World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

The impact of international cybersecurity treaties on domestic cybercrime control and national critical infrastructure protection

Amarachi F. Ndubuisi *

Legal Department, Economic and Financial Crime Commission, Nigeria.

World Journal of Advanced Research and Reviews, 2023, 20(03), 2285-2304

Publication history: Received on 04 November 2023; revised on 23 December 2023; accepted on 28 December 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.20.3.2549

Abstract

The rising frequency and severity of cyberattacks have elevated cybersecurity to a global policy imperative, prompting the negotiation and ratification of international cybersecurity treaties. These agreements aim to foster cross-border cooperation, streamline legal standards, and create mechanisms for joint response to cyber threats. This paper critically examines the impact of such international cybersecurity treaties on domestic efforts to control cybercrime and safeguard national critical infrastructure. Beginning with an overview of the evolving international cybersecurity landscape, the paper explores how treaties such as the Budapest Convention on Cybercrime, the UN Open-ended Working Group (OEWG) on cybersecurity, and regional frameworks like the African Union's Malabo Convention influence national legislation and enforcement practices. The study then assesses how these treaties translate into domestic legal reforms, including criminal code modernization, institutional capacity building, and the adoption of norms for cyber threat intelligence sharing. Particular attention is paid to the implementation challenges in lower-resourced states, where regulatory gaps, enforcement limitations, and political reluctance often dilute treaty effectiveness. Through comparative case studies from the European Union, the United States, and Southeast Asia, the research highlights divergent outcomes in treaty adoption and efficacy. It further evaluates how international legal instruments have directly contributed to the resilience of critical infrastructure sectors such as energy, finance, healthcare, and transportation through mandated compliance standards and collaborative incident response protocols. Despite notable progress, challenges persist—ranging from geopolitical fragmentation and data sovereignty concerns to inadequate enforcement mechanisms. The paper concludes with policy recommendations for enhancing treaty effectiveness through improved capacity development, multilateral trust-building, and context-specific implementation strategies.

Keywords: International Cybersecurity Treaties; Cybercrime Control; Critical Infrastructure Protection; Domestic Legal Reform; Cyber Cooperation; Treaty Implementation

1. Introduction

1.1. Background and Context of Global Cyber Threats

The global proliferation of digital systems has brought unprecedented convenience, connectivity, and economic opportunity. However, it has also introduced a vast and ever-evolving threat landscape. Cyberattacks have shifted from isolated criminal acts to large-scale, coordinated campaigns targeting critical sectors such as finance, healthcare, transportation, and energy [1]. These attacks range from ransomware and supply chain intrusions to espionage campaigns and data destruction events, many of which are conducted or supported by state actors.

* Corresponding author: Amarachi F. Ndubuisi

In 2020 alone, the global cost of cybercrime was estimated to exceed $1 trillion, with the frequency and impact of attacks continuing to rise [2]. Recent incidents—such as the SolarWinds breach, the Colonial Pipeline ransomware attack, and global hospital disruptions during the COVID-19 pandemic—have highlighted how digital threats can rapidly escalate into national security crises. The integration of operational technologies with internet-facing systems has only magnified vulnerabilities across essential services [3].

Despite advancements in defensive technologies, most cyber defenses remain reactive and fragmented, particularly across national borders. Malicious actors exploit differences in cyber laws, enforcement capacities, and geopolitical priorities to execute cross-border attacks with limited fear of prosecution. These disparities, when coupled with inadequate international cooperation, result in major enforcement gaps [4].

As cyber threats grow in scale and sophistication, there is an urgent need for synchronized legal and policy frameworks capable of deterring and responding to attacks with cross-jurisdictional implications. The emergence of international cybersecurity treaties represents an important, albeit imperfect, response to this pressing challenge.

1.2. The Rise of International Cybersecurity Treaties

Recognizing that cybercrime cannot be addressed through domestic regulation alone, governments have sought to create treaty-based mechanisms for legal cooperation, information exchange, and harmonization of laws. The Budapest Convention on Cybercrime, adopted in 2001 by the Council of Europe, remains the most comprehensive multilateral treaty dedicated to cybercrime prevention and prosecution [5]. It has since been ratified by over 65 countries and has shaped the drafting of national cybercrime legislation worldwide.

However, the treaty's reach is limited by the refusal of major cyber powers such as Russia, China, and India to ratify it. These countries cite concerns over national sovereignty and unequal control over treaty governance [6]. In response, alternative frameworks have emerged, including the Shanghai Cooperation Organisation's cybersecurity agreements and China's proposed Global Initiative on Data Security, which reflect differing ideological positions on cyberspace governance.

In addition to these treaty-based instruments, international organizations such as the United Nations have launched dialogues through the Open-ended Working Group (OEWG) and the Group of Governmental Experts (GGE) to build consensus on norms of responsible state behavior in cyberspace [7]. Although these forums have produced non-binding recommendations, they have yet to yield enforceable legal commitments.

Despite limitations, treaties remain vital in creating the legal architecture needed for states to engage in extradition, evidence sharing, joint investigation, and harmonization of cybercrime definitions. They also provide the legal justification for creating national institutions like Computer Emergency Response Teams (CERTs) and establishing formal Public-Private Information Sharing Agreements, which are often mandated under treaty provisions [8].

The growing frequency and impact of cross-border attacks have revived global interest in updating and expanding cybersecurity treaties to include issues like ransomware, cloud evidence access, and the protection of critical infrastructure—especially in light of lessons learned from recent multinational breaches.

1.3. Scope, Aims, and Structure of the Article

This article critically examines the impact of international cybersecurity treaties on domestic capabilities to control cybercrime and protect national critical infrastructure. Specifically, it assesses how international legal instruments shape national policies, affect enforcement strategies, and facilitate (or hinder) coordination among key stakeholders in government and the private sector.

While many articles address cybercrime enforcement or infrastructure protection independently, this analysis focuses on their intersection—viewing treaties not only as enforcement tools but also as instruments that influence national resilience. Drawing on case studies, treaty texts, and expert commentary, the paper investigates how treaties are implemented, what challenges persist, and which gaps remain unaddressed by current frameworks [9].

The article proceeds in eight structured sections. Section 2 presents the historical development of international cybersecurity treaties and the evolution of legal thinking on cyber threats. Section 3 analyzes how treaties influence domestic legislation and institutional reform. Section 4 examines the role of these legal instruments in facilitating threat intelligence sharing and response coordination. Section 5 discusses how treaties are operationalized in critical infrastructure sectors, highlighting real-world outcomes and limitations. Section 6 evaluates regional and geopolitical

disparities in treaty adoption and compliance. Section 7 explores technological innovations that support treaty implementation, and Section 8 offers policy recommendations grounded in legal realism and cross-sectoral insight.

Table 1, presented in Section 3, compares treaty adoption and implementation practices across major geopolitical regions, providing a comparative basis for policy analysis.

The article draws upon jurisdictions with varying legal cultures, cyber capacities, and treaty positions—including the United States, European Union, China, Russia, and Nigeria—to capture a diverse set of legal, operational, and institutional realities.

1.4. Definitions: Cybercrime, Critical Infrastructure, and International Treaties

For the purposes of this article, **cybercrime** is defined as any criminal offense committed through or against computer systems or data networks, including both traditional crimes enabled by technology (e.g., fraud, extortion) and offenses that specifically target digital infrastructure (e.g., malware deployment, denial-of-service attacks) [10].

Critical infrastructure refers to the physical and virtual systems and assets vital to a country's national security, economy, public health, and safety. Examples include electricity grids, water systems, financial markets, communication networks, and healthcare institutions. These systems are increasingly targeted by both criminal syndicates and state-linked actors seeking disruption or leverage [11].

International cybersecurity treaties are formal legal agreements between states aimed at governing conduct in cyberspace. These treaties typically address issues such as cybercrime definitions, procedural cooperation, law enforcement capabilities, jurisdictional authority, and principles for infrastructure protection. Treaties may be binding (e.g., Budapest Convention) or non-binding frameworks with normative influence (e.g., GGE recommendations) [12].

While not all cybersecurity instruments take the form of treaties, this article focuses on those that involve legal obligations, implementation mechanisms, and intergovernmental structures. Multistakeholder initiatives and soft law approaches are referenced only where they directly complement or conflict with formal treaty provisions.

Understanding the foundations of today's cybersecurity treaties requires a look at the early attempts to define, regulate, and cooperate on cyber threats across borders. In the next section, we explore the historical evolution of international cyber law, the motivations behind early treaties, and the geopolitical tensions that shaped their current limitations.

