ORIGINAL ARTICLE

National Cyber- security Strategies and International Law: A Comparative Study of State Responsibility, Cyber Governance, Resilience and Strategic Competition

SAEED AHMED BUTT[1], ABIDA HASSAN[2]

ABSTRACT

Background: Cyber security is no longer just a technical issue, but rather a critical component of national security, international law, protection of critical infrastructure, and geopolitical competition. States have broadly acknowledged the relevance of international law to cyberspace, but there are still major gaps in cyber governance, State responsibility, attribution, sovereignty, due diligence, cyber resilience and strategic competition.

Objective: To analyze and contrast the ways in which selected national cybersecurity strategies incorporate international cyber law and domestic cyber governance, resilience, and strategic priorities.

Methods: National cybersecurity strategies, governmental legal statements, international legal instruments, UN documents and related academic literature were gathered and analyzed through a qualitative comparative doctrinal and policy analysis. To represent different governance and strategic models, the United States, the United Kingdom, Australia, China and Estonia were purposively selected. The analysis revolved around five domains: governance architecture, allocation of cybersecurity responsibility, national resilience, international law, and State responsibility, and strategic competition.

Results: All five States agreed on the importance of critical-infrastructure protection, cyber resilience, incident response, national capability building, and cooperation with other countries. But significant differences were found in the philosophy of governance and legal interpretation. The USA, UK, and Australia stressed public-private responsibility, coordinated attribution, resilience, and international partnerships. China highlighted cyber sovereignty, State-led regulation, technological autonomy and multilateral governance, while Estonia showcased continuity of government and trusted digital services as the core of its digitally integrated resilience model. The areas of disagreement included sovereignty, due care, imputability and countermeasures.

Conclusion: Contemporary cybersecurity strategies demonstrate functional convergence but persistent legal and institutional divergence. To minimize escalation risks and build responsible State behavior in cyberspace, greater clarity in international legal positions, more robust resilience mechanisms, credible attribution practices, and continued multilateral cooperation will be needed.

Keywords: cybersecurity strategy; international law; State responsibility; cyber governance; cyber resilience; attribution; cyber sovereignty; critical infrastructure; strategic competition.

INTRODUCTION

Cyberspace is a very important domain for national security, economic growth, public administration, military strength and international strategic competition[1]. As a result of the increasing reliance of governments, financial systems, healthcare, energy networks, telecommunications, transportation and defence infrastructures on digital technologies, cybersecurity has become a key pillar of State policies and international relations. Modern cyber-attacks can affect critical government functions, steal government data, interfere with political operations, harm economic activity, and have global repercussions. In this way, the national cybersecurity strategies are increasingly linked to regulation, technology, critical-infrastructure resilience and the ability to withstand cyber attacks, cooperation among intelligence agencies, and diplomatic engagement, and the development of national cyber capabilities[2].

Traditional notions about responsibility and jurisdiction in international law have also been called into question with regard to the proliferation of cyber threats. Cyber operations frequently are performed remotely, directed through infrastructure across multiple jurisdictions and using compromised systems or non-State proxies[3]. These characteristics make it difficult to determine who has carried out an operation, whether it can be considered legally attributable to a State, and which International obligations have been violated. While States have increasingly reiterated that applicable international law extends to activities in cyberspace, there is still significant divergence on how to interpret the application of notions of ‘sovereignty', ‘non-intervention', ‘due diligence', ‘State responsibility', ‘countermeasures', ‘the prohibition on the use of force' and ‘the right of self-defence'[4].

The law of State responsibility is of specific relevance in this context as a cyber incident does not necessarily constitute an internationally wrongful act because of its harmful effects. International responsibility will normally involve behaviour which is legally imputable to a State and constitutes a violation of an international responsibility[5]. This distinction is important between technical attribution, political attribution and legal attribution. Technical evidence can include infrastructure, malware attributes, or operational behavior, while legal attribution entails the application of accepted standards of conduct for State organs, agents, or persons operating under the direction or control of the State. Meeting these requirements has proven challenging, leading to ongoing discussion about cyber operations by proxies, criminal organizations and other non-State actors[6].

Meanwhile, the idea of national cybersecurity strategies has shifted from deterrence and incident response to more general notions of cyber resilience[7]. A growing number of modern strategies recognize that it is impractical to stop cyber intrusion entirely, and focus on being able to predict, prepare for, respond to, and adapt to serious cyber events. Today, Resilience includes redundancy of critical systems, continuity of essential services, secure-by-design technologies, information sharing, incident-response capability, supply-chain security, workforce development and coordination between the public and private sectors. This evolution is especially significant as a large portion of the digital infrastructure that the States rely on is owned, built, and maintained by private entities, not governments[8].

The distribution of the authority and responsibility of cyber security, however, is quite different between different States[9]. It is increasingly the U.S. emphasis to shift cybersecurity responsibility to technology providers, critical-infrastructure operators, and institutions that have the biggest capacity to manage systemic risks. Cyber security is a part of the United Kingdom's thinking on national cyber power, which encompasses resilience, technological capability, intelligence, diplomacy, and international influence. Australia's approach to a whole-of-nation cyber shield is built around a series of interconnected cyber shields comprising citizens, businesses, secure technologies, threat sharing, critical infrastructure, national capability and international cooperation[10].

