Cybersecurity Law and Policy: A Comprehensive Review of Emerging Global Frameworks

Dr. Shubhendu Shukla
Associate Professor, Department of Business Administration, SR Institute of Management Sciences, Lucknow, India

Cybersecurity Law and Policy Review
Volume 1, Issue 1 | 2025 | https://clprj.com/journal/index

Abstract

The first quarter of the twenty-first century has witnessed an unprecedented proliferation of cybersecurity legal and regulatory frameworks across the world, as governments at every level of development have grappled with the escalating threats posed by cybercrime, state-sponsored cyber operations, critical infrastructure attacks, data breaches, and the systemic security vulnerabilities embedded in an increasingly digital global economy. From the European Union's landmark General Data Protection Regulation and NIS2 Directive to the United States' sector-specific regulatory evolution and emerging comprehensive legislative proposals; from China's sovereign cybersecurity architecture to the nascent but rapidly developing frameworks of Africa, Latin America, and Southeast Asia; and from the evolving treaty landscape anchored by the Budapest Convention and the newly adopted United Nations Cybercrime Convention to the voluntary norm frameworks developed by successive UN Groups of Governmental Experts, the global cybersecurity legal landscape of 2025 is simultaneously richer, more complex, and more fragmented than at any previous point in the digital era.

Keywords: *cybersecurity law; global frameworks; comparative regulation; GDPR; NIS2; Budapest Convention; UN Cybercrime Convention; critical infrastructure; data protection; cyber norms; regulatory convergence; digital governance; emerging economies; international law*

1. INTRODUCTION: THE GLOBAL REGULATORY TURN IN CYBERSECURITY

When the Council of Europe opened the Budapest Convention on Cybercrime for signature in November 2001, the governance of cyberspace was understood by most national legal systems as a narrow supplementary challenge — a matter of extending existing criminal law principles to a new technical medium. Two decades and four years later, cybersecurity law and policy has become one of the most expansive, dynamic, and consequentially important fields of public law and international governance, with dedicated legislative frameworks, specialised regulatory agencies, sector-specific security standards, mandatory breach notification regimes, critical infrastructure protection obligations, international

treaty instruments, and voluntary norm frameworks multiplying across jurisdictions at a pace that challenges even specialist scholars to maintain comprehensive awareness.

The scale of this regulatory expansion reflects the transformation of cybersecurity from a technical concern at the periphery of public policy to a central preoccupation of national security, economic regulation, and democratic governance. The economic losses attributable to cybercrime are estimated by credible sources at several trillion dollars annually — a figure that exceeds the gross domestic product of all but a handful of the world's largest economies. Major state-sponsored cyber operations have targeted electoral infrastructure, critical national systems, financial networks, defence industrial supply chains, and the personal data of government officials and private citizens at a scale and with a persistence that have prompted fundamental reassessments of national security strategy across the developed and developing world. The pervasive digitisation of economic activity — accelerated dramatically by the COVID-19 pandemic — has created dependencies on digital infrastructure whose security can no longer be treated as an afterthought of technological development rather than a foundational requirement of economic and social functioning.

The legal and policy responses to this transformed landscape have been characterised by several dominant features. First, a shift from voluntary and self-regulatory approaches to mandatory, enforcement-backed regulatory requirements — most clearly illustrated by the EU's trajectory from the non-binding Network and Information Security recommendations of the early 2000s through the mandatory NIS Directive of 2016 to the much more demanding NIS2 framework of 2022. Second, a broadening of regulatory scope from narrow computer crime statutes to comprehensive horizontal cybersecurity frameworks encompassing incident reporting, security standards, supply chain obligations, and emerging technology governance. Third, a proliferation of regulatory actors — national cybersecurity agencies, sector-specific regulators, data protection authorities, financial supervisors, and international bodies — whose overlapping mandates create coordination challenges as significant as the security challenges they seek to address. Fourth, an intensification of geopolitical competition over the architecture and norms of global cyberspace governance, reflected in the deep divisions between democratic and authoritarian states over fundamental questions of internet governance, state sovereignty in cyberspace, and the appropriate scope of government authority over digital communications.

2. THE EUROPEAN MODEL: COMPREHENSIVE REGULATION AND THE BRUSSELS EFFECT

2.1 The EU Cybersecurity Legislative Architecture

The European Union has constructed the most comprehensive and institutionally developed cybersecurity regulatory architecture of any major jurisdiction, built upon a foundations of the General Data Protection Regulation (GDPR), the Network and Information Security 2 Directive (NIS2), the Cybersecurity Act, the Digital Operational Resilience Act (DORA), the AI Act, and the proposed Cyber Resilience Act — a legislative corpus that together constitutes an ambitious attempt at comprehensive horizontal

governance of digital security across the EU single market. The architecture is characterised by several distinctive features: a rights-based foundation grounded in the EU Charter of Fundamental Rights; horizontal application across sectors supplemented by sector-specific rules; a combination of directly applicable regulations and directives requiring national transposition; significant enforcement powers delegated to national supervisory authorities operating within a coordinated EU framework; and explicit extra-territorial scope provisions that extend EU regulatory requirements to non-EU entities serving EU consumers or processing EU personal data.