2. Evolution of international cybersecurity treaties

2.1. Historical Milestones in Global Cybersecurity Cooperation

International concern over cybercrime emerged in the 1980s when global communication networks began expanding across borders. One of the earliest efforts to establish legal cooperation was the Organisation for Economic Co-operation and Development (OECD)'s 1986 guidelines, which provided foundational principles for securing personal data and fostering cross-border data flow [5]. These guidelines signaled the growing need for transnational coordination to prevent computer-related offenses.

As cyberattacks intensified in the 1990s, driven by the expansion of the internet and commercial use of IT systems, regional blocs and international organizations began drafting legal frameworks. The Council of Europe took the lead by forming expert committees in the mid-1990s, which ultimately resulted in the drafting of the Budapest Convention—the first legally binding treaty on cybercrime [6].

Meanwhile, intergovernmental discussions at the United Nations began exploring the implications of cyber threats for international peace and security. The UN General Assembly started issuing resolutions encouraging states to develop harmonized legal definitions and norms for behavior in cyberspace. However, divergent views among major powers over digital sovereignty slowed consensus-building [7].

The early 2000s marked a shift from informal guidelines to formal treaties, spurred by high-profile cyber incidents and the increasing involvement of organized crime syndicates in online operations. These milestones laid the groundwork for both regional and global initiatives that now shape national cybercrime legislation, law enforcement cooperation, and cybersecurity governance [8].

Despite progress, early cooperation efforts were hindered by the absence of common enforcement mechanisms and the unwillingness of certain powerful states to commit to binding multilateral instruments. These historical dynamics continue to affect the reach and relevance of today's cybersecurity treaties.

2.2. Overview of Key International Cybersecurity Treaties

Cybersecurity treaties differ in scope, structure, and adoption levels, but they share common goals: promoting legal harmonization, facilitating evidence sharing, and improving prosecution across borders. Several international and regional instruments have emerged as pillars of global cybersecurity governance.

2.2.1. The Budapest Convention

The Budapest Convention on Cybercrime, adopted in 2001 and enforced in 2004, remains the most influential treaty on cybercrime cooperation. It covers offenses such as illegal access, data interference, computer-related fraud, and child exploitation, alongside procedural measures like expedited data preservation and trans-border access to stored data [9].

With over 65 parties—including non-European countries like the United States, Japan, and Australia—the treaty has provided a blueprint for national cybercrime laws. Its 24/7 contact network, mutual legal assistance protocols, and emphasis on procedural harmonization have enabled real-time collaboration in investigations [10].

However, critics argue that the treaty reflects Western legal traditions and lacks inclusivity in its drafting process. Countries such as Russia, India, and China have declined to join, citing concerns over sovereignty and unilateral evidence access by foreign law enforcement [11].

2.2.2. The Malabo Convention (African Union)

Adopted in 2014, the African Union Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, aims to create a continent-wide framework for cybercrime, data protection, and e-commerce regulation. It obligates African states to adopt national cybercrime laws and develop strategies for protecting critical infrastructure [12].

Despite its ambitions, the convention suffers from poor ratification. As of 2024, fewer than 20 AU member states have ratified it. The lack of implementation undermines its potential to address cybercrime challenges across Africa's rapidly digitizing economies [13].

Still, the convention has prompted legal reforms in countries like Ghana and Kenya, and has inspired calls for greater regional interoperability and technical cooperation. Its comprehensive scope—addressing both security and rights—makes it a model for regional digital governance.

2.2.3. The Shanghai Cooperation Agreement

The Shanghai Cooperation Organization (SCO)—comprising China, Russia, and several Central and South Asian states—promotes a model of "information security" aligned with state sovereignty. The SCO's 2009 Agreement on Cooperation in the Field of International Information Security reflects a security-first approach, focusing on cyberterrorism, online extremism, and information manipulation [14].

Unlike the Budapest Convention, the SCO framework emphasizes state control over cyberspace and rejects unilateral cross-border access to data. It promotes norms where national laws prevail, even in matters of international interest. This model has attracted criticism for potentially legitimizing online censorship and surveillance under the guise of security.

Nonetheless, the SCO agreement has deepened cyber cooperation among its members, resulting in joint drills, coordinated incident response, and intelligence exchange. It represents a geopolitical counterbalance to Western-led treaties and complicates efforts to establish global norms.

2.2.4. UN GGE and OEWG Initiatives

At the global level, the United Nations Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have sought to develop consensus on responsible state behavior in cyberspace. Their non-binding norms—

such as refraining from attacking critical infrastructure during peacetime—have been endorsed in successive reports since 2015 [15].

While these initiatives lack enforcement power, they reflect the only inclusive platforms where all UN member states participate in discussions on cybersecurity governance. The OEWG's latest report in 2021 recommended voluntary norms and capacity-building programs to assist developing countries in establishing cyber laws and incident response systems.

However, disagreements over digital sovereignty, cross-border access to data, and attribution continue to divide member states. This has limited the OEWG and GGE's ability to propose binding treaty language. Nevertheless, their normative influence is evident in national cybersecurity strategies, many of which reference their principles as guiding frameworks [16].

Table 1 below summarizes the scope, adoption, strengths, and limitations of these major cybersecurity treaties and agreements.

Table 1 Comparison of Major Cybersecurity Treaties and Their Provisions

Treaty	Scope	Membership	Strengths	Limitations
Budapest Convention	Cybercrime definitions, procedures, evidence	65+ nations	Legal harmonization, operational cooperation	Lack of universal adoption, Western-centric drafting
Malabo Convention (AU)	Cybercrime, data protection, digital economy	<20 ratifications	Continental focus, rights-security balance	Weak ratification, uneven implementation
SCO Cybersecurity Agreement	Info security, state control, cyberterrorism	Russia, China, others	Sovereignty-based norms, regional coordination	Encourages censorship, lacks procedural safeguards
UN GGE / OEWG	Norms of state behavior, capacity-building	All UN members	Inclusive, norm-setting, development support	Non-binding, geopolitical gridlock

2.3. Limitations and Gaps in Treaty Enforcement

Despite their proliferation, most international cybersecurity treaties suffer from limited enforceability, uneven adoption, and conflicting philosophies. The Budapest Convention, while effective among its members, has little traction in countries that view cross-border data access as a sovereignty violation. This division hinders uniform implementation and fosters legal fragmentation [17].

The Malabo Convention's slow ratification weakens Africa's ability to build regional cyber resilience. Meanwhile, SCO agreements reinforce state-centric control but avoid accountability mechanisms that underpin liberal legal traditions. These disparities create an inconsistent global legal architecture, exploited by cybercriminals who operate across borders with impunity.

Moreover, most treaties lack robust compliance mechanisms. There are no formal penalties for non-cooperation, delayed evidence sharing, or failure to criminalize treaty-defined offenses. Implementation often depends on political will, which fluctuates with diplomatic priorities and resource availability [18].

Finally, the absence of binding global enforcement bodies—akin to an international cyber court—means that treaties often serve more as guidelines than guarantees of justice. As threats evolve, the legal tools to respond remain uneven and inadequately aligned.

3. Translation of treaties into national legal frameworks

3.1. Challenges in Legal Harmonization Across Jurisdictions

The effectiveness of international cybersecurity treaties is significantly dependent on the degree to which their provisions are transposed into national legal systems. Yet, achieving harmonization across jurisdictions remains a major challenge due to differences in legal traditions, political priorities, and resource capacities [9].

One of the primary hurdles lies in definitional inconsistency. What constitutes "unauthorized access" or "critical infrastructure interference" varies from one legal code to another. For instance, countries following the common law tradition, like the United Kingdom or the United States, often use case law and broad statutory interpretation, whereas civil law nations, like France or Germany, codify specific offense categories. These variances complicate efforts to standardize prosecution procedures and extradition requirements [10].

Moreover, the implementation of treaty provisions often occurs unevenly. Some states adopt only partial elements of a treaty or pass legislation that nominally complies but lacks practical enforcement mechanisms. These legal half-measures undermine coordinated action, particularly when cybercrime actors exploit jurisdictional gaps to stage and route attacks across "soft" states with minimal risk of arrest or asset seizure [11].

The challenge is further amplified in federal systems, where subnational units retain significant legislative autonomy. In the United States, for example, state and federal laws may diverge on surveillance, breach notification, or criminal liability thresholds, creating inconsistencies within a single jurisdiction [12].