[1]Assistant Professor, Government College University, Lahore, Pakistan.
[2]Assistant Professor, Dr. Muhammad Iqbal Law School, Government College University, Lahore, Pakistan.
Correspondence to: Dr. Saeed Ahmed Butt, Email: saeedbutt@gcu.edu.pk

One of the unique and significant ways to approach cyber governance is through a Chinese lens. In its policy framework, it gives a high priority to cyber sovereignty, national security, State regulatory power, critical information infrastructure, data governance, technological innovation, and multilateral cooperation with other nations[11]. In this context, States have the sovereign right to maintain their own models of cyberspace governance, technological evolution, in accordance with the principles of the United Nations Charter and international cooperation[8]. Estonia offers a counter-model where cyber security is tightly coupled in the work of a highly digitalized State. Its experience has shown that cyber resilience is not just about network protection but also about the continuity of public administration, digital identity systems and trusted electronic services in the event of significant disruption[9].

Both of these differing national strategies are embedded in an international context in which geopolitical and technological competition is growing[10]. Cybersecurity is now linked with artificial intelligence, semiconductor manufacturing, telecommunications networks, cloud systems, digital platforms, data governance and control, encryption, quantum technologies and international technical standards. Strategic competition is thus increasingly no longer just about cyber operations, but about control of technological ecosystems and the critical dependency on digital products. This has led to tensions in the international governance of cyber technologies, where a lot of technological competition is legal but has important strategic implications. International law needs therefore to differentiate between 'legitimate' national competition and intervention, prohibited uses of force, internationally wrongful cyber operations, and actions that are likely to pose a 'threat' to international peace and security[11,12].

These uncertainties have been addressed with multilateral efforts. The applicability of international law, voluntary norms of responsible State behaviour, confidence building measures, capacity building and ongoing institutional dialogue have been gradually evolving in the United Nations processes[12]. This has helped to build consensus on general principles, such as critical infrastructure protection and the importance of international cooperation. However, while there is some consensus at the level of the general principles, complete consensus on their use has not been reached. States remain divided on the existence of an independently enforceable rule of sovereignty in cyberspace, on whether there is a general duty of 'cyber due diligence' and on what standard of evidence should be used in public attribution and what circumstances, if any, would justify taking countermeasures or other responsive action[13,14].

Another challenge is that the current literature focuses on Cyber Law and Cyber Security Policy separately from an international perspective. Legal scholarship often considers doctrinal issues like attribution, sovereignty, intervention, use of force, or countermeasures, while policy studies tend to highlight institutional governance, cybersecurity capacity, or infrastructure protection, or strategic competition. Fewer studies focus on the interaction between these elements in national cybersecurity strategies, and what influence different internal governance models have on States' accountability regarding their international obligations and global cyber stability[15,16].

The present study therefore, aims at carrying out a comparative study of the cybersecurity strategies and legal stance of the United States, United Kingdom, Australia, China and Estonia, Pakistan. The selection of these jurisdictions is based on the diverse perspectives regarding cyber power, governance, resilience, technological sovereignty, public-private responsibility and international cooperation. The study assesses them on four core aspects: State responsibility and international law; domestic and international cyber governance; national resilience and protection of critical infrastructure; and the emerging strategic and technological competition. By examining these dimensions within a common analytical framework, the study seeks to identify areas of convergence, continuing legal divergence, and policy lessons relevant to the development of a more stable, resilient, and rules-based international cyber environment[17-20].

METHODOLOGY

Study Design: The qualitative comparative doctrinal and policy-analysis approach was used to analyze the connection between national cybersecurity strategies and international law. The analysis concentrated on selected States' approaches to the concept of cyber governance, their distribution of responsibility for cyber security, the national resilience of their societies, their understanding of the rules of State responsibility, and their reactions on strategic competition in cyberspace. A comparative approach was chosen due to the fact that national cybersecurity frameworks vary in terms of how they define critical infrastructure, public-private responsibility, international cooperation, due diligence, and countermeasures, as well as their approach to sovereignty and attribution.

The study combined doctrinal legal analysis with structured comparative policy analysis. Relevant principles of international law, such as those on State responsibility, sovereignty, non-intervention, prohibition of the use of force, self-defence, due diligence, attribution and countermeasures, were interpreted by doctrinal analysis. The national cybersecurity strategies and other governmental documents were analyzed to evaluate the explicit or implicit presence of these principles in policies.

Selecting Comparative Cases: To make comparisons, five States were purposively selected: the United States, United Kingdom, Australia, China and Estonia. They were selected based on their relevance to cyber governance today and differences in their legal, political, technological and strategic orientations.

The United States was selected because of its substantial technological capacity, global cyber influence, extensive public-private digital infrastructure, and emphasis on collective cyber defence and strategic competition. The United Kingdom was included due to its maturity with respect to cyber governance institutions and specific public statements on the use of international law for cyber operations. Australia was chosen due to its national strategy, which includes whole-of-nation resilience, protection of critical infrastructure, regional capacity building, and relatively clear international-law stance.

China was included to represent a State-centered model emphasizing cyber sovereignty, national security, technological autonomy, domestic regulatory authority, and multilateral governance. Estonia was chosen as an advanced digital State, where there is a high dependency on digital public services, and the cybersecurity model is focused on resilience, continuity of government, digital identity and international cooperation. These jurisdictions had enough institutional and normative differences to make for significant inter-jurisdictional comparison.