NIS2, the centrepiece of the EU's critical infrastructure protection framework, significantly expands upon its predecessor in scope, obligations, and enforcement mechanisms. By classifying both 'essential' and 'important' entities across eleven critical sectors as subject to mandatory risk management and incident reporting obligations, NIS2 brings a substantially larger population of organisations within the mandatory cybersecurity framework than any previous EU instrument. Its requirements for security measures covering incident handling, business continuity, supply chain security, cryptography, access control, and multi-factor authentication represent the most specific mandatory technical security requirements yet imposed by EU law. The directive's management body liability provisions — holding senior executives personally accountable for NIS2 compliance failures — mark a significant shift toward individual as well as corporate accountability for cybersecurity governance.

The Cyber Resilience Act, applicable to products with digital elements, addresses the supply chain dimension of cybersecurity by imposing security-by-design requirements on manufacturers throughout a product's lifecycle — requiring vulnerability handling processes, software bills of materials, security updates for the expected product lifetime, and incident reporting to ENISA. When fully implemented, the CRA will create a mandatory security baseline for the vast majority of internet-connected devices and software products placed on the EU market, addressing a structural vulnerability that has been a significant source of systemic cybersecurity risk. The combination of the NIS2 framework (governing operators) and the CRA (governing products) represents the most comprehensive attempt yet by any major jurisdiction to address cybersecurity comprehensively across both the demand and supply sides of the digital security ecosystem.

2.2 The Brussels Effect in Cybersecurity

The EU's cybersecurity regulatory framework has generated substantial extra-territorial influence through the 'Brussels Effect' — the dynamic by which EU regulatory standards become de facto global standards as multinational corporations adjust their practices globally to comply with the most demanding requirements they face in any significant market. This effect, well-documented in the GDPR context, is increasingly observable in the cybersecurity domain: the GDPR's breach notification requirements have driven the adoption of breach notification processes and technical detection capabilities in organisations worldwide that have no regulatory obligation to notify under domestic law; NIS2's supply chain security requirements are influencing procurement standards in third countries; and the Cyber Resilience Act's security-by-design requirements for connected products are already shaping product development roadmaps in markets from Asia to North

America as manufacturers seek to produce a single globally compliant product rather than separate products for the EU and non-EU markets.

The Brussels Effect is not without its critics, who argue that EU regulatory standards may not be optimally calibrated for all markets and that the imposition of EU standards through market leverage is a form of unilateral regulatory imperialism that bypasses the legitimacy of multilateral norm development. These critiques have particular resonance in developing country contexts, where compliance with EU-derived standards may impose disproportionate costs and where the institutional frameworks necessary to implement and enforce equivalent standards may be absent. The balance between the genuine benefits of globally harmonised security standards — which facilitate interoperability, reduce compliance fragmentation, and raise security baselines — and the costs of standards that reflect the specific priorities and institutional capacities of the world's largest and most developed regulatory bloc deserves serious attention in the international governance literature.

2.3 Member State Implementation and Divergence

Despite the EU framework's harmonisation aspirations, significant divergence persists in the implementation and enforcement of cybersecurity obligations across EU member states. The NIS2 Directive's transposition deadline of October 2024 was met by only a minority of member states, with several major EU economies still in the process of transposition as of early 2025 — creating a transitional period of regulatory uncertainty for organisations subject to the framework. The enforcement practices of national competent authorities — which retain significant discretion in how they supervise and sanction covered entities — vary substantially, creating a risk of regulatory arbitrage in which entities seek to establish their principal establishment in member states with lighter-touch enforcement regimes.

The coordination mechanisms established by NIS2 — including the NIS Cooperation Group, the CSIRT Network, and the European Cyber Crisis Liaison Organisation (EU-CyCLONe) — represent significant institutional infrastructure for EU-level cybersecurity coordination that have no equivalent in other regional governance systems. Their effectiveness in practice, however, depends on the willingness of member states to share threat intelligence, coordinate incident responses, and align enforcement priorities in ways that national security interests and institutional silos have historically constrained. The development of these coordination mechanisms into genuinely effective instruments of collective EU cybersecurity governance represents one of the most important ongoing challenges of European cybersecurity policy.

3. THE UNITED STATES: FEDERALISM, SECTORALISM, AND THE LIMITS OF VOLUNTARISM

3.1 The Architecture of US Cybersecurity Regulation

The United States' approach to cybersecurity regulation is the product of its constitutional structure, its regulatory philosophy, and its political economy in ways that distinguish it sharply from the EU model and that generate both significant strengths and significant

weaknesses as a framework for addressing the full range of contemporary cybersecurity challenges. The division of legislative authority between the federal government and fifty states, combined with a regulatory philosophy historically sceptical of broad horizontal mandates on private enterprise, has produced a regulatory architecture characterised by sector-specific requirements of varying specificity and enforcement rigour, a dominant role for voluntary frameworks and industry self-regulation supplemented by mandatory requirements in the most sensitive sectors, and a proliferating body of state-level legislation that creates significant compliance fragmentation for nationally and internationally operating businesses.