Finally, resource disparities hinder the translation of treaties into effective law. Low-income or digitally emerging states may lack the institutional capacity to draft, revise, or enforce comprehensive cybercrime laws. Without international support, these jurisdictions remain vulnerable despite treaty membership.

3.2. Case Studies in Domestic Policy Transformation

3.2.1. United States: CFAA Modernization and DHS Policy

The United States was among the first non-European countries to ratify the Budapest Convention and has used it as a guide to reform its domestic cybersecurity legislation. The Computer Fraud and Abuse Act (CFAA)—originally enacted in 1986—has undergone multiple revisions to align more closely with international norms, particularly around procedural enforcement and scope [13].

Recent amendments have addressed concerns over prosecutorial overreach, narrowing the definition of "unauthorized access" and clarifying that routine terms-of-service violations should not lead to felony charges. This modernization effort reflects pressures from both domestic civil liberties groups and international stakeholders calling for proportional cybercrime penalties [14].

In parallel, the Department of Homeland Security (DHS) has institutionalized treaty-inspired practices such as information sharing, infrastructure mapping, and critical sector protection through the Cybersecurity and Infrastructure Security Agency (CISA). The agency's role in coordinating cross-sector cyber risk mitigation reflects treaty mandates for public-private collaboration and proactive threat monitoring [15].

Still, U.S. policy is not without criticism. Some international partners argue that the U.S. maintains an asymmetric approach—demanding cooperation abroad while reserving unilateral enforcement prerogatives at home. Nonetheless, American legal and institutional reforms have been among the most aggressive and operationally aligned with treaty objectives.

3.2.2. European Union: NIS and NIS2 Directives

The European Union's response to international cybersecurity obligations has taken the form of highly structured regulatory directives, particularly the Directive on Security of Network and Information Systems (NIS Directive) and its successor, NIS2. These frameworks aim to harmonize cybersecurity standards across member states while aligning with the procedural mandates of the Budapest Convention [16].

The NIS Directive, adopted in 2016, required EU countries to develop national strategies, designate competent authorities, and mandate incident reporting across critical sectors. This was one of the first regionally binding efforts to operationalize treaty commitments at scale.

However, variations in national implementation soon emerged. While countries like Germany and the Netherlands developed robust enforcement protocols, others lagged behind, leading to compliance discrepancies that undermined the directive's collective strength [17].

In response, **NIS2**, introduced in 2022, expanded sectoral coverage, clarified incident reporting timelines, and imposed stricter supervisory measures. It also emphasized supply chain risk management and enforced cross-border information exchange obligations among Computer Security Incident Response Teams (CSIRTs).

These policy transformations demonstrate how international treaties can evolve into regional legislation with legally binding enforcement. EU member states are now required not only to transpose the directive into domestic law but to ensure real-time coordination with peers—a substantial leap forward in regional cyber resilience [18].

3.2.3. Nigeria: Budapest-aligned Cybercrime Act

Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 was explicitly influenced by the Budapest Convention, marking a significant step in aligning domestic cyber legislation with international norms. The law criminalizes offenses such as identity theft, cyberstalking, system interference, and online fraud—many of which mirror the language of the treaty [19].

It also establishes the National Computer Emergency Response Team (ngCERT), assigns legal responsibilities to service providers, and outlines procedures for data preservation and access by law enforcement. The Act was instrumental in enabling Nigeria's Financial Intelligence Unit (NFIU) and Economic and Financial Crimes Commission (EFCC) to pursue digital fraud and cross-border scams more aggressively [20].

Nevertheless, enforcement remains inconsistent. Judicial capacity, technical training, and inter-agency coordination challenges persist. Some critics argue that the Act is applied more effectively against domestic cyber actors than transnational syndicates due to limited diplomatic channels and slow MLAT responses [21].

Nigeria's case highlights the complex path from treaty inspiration to full operationalization. While the country has taken laudable steps toward legal harmonization, the gap between legislation and implementation remains wide.

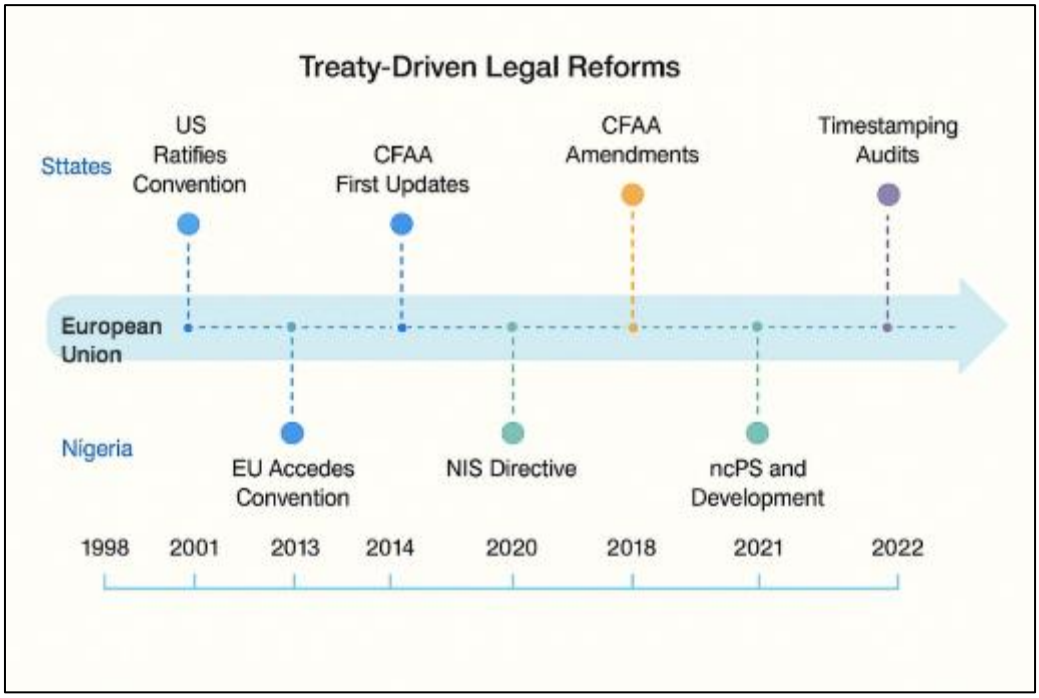

Figure 1 Timeline of Treaty-Driven Legal Reforms in Selected Nations

3.3. Persistent Legislative Gaps and Enforcement Deficiencies

Despite progress in many jurisdictions, legislative gaps and enforcement shortcomings persist. One common issue is the lack of clarity around procedural aspects such as evidence collection, international data access, and admissibility standards—often leading to cases being dismissed or delayed [22].

In some countries, treaty-inspired laws exist on paper but are rarely invoked due to institutional reluctance, insufficient capacity, or political interference. Others suffer from outdated criminal codes that fail to encompass newer cyber threats like cryptocurrency laundering or AI-enhanced intrusion [23].

Furthermore, many national systems lack inter-agency coordination, particularly between law enforcement, judicial authorities, and cybersecurity response teams. Without integrated operational workflows, even well-written laws cannot translate into actionable enforcement.

The uneven domestic adoption of key treaty provisions undermines global cybercrime deterrence. Criminals increasingly exploit countries with weak enforcement regimes, creating **safe havens** and routing points that fragment international investigative efforts.

Until nations not only ratify but fully implement and operationalize treaty-aligned laws—with adequate funding, training, and oversight—treaties will remain aspirational instruments, unable to meet the demands of modern cybercrime complexity.

4. Treaty-driven cybercrime enforcement and intelligence sharing

4.1. Mutual Legal Assistance Treaties (MLATs) and Extradition Practices

Mutual Legal Assistance Treaties (MLATs) represent one of the most widely used instruments for facilitating cross-border cooperation in cybercrime cases. These treaties enable countries to formally request and provide assistance in the collection of evidence, service of documents, and enforcement of judgments in criminal matters [14]. When properly executed, MLATs allow for the timely retrieval of digital data stored across jurisdictions and the lawful extradition of suspects.

However, the procedural complexity of MLATs often leads to bureaucratic delays. Requests typically pass through multiple agencies, including ministries of justice, foreign affairs, and central authorities, creating substantial lag—especially in cases requiring real-time responses [15]. For instance, investigations involving live server data or volatile metadata may become futile if a delay in cooperation leads to the destruction or modification of digital evidence.

Additionally, political considerations frequently influence MLAT outcomes. States may refuse assistance if the requested act conflicts with their national security, public order, or dual criminality requirements. A notable challenge is the dual criminality standard, which requires that the alleged offense be considered a crime in both jurisdictions. Given the variation in cybercrime definitions worldwide, this condition often blocks cooperation even in high-stakes cases [16].