Sources of Data: The study was based on purely documentary sources i.e. primary and secondary sources which were available in public domain. The sources of primary materials ranged from national cybersecurity strategies and cyber action plans to governmental policy statements, national legal stances on international law in cyberspace, official cyber-governance documents, relevant legislation and regulatory frameworks, and documents published by international organisations.

International law materials comprised: the Charter of the United Nations; the International Law Commission Articles on Responsibility of States for Internationally Wrongful Acts; reports of the United Nations Group of Governmental Experts on security in the use of information and communications technologies; reports and outcomes of the United Nations Open-Ended Working Group on security in the use of information and communications technologies; relevant United Nations General Assembly resolutions and other authoritative international instruments concerning responsible State behaviour in cyberspace.

The secondary sources comprised peer-reviewed journal articles, scholarly books, legal commentaries, institutional reports, and well-known academic analyses related to international cyber

law, State responsibility, cyber governance, cyber resilience, attribution, and strategic competition.

Search Strategy: Systematic searches of governmental websites, United Nations repositories, international legal databases and academic databases identified relevant literature and official documents. Searches included combinations, such as "national cybersecurity strategy," "international law cyberspace," "State responsibility cyber operations," "cyber sovereignty," "cyber attribution," "due diligence cyberspace," "cyber countermeasures," "critical infrastructure cybersecurity," "cyber resilience," "strategic competition cyberspace," "cyber governance," and "responsible State behaviour."

The following country-specific searches were carried out by adding the names of the United States, United Kingdom, Australia, China, and Estonia to these terms. Additionally, relevant legal and policy publications were consulted through reference lists to find more authoritative materials. Where the legal or strategic position of a State was under consideration, preference was given to primary governmental and intergovernmental sources.

Eligibility Criteria: Documents were included if they met one or more of the following criteria: they were an official national cybersecurity or cyber-governance strategy; they were an authoritative governmental statement about the application of international law in cyberspace; they described national approaches to cyber resilience, critical infrastructure or cyber governance; they dealt with international norms of responsible State behaviour; and they were a substantive scholarly analysis directly relevant to the comparative framework.

Documents were excluded if they were commercial cybersecurity commentary, unverified media reporting, purely technical descriptions not relevant to legal and policy issues, or duplicated documents, or opinion pieces that did not provide sufficient analytical or evidentiary content. If there were several different versions of a governmental strategy, the latest version in force was used; earlier versions were included if required to clarify the development of national policy.

Period of Review: Documents from 2017 to 31 July 2026 were analysed, giving the study a chance to include the most current evolutions in national cyber security policy and international cyber governance. Previous international law documents have been incorporated where they continue to be relevant for the interpretation of State responsibility or the regulation of cyber operations.

This review period was chosen to cover significant national cybersecurity strategies, the coming of age of United Nations cyber diplomacy, growing geopolitical rivalry over digital technologies and the rising value of cyber resilience and critical-infrastructure protection.

Analytical Framework: Comparative interpretation was carried out after developing a structured analytical framework. The national frameworks were analysed according to five key areas.

1. Cyber Governance Architecture: This domain evaluated the institutional organisation of national cybersecurity, namely its level of centralisation, interagency cooperation, regulatory frameworks, government–industry collaboration, and specialised cybersecurity institutions.

2. Distribution of Cybersecurity Responsibility: This domain explored the distribution of cyber security responsibilities among the central government, regulatory bodies, critical infrastructure operators, technology companies, software developers, companies and end-users. Special care was taken to see if national policies focused on voluntary cooperation, regulatory responsibilities, market incentives, secure-by-design standards, or State oversight.

3. Cyber Resilience and Critical-Infrastructure Protection: National strategies for cyber incident prevention, absorption, response and recovery were analysed. They featured continuity planning, incident response, redundancy, sharing of threat information, supply-chain security, workforce development, secure technology, protection of essential services, and recovery capabilities.

4. International Law and State Responsibility: This domain looked at national views on the relevance of international law to the use of cyberspace, on national sovereignty, prohibited intervention, attribution, due diligence, State responsibility, countermeasures, use of force, self-defence and international humanitarian law, when applicable. Special focus was given to the scope for convergence and divergence in the chosen States.

5. Strategic and Technological Competition: The final domain examined the level of integration of cybersecurity strategies with geopolitical competition, technological leadership, artificial intelligence, telecommunications, supply chains, semiconductor technologies, digital standards, data governance, alliance structure, and national technological autonomy.

Data Extraction: The same comparative extraction schema was applied to capture information from each of the selected documents. For each State, data was gathered on the government institutions involved, key strategic goals, involvement of private sector entities, critical infrastructure, resilience strategies, international collaboration, legal stance on State responsibility, attribution, respect of sovereignty and due diligence, and strategic competition.

The policy statements and provisions were sorted into the a priori analytical domains. When more than one domain was discussed in the documents, the content was coded in the relevant domain(s). Then, recurring themes and key differences were examined between jurisdictions.

Comparative Legal Analysis: The legal analysis was carried out in a doctrinal way. International law rules were first found in treaties, customary international law, authoritative United Nations documents, the work of the International Law Commission on State responsibility and State positions. These rules were then compared with the cyber security strategies and legal statements of the selected States.

Particular attention was given to distinguishing technical attribution, political attribution, and legal attribution. Technical attribution indicated the detection of some infrastructure, malware, or operational attributes or probable actors using cybersecurity and intelligence techniques. Political attribution was defined as a governmental decision to designate publicly or privately a responsible actor. The notion of legal attribution was specifically concerned with the applicability of the rules of international responsibility to determine whether conduct could be attributed to a State.