At the federal level, the Cybersecurity and Infrastructure Security Agency (CISA) established by the Cybersecurity and Infrastructure Security Agency Act of 2018 serves as the primary civilian federal cybersecurity authority, with a broad mandate to coordinate cybersecurity across federal civilian agencies and critical infrastructure sectors. CISA's operational tools — which include the sharing of threat intelligence, technical assistance to affected organisations, and the issuance of binding operational directives to federal agencies — have been progressively strengthened through legislation and executive action, though its authority over private sector critical infrastructure remains primarily coordinative rather than directly regulatory. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) represents the most significant expansion of mandatory cybersecurity obligations for private sector critical infrastructure in recent US legislative history, though its implementing regulations remain under development.

The NIST Cybersecurity Framework — now in its 2.0 iteration released in February 2024 — remains the most influential single articulation of cybersecurity best practice in the US context, widely adopted across sectors as a basis for cybersecurity programme design and board-level governance. The Framework's voluntary character has been the subject of sustained debate: proponents argue that its flexibility and adaptability make it more practically effective than rigid prescriptive mandates; critics argue that voluntary adoption produces systematic under-compliance in sectors where market incentives for security investment are insufficient to drive adoption without regulatory compulsion. The current administration's National Cybersecurity Strategy, released in March 2023, signals a significant shift in the balance of this debate — explicitly committing to shifting liability to technology manufacturers, imposing minimum security requirements on critical sectors, and moving away from the voluntary model as the primary mechanism for private sector cybersecurity governance.

3.2 The State Privacy and Cybersecurity Mosaic

In the absence of a comprehensive federal privacy and cybersecurity statute, US states have exercised their legislative authority to create an increasingly complex and divergent patchwork of state-level requirements that imposes substantial compliance burdens on businesses operating across multiple states and that has generated significant pressure for federal preemption. California has led this legislative evolution through the California Consumer Privacy Act (CCPA) of 2018 and its successor the California Privacy Rights Act (CPRA) of 2020, which together create a consumer privacy framework with significant structural similarities to the GDPR. Virginia, Colorado, Connecticut, Texas, Florida, and numerous other states have enacted comparable consumer privacy legislation, though with

varying substantive requirements, enforcement mechanisms, and exemptions that create a compliance landscape of bewildering complexity for national businesses.

State-level data breach notification laws — now enacted in all fifty states plus the District of Columbia, Puerto Rico, and Guam — represent the most pervasive mandatory cybersecurity obligation in the US system, requiring notification of affected residents and state attorneys general within defined timeframes following security incidents involving personal information. The diversity of these notification requirements — in the definition of personal information, the triggering threshold, the notification timeline, the required content of notifications, and the enforcement mechanisms — exemplifies the compliance fragmentation problem that characterises the US approach and that provides the primary practical argument for federal preemption through a comprehensive national breach notification and cybersecurity standard.

Multiple federal comprehensive cybersecurity and privacy legislative proposals have been introduced and failed over the past decade, reflecting deep disagreements between proponents of strong consumer rights and business advocates of preemptive federal standards, between privacy maximalists and national security interests that seek to maintain surveillance authorities, and between advocates of rights-based and market-based regulatory approaches. The prospects for comprehensive federal cybersecurity legislation appear more favourable in 2025 than at any previous point in the post-GDPR era, driven by the growing political salience of data breaches, the complexity of state law compliance, and the demonstrated inadequacy of the voluntary framework in preventing major incidents — but the fundamental political obstacles to comprehensive reform remain substantial.

4. ASIA-PACIFIC: DIVERSITY, INNOVATION, AND AUTHORITARIAN DIVERGENCE

4.1 China's Sovereign Cybersecurity Architecture

China's cybersecurity legal framework — built upon the Cybersecurity Law of 2016, the Data Security Law of 2021, the Personal Information Protection Law (PIPL) of 2021, and the Critical Information Infrastructure Security Protection Regulations of 2021 — represents the most comprehensively developed cybersecurity legislative architecture among major non-Western jurisdictions, and one that embodies a fundamentally different conception of the relationship between digital security, state authority, and individual rights from the frameworks of the EU and the United States. China's framework is characterised by: explicit subordination of cybersecurity to national security imperatives and the authority of the Communist Party; strong data localisation requirements that restrict the cross-border flow of data designated as important or as involving personal information at scale; extensive supervisory powers enabling government access to data held by private entities; mandatory security reviews for critical information infrastructure operators and for certain data-processing activities; and a multi-layered enforcement apparatus involving the Cyberspace Administration of China (CAC), the Ministry of Public Security, and the State Council's sector-specific regulatory bodies.

