequences. The attribution challenge undermines traditional deterrence strategies and complicates the application of international law to cyber incidents.[96] Also, Cyber operations often involve data passing through multiple jurisdictions, raising questions about where an attack can be said to have occurred and which state's laws apply. Determining the location of a cyber-attack for jurisdictional purposes is challenging. Applying territorial-based legal concepts to inherently non-territorial cyberspace creates conflicts arising from extraterritorial application of national laws to cyberspace. These challenges have led to calls for new legal frameworks that better reflect the realities of the digital domain.[97] Establishing state responsibility for cyber activities, particularly those conducted by

[92] French Ministry for Europe and Foreign Affairs, 'Paris Call for Trust and Security in Cyberspace' (12 November 2018) <https://pariscall.international/en/> accessed 13 September 2024.
[93] Christchurch Call, 'The Call' <https://www.christchurchcall.com/call.html> accessed 13 September 2024.
[94] U.S. Department of Justice, 'Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election' (13 July 2018) <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election> accessed 12 September 2024
[95] Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts' (2016) 70 *Journal of International Affairs* 75.
[96] Michael N Schmitt and Liis Vihul, (n 71)
[97] Jennifer Daskal, 'The Un-Territoriality of Data' (2015) (125) *Yale Law Journal* 326

non-state actors, presents another concern. The International Law Commission's Articles on State Responsibility provide a framework for attributing actions to states, but their application in cyberspace remains contentious.[98] Determining the threshold of state involvement necessary for attribution, also, addressing the use of proxy actors to conduct cyber operations on behalf of states. The concept of data sovereignty has gained prominence, with states asserting the right to regulate and control data generated within their borders. This has led to conflict between states and multinational tech companies, as well as between different national legal regimes.[99] The conflicts between data localization requirements and the global nature of the internet. Balancing national security concerns with the free flow of information. The EU's General Data Protection Regulation (GDPR) and China's Cybersecurity Law exemplify different approaches to asserting sovereignty over data, each with implications for global internet governance.[100] Determining when a cyber-attack constitutes a use of force or an armed attack under international law remains a complex issue. The Tallinn Manual 2.0 provides some guidance, but there is no international consensus on the thresholds for these classifications. For example, defining the point at which a cyber operation becomes a use of force, determining appropriate responses to cyber-attacks under the law of armed conflict, and addressing the potential for escalation in cyber conflicts. These issues have serious implications for state sovereignty and national security in the digital age. The current multi-stakeholder model, involving governments, the private sector, civil society, and technical experts, contrasts with state-centric approaches to governance. The key issues include balancing state interests with the global nature of Internet infrastructure, addressing calls for greater state control over Internet governance, and maintaining the openness and innovativeness of the Internet while addressing security concerns. These challenges compound efforts to hold states accountable for malicious cyber activities and enforce international norms in cyberspace. Rapid advancements in technologies such as artificial intelligence, quantum computing, and the Internet of Things present new challenges to sovereignty. These technologies have the potential to dramatically alter the cyber landscape, potentially rendering current legal and policy frameworks obsolete.[101] As states fight with these different challenges, the concept of sovereignty in the digital age continues to evolve. Addressing these issues will require innovative legal thinking, enhanced international cooperation, and a delicate balance between national interests and the global nature of

[98] International Law Commission, 'Articles on Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc A/56/10.
[99] Anupam Chander and Uyên P Le (n 30).
[100] Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 *New York University Law Review* 771.
[101] Peter J Katzenstein and Lucia A Seybert (eds), Protean Power: Exploring the Uncertain and Unexpected in World Politics (Cambridge University Press 2018).

 [ISSN 2581-5369]

cyberspace.

VI. THE FUTURE OF SOVEREIGNTY AND ELECTION INTEGRITY

The potential development of new international treaties and the evolution of customary international law norms regarding election interference reflect a growing recognition of the need for global governance frameworks in cyberspace. However, the effectiveness of such efforts may be limited by the pace of technological change and the divergent interests of state actors.[102] The increasing involvement of non-state actors, including tech companies and civil society organizations, in shaping norms around election integrity introduces new dynamics to the traditional state-centric model of international relations, potentially leading to more inclusive but also more complex governance structures. The promise of emerging technologies such as blockchain, artificial intelligence, and quantum computing in enhancing election security and integrity is significant.[103] These technologies offer potential solutions for creating more secure and transparent voting systems, real-time detection of anomalies and interference, and enhanced communication security.[104] However, these same technologies also present new vulnerabilities and challenges, particularly in terms of privacy, accessibility, and the likelihood of technological arms races. The dual-use nature of these technologies requires a careful consideration of their implementation and regulation in electoral contexts.[105] Moreover, the continued sophistication of cyber threats may outpace the development and deployment of defensive technologies, creating a persistent cat-and-mouse game between attackers and defenders. While such measures may enhance state control and perceived security, they also risk undermining the global collaboration necessary to effectively combat transnational cyber threats to election integrity. This concern between asserting national digital sovereignty and maintaining an open, global internet will likely shape the future landscape of international relations and cybersecurity cooperation. Addressing future challenges will require unprecedented levels of international cooperation. Improved mechanisms for sharing threat intelligence across borders could enhance collective defense against election interference. Countries may need to collaborate more closely on attributing cyber-attacks, potentially through international bodies or alliances. Additionally, there may be increased efforts by developed nations to build cybersecurity and election integrity capacities in developing countries, recognizing that vulnerabilities in any part of the global system can have far-reaching

[102] UN GGE, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174
[103] Nir Kshetri and Jeffrey Voas, 'Blockchain-Enabled E-Voting' (2018) 35(4) IEEE Software 95
[104] Michele Mosca and Marco Piani, 'Quantum Threat Timeline Report' (Global Risk Institute, 2021).
[105] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks' (2015) 38(1-2) *Journal of Strategic Studies* 4.