Extradition under MLAT frameworks has also proven contentious. Cybercrime suspects often exploit non-extradition safe havens, particularly in countries with weak political ties or adversarial relationships with the requesting state. For example, several high-profile hacking suspects from Russia and China have avoided extradition due to the absence of bilateral treaties or the invocation of sovereignty concerns [17].

These challenges underscore the need to streamline MLAT procedures and create expedited channels for cyber-related cooperation—possibly through treaty addenda or multilateral digital cooperation platforms.

4.2. Cross-Border Intelligence Sharing Frameworks

While MLATs deal with formal legal requests, intelligence sharing mechanisms facilitate real-time operational collaboration among law enforcement, cybersecurity agencies, and intelligence entities. Key institutions driving cross-border intelligence sharing include INTERPOL, EUROPOL, the Cybercrime Atlas, and global Computer Emergency Response Teams (CERTs).

INTERPOL's Cybercrime Directorate, headquartered in Singapore, operates a 24/7 communication network linking national police forces worldwide. It houses a Cyber Fusion Centre where private-sector experts and law enforcement

jointly analyze threat intelligence, issue alerts, and coordinate takedowns [18]. INTERPOL's I-24/7 platform allows for rapid dissemination of alerts, red notices, and cyber threat indicators.

In Europe, EUROPOL's European Cybercrime Centre (EC3) plays a similar role, serving as a focal point for operational and forensic support in transnational investigations. EC3 assists member states by analyzing malware campaigns, facilitating joint task forces, and linking cyber operations to organized crime syndicates [19].

Another significant platform is the Cybercrime Atlas, launched by the World Economic Forum in collaboration with leading cybersecurity firms. The Atlas aggregates real-time threat data from global partners to identify persistent cybercrime infrastructure, enabling coordinated mitigation strategies and law enforcement action [20].

Complementing these efforts are CERTs, which function as national-level response units for cyber incidents. Through frameworks like the Forum of Incident Response and Security Teams (FIRST) and ENISA's CSIRT Network, these teams share technical indicators, threat trends, and mitigation strategies [21]. CERTs are particularly crucial for detecting attacks targeting critical infrastructure and for managing sector-specific incidents across borders.

Despite these strengths, intelligence sharing frameworks face interoperability, legal, and trust-related barriers. Not all countries have fully operational CERTs, and some are reluctant to share intelligence due to concerns over data sensitivity, national reputation, or retaliation. Addressing these issues requires the creation of binding information-sharing protocols embedded within international cybersecurity treaties.

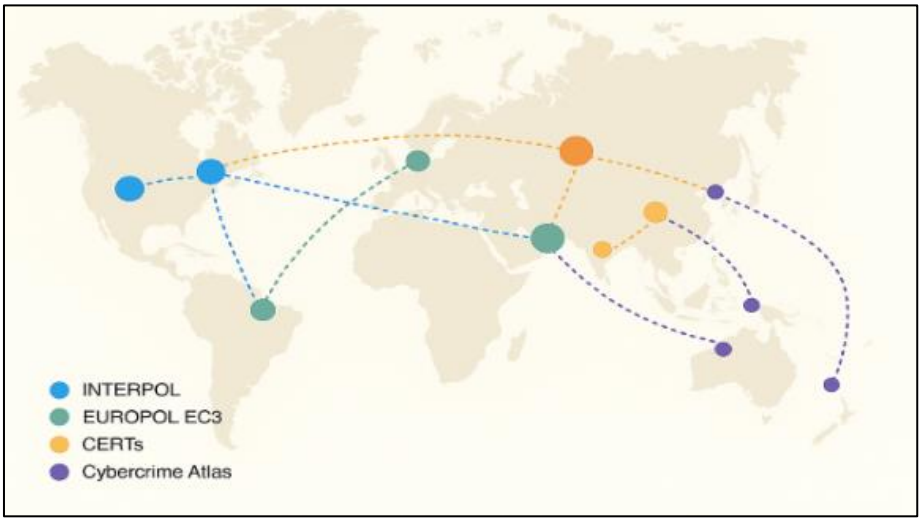

Figure 2 Map of Cross-Border Cybercrime Intelligence Channels

4.3. Law Enforcement Capacity and Joint Operations

The effectiveness of international cybersecurity treaties is not only contingent on legal harmonization and intelligence sharing but also on the operational capacity of law enforcement agencies to conduct cross-border joint operations. Successful treaty implementation depends on the ability of national agencies to act swiftly, cooperatively, and with appropriate technical expertise.

Joint operations, often orchestrated under the umbrella of INTERPOL or EUROPOL, have demonstrated that cybercrime can be effectively countered when legal cooperation is matched with tactical coordination. These operations typically involve joint investigation teams (JITs), digital forensic support, synchronized raids, and simultaneous arrests across multiple countries [22].

One such example is Operation Bayonet (2017), where Europol, Dutch police, and the FBI jointly took down the AlphaBay and Hansa darknet markets. This operation disrupted two of the largest online platforms for illicit trade, including malware, stolen data, and hacking tools. It involved covert infiltration, synchronized server seizures, and multi-agency prosecution [23].

Another notable case is Operation Falcon, where INTERPOL coordinated with West African states to dismantle a cybercrime ring responsible for business email compromise (BEC) scams worth over $40 million. The operation was

enabled by INTERPOL's Global Rapid Intervention of Payments (I-GRIP) mechanism and supported by the ECOWAS Cybercrime Framework [24].

In Table 2, we present selected examples of successful cross-national cybercrime operations facilitated by treaty-based legal cooperation and intelligence sharing.

Table 2 Examples of Successful Treaty-Based Cross-National Cybercrime Operations

Operation Name	Year	Lead Agencies	Focus Area	Treaty/Framework Used	Outcome
Operation Bayonet	2017	Europol, FBI, Dutch Police	Darknet marketplaces	Budapest Convention	Shutdown of AlphaBay and Hansa, arrests worldwide
Operation Falcon	2021	INTERPOL, ECOWAS partners	Business email compromise	ECOWAS Cybercrime Framework	11 suspects arrested, $40M fraud prevented
Silver Terrier Takedown	2022	Nigerian EFCC, INTERPOL	Advance-fee and phishing scams	Budapest-aligned Nigeria Act	Dozens of Nigerian cyber actors apprehended
EMOTET Dismantling	2021	Europol, FBI, Germany, Ukraine	Malware infrastructure	MLAT and EUROPOL coordination	Botnet disrupted, core actors prosecuted

Beyond operational success, these cases highlight a deeper insight: international cooperation is most effective when treaties provide not just legal alignment but real-time enforcement pathways. Technical support, joint training exercises, and shared cyber forensics capacity are critical to scaling treaty commitments into tactical realities [25].

Yet, resource asymmetries continue to limit some countries' participation in joint operations. Several African, Latin American, and Southeast Asian nations still lack digital forensics labs, secure evidence repositories, or the means to deploy cross-border task forces. Without treaty-backed development support and regional centers of excellence, global cyber defense remains unequal and fragile.

Building enforcement capacity must be treated as an intrinsic element of treaty design, not a post-ratification afterthought. Embedding requirements for skills development, intelligence integration, and funding mechanisms into treaty clauses could bridge these disparities and enhance systemic resilience.

5. Critical infrastructure protection under treaty influence

5.1. National Policy Shifts in CIIP Linked to Treaty Commitments

Cybersecurity treaties have increasingly influenced national policy shifts around Critical Information Infrastructure Protection (CIIP). Nations that are party to international instruments such as the Budapest Convention, the Malabo Convention, and UN GGE frameworks have amended domestic statutes to prioritize CIIP within their national cybersecurity strategies [19].

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) has adopted treaty-aligned models for identifying and securing sixteen critical infrastructure sectors. Treaty commitments have reinforced executive orders like EO 13636 and EO 14028, which emphasize public-private cooperation, threat intelligence sharing, and resilience testing [20].

Similarly, Germany's IT Security Act 2.0, implemented in alignment with the EU's NIS2 Directive, establishes CIIP obligations for operators of essential services. The legislation mandates real-time breach notification, supply chain security reviews, and standardized protection thresholds for energy, transport, and health sectors [21].

In Nigeria, alignment with the Budapest Convention has prompted amendments to the National Cybersecurity Policy and Strategy (NCPS 2021), explicitly recognizing sectors such as telecoms, financial services, and power as priority CIIP

domains. Guidelines issued by the National Information Technology Development Agency (NITDA) now require CIIP operators to report incidents to ngCERT and maintain data localization compliance [22].