China's cybersecurity framework has generated significant international frictions on multiple dimensions. The PIPL's extra-territorial provisions — applicable to personal

information processing outside China that affects Chinese residents — create compliance obligations for foreign entities that parallel, though do not replicate, those of the GDPR. China's data localisation requirements conflict with the cross-border data flow provisions of trade agreements including the CPTPP, whose accession China has sought. And the security review requirements of the Data Security Law — including the requirement for government review of certain data export arrangements — have been cited by foreign technology companies as creating operational barriers that functionally restrict their ability to conduct business in China. The use of China's cybersecurity legal framework as an instrument of national industrial policy — preferencing domestic technology providers in critical sectors — is a further dimension of the framework's international significance that has provoked regulatory and trade responses in multiple jurisdictions.

4.2 Singapore, Japan, Australia, and India

Among Asia-Pacific democracies, Singapore has established itself as the regional leader in cybersecurity regulatory sophistication, with the Monetary Authority of Singapore's Technology Risk Management Guidelines, the Cybersecurity Act 2018 (as amended), the Personal Data Protection Act, and the Payment Services Act collectively providing a comprehensive and technically sophisticated framework for cybersecurity governance. Singapore's Cybersecurity Act is notable for its establishment of a national cybersecurity licensing framework for providers of certain cybersecurity services — a regulatory innovation that has not been widely replicated but that addresses the accountability gap created by the provision of cybersecurity services by unaccountable or inadequately qualified providers. Singapore's Cyber Security Agency (CSA) has emerged as a credible and respected regional cybersecurity authority, whose regulatory guidance and international engagement provide a model for other ASEAN member states.

Japan's cybersecurity framework has evolved significantly since the enactment of the Basic Act on Cybersecurity in 2014, which established the National Cybersecurity Incident Readiness and Strategy Centre (NISC) and the basic institutional architecture for national cybersecurity coordination. Subsequent legislation has addressed specific sectoral requirements, most recently through amendments to the Act on the Protection of Critical Infrastructure from Cyberattacks (2022) that expanded the scope of critical infrastructure sectors subject to mandatory security planning and incident reporting obligations. Japan's Active Cyber Defence legislation, enacted in 2025 after years of policy debate, represents a significant doctrinal shift — authorising the government to take proactive measures, including access to foreign computer systems, to counter imminent cyberattacks — with significant constitutional and international law implications that the scholarly community is only beginning to analyse.

Australia's cybersecurity legal architecture has undergone rapid development since 2021, driven by a series of high-profile incidents including the Medibank Private and Optus data breaches, which together exposed the personal information of a substantial fraction of the Australian population and generated intense political pressure for regulatory reform. The Security of Critical Infrastructure Act, as progressively amended to extend its scope and strengthen its obligations, now represents one of the most comprehensive critical infrastructure protection frameworks among common law jurisdictions. The Australian government's 2023 Cyber Security Strategy committed to the development of Australia's first standalone Cyber Security Act — enacted in 2024 — which consolidates and

strengthens the cybersecurity regulatory framework and introduces new obligations including mandatory ransomware reporting, device security standards, and government assistance powers for cyber incidents affecting critical infrastructure.

India's cybersecurity legal framework is in a period of significant transition, driven by the enactment of the Digital Personal Data Protection Act 2023 (DPDPA) — India's first comprehensive personal data protection statute — alongside the ongoing development of sector-specific cybersecurity requirements under the Computer Emergency Response Team (CERT-In) rules, the Reserve Bank of India's IT and cybersecurity frameworks for financial sector entities, and the telecommunications and energy sector cybersecurity regulations. The DPDPA's provisions on data breach notification — requiring notification to the Data Protection Board and to affected data principals — create the foundation for a comprehensive breach notification regime, though the Act's delayed implementation and the as-yet-unestablished Data Protection Board leave significant regulatory uncertainty for covered entities. India's cybersecurity framework is also notable for its development outside the major treaty frameworks — India is not party to the Budapest Convention — and for the government's advocacy of a sovereign internet model in multilateral forums that has placed it in alignment with China and Russia on key questions of internet governance.

4.3 ASEAN's Collective Cybersecurity Governance

The ASEAN region's approach to cybersecurity governance reflects the bloc's fundamental principle of non-interference in member states' internal affairs, which has historically constrained the development of binding regional cybersecurity standards in favour of voluntary coordination mechanisms and capacity-building initiatives. The ASEAN Cybersecurity Cooperation Strategy and the ASEAN Digital Master Plan provide high-level frameworks for regional cybersecurity cooperation, while the ASEAN Regional Forum (ARF) and the ASEAN Ministerial Conference on Cybersecurity (AMCC) provide forums for political-level dialogue on cybersecurity policy. The substantive convergence of national cybersecurity frameworks across ASEAN member states — which range from the sophisticated and comprehensively regulated environment of Singapore to the nascent frameworks of less developed member states — remains limited, with significant disparities in both regulatory content and institutional capacity.

