

Chapter 9

State and Sovereignty in Cyber Space: Government Frameworks, Laws, and Security Tools

Aungshuman Ghosh, Advocate Supreme Court of India & Visiting Faculty Department of Legal Studies Swami Vivekananda University, Barrackpore, West Bengal.

Abstract

The emergence of cyberspace as a domain of geopolitical contestation has fundamentally disrupted conventional notions of territorial sovereignty and state authority. Unlike physical domains where boundaries are cartographically defined and legally recognized, cyberspace operates as a borderless, decentralized, and asymmetric environment — one in which the traditional Westphalian framework of state sovereignty faces its most formidable challenge yet. This chapter examines the intricate relationship between state power and cyberspace, interrogating how governments across the world have responded to the imperatives of digital governance through the development of legal frameworks, regulatory architectures, and technological security tools.

The chapter begins by deconstructing the myth that cyberspace exists beyond the reach of sovereign authority. While early internet discourse celebrated its emancipatory and ungovernable character, the reality of contemporary cyberspace reflects an increasingly fragmented landscape — one shaped by competing national interests, divergent regulatory philosophies, and the growing assertion of digital sovereignty by state actors. From China's "Great Firewall" and Russia's sovereign internet legislation to the European Union's General Data Protection Regulation (GDPR) and India's evolving data protection jurisprudence under the Digital Personal Data Protection Act, 2023, states have demonstrated both the will and the capacity to territorialize the digital domain.

Central to this analysis is a critical assessment of the international legal frameworks governing state conduct in cyberspace. The chapter evaluates the applicability of existing instruments of public international law — including the UN Charter, customary international law, and the Tallinn Manual 2.0 — to cyber operations, exposing significant normative gaps and interpretive ambiguities that states and non-state actors routinely exploit. The absence of a binding multilateral treaty on cybersecurity, combined with the attribution challenge inherent to cyber incidents, continues to undermine accountability and collective security in the digital realm.

The chapter further explores the domestic legal responses of key jurisdictions, analyzing how national cybersecurity laws, cybercrime legislation, and critical information infrastructure protection regimes function as instruments of both security and control.

Particular attention is given to the tension between state surveillance imperatives and the fundamental rights of citizens — a tension that legislation such as India's Information Technology Act, 2000 and its amendments, the United Kingdom's Investigatory Powers Act, 2016, and the United States'

Cybersecurity Information Sharing Act, 2015 have only partially resolved. The chapter argues that effective cybersecurity governance cannot be reduced to a technical exercise in deploying firewalls, encryption protocols, or intrusion detection systems; it is, at its core, a normative and institutional challenge demanding coherent legal architecture, inter-agency coordination, and meaningful democratic oversight.

The chapter concludes by proposing a multi-stakeholder model of cyber governance that reconciles state sovereignty with the transnational character of cyberspace. It advocates for enhanced international cooperation, capacity-building in developing nations, and the embedding of human rights principles within national cybersecurity strategies. Ultimately, the chapter contends that the myth of the impenetrable digital fortress — whether technological or legislative must yield to a more honest and resilient conception of cyber governance, one grounded in accountability, adaptability, and the rule of law.

Keywords: *Cyber Sovereignty, Digital Governance, Cybersecurity Law, International Law, Data Protection, State Surveillance, Critical Infrastructure, Cyber Warfare, Information Technology Act, Tallinn Manual.*

Key Outcomes

- Researching how state sovereignty developed through borderless cyberspace and digital domains shows its current state.
- The study examines international legal frameworks which control cyber operations to determine how these laws apply to state activities.
- The study analyzes domestic cybersecurity laws which exist in major jurisdictions such as India the United States the European Union and China.
- An examination involving the degree of state-security requirements that may infringe on fundamental human rights in cyberspace governance.
- An analysis into how security technologies or systems interact with prevailing legal and regulatory regimes.