The analysis also separated out voluntary norms of responsible State conduct from legally binding international obligations so as not to confuse politically agreed norms of responsible State behaviour with rules of customary or treaty law.

Comparative Synthesis: After analyzing each country, cross-case comparative matrix was used for synthesizing findings. Comparisons and contrasts were analyzed in terms of governance architecture, resilience, assignment of responsibility, positions concerning international law and strategic orientation.

The comparative synthesis was not intended to measure the performance of the selected States in cybersecurity; therefore, no numerical ranking was assigned. Rather, the focus was on capturing the trends of normative convergence, institutional divergence and strategic variation in the various national models.

Quality and Reliability of the Analysis: Primary and authoritative sources, especially official government publications, United Nations publications and well-established international law publications, were preferred in order to enhance analytical reliability. Wherever possible, major legal propositions were corroborated with more than one authoritative source.

To minimize selective interpretation, all five cases were analysed using the same framework. Throughout the analysis, the distinction between legally-binding rules, non-binding norms, political commitments and strategic policy objectives have been upheld. When a principle was not clearly established, such as the role of cyber due diligence or the exact legal implications of sovereignty in cyberspace, the study did not attempt to give a

disputed interpretation of the principle an appearance of legal certainty.

Ethical Considerations: Ethical approval was not necessary as there were no human subjects, no confidential records, no experimental intervention, and no private information was collected. Every document analysed was publicly accessible governmental, intergovernmental, legal and scholarly documents.

Methodological Limitations: There were a number of limitations to the methodology. National cybersecurity strategies are public policy documents and can not reveal classified cyber capabilities, intelligence practices, offensive operations or internal decision-making procedures. Thus, the analysis documents the State materials that have been publicly stated and do not necessarily represent all national cyber practice.

The direct comparison was also restricted in some areas by inconsistencies in terminology and structure of documents used between countries. Moreover, the international law on cyber is still developing and some principles are yet to be disputed. Hence, the study did not aim to solve all the doctrinal issues, but to see the State positions documented, as well as legally acceptable areas of convergence and disagreement.

RESULTS

Overview of Comparative Findings: The comparative analysis revealed significant convergence across all five States selected on the importance of cybersecurity, critical infrastructure protection, national resilience, public-private cooperation, and international cooperation. But, significant variations have been seen in the structuring of cyber governance, the allocation of cybersecurity responsibilities, the understanding of international legal principles, and the importance placed on strategic and technological competition.

The five recurrent dimensions in the national strategies and official legal stances were cyber-governance architecture, distribution of responsibility, resilience and critical-infrastructure protection, international law and State responsibility, and strategic competition. The U.S., U.K. and Australia showed relatively high scores for public-private partnerships, resilience, international partnerships, attribution and coordinated responses to malicious cyber activities. China's focus was on State-led governance, cyber sovereignty, technological autonomy, regulation, and multilateral rulemaking. Estonia's unique features were the embedding of cyber security into the design of digital government and continuity of critical public services, as illustrated in table 1.

Cyber-Governance Architecture: One of the obvious results of the comparison was the variation in institutional design. In the United States, the governance of cybersecurity is decentralized with the Federal government, sector-specific regulating agencies, the States, critical infrastructure operators, and technology companies all playing a role, along with cyber security agencies. Instead of focusing on a single authority, the US model emphasizes inter-governmental and inter-industry coordination and a transfer of responsibility for the systemic security of the cyber space to organizations that have the technical and financial resources to manage risks on a scale that matters.

The United Kingdom had a more centralized approach to strategy. The concept of cybersecurity was embedded in the concept of national cyber power, in which cyber defense resilience is related to intelligence, technological prowess, diplomacy, economic strength and operational capacity. Technical guidance and incident management are highly dependent on the cooperation between government and industry and specialized national institutions have a prominent role.

Australia has embraced a whole-of-nation strategy with layers of resilience. Responsibility for cybersecurity is not just the government's; it's everybody's, including businesses, critical-infrastructure operators, technology providers, communities, and individuals. The Australian strategy had a significant focus on embedding the idea of domestic resilience with regional cyber capacity building and international cooperation, which was more visible than in the other jurisdictions.

China demonstrated the most State-centered governance model among the five cases. Large regulatory and administrative structure for cybersecurity, data security, critical information infrastructures, platform governance, technological development. The State remains at the heart of the establishment of security commitments, the regulation of digital platforms, oversight of critical infrastructure and national cyber sovereignty.

Estonia was neither highly centralized nor strongly distributed. Cybersecurity has become a part of the operations of the digital State. Digital identity, electronic public services, data exchange, government continuity and public trust were considered as elements of national cybersecurity. This model accounted for Estonia's reliance on public administration in its electronic environment and thus focused on the need to ensure core State functionality in a cyber disruption as shown in table 2.

Responsibility for Cybersecurity Distribution: The analysis demonstrated broad agreement that cybersecurity cannot be managed exclusively by government. However, major variations were found when it came to the allocation of responsibilities between States, companies, infrastructure operators and individual users.

The United States demonstrated the most distinct progress in redistributing responsibilities between individuals and small organizations, and technology manufacturers, software vendors, major service providers, and critical-infrastructure operators. The rationale was that those with the highest level of technical ability in reducing systemic risk should be held to the highest standard of responsibility for secure products and services.