The development of ASEAN cross-border data flow frameworks and digital trade rules under the ASEAN Digital Integration Framework and in the context of regional trade agreements including the Regional Comprehensive Economic Partnership (RCEP) creates a potential driver for greater cybersecurity regulatory convergence — as the interoperability of digital infrastructure across borders requires some harmonisation of the security standards that protect that infrastructure. The ASEAN Data Management Framework and the ASEAN Model Contractual Clauses for Cross Border Data Flows represent initial steps toward the development of regional data protection standards, though their cybersecurity dimensions remain underdeveloped relative to the privacy dimensions.

5. AFRICA, LATIN AMERICA, AND THE MIDDLE EAST: FRAMEWORKS IN FORMATION

5.1 Africa: The Malabo Convention and National Framework Development

Africa's cybersecurity legal landscape is characterised by a combination of ambitious regional framework-setting through the African Union and its institutions, rapid national legislative development across a growing number of African states, and significant disparities in institutional capacity that create substantial gaps between legislative intent and operational reality. The African Union Convention on Cybersecurity and Personal Data Protection — the Malabo Convention, adopted in 2014 and entering into force in June 2023 after achieving the required fifteen ratifications — represents the continent's primary regional cybersecurity and data protection instrument, though its limited ratification base and the absence of implementation mechanisms with meaningful enforcement authority limit its immediate practical impact.

At the national level, a growing number of African states have enacted or are in the process of enacting cybercrime, cybersecurity, and data protection legislation, often drawing on model law frameworks developed by the Economic Community of West African States (ECOWAS), the East African Community, the Commonwealth, or international organisations. South Africa's Protection of Personal Information Act (POPIA) — which entered into force in 2021 — represents the most advanced data protection framework on the continent, modelled substantially on GDPR principles and enforced by the Information Regulator with meaningful civil penalty authority. Kenya's Computer Misuse and Cybercrime Act (2018) and Data Protection Act (2019) have similarly established a relatively comprehensive cybersecurity and data protection framework in East Africa. Nigeria's cybercrime legislation and its evolving data protection framework — the Nigeria Data Protection Act (2023) establishing a dedicated National Data Protection Commission — represent significant developments in Africa's most populous country.

The capacity challenges facing African cybersecurity governance are substantial. Many African national computer emergency response teams (CERTs) are severely under-resourced relative to the cybersecurity challenges they face; judicial and prosecutorial capacity for complex cybercrime cases is limited; and the technical expertise necessary to supervise sophisticated digital financial services, cloud infrastructure, and telecommunications systems is scarce across the region. International capacity-building initiatives — including the Commonwealth Telecommunications Organisation's cybersecurity programmes, the International Telecommunication Union's cybersecurity assistance programmes, and the bilateral cooperation programmes offered by the EU, the United States, and various member state governments — are making progress in addressing these deficits, but the scale of the capacity gap means that significant investment over extended periods will be required before effective implementation of enacted cybersecurity frameworks is achieved across the continent.

5.2 Latin America: The LGPD and Regional Regulatory Development

Latin America has experienced a significant acceleration in cybersecurity and data protection legislative activity over the past decade, driven by a combination of domestic political pressure following high-profile data breaches and cyber incidents, the influence

of the EU's GDPR as a model legislation, and the growing digital integration of Latin American economies that exposes their infrastructure and populations to global cyber threats. Brazil's Lei Geral de Proteção de Dados (LGPD) — enacted in 2018 and in force since 2020, enforced by the Autoridade Nacional de Proteção de Dados (ANPD) — represents the most comprehensive data protection framework in the region, establishing GDPR-equivalent rights for data subjects, obligations for data controllers and processors, and enforcement powers including administrative fines. Colombia, Chile, Argentina, and Mexico have enacted or are developing updated data protection and cybersecurity frameworks that reflect GDPR influence alongside regional legal tradition.

The Organisation of American States (OAS) has played an active role in promoting cybersecurity governance development across Latin America and the Caribbean through its Inter-American Committee against Terrorism (CICTE) and the OAS/CITEL cybersecurity programme, which has provided technical assistance to member states in the development of national cybersecurity strategies, legislative frameworks, and operational capacity. The OAS's 2020 report on cybersecurity in Latin America and the Caribbean documented significant progress in the development of national cybersecurity strategies across the region alongside persistent gaps in implementation capacity, inter-agency coordination, and private sector engagement. The development of regional cybersecurity frameworks through MERCOSUR, the Andean Community, and the Pacific Alliance provides potential vehicles for greater regulatory harmonisation, though the political complexity of regional economic integration in Latin America has limited the pace of progress.

5.3 The Middle East and North Africa: Regulatory Ambition and Governance Constraints

The Middle East and North Africa (MENA) region presents a distinctive cybersecurity governance landscape characterised by high levels of ambition in digital transformation and cybersecurity framework development in the Gulf Cooperation Council states, alongside more constrained regulatory development in North Africa and the Levant. The United Arab Emirates has established an ambitious national cybersecurity agenda under the UAE Cybersecurity Strategy, with the UAE Cybersecurity Council and its affiliated agencies developing comprehensive regulatory frameworks for government and critical infrastructure cybersecurity, cloud security, and personal data protection. Saudi Arabia's National Cybersecurity Authority (NCA) has developed an extensive framework of cybersecurity regulations applicable to both government and private sector entities, including the Essential Cybersecurity Controls (ECC) that impose specific technical and organisational security requirements on critical national infrastructure operators.