Introduction: Sovereignty in the Digital Age

The concept of state sovereignty is rooted in the Westphalia Treaty (1648), which lays out a definition of sovereignty in terms of state action, which is made exclusive within its walls. The

classic concept of "sovereignty of the state"¹⁷³ holds that a country is supreme in terms of both the citizens and the inhabitants of the physical territory, undisturbed morally or physically from outside forces. In the cyberspace paradigm that has been introduced to undermine and alter the concept of territoriality, cyberspace is based on a network system that extends beyond physical boundaries and is devoted to global (data; aural, oral) communications. Specifically, the Internet has created great ambiguity in the manner people considered sovereignty when words like "sovereign"¹⁷⁴ evaporated, while some positions were creating questions about the probability of extant sovereignty structures ensuring some control over online operations, and there is a strong case for some urgency in considering novel structures of power and governance.¹⁷⁵ In the early years of the Internet, most discussions were full of a kind of techno-utopianism—a viewing of cyberspace as a wild, interstice, a digital common beyond the reach of any State, no matter how authoritative. From the "Declaration of the Independence of Cyberspace"¹⁷⁶ proposed by John Perry Barlow, came the idea that digital networks constitute an area that can slip outside the sovereignty of nation-states. That romantic viewpoint is totally prescription today on account of the stress these past twenty years have put on the governments. Basically, throughout the world governments have displayed both desire and ability regarding the employment of technology and law to capture the control over Cyberspace and to in fact disintegrate the once lofty dream of a worldwide digital network into a group of disjointed national online territories.¹⁷⁷

Cyber sovereignty assertion has occurred through different methods which include technical infrastructure controls and legal frameworks and surveillance systems and international coordination efforts. China's internet filtering system and Russia's internet sovereignty system both demonstrate Cyber sovereignty through their operations.

Conceptualizing Cyber Sovereignty: Theoretical Foundations: The Westphalian Challenge

In order from minor to major, the Westphalian concept of sovereignty is framed upon the notions of territorial integrity, political autonomy, and legal equality among independent states. None of these three can be realized in the digital domain. The constitution of digital territory presently finds itself taking a wholly digital-oriented form that comprises a pattern of meshed networks as well as sets of servers and data flows enforced by user information across different legal domains. In a very practical setting, an email will take just a couple of seconds to transmit from one server

¹⁷³ Arora, S. (2023). Digital Personal Data Protection Act, 2023: A critical analysis of exemptions and enforcement mechanisms. *Indian Journal of Law and Technology*, 19(2), 145-172.

¹⁷⁴ Ibid..

¹⁷⁵ Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24-42). National Defense University Press.

¹⁷⁶ Arora, S. (2023). Digital Personal Data Protection Act, 2023: A critical analysis of exemptions and enforcement mechanisms. *Indian Journal of Law and Technology*, 19(2), 145-172.

¹⁷⁷ Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

to another located in various places around the world, providing itself many entangled problems about which state has the right to monitor, control, regulate, etc., the transaction.¹⁷⁸

The necessary algorithm for this process to make political independence challenging is to form a web with its infrastructure spreading throughout all systems. No state, on the grounds of a statewide economy, can ever completely become independent of cyberspace. There is an interface between national networks international protocols and domain name systems, while the physical cyber infrastructure functions from one legal territory to another. Thus, the internet control mechanism quite naturally works on simplistic lines as a multi-stakeholder system rather than being state-led to isolate internet resources and root servers and global routing systems. Such a mechanism virtually binds together all territorial statuses, hugely contrasting with the rights-of-sovereignty that are given to states on land.¹⁷⁹

Third-party assessor discusses that the concept of Westphalian sovereignty of international equality is now diminishing due to technological disparities in cyber capabilities of different national states.¹⁸⁰ A plethora of technical capacities, its extensive know-how - whether about the good sophistication, security, offensive cyber warfare, and what have you-needed contribute considerably to the degree to which one of the countries is able to tag along, with the US and China or Russia of established giant cyber powers, or Israel running with high-tech cyber abilities, whereas the relatively low-cyber-capacities within individual member states could all be derived from the European Union. Some contrast to this, however, exists in the sense that most low-income countries lack even rudimentary cybersecurity measures. These differences in capability between countries mean that sometimes one country may just end up controlling another distant territory with the state remaining quite penetrable from beyond against international threats or internal, for that matter.¹⁸¹

Competing Models of Digital Governance

Two contrasting narratives are brought up currently around the very contemporary topic of cybersecurity. One points towards a liberal democracy-like model which offers a power-sharing platform in governance between many entities, be they governments, private sector, NGOs, and tech industry. The system could then be aligned like CSC group IANA or Internet Engineering Group around the three fundamental principles: public access; systems operability; and constraint of state power.¹⁸²

Another model, the complete central authority or the government with some underlying authority, states that the cyberspace in any nation should come under the complete control of the state as if it were an indispensable part of the territory, with no scope for trade-off on grounds of national security or police integration and internet censorship. China's argument on "cyber sovereignty"¹⁸³

¹⁷⁸ Brenner, S. W. (2007). At light speed: Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law and Criminology*, 97(2), 379- 475.