These policy reforms demonstrate how treaty obligations catalyze internal transformation, moving CIIP from a voluntary compliance issue to a state mandate. As countries seek to deter sophisticated attacks on national lifelines, treaty frameworks serve both as justification and blueprint for proactive policy advancement.

5.2. Sectoral Case Studies on Treaty Impact

5.2.1. Energy Grid and Utilities

Energy systems have become primary targets for cyberattacks due to their systemic importance and digital interdependencies. In response, nations have implemented treaty-aligned CIIP strategies to protect grid control systems, SCADA networks, and smart meter data [23].

For instance, following the 2015 Ukrainian blackout attributed to Russian cyber actors, Ukraine partnered with EU cyber agencies and updated its energy protection protocols under the Budapest Convention's guidance. This included the creation of a sector-specific CERT and the adoption of digital forensics protocols aligned with international evidence preservation standards [24].

In France, the energy sector was among the first to fall under mandatory risk assessment provisions in accordance with the NIS Directive. Operators are required to conduct annual resilience audits and share threat intelligence with ANSSI, the national cybersecurity agency. These measures reflect treaty-inspired enforcement models that go beyond passive policy statements [25].

5.2.2. Financial Systems (e.g., SWIFT and Banking Sector)

The financial sector's reliance on digital transactions and cross-border systems like SWIFT has made it a top priority in cybersecurity treaty implementation. International norms have shaped banking regulations, breach disclosure policies, and payment network controls [26].

In Belgium, where SWIFT is headquartered, national financial regulators have incorporated cybersecurity obligations from the EU's Digital Operational Resilience Act (DORA), which builds on NIS2 treaty directives. This includes mandatory reporting of payment manipulation and data breaches, especially in high-value transfer corridors [27].

In Singapore, the Monetary Authority of Singapore (MAS) has aligned with the ASEAN Cybersecurity Cooperation Strategy, itself modeled after international treaties. MAS's Technology Risk Management Guidelines now mandate encryption protocols, incident classification, and coordination with INTERPOL in transnational financial crime cases [28].

5.2.3. Healthcare Sector (Post-COVID Ransomware Resilience)

The COVID-19 pandemic exposed severe vulnerabilities in the healthcare sector, with hospitals worldwide facing unprecedented ransomware attacks. In response, several nations embedded treaty-aligned protections into their healthcare cybersecurity mandates.

In Canada, the 2021 National Cyber Threat Assessment recognized healthcare as critical infrastructure and established federal coordination channels between Public Safety Canada, the Canadian Centre for Cyber Security, and hospital IT departments. This initiative was modeled on frameworks from the UN OEWG and GGE initiatives [29].

South Korea, operating under the Asia-Pacific CERT collaboration aligned with the Budapest Convention, implemented emergency preparedness drills and real-time medical data protection protocols across major hospital networks. These measures were codified into the country's Critical Information Infrastructure Protection Act in 2022 [30].

Figure 3 below presents a visual comparison of dominant cyberattack vectors and the sector-specific CIIP measures adopted in treaty-compliant nations.

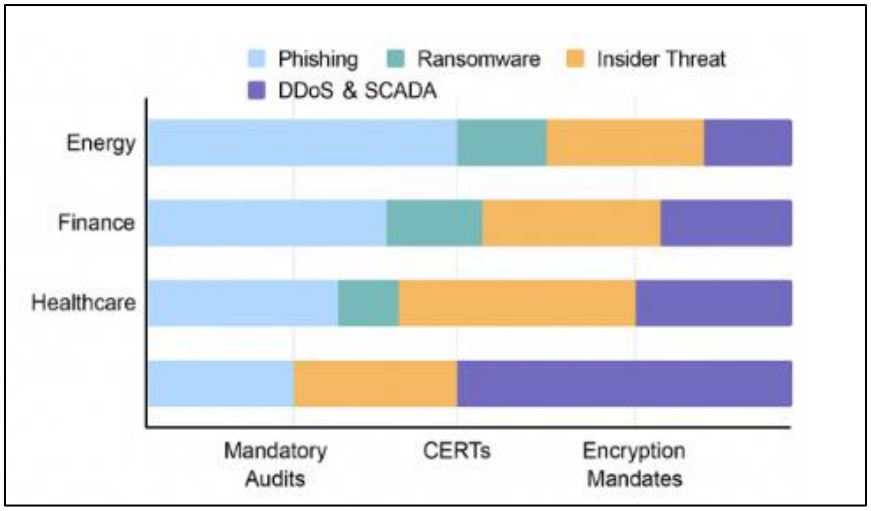

Figure 3 Attack Vectors vs. Sectoral CIIP Measures Aligned with Treaty Mandates

5.3. Incident Response, Recovery, and Simulation Exercises

Beyond policy and legislative alignment, cybersecurity treaties also promote practical preparedness mechanisms such as national-level incident response teams, cyber drills, and cross-border recovery frameworks.

Computer Security Incident Response Teams (CSIRTs) have become the primary institutional actors in operationalizing treaty provisions. In the European Union, CSIRTs are required by NIS2 to coordinate incident reporting, conduct impact assessments, and participate in ENISA-led simulation exercises. These exercises, such as Cyber Europe 2022, emulate ransomware and supply chain disruptions to test real-time response capacity [31].

In India, the National Critical Information Infrastructure Protection Centre (NCIIPC) conducts "Suraksha" cyber war games to simulate attacks on energy and financial assets. These drills are based on policy templates derived from international frameworks, including the UN OEWG recommendations on response readiness [32].

Canada's Cyber Storm series is another prominent example. Organized biennially by Public Safety Canada in conjunction with treaty-aligned partners like the U.S. DHS and UK NCSC, these exercises test coordinated response to infrastructure-wide attacks. Participants simulate data exfiltration, SCADA interference, and coordinated misinformation campaigns [33].

Table 3 lists select national participation in treaty-related cyber exercises.

Table 3 Participation of Nations in Cybersecurity Exercises Tied to International Treaties

Country	Exercise Name	Treaty Alignment	Primary Sector Focused	Year	Outcome
Canada	Cyber Storm VI	UN OEWG / Budapest Convention	Healthcare, energy	2022	Strengthened CERT coordination, refined escalation protocols
India	Suraksha Cyber Drill	UN OEWG / ITU Guidelines	Financial, energy	2023	Introduced automated response testing
Germany	LÜKEX Simulation	EU NIS/NIS2	Telecoms, public services	2022	Enhanced public-private coordination
South Korea	KISA National Exercise	Budapest Convention / APCERT	Healthcare, energy	2023	Identified lag in forensic data preservation
Nigeria	Cyber Secure Nigeria	Budapest-aligned framework	Telecoms, banking	2022	Launched sectoral CERTs and updated CIIP policy

Simulation exercises reinforce the treaty-mandated principles of multi-stakeholder readiness, real-time response coordination, and recovery planning. They expose operational gaps, validate escalation chains, and promote cross-agency trust.

However, participation remains uneven across regions. While NATO, EU, and ASEAN countries regularly conduct simulations, several African and Latin American nations are yet to institutionalize drills. Inclusion of mandatory readiness assessments within treaties and funding for drill execution would bridge this gap.

6. Regional and geopolitical disparities in treaty implementation

6.1. Global South vs. Global North: Implementation Asymmetries

The divide between the **Global North and South** in implementing international cybersecurity treaties is pronounced, reflecting underlying disparities in technical capacity, economic resources, and geopolitical priorities. Although many developing nations have signed or acceded to key treaties like the Budapest Convention, their domestic enforcement remains hindered by limited infrastructure, inadequate funding, and institutional fragmentation [24].

For example, while Germany and the Netherlands boast sector-specific CSIRTs and mature legal frameworks compliant with NIS2, many Sub-Saharan African countries lack national CERTs or centralized cybercrime units capable of responding to sophisticated threats. According to ITU's 2022 Global Cybersecurity Index, over 40% of countries in Africa remain in the early implementation stage of CIIP mandates despite treaty ratification [25].

The capacity gap is not just technical but also procedural. Many Global South nations struggle with sustained legislative reform, talent retention, and forensic capability to meet treaty provisions. These shortcomings leave treaty obligations unfulfilled or inconsistently applied, particularly in cross-border cases involving encrypted data and cloud infrastructure [26].

Furthermore, geopolitical motivations shape treaty participation. High-income states often treat cybersecurity treaties as extensions of their national defense postures. In contrast, low- and middle-income countries may approach them as diplomatic bargaining tools or prerequisites for development aid and foreign investment. This divergence impacts enforcement vigor and priorities.