The United Kingdom also had a high degree of governmental–industrial cooperation and maintained greater central strategic coordination. Businesses & infrastructure operators were expected to take suitable cybersecurity measures, and government institutions were expected to deliver national level intelligence, technical guidance, incident response and strategic direction.

Australia adopted a shared-responsibility model in which individuals, businesses, government institutions, and technology providers were incorporated into a common national resilience structure. This meant that responsibility was spread widely, but with an increasing focus on secure technologies, information sharing and protection of critical infrastructure.

China also has imposed large commitments to private actors; but to a large extent, these commitments are the result of State regulation and statutory requirements, and not of market-based risk redistribution. In the world of technology firms, data processors and critical information infrastructure operators, national security and regulatory compliance are key concerns in the governance framework.

In Estonia, responsibility was shared by involving government, service providers, digital platforms and citizens closely together. Resilience of private and public infrastructure was considered as part of a common national digital ecosystem as this is heavily relied on in providing public services.

National Cyber Resilience and Critical-Infrastructure Protection: The most common area of overlap among the five national frameworks was critical-infrastructure protection. Every State understood that a cyber incident involving energy, communications, financial, health, transportation, government or other critical infrastructure sector information systems can have ramifications beyond the system itself. The United States underscored the importance of critical-infrastructure resilience, secure technology, coordinated incident response, and systemic risk reduction. It is an approach that increasingly accepts that some cyber intrusions will be successful and as such integrates prevention, detection, continuity, recovery and capability to disrupt malicious actors.

The UK also considered resilience as a national-security need. Resilience and response to cyber incidents were tied to protection of government systems, essential services, businesses

and the economy, in general. Cyber resilience was thus defined as an ongoing national capability, not solely technical controls. Australia's the most explicit whole-of-society articulation of resilience. It was built around the cyber-shield concept, which integrated the protection of citizens and businesses with secure technology, threat sharing, critical-infrastructure protection, sovereign capability, and international cooperation. This way of thinking revealed that the national cyber resilience also relies more and more on interdependent systems within and across the country.

China's resilience model was heavily linked to the protection of critical information infrastructure, data security, national security and the control of strategically significant digital systems. Besides operational recovery, focus was given to decrease the reliance on potential sources of vulnerability foreign technologies and to increase the technological capability. What was unique about Estonia's approach was the linkage of national resilience to continuity of government. Cybersecurity measures were developed to maintain the continuity of public administration, public electronic services, public electronic identities and governmental public services in the event of significant disruption as shown in table 3.

International Law and State Responsibility: While all States selected indicated that international law is relevant to activities in cyberspace, key disparities arose with respect to the meaning and application of specific principles of international law.

The U.S., U.K., and Australian general positions were that when internationally wrongful cyber conduct is attributable to a State, and constitutes a violation of an applicable international obligation, a matter may implicate State responsibility. They also noted that technical attribution does not equal legal attribution. Identification of the malicious infrastructure, malicious code, or operational characteristics could aid in an attribution assessment, but legal responsibility is governed by the international rules relating to State organs, agents, instructions, direction or control.

The United Kingdom had one of the most explicit positions on the public with regard to State responsibility. It recognized the difference between public/publicity or public political attribution and the attribution of acts to a State under international law; and it confirmed that States can take action in response to internationally wrongful cyber operations consistent with international law, including countermeasures if appropriate under applicable international law.

Australia showed significant movement towards the UK on issues of attribution and State responsibility, while having necessary differences on due diligence. The Australian government has affirmed that it agrees with the idea that when a State is aware of cyber activity that is harmful to it and is in a position to take reasonable measures to address the activity, it should do so. The United Kingdom, by contrast, has been more cautious on the question whether such a general obligation of cyber due diligence actually has emerged as a customary international-law rule.

China always spoke strongly about the four principles of sovereignty, non-interference, sovereign equality and the central role of the United Nations in establishing international rules regarding cyberspace. It tended to play down unilateral public attribution and countermeasure doctrine and up the multilateral rule-making, dialogue and sovereign control of domestic cyberspace.

Estonia has generally agreed with the view that international law in its entirety is applicable in cyberspace and has endorsed the rules-based approach that has been established through European and transatlantic institutions. Its more general policy perspective involved the notions of collective security, international co-operation and the development of shared understandings of responsible State behaviour as presented in table 4.

Attribution and Accountability: Attribution was a major link between cybersecurity strategy and international law. Technical attribution identifies the likely source of an attack, legal attribution determines State responsibility, and political attribution involves publicly assigning responsibility. The United States, United Kingdom, Australia, and Estonia used public attribution more actively, while China favored a more cautious and multilateral approach. Attribution remained difficult when proxies or third-party infrastructure were involved.

Sovereignty, Non-Intervention, and Due Diligence: All States recognized sovereignty and non-intervention, although their interpretations differed. China strongly emphasized cyber sovereignty, while the United Kingdom was more cautious about treating sovereignty as a standalone legal rule. Due diligence also remained contested, with Australia supporting stronger State responsibility for harmful activity originating from national infrastructure.

Countermeasures and Cyber Responses: The United States, United Kingdom, Australia, and Estonia supported sanctions, prosecution, technical disruption, and lawful countermeasures against malicious cyber activity. China emphasized dialogue, sovereign equality, and multilateral cooperation. This reflected differing preferences for deterrence-based versus sovereignty-centered cyber governance.