¹⁷⁹ Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press.

¹⁸⁰ Ibid.

¹⁸¹ Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

¹⁸² DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

¹⁸³ DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press

is probably the most complete implementation of such a model. According to the statement of the government of China, countries as states are entitled, and in the matter of policy commitment, obligated to manage their Internet intern systems in compliance with national laws and culture, while there is an added dimension that sees criticism from outsiders as an intrusion into sovereign rights.¹⁸⁴ The European Union develops its third model which establishes a system for government control that protects rights through its strong legal frameworks which govern both state and private sector operations. The General Data Protection Regulation (GDPR) serves as a regulatory sovereignty example because it enables EU legal standards to reach worldwide through its global enforcement power. The EU governance model requires effective control systems which include strong legal frameworks to limit state surveillance and corporate data operations while ensuring democratic oversight and fundamental rights protection.¹⁸⁵

Table 1: Comparative Models of Cyber Governance

Governance Model	Primary Actors	Key Principles	Representative Examples
Multi-stakeholder	States, Private Sector, Society, Technical Community	Openness, Minimal Intervention, Distributed Authority	ICANN, Internet Governance Forum, Early Internet Architecture
State-Centric Sovereignty	National Governments	Territorial Control, Regulatory Authority, Security Primacy	China's Great Firewall, Russia's Sovereign Internet Law, Iranian National Network
Regulatory Sovereignty	State Institutions with Rights Constraints	Legal Frameworks, Rights Protection, Democratic Accountability	EU GDPR, German NetzDG, French Data Protection Authority
Hybrid	Mixed State and	Pragmatic Balance,	India's IT Act, UK
Models	Private Coordination	National Security with Limited Openness	Investigatory Powers Act, Singapore Cybersecurity Act

¹⁸⁴ Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 107- 145). Rowman & Littlefield.

¹⁸⁵ Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

International Legal Frameworks: Norms, Gaps, and Ambiguities:

Applicability of Public International Law to Cyberspace

Scholars and policymakers have ongoing discussions about how existing public international law applies to activities in cyberspace. The United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security reached its 2013 and 2015 conclusions about state behavior in cyberspace by stating that international law, together with the UN Charter, governs state activities in cyberspace. The agreement established a major achievement because it proved that states cannot treat cyberspace as an area without laws which protects them from their duty to follow international treaties.¹⁸⁶

International law applicability remains an area now needing further attention. It does nothing to help with the ultimate question as to how legal rules become applied to cyberspace. The example of using force rendered illegal by the UN Charter, under Article 2(4), brings to light the difficulties of interpreting that signal. This prohibition is meant to prohibit kinetic military operations, but creates limitless uncertainties when applied to cyber operations. So, should a more active breakdown in the functionality of critical infrastructure achieved by a distributed denial-of-service cyber attack be considered as a use of force? Likewise, what about cyberspying, for instance by foreign intelligence agencies, wherever large-scale operation is concerned? On these questions, States are significantly divided, largely because of broader consensus as to where the threshold should be when assessing cyber activities as violations of sovereignty or acts of aggression.¹⁸⁷

Test your understanding: In what way did poetry advance your understanding of love, death, or history in War of the Physicians? Stick to three examples from case materials supportive of your opinion, duly accepted by the community.

The Tallinn Manual Framework

There is no longer to wait to embellish the desktop with fascinating wallpapers by exploring your photographic abilities. By now, your picture frames are quite packed, but they prove inadequate. Even though unemployment forms are discussed by people, usually the hard-core job seekers fare well with handwriting superficial questions on resumes, the just conditions for face-to-face interviews vanish, and there is excessive weight on the question of what a person did.¹⁸⁸ However, by recording their portfolios online, several job seekers are entitling their fates to companies to evaluate their applications seriously through the information they supply directly. In terms of time, the concept should start with shots so less saleable they do not want them; [uploaders] may well have kept these images to this moment. Although the authors of the first

¹⁸⁶ Tikk, E., & Kerttunen, M. (2017). The alleged demise of the UN GGE: An autopsy and eulogy. *Cyber Policy Institute Brief*, November 2017, 1-8.

¹⁸⁷ Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.