Some nations also face donor dependency for implementing treaty-compliant reforms. Programs funded by the EU, World Bank, or ITU have helped countries like Ghana, Laos, and Jordan establish legal and operational frameworks. However, sustainability becomes a challenge once external funding ends, threatening long-term adherence and effectiveness [27].

This imbalance raises concerns about the legitimacy and fairness of treaty-based cooperation, especially when enforcement mechanisms disproportionately benefit better-resourced nations.

6.2. Political Distrust and Competing Cyber Norms

A major impediment to cohesive treaty enforcement is the ideological divergence between cyber powers, particularly between the United States and its allies and countries like China and Russia. These geopolitical blocs promote competing visions of cyberspace governance, complicating consensus on treaty language, operational definitions, and data exchange standards [28].

The U.S. and the European Union advocate for an open, rules-based internet underpinned by individual privacy rights, market freedom, and international law. In contrast, China and Russia have pushed for state-centric sovereignty-based models, arguing that each nation should exercise full control over its digital infrastructure and information environment [29].

This divergence surfaced during negotiations within the UN Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE), where disagreements over terms such as "responsible state behavior" and "norms of non-intervention" led to diluted resolutions and partial endorsements [30].

As a result, many multilateral treaties lack clear mechanisms for cross-bloc enforcement, especially in attribution and prosecution. Countries that do not recognize each other's legal legitimacy or cyber jurisdiction are unlikely to cooperate effectively in handling mutual legal assistance requests, extradition of cybercriminals, or joint intelligence operations.

Moreover, political distrust leads to selective compliance. While Russia has signed bilateral cybersecurity pacts with countries in Central Asia and Latin America, it has resisted cooperation frameworks led by NATO or the EU. Similarly, China has advanced digital cooperation within the Shanghai Cooperation Organization, largely excluding Western democracies [31].

This multipolar fragmentation reduces the universality and enforceability of cybersecurity treaties, reinforcing jurisdictional loopholes and impeding global cybercrime control.

6.3. Cross-Border Data Sovereignty and Regulatory Conflicts

Beyond geopolitical alignments, data sovereignty laws and privacy regulations present structural conflicts in the operationalization of international treaties. The European Union's General Data Protection Regulation (GDPR) is a prime example. While GDPR aims to protect citizens' data from unwarranted surveillance, it has clashed with treaty provisions requiring data exchange for cybersecurity purposes [32].

Under GDPR, transferring personal data outside the EU is highly regulated and, in many cases, restricted unless the receiving country offers adequate legal safeguards. This creates friction in treaties such as the Budapest Convention, which assumes expeditious access to data held in foreign jurisdictions for cybercrime investigations [33].

For instance, when U.S. agencies requested user data from a Dublin-based data center, Irish authorities initially refused, citing incompatibility with GDPR provisions. This legal impasse delayed an investigation into ransomware attacks targeting multiple EU and U.S. critical infrastructure operators [34].

Additionally, laws like China's Cybersecurity Law and Russia's Sovereign Internet Law impose data localization requirements, mandating that certain data remain physically within national borders. These constraints obstruct lawful cross-border data flows central to treaty enforcement [35].

Without clear treaty exemptions or standard conflict resolution protocols, data sovereignty laws risk rendering international cybersecurity cooperation both legally and technically unworkable.

7. Emerging technologies enabling treaty execution

7.1. AI for Threat Detection and Predictive Enforcement

The integration of Artificial Intelligence (AI) into treaty-based cybersecurity operations has significantly enhanced cross-border threat detection and predictive enforcement. AI-driven threat intelligence systems are now capable of identifying anomaly patterns, classifying malware behavior, and generating early warnings based on global data streams—capabilities that align directly with the operational requirements of treaties such as the Budapest Convention and the OECD Recommendation on Enhanced Access to Encrypted Data [29].

Under the EU-US Cyber Dialogue, machine learning models are being shared between CERT-EU and U.S. CISA to improve ransomware detection and phishing campaign attribution. These models, trained on millions of global incident data points, support real-time scoring of threats with jurisdictional tagging, enhancing both investigatory prioritization and legal triage [30].

AI tools also facilitate predictive enforcement, forecasting high-risk sectors and entities based on known vulnerabilities, geopolitical tension maps, and financial transaction histories. Countries like Estonia and Singapore are employing these systems in national cyber fusion centers, allowing for treaty-aligned, proactive measures such as coordinated patch cycles and policy interventions before attacks manifest [31].

The success of such collaboration depends on standardization. Frameworks like the MITRE ATT&CK matrix and the Common Attack Pattern Enumeration and Classification (CAPEC) system are now embedded within treaty cooperation protocols to ensure that AI outputs are interoperable across borders and institutions [32].

Nonetheless, disparities in AI capacity—especially among lower-income states—highlight the need for treaty provisions to include technical assistance and shared modeling infrastructure, ensuring equitable participation in AI-enhanced enforcement initiatives.

7.2. Blockchain for Evidence Authentication and Cross-Border Validation

Blockchain technology is increasingly deployed to validate digital evidence in cross-border cybercrime cases, addressing long-standing concerns about data authenticity, tampering, and chain-of-custody breakdowns. Treaty provisions such as those under the Council of Europe's Second Additional Protocol to the Budapest Convention now explicitly encourage the adoption of decentralized ledger systems for forensic integrity [33].

In a recent Interpol-Europol pilot, blockchain-based timestamping protocols were implemented to log and track forensic evidence collected during coordinated takedowns of darknet marketplaces operating across Germany, the Netherlands, and Canada. These logs, which could be independently verified by participating jurisdictions, helped ensure evidence admissibility without physical transfer [34].

Jurisdictional transparency is another key advantage. Smart contracts embedded within blockchain protocols can log jurisdictional data access permissions, ensuring that only authorized authorities—per treaty stipulations—can retrieve or submit evidence. This transparency reduces the risk of unauthorized surveillance or parallel criminal procedures that may violate sovereignty agreements [35].

Moreover, immutable blockchain records offer a trustworthy medium for digital evidence transfer in MLAT processes. Countries such as South Korea and Estonia have formalized blockchain authentication in cybercrime proceedings, demonstrating that even adversarial states may accept third-party blockchain records when treaty-compliant.

Figure 4 below illustrates a generic architecture for blockchain-enabled cross-border evidence management.

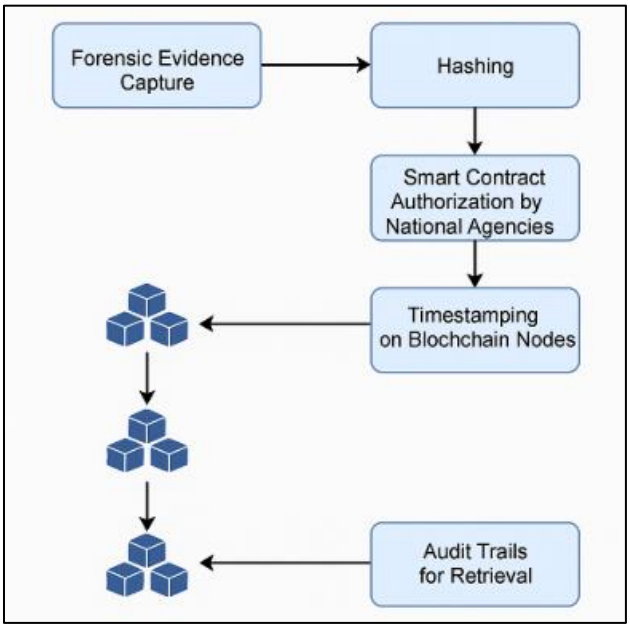

Figure 4 Blockchain Chain-of-Custody Architecture for Cross-Jurisdictional Evidence Management

7.3. Secure Protocols for Treaty-Based Communications

In operationalizing treaties, the security of intergovernmental communication remains paramount. As cross-border cybercrime investigations rely on rapid data exchange, robust encryption frameworks and secure protocol stacks are essential to uphold confidentiality, integrity, and legal validity [36].

Public Key Infrastructure (PKI) forms the foundation for many treaty-aligned communication systems, enabling mutual authentication and non-repudiation across national agencies. Within the EU's Cyber Crisis Liaison Organisation Network (CyCLONe), digitally signed communications ensure real-time verification of sensitive cyber incident reports and law enforcement alerts [37].