Strategic and Technological Competition: Cybersecurity was increasingly linked with artificial intelligence, supply chains, critical technologies, and national security. The United States, United Kingdom, Australia, and China emphasized technological capability and strategic resilience, while Estonia focused more strongly on digital-government continuity and collective security, as shown in Table 5.

Convergence Across the Five National Models: All five States treated cybersecurity as a national-security priority, with common emphasis on critical-infrastructure protection, domestic cyber capability, private-sector participation, international cooperation, and the relevance of international law. This reflects a shared baseline of cybersecurity responsibility despite differences in implementation.

Table 1. Comparative characteristics of national cybersecurity frameworks

Domain	United States	United Kingdom	Australia	China	Estonia
Governance architecture	Distributed federal system with strong public-private participation	Centrally coordinated model supported by specialized cyber institutions	Whole-of-government and whole-of-nation approach	State-centered and regulation-intensive model	Integrated digital-government model
Dominant strategic orientation	Risk redistribution, critical infrastructure, disruption of threats	Cyber power, resilience, capability and international influence	National resilience through interconnected cyber shields	Cyber sovereignty, national security and State authority	Digital continuity, trust and resilient public services
Role of private sector	Central operational role with increasing responsibility placed on major technology providers	Strong government-industry partnership	Shared responsibility across government, business and citizens	Private actors operate within extensive State regulatory requirements	Closely integrated with digital public-service ecosystem
Critical-infrastructure protection	Major strategic priority	Major strategic priority	Core component of cyber shields	Integrated with national and information security	Closely linked with continuity of government
International orientation	Alliances, collective defence, attribution and coordinated consequences	International partnerships and responsible cyber power	Rules-based cooperation and regional capacity-building	UN-centered multilateralism and sovereign equality	Strong EU and NATO cooperation
Strategic competition	Explicitly linked with technological leadership and national security	Linked with national cyber power and technological advantage	Linked with regional security and sovereign capability	Closely linked with technological independence and sovereignty	Primarily resilience- and alliance-oriented

Table 2. Distribution of cybersecurity responsibilities

Responsibility Area	United States	United Kingdom	Australia	China	Estonia
Government leadership	Strong	Strong	Strong	Dominant	Strong
Private-sector participation	Extensive	Extensive	Extensive	Extensive but heavily regulated	Extensive
Technology-provider responsibility	Strongly emphasized	Increasingly emphasized	Strongly emphasized	Defined primarily through regulation	Integrated into digital-service security
Individual responsibility	Present but increasingly de-emphasized as sole line of defence	Shared with organizations	Explicit component of whole-of-nation model	Subject to regulatory and security obligations	Linked with digital literacy and identity security
Regulatory approach	Mixed regulation, incentives and procurement	Regulation plus partnership	Regulation plus national coordination	Extensive statutory and administrative control	Integrated regulation and digital governance
Secure-by-design orientation	Strong	Strong	Strong	Increasingly embedded in security regulation	Closely linked with trusted digital architecture

Table 3. Comparative cyber-resilience priorities

Resilience Component	United States	United Kingdom	Australia	China	Estonia
Critical-infrastructure protection	Central	Central	Central	Central	Central
Incident-response capability	Strong	Strong	Strong	Strong	Strong
Continuity of essential services	Strong	Strong	Strong	Strong	Very strong
Public-private information sharing	Major emphasis	Major emphasis	Major emphasis	More State-directed	Integrated
Supply-chain security	Major priority	Important priority	Important priority	Closely linked with technological autonomy	Important
Secure-by-design systems	Strong emphasis	Strong emphasis	Strong emphasis	Increasing regulatory emphasis	Embedded in digital architecture
National cyber skills/capability	Major priority	Major priority	Major priority	Major priority	Major priority
International capacity-building	Extensive	Extensive	Particularly strong regional focus	Multilateral cooperation emphasized	Strong through EU/NATO partnerships

Table 4. Comparative treatment of key international-law principles

Legal Principle	United States	United Kingdom	Australia	China	Estonia
Existing international law applies to cyberspace	Yes	Yes	Yes	Yes	Yes
State responsibility for attributable cyber conduct	Recognized	Explicitly recognized	Explicitly recognized	Recognized within sovereignty-centered framework	Recognized
Public attribution of malicious activity	Frequently used	Explicit policy instrument	Used with partners	More cautious emphasis	Used largely through coordinated partnerships
Sovereignty	Fundamental principle	Fundamental, but cautious regarding standalone cyber rule	Strong legal relevance	Central organizing principle	Strongly recognized
Non-intervention	Recognized	Explicitly recognized	Explicitly recognized	Strongly emphasized	Recognized
Cyber due diligence	Supported in policy/legal discussions	Does not clearly recognize a general standalone customary rule	More explicitly supported	Addressed primarily through sovereignty and State responsibility	Generally supportive of responsible State behaviour
Countermeasures	Accepted under international law	Explicitly accepted	Explicitly accepted	Less prominently emphasized publicly	Generally accepted within rules-based framework
UN-centered cyber governance	Important but combined with alliances	Important but combined with alliances	Strong support	Particularly strong emphasis	Strong support
Alliance-based cyber cooperation	Very strong	Very strong	Very strong	Limited	Very strong