¹⁸⁸ Ibid.

paragraph point to endorsements of the Tallinn Manual, the text originated from an academic study conducted with no government intervention. This study was built on expert opinions rather than on established international practice. Such study has not been based on actual international customary law or an ensuing legal doctrine. Its judgment on contested issues such as: the point at which a cyber operation will be characterized as a use of force or as an infringement on sovereign rights is accepted but not uniformly accepted as a legal principle.¹⁸⁹ Though the Manual has policy relevance, it does not serve as an effective tool for understanding state behavior in cyberspace because there remains no among legal experts about what a given legal definition.

Domestic Legal Responses: National Cybersecurity Frameworks:

The Indian Framework: Information Technology Act and Beyond

India's cyberspace legal system developed significantly from 2000 because of the Information Technology Act implementation. The IT Act enables electronic commerce through digital transaction recognition which later required legal amendments to solve new cybersecurity threats and cybercrime issues and content management requirements. The 2008 amendments created new laws which addressed cyber terrorism and data protection and set intermediary liability standards because the government had started to view cyberspace as a legal area that needed complete control.¹⁹⁰

The IT Act center section 69 gives central and state governments special rights to monitor and intercept all information which people send through computer systems to protect national security and public safety and international relations and territorial integrity. Civil rights defenders have raised major privacy issues about government monitoring systems because these systems depend on special rules which the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 establish for monitoring and protecting information.¹⁹¹ (Bhatia, 2019).

The Digital Personal Data Protection Act 2023 stands as India's current attempt to create a complete framework for data protection rights. The Act establishes three data protection principles which require data minimization and purpose limitation and individual consent in addition to establishing the Data Protection Board as the nation's data protection authority. The Act imposes major restrictions on government surveillance activities because its main exemptions allow security agencies to operate without restrictions when they conduct operations for national security or public safety or territorial integrity. The government has chosen to protect

¹⁸⁹ Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.

¹⁹⁰ Maini, T. S. (2012). The Information Technology Act, 2000: A legal framework for cyber law in India. *Indian Journal of Law and Technology*, 8(1), 89-112.

¹⁹¹ Bhatia, R. (2019). Surveillance, privacy, and the Information Technology Act: Examining Section 69 and procedural safeguards. *Journal of Indian Law and Society*, 10(1), 34-58.

national security and maintain flexible control over operations instead of protecting user privacy through this system of exemptions which has resulted in privacy complaints from users.

The United States Approach: Fragmented Regulation

The United States lacks a comprehensive federal cybersecurity law which matches the cybersecurity systems that other major jurisdictions have implemented. American cyber governance functions through a broken system which consists of specific industry rules and executive directives and optional security partnerships between public and private sectors. The Cybersecurity Information Sharing Act (CISA) of 2015 represents one of the few cross- sectoral federal initiatives which enable private companies and government bodies to exchange cybersecurity threat data. CISA fails to function as an all-encompassing governance instrument because its implementation depends on voluntary participation and the law provides only minimal liability coverage according to Watters.

Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience designates sixteen critical infrastructure sectors and establishes a framework for protecting these sectors from cyber threats through coordination between sector-specific agencies and private sector partners. The public-private partnership model serves as the American market- driven solution which requires minimal regulatory oversight while creating a stark contrast to standard regulatory methods that other jurisdictions employ. The Federal Information Security Modernization Act (FISMA) governs cybersecurity for federal agencies which need to do continuous monitoring and annual assessments and follow standardized security controls that use National Institute of Standards and Technology (NIST) guidelines.¹⁹²

The Fourth Amendment of the United States Constitution protects citizens from government surveillance through its prohibition of unreasonable searches and seizures yet the extent of these protections remains disputed in relation to online activities. The Foreign Intelligence Surveillance Act (FISA) establishes procedures for electronic surveillance and physical searches related to foreign intelligence gathering while Section 702 of the FISA Amendments Act authorizes warrantless surveillance of non-U.¹⁹³

The European Union: Rights-Based Regulatory Sovereignty

The European Union currently leads worldwide rights-based cyber governance because it developed extensive legal systems which regulate online activities while safeguarding essential human rights. The General Data Protection Regulation (GDPR), which entered into force in 2018, establishes stringent requirements for data processing, including principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. The GDPR applies extraterritoriality because it governs all

¹⁹² Paganini, P. (2018). The evolution of U.S. federal cybersecurity policy: From FISMA to continuous monitoring. *International Journal of Cyber Warfare and Terrorism*, 8(3), 45-67.