The cybersecurity frameworks of MENA states share certain characteristics that reflect the political and governance structures of the region: a strong emphasis on government authority and national security considerations in cybersecurity governance, limited civil society engagement in regulatory development, and in some states the deployment of cybersecurity legal frameworks as instruments of political control that restrict legitimate online expression and privacy. The use of cybersecurity legislation to criminalise online dissent, journalism, and political opposition in several MENA states — documented by human rights organisations including Human Rights Watch, Amnesty International, and the Electronic Frontier Foundation — illustrates the dual-use character of cybersecurity law that democratic governance frameworks must explicitly address.

6. THE INTERNATIONAL LEGAL FRAMEWORK: TREATIES, NORMS, AND THE HARMONISATION CHALLENGE

6.1 The Budapest Convention and Its Evolution

The Budapest Convention on Cybercrime, adopted in 2001 and now with sixty-eight states parties as of 2025, remains the primary binding multilateral instrument for international cybercrime cooperation. Its substantive criminal law provisions — establishing a common framework of computer crime offences — and its procedural cooperation mechanisms — including expedited evidence preservation, mutual legal assistance, and extradition provisions — have provided a functional foundation for international cooperation in cybercrime investigation and prosecution that has significantly outperformed the expectations of its critics when it was initially negotiated. The Convention's First Additional Protocol on Xenophobia and Racism (2003) and the Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence (2022) have extended its scope and, in the case of the Second Protocol, substantially modernised its evidence cooperation mechanisms to address the cloud computing era.

The Budapest Convention's limitations are real and well-documented. Its geographic scope — though now extending well beyond the Council of Europe membership through the mechanism of invitation for non-member states — does not include China, Russia, or several other major cyber powers whose cooperation is essential for effective international cybercrime law enforcement. The Second Additional Protocol, while a significant technical advance, has attracted criticism for its cross-border direct cooperation mechanisms that some governments and civil society organisations argue may undermine existing human rights safeguards. And the Convention's fundamental architecture — focused on individual computer offences rather than the organised criminal enterprises and state-sponsored actors that perpetrate the most consequential contemporary cyber threats — limits its utility as the primary vehicle for international cybersecurity law enforcement.

6.2 The UN Cybercrime Convention

The adoption by the United Nations General Assembly in December 2024 of the UN Cybercrime Convention — the first universal multilateral cybercrime treaty — represents both the most significant development in international cybercrime law since the Budapest Convention and, in the view of many civil society organisations and democratic governments, a source of significant risk to human rights and the integrity of international cybercrime cooperation. The Convention's negotiation through the Ad Hoc Committee process established by General Assembly Resolution 74/247, over six years and through forty-plus days of negotiations, reflected the deep political divisions between states that prioritise effective international law enforcement cooperation and those that prioritise expansive state authority to criminalise online content and conduct.

The Convention's potential contribution to international cybercrime law enforcement — particularly through its prospect of bringing China, Russia, and other non-Budapest states into a binding framework of cybercrime cooperation — must be assessed against the human rights risks embedded in its text. The Convention's broad substantive scope, encompassing crimes 'using ICT' that go substantially beyond computer-specific offences, creates a risk that its cooperation mechanisms will be invoked to pursue conduct that is protected under

international human rights law in democratic jurisdictions. The adequacy of the Convention's human rights safeguards — including the dual criminality requirement for mutual legal assistance and the political offence exception — to protect against such abuse has been contested, with different expert assessments reaching diametrically opposed conclusions about whether the safeguards are robust enough to prevent the Convention becoming an instrument of political repression.

6.3 Voluntary Norms and the Prospects for Treaty-Based International Cybersecurity Law

Beyond the Budapest and UN Cybercrime Convention frameworks, the international legal landscape for cybersecurity is dominated by the voluntary norm framework developed through successive UN Groups of Governmental Experts (GGEs) and the UN Open-Ended Working Group (OEWG). The 2021 GGE consensus report confirmed the applicability of international law to state conduct in cyberspace and elaborated eleven voluntary peacetime norms of responsible state behaviour, including norms against attacking critical infrastructure, against conducting cyber operations that damage computer emergency response capabilities, and requiring due diligence in preventing territory from being used as a base for internationally wrongful cyber acts. These norms — though voluntary and without formal enforcement mechanisms — represent the current consensus understanding of responsible state behaviour in cyberspace and provide a normative foundation for diplomatic and political responses to state cyber operations that violate them.