 [ISSN 2581-5369]

consequences. However, these cooperative efforts will need to navigate the complex terrain of national interests, technological disparities, and evolving notions of sovereignty in the digital age. The success of these initiatives will largely depend on the international community's ability to forge consensus on shared norms and practices in cyberspace while respecting the legitimate sovereignty concerns of individual states.

VII. FUTURE DIRECTIONS

Looking ahead, several areas require continued attention:

a. Comprehensive Federal Legislation: There are ongoing efforts to pass more comprehensive federal legislation addressing various aspects of election security.

b. Increased Funding: Sustained and increased funding for election security measures at all levels of government.

c. Enhanced Information Sharing: Improving mechanisms for sharing threat information between government entities and with the private sector.

d. Public Education: Expanding efforts to educate the public about foreign interference tactics and promoting digital literacy.

e. Technology Innovation: Encouraging the development of new technologies to enhance election security while maintaining accessibility and efficiency.

f. Development of Clearer Norms: There is a need for more specific international norms regarding what constitutes unacceptable behaviour in the context of elections and democratic processes.

g. Enhanced Attribution Capabilities: Improving the ability to attribute cyber operations reliably could strengthen the application of international law to cases of election interference.

h. Capacity Building: Supporting states in developing their cybersecurity capabilities and resilience against election interference is crucial for global security.

i. Multi-stakeholder Approach: Engaging non-state actors, including tech companies and civil society organizations, in developing responses to election interference is increasingly important.

 [ISSN 2581-5369]

j. Balancing Security and Rights: Any international legal responses must balance the need for security with the protection of human rights, particularly freedom of expression and privacy.

k. Dynamics Laws may need to be designed with built-in flexibility to adapt to rapidly changing technological landscapes.

l. Extraterritorial Application: There may be increased efforts to apply domestic laws extraterritorially to combat foreign election interference.

m. Harmonization of Laws: Greater international efforts to harmonize cybercrime and election laws could facilitate cross-border enforcement.[106]

VIII. Conclusion

The intersection of sovereignty and election integrity in the digital age presents a complex environment of challenges and opportunities. As we have explored throughout this article, the traditional notions of state sovereignty are fundamentally reshaped by cyberspace's borderless nature and the evolving tactics of foreign interference in electoral processes. The alleged Russian and Chinese interference in U.S. elections serves as a stark reminder of the vulnerabilities inherent in our increasingly digitized democratic systems. These incidents have exposed technical weaknesses and challenged our legal and diplomatic frameworks, pushing us to reconsider how we define and protect sovereignty in the 21st century. International legal responses, while evolving, still struggle to keep pace with the rapidly changing technological landscape. The efforts of the United Nations, regional organizations, and individual states to establish norms and regulations for cyberspace are commendable, but significant gaps remain. The challenge lies in creating a framework that is both robust enough to deter malicious actors and flexible sufficient to adapt to future technological advancements. The United States legal and policy responses demonstrate a growing awareness of the threat posed by foreign election interference. From executive orders to legislative measures and interagency coordination, these efforts reflect a whole-of-government approach to safeguarding electoral integrity. However, the decentralized nature of U.S. elections and the constant evolution of cyber threats necessitate ongoing vigilance and adaptation. Looking to the future, it is clear that preserving sovereignty and election integrity will require a multifaceted approach. Technological solutions such as blockchain and artificial intelligence offer promising avenues for enhancing election security, but they must be balanced against concerns of privacy and accessibility. The concept of digital

[106] Jonathan Clough, Principles of Cybercrime (2nd edn, Cambridge University Press 2015).

 [ISSN 2581-5369]

sovereignty will likely continue to evolve, potentially reshaping international relations and internet governance. Crucially, any solution must involve not just governments and tech companies, but also civil society and individual citizens. Enhancing digital literacy, fostering media awareness, and promoting transparent political processes are essential components of building societal resilience against foreign interference. The challenges posed by foreign election interference to sovereignty and democratic processes are significant, but not insurmountable. By fostering international cooperation, embracing technological innovation, adapting legal frameworks, and empowering citizens, we can work towards a future where digital sovereignty and election integrity are strengthened rather than undermined by technological progress. The path forward requires constant vigilance, adaptability, and a commitment to the fundamental principles of democracy in the digital age. As we navigate this complex terrain, we must remember that the goal is to protect the mechanics of elections and preserve the essence of democratic self-determination. In doing so, we can ensure that sovereignty in the digital age empowers rather than constrains and that our electoral processes reflect the people's will.

*****

 [ISSN 2581-5369]