¹⁹³ Ibid.

organizations that handle personal data from EU residents, which extends European Union legal standards throughout the world according to Bradford.¹⁹⁴

The Network and Information Security (NIS) Directive, adopted in 2016 and updated as NIS2 in 2022, establishes cybersecurity requirements for operators of essential services and digital service providers. The directive requires member states to designate competent authorities, establish computer security incident response teams (CSIRTs), and implement national strategies for network and information security. The 2019 Cybersecurity Framework Act of the European Union gives EU Cybersecurity Agency (ENISA) added powers in setting up a European Certification Framework for cybersecurity-certification schemes. Certification guarantees that ICT products, services, and processes satisfy certain security requirements for trustworthiness and integrity of the single market where applicable. The legislation is the EU's endeavor to use regulation to shape security standards worldwide and extend influence.

China's Comprehensive Control Architecture

The Chinese government has established its cyber sovereignty system which functions as the most advanced system for state control over online activities through its comprehensive digital presence.

The Chinese Cybersecurity Law which became effective in 2017 requires network operators to implement security measures which include conducting security assessments and storing data within national borders and working with government intelligence agencies and security organizations. The law defines critical information infrastructure as essential systems which protect approximately 80 percent of China's digital economy from security threats through government monitoring.¹⁹⁵ The Chinese government uses its cybersecurity framework to implement multiple regulatory systems which include monitoring online content and monitoring social credit systems and conducting full-scale surveillance operations. The Great Firewall functions as an advanced system which uses technical filtering methods and DNS manipulation techniques and deep packet inspection methods to prevent users from accessing foreign websites and services which the government considers dangerous for national security and public order. Social media platforms in the country must enforce strict content control measures which create heavy legal liability for them if they do not delete banned materials without delay. The Chinese government uses advanced technological systems for social control through its implementation of artificial intelligence and big data surveillance technologies which operate in Xinjiang and other areas.¹⁹⁶

The Data Security Law and Personal Information Protection Law establish the complete legal structure which governs China's digital operations through their 2021 enactment. The laws create a framework for data classification which establishes rules for cross-border data transfers and

¹⁹⁴ Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

¹⁹⁵ Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In *Governing Cyberspace: Behavior, Power, and Diplomacy* (pp. 107- 145). Rowman & Littlefield.

¹⁹⁶ Mozur, P. (2019). One month, 500,000 face scans: How China is using AI to profile a minority. *The New York Times*, April 14, 2019.

specifies conditions under which government authorities can access information stored by private companies.¹⁹⁷

The framework shows China's intention to treat data as a national resource which the government will control while giving precedence to state security needs above individual and business rights. The current strategy uses data.

Table 2: Comparative National Cybersecurity Frameworks

Jurisdiction	Primary Legislation	Governance Approach	Key Features
India	IT Act 2000 (amended), Digital Personal Data Protection Act 2023	Centralized with security emphasis	Government interception powers, intermediary liability, broad security exemptions, emerging data protection
United States	CISA 2015, FISMA, Sector-specific regulations	Fragmented, public-private partnerships	Voluntary information sharing, critical infrastructure protection, Fourth Amendment constraints, sector-based regulation
European Union	GDPR 2018, NIS Directive/NIS2, Cybersecurity Act	Rights-based regulatory sovereignty	Extraterritorial application, comprehensive data protection, mandatory breach notification, certification schemes
China	Cybersecurity Law 2017, Data Security Law 2021, Personal Information Protection Law 2021	Comprehensive state control	Data localization, critical infrastructure security, content control, government access
			requirements, social credit integration
United Kingdom	Investigatory Powers Act 2016, Data Protection Act 2018, Network and Information Systems Regulations 2018	Balanced security and rights (post-Brexit hybrid)	Bulk interception powers, judicial authorization, incident reporting, GDPR adequacy maintenance

¹⁹⁷ Mozur, P. (2019). One month, 500,000 face scans: How China is using AI to profile a minority. *The New York Times*, April 14, 2019.