Virtual Private Networks (VPNs) and end-to-end encrypted messaging frameworks such as Threema and Signal are also endorsed in some bilateral cybersecurity treaties as trusted channels for operational correspondence between CERTs, national police, and judiciary bodies [38].

Beyond confidentiality, treaties increasingly call for protocol standardization to ensure system compatibility. The Global Forum on Cyber Expertise (GFCE) has recommended use of open standards like Transport Layer Security (TLS) 1.3, X.509 certificates, and IPsec in treaty-based communication layers [39].

Without such secure communication frameworks, treaty cooperation is vulnerable to interception, spoofing, or misinformation injection—risks that can delegitimize evidence, delay response, or undermine intergovernmental trust.

8. Successes, setbacks, and lessons from treaty implementation

8.1. Case Studies of Treaty Success Stories

While international cybersecurity treaties face numerous implementation barriers, there have also been notable success stories that showcase the power of coordinated global enforcement. One such example is Operation GoldDust, a joint law enforcement initiative targeting the REvil ransomware-as-a-service (RaaS) network, with the backing of treaty-aligned frameworks such as the Budapest Convention and INTERPOL collaboration protocols [34].

Involving over 17 countries including the United States, South Korea, Germany, and Romania, the operation resulted in multiple arrests, digital asset seizures, and takedowns of command-and-control infrastructure. The cross-border coordination was facilitated through streamlined Mutual Legal Assistance Treaty (MLAT) requests and shared threat intelligence channeled via EUROPOL's Joint Cybercrime Action Taskforce (J-CAT) [35].

In another case, Operation Quicksand, treaty mechanisms enabled the tracing of cryptocurrency wallets used by a ransomware group operating from Eastern Europe. Blockchain records authenticated through treaty-guided forensic standards provided prosecutable evidence in Germany, despite servers being hosted in Russia and the U.S. [36].

These operations demonstrate that treaties—when backed by political will and standardized technical frameworks—can overcome geographic, legal, and linguistic barriers. Real-time interoperability among national CSIRTs, adherence to international chain-of-custody standards, and synchronized indictment timelines are key features that underpin such treaty-driven successes.

Moreover, global trust networks fostered by treaties often outlive the operation itself, creating institutional momentum for future collaboration.

8.2. Limitations and Political Deadlocks

Despite progress, the limitations of current treaty structures are stark. Mutual Legal Assistance Treaties (MLATs) remain notoriously slow and bureaucratic, often taking months to process requests for data exchange or evidence collection—rendering them ill-suited for the dynamic nature of cyber threats [37].

Moreover, treaty implementation is often obstructed by political deadlocks. The ongoing disagreement at the United Nations over a global cybercrime treaty, particularly between the U.S.-EU bloc and Russia-China alliance, illustrates the challenge of crafting universally accepted frameworks. These divides result in ambiguous language, lack of enforcement mechanisms, or outright withdrawal from negotiations [38].

In addition, some states exploit treaty loopholes to provide safe havens for cybercriminals. Countries that refuse to extradite or lack dual criminality clauses often stall international investigations, particularly in ransomware and state-sponsored disinformation cases [39].

Technical limitations also persist. Disparities in digital forensics capability, lack of encryption interoperability, and inconsistent legal thresholds for admissibility of digital evidence continue to challenge uniform enforcement, particularly in the Global South.

8.3. Lessons Learned and Future Treaty Design Recommendations

The evolution of international cybersecurity treaties must incorporate lessons from the past two decades. First, inclusive treaty negotiation is critical. Many African, Latin American, and Southeast Asian nations have expressed frustration with Eurocentric treaty designs that overlook their legal systems, infrastructure realities, or cultural norms. Future agreements must provide capacity-building incentives, not just compliance requirements [40].

Second, treaties must be tech-forward, anticipating future trends in quantum cryptography, AI-based attacks, and blockchain-driven infrastructures. Static legal definitions quickly become obsolete in fast-moving digital ecosystems. Provisions for periodic technical annex updates—as seen in the revised Budapest Convention—should become standard [41].

Third, treaty design should prioritize modular enforceability, allowing countries to opt into specific operational layers like data exchange, incident reporting, or attribution collaboration, without requiring full accession. This ensures wider participation while still promoting incremental trust-building.

Lastly, effective treaties must be enforceable. This means integrating sanction triggers, compliance assessments, and third-party mediation bodies for dispute resolution. Without such accountability mechanisms, treaties risk being symbolic rather than operational.

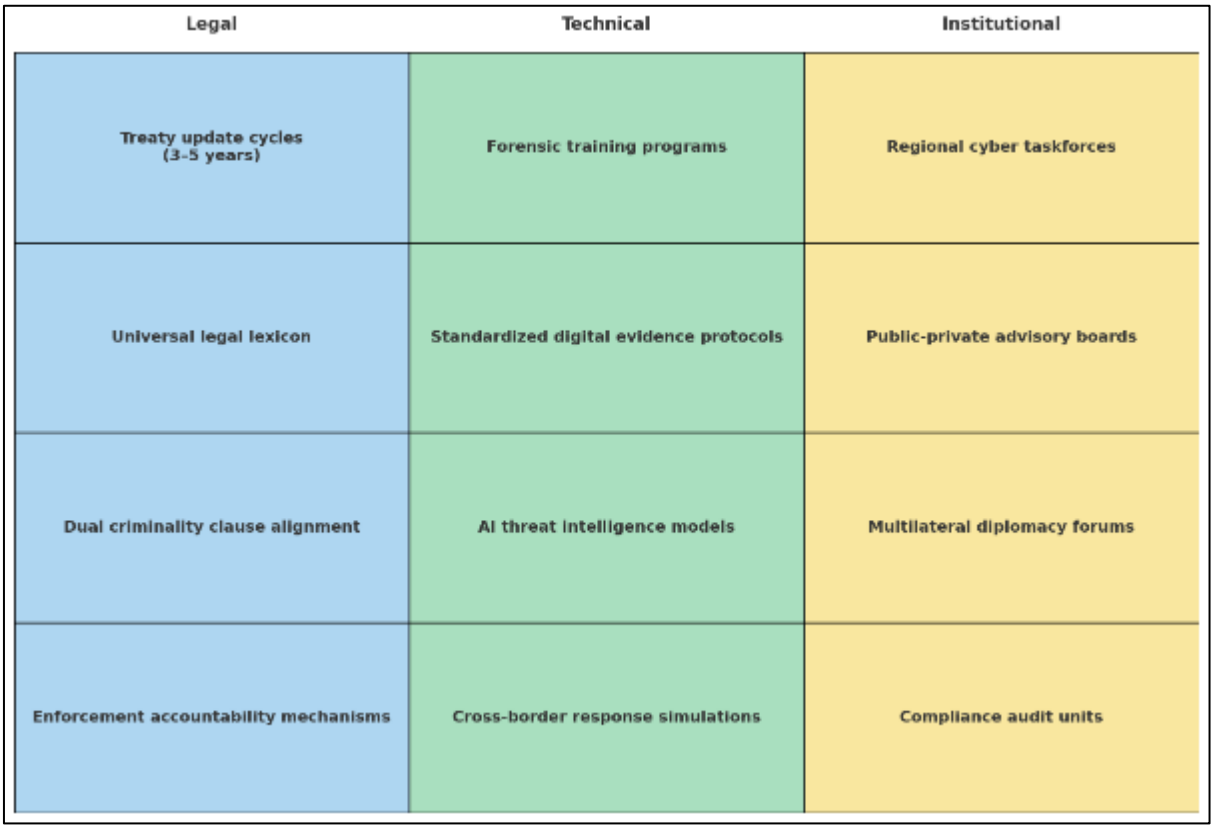

Figure 5 Policy Recommendation Matrix Across Legal, Technical, and Institutional Domains

9. Policy recommendations and conclusion

9.1. Policy Roadmap for Treaty Optimization

The effectiveness of international cybersecurity treaties depends not only on their legal framing but also on the practical pathways for implementation, enforcement, and adaptive relevance. A forward-looking policy roadmap must therefore prioritize three interdependent domains: legal harmonization, technical capacity building, and regional enforcement mechanisms.

First, treaty optimization begins with legal harmonization across jurisdictions. Current treaties often suffer from vague definitions, inconsistent enforcement provisions, and incompatibility with national laws. A standardized legal lexicon for terms such as “critical infrastructure,” “cyber sabotage,” and “digital evidence” must be universally adopted. This lexicon should be updated periodically through a standing committee of treaty signatories and legal experts. Aligning cybercrime statutes and extradition protocols across nations will reduce prosecution delays and eliminate dual criminality conflicts that allow cybercriminals to exploit legal loopholes.