The prospects for the development of binding treaty law governing state conduct in cyberspace beyond the cybercrime domain remain limited in the near to medium term, given the depth of the geopolitical divisions between major cyber powers over fundamental questions about internet governance, state sovereignty, and the scope of permissible cyber operations. The Tallinn Manual 2.0 process — through which a group of international law experts has developed detailed analysis of how existing international law applies to cyber operations — provides an invaluable scholarly resource for the development of customary international law in the cyber domain, even in the absence of treaty codification. The systematic engagement of state legal advisers with the Tallinn Manual analysis — reflected in the growing body of official government positions on specific questions of international cyber law — is gradually building the opinio juris that is a prerequisite for the development of binding customary norms.

7. DOMINANT TRENDS AND PERSISTENT TENSIONS IN GLOBAL CYBERSECURITY GOVERNANCE

7.1 Convergence Trends

Despite the diversity of national approaches surveyed above, several dominant convergence trends are observable across the global cybersecurity governance landscape that suggest the development, albeit uneven and contested, of shared global norms for cybersecurity law and policy. First, the near-universal adoption of mandatory data breach notification requirements — by which organisations are required to notify affected individuals and regulatory authorities following security incidents involving personal data — represents a global convergence on a core cybersecurity accountability mechanism that was virtually absent from national legal systems before 2002 and is now present, in some

form, in the legal systems of virtually every major economy. Second, the adoption of risk-based approaches to cybersecurity regulation — requiring organisations to implement security measures proportionate to the risks they face rather than compliance with prescriptive checklists — is evident across the EU, US, Australian, Singaporean, and many other national frameworks, reflecting a shared recognition that prescriptive rules cannot keep pace with the evolution of both technology and threats.

Third, the emergence of critical infrastructure protection as a central preoccupation of national cybersecurity frameworks — with dedicated legislation, sector designation processes, and mandatory security requirements for critical infrastructure operators — is observable across virtually all major jurisdictions, reflecting the shared understanding that the protection of essential services from cyber attack is a core function of state security provision. Fourth, the growing emphasis on supply chain security — requiring organisations to assess and manage the cybersecurity risks posed by their technology vendors and service providers — is visible across the NIS2 Directive, CIRCIA, Australia's SOCI framework, and many other national instruments, driven by the cascade of major incidents attributable to supply chain compromises. Fifth, the integration of cybersecurity into the governance of emerging technologies — particularly AI and IoT — through frameworks such as the EU AI Act, the Cyber Resilience Act, and the FDA's medical device cybersecurity requirements, reflects a shared recognition that cybersecurity must be addressed as a design requirement of new technologies rather than retrofitted after deployment.

7.2 Persistent Tensions

Against these convergence trends, several persistent and fundamental tensions characterise the global cybersecurity governance landscape and present serious obstacles to greater international harmonisation. The most fundamental is the tension between security and liberty — between the surveillance and access authorities that governments claim are necessary for effective cybersecurity and law enforcement, and the privacy, freedom of expression, and due process rights that individuals claim against government intrusion. This tension is not resolvable by technical or legal means — it reflects genuine value disagreements that different political communities resolve differently, generating divergent frameworks that will resist harmonisation as long as the underlying value disagreements persist.

A second fundamental tension is between national sovereignty and the transnational character of cyber threats. States assert sovereign authority over their digital infrastructure and the data of their citizens, enacting localisation requirements, security review obligations, and government access powers that create fragmented digital markets and impede the cross-border data flows that the global digital economy requires. Simultaneously, the most significant cyber threats are inherently transnational — perpetrated by actors in one or more jurisdictions against victims in others, using infrastructure spread across the globe — and effective responses require international cooperation that sovereignty claims complicate and sometimes preclude. The resolution of this tension requires states to accept limitations on their sovereign authority over cyberspace in exchange for the collective security benefits of greater international cooperation — a bargain that the current geopolitical climate makes politically difficult to achieve.

A third tension is between the pace of technological change and the deliberative processes of lawmaking. Cybersecurity law consistently finds itself regulating threats and technologies that were not anticipated when the relevant legislative instruments were designed, requiring constant adaptation through subsidiary regulation, regulatory guidance, and interpretive creativity that can only partially compensate for the structural mismatch between legislative timelines and technological development cycles. The adaptive regulatory design approaches discussed elsewhere in this issue — including outcome-based obligations, mandatory review clauses, and regulatory sandbox mechanisms — represent partial responses to this tension that deserve wider adoption but cannot fully resolve the fundamental challenge of governing a technologically dynamic domain through the necessarily slower instruments of law.

8. A RESEARCH AGENDA FOR CYBERSECURITY LAW AND POLICY SCHOLARSHIP

8.1 Priority Research Areas

The global cybersecurity governance landscape surveyed in this article generates a rich and urgently needed research agenda for cybersecurity law and policy scholarship. Several priority research areas merit identification. First, the comparative effectiveness of different regulatory models for cybersecurity — mandatory versus voluntary; prescriptive versus outcome-based; sector-specific versus horizontal — is an empirical question on which relatively little rigorous evidence exists. The expansion of mandatory cybersecurity requirements across jurisdictions, and the growing availability of incident data through mandatory reporting regimes, creates the conditions for comparative empirical research that can generate evidence-based insights into which regulatory approaches actually improve security outcomes rather than merely satisfying compliance expectations.