Security Tools and Technological Governance:

Technical Infrastructure and Control Mechanisms

The sovereignty of states to control their cyberspace depends on their capabilities to secure networks and manage their technology systems. States establish a framework of digital activity monitoring which includes technological systems that enable them to observe and control their online operations. The system provides two types of monitoring systems, with one being the lawful interception interface, which telecommunications networks must use and the other being advanced surveillance systems, which operate without public knowledge and democratic control.¹⁹⁸

China's Great Firewall uses network filtering systems, which combine multiple technical strategies, including IP address blocking, DNS filtering, and redirection, URL filtering, and packet inspection, together with connection reset. States use these systems to block access to international websites and online services, while permitting users to connect to local services. Different jurisdictions show various degrees of technical development for these systems, as some countries use simple blocking methods, which users can bypass, while other countries use deep packet inspection and machine learning systems, which can detect and block encrypted data together with its circumvention tools.

Countries such as the United States, India, Australia, Spain, and the United Kingdom passed laws that enacted Telecommunications Assistance for Law Enforcement or CALEA to make telecommunications service providers build a system capable of lawful interception for government surveillance.¹⁹⁹ However, such countries had put certain regulations to incentivize end-to-end encryption and banned unnoticed crypto, condemned attempts to weaken any network design, or innovations for government.

Cyber Defense and Critical Infrastructure Protection

In the case of national cybersecurity strategies, attention to the protection of critical infrastructure as topically represented is now seeing several cyberattacks threatening the likes of all digital systems that support energy distribution, critical telecommunications networks, financial systems, water supplies, ground transportation infrastructures, and healthcare systems. Providing for the shortening of regulatory frameworks, the states have imposed baseline security measures, a requirement for incident reporting, and the provision for information sharing among privatesector operators in collaboration with government agencies.²⁰⁰

¹⁹⁸ Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, 21(4), 43-57.

¹⁹⁹ Ibid.

²⁰⁰ Lewis, J. A. (2019). *Critical Infrastructure Protection and Cyber Resilience*. Center for Strategic and International Studies.

The elegance of the Cybersecurity Framework from the National Institute of Standards and Technology in the United States is a voluntary scheme that has been launched to voluntarily moderate the efforts to combat cybersecurity risks for critical infrastructure. It is based on the classification of its cybersecurity activities into five core functions: Identification, Protect, Detect, Response, and Recovery. It remains the most dominant standard in most sectors, while on a voluntary basis, because the standard asserts standardization presentations that are beneficial in business ventures involving large installations, exercising joint acceptance of them.²⁰¹ So, some concerted endeavor is most pressing for the intention to make possible the most viable arrangement of technical, procedural, and control mechanisms guaranteeing a likely assurance against intrusion vectors, devoid of a cumbersome, overly stringent tigris of imminent regulation that would be rendered obsolete too hastily by rapidly changing technology behaviors.

Having the Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) solve cybersecurity incidents also resulted in working with the national and sector teams that are a part of these consortia. National CERTs operate in most countries to manage cyber incidents through their response coordination, threat intelligence sharing, and technical aid provision to government bodies and critical infrastructure operators. International coordination among CERTs through forums such as FIRST (Forum of Incident Response and Security Teams) enables international collaboration to combat cyber threats because effective cyber defense needs both national capabilities and international partnerships.²⁰²

The Surveillance-Rights Tension: Democratic Accountability in Cyber Governance

The declaration of state control over cyberspace leads to conflicts between security needs and essential human rights which include privacy rights and freedom of speech and the right to fair legal proceedings. Democracy requires security systems to function within established constitutional boundaries which demand proper supervision and which should only be used for genuine government needs. The combination of complex technical systems for cyber surveillance together with hidden intelligence work and ineffective control systems prevents organizations from achieving their accountability standards according to Diffie and Landau.²⁰³

The Edward Snowden disclosures from 2013 revealed how the United States National Security Agency and its partner intelligence agencies operated extensive and sophisticated surveillance programs. The programs conducted bulk telephone metadata collection which enabled them to intercept internet traffic through their partnerships with telecommunications companies and they used commercial encryption system weaknesses to conduct their operations. The revelations created a global scandal which led to multiple countries implementing changes including USA FREEDOM Act in the United States and legal actions that resulted in the Schrems II decision by

²⁰¹ Ibid.

²⁰² Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45, 42-57.