Table 5. Strategic competition within national cyber strategies

Strategic Dimension	United States	United Kingdom	Australia	China	Estonia
Cybersecurity linked with national security	Very strong	Very strong	Very strong	Very strong	Very strong
Technological leadership	Major objective	Major objective	Important objective	Major objective	Important
Supply-chain security	Major strategic concern	Strong concern	Strong concern	Linked with technological autonomy	Increasing concern
Artificial intelligence security	Increasingly central	Increasingly important	Increasingly important	Increasingly central	Emerging priority
International alliances	Core component	Core component	Core component	Multilateral cooperation preferred over alliance blocs	Core component
Technological sovereignty/autonomy	Increasing emphasis	Moderate emphasis	Sovereign capability emphasized	Central emphasis	Selective emphasis
Use of cyber policy in geopolitical competition	Explicit	Explicit	Increasingly explicit	Explicit	More limited

Principal Areas of Divergence: Major differences concerned cyber sovereignty, due diligence, attribution, countermeasures, and technological competition. The United States, United Kingdom, Australia, and Estonia favored stronger collective attribution and coordinated responses, whereas China emphasized sovereignty, multilateralism, and technological autonomy.

Overall Comparative Synthesis: Three broad models emerged: a distributed resilience model represented by the United States, United Kingdom, and Australia; a sovereignty-centered model represented by China; and a digitally integrated resilience model represented by Estonia. Overall, the findings showed strong functional convergence but continuing legal and institutional divergence in national cyber governance.

DISCUSSION

The results of this comparative study reveal that the national cybersecurity strategies are becoming more similar in terms of the priorities they are choosing, with critical infrastructure protection, cyber resilience, public–private cooperation, incident response and international engagement being some of the shared priorities[1]. But there are still important variations in how States are structuring cyber governance, allocating responsibilities, interpreting international law, and embedding cyber security into strategic competition. This kind of practical convergence with legal-policy divergence may be a sign of the changing nature of cyberspace as a global public space and as a space of State power[2].

In the United States, United Kingdom, and Australia, cybersecurity governance is largely distributed, with government

remaining in a strategic leadership position, but a strong reliance on private technology firms, infrastructure providers, and other non-State actors[3]. This is indicative of the reality that a significant portion of critical digital infrastructure is privately owned and/or operated. Their practices highlight the need for secure-by-design technologies, information sharing, public-private coordination and the shifting of cybersecurity risks to entities that have the greater capacity to manage systemic risks[4].

China will take a relatively more State-centric perspective. It is based on a framework that gives greater attention to cyber sovereignty, governmental regulatory power, national security, data governance, critical information infrastructure, and technological autonomy[5]. China also emphasizes international cooperation, but in its policy stance, the principle of sovereign equality, non-interference, and multilateral rule-making have been prioritized. Thus, it can be concluded that states can have similar security objectives and may differ significantly in the institutional and legal means of reaching them.

Estonia is a unique resilience model. The interdependence of government services, digital identity and public administration on interconnected digital systems makes cybersecurity closely related to continuity planning at national level[7]. This reflects a key broader observation: cyber resilience is becoming a national resilience problem, not an information-technology problem alone[8].

Another key field of convergence and disagreement is international law. All selected States have stated that international law is relevant in activities in cyberspace. However, there are still some points of disagreement in the interpretation of sovereignty, due diligence, attribution and countermeasures. The challenge is thus no longer so much whether legal rules are applicable, but their interpretation in concrete cyber incidents[9,10].

The importance of state responsibility is even greater because technical evidence of a cyber operation originating from infrastructure in a State does not necessarily prove international legal responsibility[11]. Technical, political and legal attribution is still important. Legal attribution must satisfy the criterion of being linked to the State based on the relevant international rules, while political attribution can be based on a wider intelligence assessment and strategic thinking. This is particularly true when cyber operations are performed via proxies, criminal groups, contractors or compromised third party infrastructure[12].

The U.S., U.K., Australia, and Estonia have been more willing to adopt coordinated public attribution and collective response to malicious cyber activity[13]. These can range from sanctions, diplomatic statements, criminal proceedings, technical advisories, or other lawful responses. Especially in cases where supporting evidence is not made public, China has been more circumspect about unilateral attribution and has pointed to the dangers of politicization. Both these contrasting approaches demonstrate the ongoing dichotomy of accountability and evidentiary transparency in cyber diplomacy[14].

There are also disparities when it comes to sovereignty and due diligence. All States consider sovereignty as an essential principle in international relations, however, there is a difference of opinion regarding the question of whether or not unauthorised cyber activity should be treated as an independent case of violation of sovereignty[15]. Similarly, the issue of due diligence is controversial as it relates to the requirement for States to prevent or stop the activities of harmful cyber actors that operate from infrastructure located on its territory, but are not directly performed by the State itself[17].

The interaction between law and cyber deterrence is also illustrated by countermeasures. The United Kingdom and Australia have made it abundantly clear that countermeasures are potentially available to respond to ‘internationally wrongful cyber activity' under the right legal circumstances[17]. This will enable States to act with a variety of diplomatic, economic, legal or cyber means before they resort to force. This is crucial as cyber operations often fall short of an armed attack but nonetheless cause significant economic or political injury[18].

One key discovery is that cybersecurity is becoming more enmeshed with technology and geopolitical competition. AI, telecommunications, semiconductors, cloud computing, data governance, software supply chains and technical standards are now considered national-security issues. Thus, cyber strategy is moving beyond the protection of hacking to the control of technological dependency and strategic infrastructure[19,20].