Second, the governance of cybersecurity in developing economies — where the combination of rapid digitalisation, limited institutional capacity, governance integrity challenges, and acute exposure to criminal and state-sponsored cyber threats creates a governance challenge qualitatively different from that faced by well-resourced, institutionally sophisticated developed country regulators — deserves substantially more scholarly attention than it has received. The existing scholarship on cybersecurity law and policy is heavily weighted toward the EU, US, and a small number of advanced economy jurisdictions.

Third, the intersection of cybersecurity law with other domains of public law and policy — including competition law, trade law, human rights law, investment law, and the law of armed conflict — generates complex interactions that are inadequately theorised in the existing literature. The use of cybersecurity regulations as instruments of industrial policy and trade protection; the tension between data protection and national security surveillance; the application of international humanitarian law to AI-enabled cyber operations; and the implications of cybersecurity requirements for investment treaty protections are among the cross-disciplinary questions that require sustained scholarly attention from researchers with expertise spanning multiple legal domains.

8.2 Methodological Directions

The methodological toolkit of cybersecurity law and policy scholarship should be expanded beyond the doctrinal analysis that dominates the existing literature to encompass a more diverse range of approaches suited to the empirical and comparative dimensions of the research agenda outlined above. Quantitative empirical approaches — including analysis of breach notification data, regulatory enforcement records, incident databases, and survey data from regulated organisations — can provide systematic evidence about the real-world effects of legal and regulatory interventions that doctrinal analysis cannot access. Qualitative comparative case study methods can illuminate the mechanisms through which different regulatory approaches achieve their effects and the contextual factors that condition their success or failure across different institutional and economic environments.

9. CONCLUSION: CYBERSECURITY LAW AT THE THRESHOLD OF MATURITY

The global cybersecurity legal landscape of 2025 presents a picture of a field in rapid and consequential development — one that has moved, within the span of two decades, from the margins of public law to its centre, from a narrow technical specialism to a multidisciplinary enterprise engaging the full range of legal knowledge and legal institutions, and from voluntary aspirations to mandatory obligations enforced by specialised agencies with significant sanction powers. The quantity and quality of national and international cybersecurity legislation enacted since 2016 alone — including the GDPR, NIS2, the Cyber Resilience Act, DORA, the AI Act, CIRCIA, Australia's SOCI amendments, India's DPDPA, the UN Cybercrime Convention, and dozens of other instruments surveyed in this article — represents a legislative output whose scope and significance few could have anticipated when the Budapest Convention was negotiated.

Yet this legislative abundance has not yet produced the governance coherence that the scale and character of global cyber threats demands. The fragmentation of the international regulatory landscape — across geopolitical blocs, developmental contexts, and regulatory philosophies, generates compliance burdens, enforcement gaps, and coordination failures that benefit threat actors who can exploit jurisdictional seams with a facility that law-abiding organisations cannot match.

REFERENCES

African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), adopted 27 June 2014, entered into force 8 June 2023.

Australia, Cyber Security Act 2024 (Cth).

Australia, Security of Critical Infrastructure Act 2018 (Cth), as amended.

Basic Act on Cybersecurity, Act No. 104 of 2014 (Japan).

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

Brazil, Lei Geral de Proteção de Dados Pessoais (LGPD), Law No. 13,709 (14 August 2018).

Budapest Convention on Cybercrime (Council of Europe), ETS No. 185, opened for signature 23 November 2001, entered into force 1 July 2004.

California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199.100 (2018).

China, Cybersecurity Law of the People's Republic of China (2016).

China, Data Security Law of the People's Republic of China (2021).

China, Personal Information Protection Law of the People's Republic of China (2021).

China, Regulations on the Security Protection of Critical Information Infrastructure (2021).

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Pub. L. No. 117-103.

Cybersecurity Act, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019.

Cyber Resilience Act, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024.

Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022.

European Union AI Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

India, Digital Personal Data Protection Act 2023, Act No. 22 of 2023.

Kenya, Data Protection Act No. 24 of 2019.

Klimburg, A. (ed.), 'National Cyber Security Framework Manual' (NATO CCD COE Publication, 2012).

Kosseff, J., 'Cybersecurity Law' (3rd ed., John Wiley & Sons, 2022).

Lotrionte, C., 'Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law' (2012) 5 Cyber Defense Review 73.

Maurer, T., 'Cyber Mercenaries: The State, Hackers, and Power' (Cambridge University Press, 2018).

Network and Information Security 2 Directive (NIS2), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022.

Nigeria, Nigeria Data Protection Act, Act No. 41 of 2023.

NIST, 'Cybersecurity Framework 2.0' (National Institute of Standards and Technology, 2024).

OECD, 'Recommendation on Digital Security Risk Management for Economic and Social Prosperity' (OECD, 2015).