²⁰³ Diffie, W., & Landau, S. (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT Press.

the European Court of Justice which rendered the EU US Privacy Shield agreement invalid according to Greenwald 2014.²⁰⁴

To achieve proper democratic control over cyber surveillance, multiple institutional structures need to be established. First, democratic legitimacy requires legal authorization through legislation instead of using executive power to establish limits on discretionary authority. Second, judicial oversight needs to include specific requirements for individualized warrants which must meet the probable cause standard or an equivalent threshold, to prevent unauthorized surveillance. Third, all organizations need to meet legal security requirements when disclosing their surveillance activities and operations according to defined requirements.

Toward a Multi-Stakeholder Model: Reconciling Sovereignty with Transnational Governance

The existing conflict between territorial sovereignty and cyberspace's transnational nature needs more than state actions and technical solutions to achieve its resolution. Cyber governance requires multiple stakeholders to work together because states and international organizations and private sector entities and civil society organizations and technical communities need to cooperate. Stakeholders in governance frameworks possess separate abilities and requirements and viewpoints which need to be unified.²⁰⁵

Certainly, there are significant political DPI issues in international cybersecurity cooperation.

Antagonism among the great powers turned on fundamental differences over norms governing the behavior of states in cyberspace, with authoritarian regimes speaking of state sovereignty and content control, while liberal democracies argue for openness and fundamental rights. At the international level, cybersecurity endeavor could not proceed, due to an irreconcilable normative position between two Chinese and Russian proposal for an International Code of Conduct for Information Security and the Western countries taking up the United Nation Group of Governmental Experts (UN GGE) meeting process which was to frame a voluntary, agreed-upon set of norms.²⁰⁶

Operational partnerships offer proof positively that cybersecurity cooperation has succeeded, in the face of the political impediments. Intergovernmental cooperation targeting the implementation of law enforcement in transnational cybercrime, inter alia, with Interpol cybercrime programs and mutual legal assistance frameworks, remains a possibility. ICANN and Internet Engineering Task Force (IETF) and the regional internet registries are technical bodies for coordination, which, through their capabilities of operational coordination, maintain the global internet infrastructure.²⁰⁷ It thus may be observed that effective cyber governance is

²⁰⁴ Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

²⁰⁵ DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

²⁰⁶ Tikk, E., & Kerttunen, M. (2017). The alleged demise of the UN GGE: An autopsy and eulogy. *Cyber Policy*

²⁰⁷ Watters, P. (2016). The Cybersecurity Information Sharing Act: A legislative response to cyber threat proliferation. *Georgetown Journal of International Affairs*, 17(3), 125-138.

security-held by a formal operational partnership of an international nature, rather than the great many multilateral agreements.

Conclusion

The developing international system in cyberspace shifts the compartments. It is simply untenable to propose that cyberspace is ungovernable and therefore free from sovereignty. States have increasingly asserted their will to exert control over digital networks and thus raise legal and technological mechanisms and regulatory architectures that position the space closer to the national interest and political system; thus, governance systems across jurisdictions have a range of effectiveness and legitimacy, depending on their operational standpoint and doctrinal inconsistency. Based on many widely accepted international norms, domestic forces may thus be useful in providing such guidelines for the behavior of states in cyberspace, with many needs to fill gaps and resolve ambiguities in frames of reference of rights regarding the "non-usage" of borders.²⁰⁸ Public international law, a term preferred by many supportive professors, is claimed to govern cyberspace operations everywhere while details such as points of threshold and proportionality in attribution raise yet more complex questions, not to mention the policy questions of how to respond to incidents. The increasingly frequent collusion that states mount in the grey areas operating less than formal legal limits makes it difficult for everyone to anticipate the behavior of the said nations or for resulting actions to subsequently be condemned by the accepted norms of international law. Variably different domestic legal frameworks create varied governance models-some riotous,

while others would be bordering on regulatory sovereignty or semi-principle-based regulatory sovereignty; where they seek a balance between state authority and private sector participation in various ways, each one putting the security vs rights argument first and then the economic efficiency vs equal access- to-innovation one.

The second concept (that is, equal access for all) runs parallel to the idea of ensuring all rights for all people and places; to what safeguards will the governance apparatus subscribe at the price of other rights? Vigorous debate about surveillance versus rights would now set out greener and more incipient paths that are not-and indeed never will be-hatch for established regulatory bodies. Thus, accounting for probable restraining conditions on surveillance by state institutions does require intense democratic oversight specimens accompanying judicial review and compliance with transparency demands on independent data protection.

²⁰⁸ Tikk, E., & Kerttunen, M. (2017). The alleged demise of the UN GGE: An autopsy and eulogy. *Cyber Policy*