While this is a significant legal issue, as technological competition is not inherently illegal. Technological capacity may be sought at the national level, regime control over foreign suppliers, or domestic industry promotion may be pursued without infringing international law. Thus the primary challenge is to differentiate between free competition and coerced interference, internationally wrongful cyber activity and activities that pose a threat to international peace and security[1-5].

The study also shows the increasing value of resilience. In today's increasingly interconnected and complex digital landscape, achieving absolute cyber incident prevention is unattainable. National strategies should thus not only emphasize prevention of attacks, but the continuity of essential services, rapid detection of attacks, damage containment, system restoration, and the preservation of public trust. The resilience-by-design approach can ultimately offer more sustainable long-term security than just deterrence or response after the event[6-10].

Cooperation is necessary on an international scale, as cyber threats regularly traverse borders. Increased clarity on the national legal positions, enhanced confidence-building mechanisms, information sharing, building capacity and further dialogue in the United Nations processes could contribute to lessening misunderstandings and escalation. However, States will need to do more than agree in principle that international law has relevance for cyber operations to define how they understand the meaning of some of these principles in specific scenarios[10-15].

There are certain limitations in the study. It relies largely on information that is publicly available, such as strategies and legal statements, and this may not fully reflect classified capabilities, intelligence practices or operational doctrine. Also, national strategies may shift with the development of new technologies and shifts in geopolitical situations. Nevertheless, the comparative approach demonstrates that the future of cyber governance will likely depend not on complete uniformity among States, but on the development of sufficiently clear legal boundaries and shared expectations for responsible behaviour[16-20].

CONCLUSION

Modern cybersecurity policies are becoming more and more comprehensive, integrating national security, technological resilience, critical infrastructure protection, international law, and strategic competition. While the United States, the United Kingdom, Australia, China and Estonia share a number of common cybersecurity priorities, there are significant differences in many areas of governance, notions of sovereignty, attribution, due diligence and mechanisms of accountability.

National cyber stability will require more to be resilient, more to be clear about their legal stance, more to be credible about attribution, more to be clear about protecting critical infrastructure and more to be agreed upon internationally. The key issue is to create effective and transparent legal and strategic guidelines that enable legitimate technological competition whilst reducing the opportunity for internationally wrongful cyber activity and minimising potential escalation.

REFERENCES

1. United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/70/174. New York: United Nations; 2015.
2. Schmitt MN, editor. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press; 2017.

3. Mačák K. Decoding Article 8 of the International Law Commission's Articles on State Responsibility: attribution of cyber operations by non-State actors. J Conflict Secur Law. 2016;21(3):405-428. doi:10.1093/jcsl/krw014.
4. Finnemore M, Hollis DB. Constructing norms for global cybersecurity. Am J Int Law. 2016;110(3):425-479. doi:10.1017/S0002930000016894.
5. Schmitt MN. Beyond State-centrism: international law and non-State actors in cyberspace. J Conflict Secur Law. 2016;21(3):595-611. doi:10.1093/jcsl/krw019.
6. Huang Z, Mačák K. Towards the international rule of law in cyberspace: contrasting Chinese and Western approaches. Chin J Int Law. 2017;16(2):271-310. doi:10.1093/chinesejil/jmx011.
7. Schmitt MN, Vihul L. Sovereignty in cyberspace: lex lata vel non? AJIL Unbound. 2017;111:213-218. doi:10.1017/aju.2017.55.
8. Corn GP, Taylor R. Sovereignty in the age of cyber. AJIL Unbound. 2017;111:207-212. doi:10.1017/aju.2017.57.
9. Mačák K. From cyber norms to cyber rules: re-engaging States as law-makers. Leiden J Int Law. 2017;30(4):877-899. doi:10.1017/S0922156517000358.
10. Efrony D, Shany Y. A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent State practice. Am J Int Law. 2018;112(4):583-657. doi:10.1017/ajil.2018.86.
11. Nye JS Jr. Deterrence and dissuasion in cyberspace. Int Secur. 2017;41(3):44-71. doi:10.1162/ISEC_a_00266.
12. Lindsay JR. Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. J Cybersecur. 2015;1(1):53-67. doi:10.1093/cybsec/tyv003.
13. Gartzke E, Lindsay JR. Weaving tangled webs: offense, defense, and deception in cyberspace. Secur Stud. 2015;24(2):316-348. doi:10.1080/09636412.2015.1038188.
14. Borghard ED, Lonergan SW. The logic of coercion in cyberspace. Secur Stud. 2017;26(3):452-481. doi:10.1080/09636412.2017.1306396.
15. Hollis DB, Ohlin JD. What if cyberspace were for fighting? Ethics Int Aff. 2018;32(4):441-456.
16. US Department of Defense. *The Department of Defense Cyber Strategy*. Washington (DC): US Department of Defense; 2015.
17. Cabinet Office, HM Treasury. *National Cyber Security Strategy 2016-2021*. London: HM Government; 2016.
18. Australian Government. *Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity*. Canberra: Commonwealth of Australia; 2016.
19. Ministry of Foreign Affairs of the People's Republic of China, Cyberspace Administration of China. *International Strategy of Cooperation on Cyberspace*. Beijing: Ministry of Foreign Affairs of the People's Republic of China; 2017.
20. Ministry of Economic Affairs and Communications, Republic of Estonia. *Cyber Security Strategy 2014-2017*. Tallinn: Ministry of Economic Affairs and Communications; 2014.