Second, capacity building is essential for ensuring global equity in cybersecurity enforcement. Many lower- and middle-income countries struggle to meet treaty obligations due to inadequate cyber forensic capabilities, insufficient training, and a lack of secure data-sharing infrastructure. Treaties must include clauses mandating technical and financial assistance, with defined benchmarks for progress and reciprocal benefits. Building local cyber defense ecosystems will not only strengthen global security but also incentivize active participation in multilateral cyber governance.

Third, there is a need to develop regional enforcement hubs that complement global treaty bodies. These hubs—anchored within regional organizations like the African Union, ASEAN, or the Gulf Cooperation Council—can serve as decentralized centers for intelligence exchange, joint operations, and treaty monitoring. Regional proximity improves response time, cultural alignment, and shared risk assessment.

Figure 5 below presents a policy recommendation matrix categorizing key reforms across legal, technical, and institutional dimensions.

9.2. Final Reflections and Future Research Directions

As cyber threats grow in scale, frequency, and geopolitical complexity, international treaties must evolve from static legal instruments to dynamic governance ecosystems. Treaties must not only codify rules but also facilitate real-time threat response, data exchange, and evidence authentication in ways that are technologically secure and politically sustainable.

Looking forward, there is a clear need for multilateral cyber diplomacy that bridges ideological divides and fosters inclusive treaty drafting. This involves expanding participation beyond traditional cyber powers to include the Global South, indigenous communities, civil society, and the private sector. Only with such pluralism can treaties reflect the true diversity of cyber risks and interests.

Future treaty revisions should also embrace modular and scalable designs, allowing states to opt into layers of cooperation (e.g., attribution sharing, AI threat analysis, forensic toolkits) based on readiness and relevance. This model supports incremental trust-building and lowers the barrier for entry.

Additionally, academic and institutional research should focus on evaluating the effectiveness of treaty enforcement mechanisms, including the impact of cyber drills, compliance audits, and joint prosecutions. Longitudinal studies that track treaty compliance over time will provide evidence for refining treaty structures and dispute resolution clauses.

Ultimately, sustainable cybersecurity governance will require a blended architecture of treaties, regional coalitions, and automated enforcement mechanisms capable of responding to the volatile and borderless nature of digital threats. Only through such integration can the international community ensure that cyber treaties remain not only relevant but truly resilient.

References

[1] Hohmann M, Pirang A, Benner T. Advancing Cybersecurity Capacity Building. Global Public Policy Institute (GPPi). 2017 Mar.

[2] Brenner Susan W. Cybercrime: Criminal Threats from Cyberspace. Praeger; 2010.

[3] Schjolberg Stein. A Global Treaty on Cybercrime and Cybersecurity. Cyberspace Law and Policy Centre, UNSW; 2013. https://doi.org/10.2139/ssrn.2412164

[4] Mueller Milton. Networks and States: The Global Politics of Internet Governance. MIT Press; 2010.

[5] Kerttunen Mika. International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCDCOE; 2016.

[6] Creese S, Dutton WH, Esteve-Gonzalez P, Shillair R. Cybersecurity capacity-building: cross-national benefits and international divides. Journal of Cyber Policy. 2021 May 4;6(2):214-35.

[7] Deibert Ronald J, Palfrey John G, Rohozinski Rafal, Zittrain Jonathan L. Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. MIT Press; 2010.

[8] Tsagourias Nicholas, Buchan Russell. Cyber War and International Law. Cambridge University Press; 2015. https://doi.org/10.1017/CBO9781107281644

[9] Shackelford Scott J. Managing Cyber Attacks in International Law, Business, and Relations. Cambridge University Press; 2014.

[10] Dorgbefu EA. Driving equity in affordable housing with strategic communication and AI-based real estate investment intelligence. International Journal of Computer Applications Technology and Research. 2019;8(12):561–74. Available from: https://doi.org/10.7753/IJCATR0812.1012

[11] Seger Alexander. The Budapest Convention on Cybercrime: Benefits and Impact in Practice. Cybercrime Division, Council of Europe; 2020. https://doi.org/10.2861/709540

[12] Carr Madeline. US Power and the Internet in International Relations: The Irony of the Information Age. Palgrave Macmillan; 2016.

[13] Chibogwu Igwe-Nmaju, Christianah Gbaja, Chioma Onyinye Ikeh. Redesigning customer experience through AI: a communication-centered approach in telecoms and tech-driven industries. International Journal of Science and Research Archive. 2023 Dec;10(2). doi: https://doi.org/10.30574/ijsra.2023.10.2.1042

[14] Tikk Eneken, Kaska Kadri, Vihul Liis. International Cyber Incidents: Legal Considerations. NATO CCDCOE; 2010.

[15] Brown Ian, Korff Douwe. Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online. Global Network Initiative; 2012.

[16] Lin Herbert S. Offensive Cyber Operations and the Use of Force. J Natl Secur Law Policy. 2012;4(1):63-86.

[17] Finn Rachel L, Wright David. Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications. Comput Law Secur Rev. 2012;28(2):184-194. https://doi.org/10.1016/j.clsr.2012.01.005

[18] Rees Wyn, Aldrich Richard J. Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence? Int Aff. 2005;81(5):905–923. https://doi.org/10.1111/j.1468-2346.2005.00493.x

[19] Dorgbefu EA. Using business analytics to tailor real estate messaging for inclusive housing solutions and investment impact. Int J Eng Technol Res Manag. 2020;4(12):156. Available from: https://doi.org/10.5281/zenodo.15708955.

[20] ENISA. Threat Landscape for Critical Sectors. European Union Agency for Cybersecurity; 2022. https://doi.org/10.2824/143882

[21] Sanger David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown; 2018.

[22] Ayobami, A.T. et al., 2023. Algorithmic Integrity: A Predictive Framework for Combating Corruption in Public Procurement through AI and Data Analytics. Journal of Frontiers in Multidisciplinary Research, 4(2), pp.130–141. Available at: https://doi.org/10.54660/.JFMR.2023.4.2.130-141.

[23] NIS Cooperation Group. NIS Investments: Strengthening Capabilities Across the EU. European Commission; 2023.

[24] Betz David J, Stevens Tim. Cyberspace and the State: Toward a Strategy for Cyberpower. Routledge; 2011.

[25] Pawlak P, Barmpaliou PN. Politics of cybersecurity capacity building: conundrum and opportunity. Journal of Cyber Policy. 2017 Jan 2;2(1):123-44.

[26] ITU. Global Cybersecurity Index 2022. International Telecommunication Union; 2023. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[27] OECD. Enhancing the Role of SMEs in Global Value Chains. OECD Digital Economy Papers; 2020.

[28] Zegart Amy B. Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University Press; 2022. https://doi.org/10.2307/j.ctv2zcdm62

[29] Marczak Bill, Scott-Railton John, McKune Sarah, Abdul Razzak Bahr, Deibert Ronald J. The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender. The Citizen Lab; 2016.

[30] Lewis James A. Sovereignty and the Role of Government in Cyberspace. CSIS; 2017.

[31] Klimburg Alexander. The Darkening Web: The War for Cyberspace. Penguin Press; 2017.

[32] Chibogwu Igwe-Nmaju. AI and automation in organizational messaging: ethical challenges and human-machine interaction in corporate communication. International Journal of Engineering Technology Research & Management. 2021 Dec;5(12):256. Available from: doi: https://doi.org/10.5281/zenodo.15562214

[33] Ohlin Jens David. The Assault on International Law. Oxford University Press; 2015.

[34] Kello Lucas. The Virtual Weapon and International Order. Yale University Press; 2017.

[35] West Sarah Myers. Data Localization Laws and Their Impact on Privacy, Free Expression, and the Global Internet. UC Berkeley Law School; 2016.

[36] Dorgbefu EA. Translating complex housing data into clear messaging for real estate investors through modern business communication techniques. International Journal of Computer Applications Technology and Research. 2018;07(12):485–499. Available from: https://doi.org/10.7753/IJCATR0712.1010

[37] Chin Larry. China's Cybersecurity Law and Its Global Impact. Int Cyber Law Rev. 2020;1(2):44-58.

[38] DeNardis Laura. The Global War for Internet Governance. Yale University Press; 2014.

[39] Daskal Jennifer. The Un-Territoriality of Data. Yale Law J. 2015;125(2):326-398.

[40] Brantly Aaron F. The Decision to Attack: Military and Intelligence Cyber Decision-Making. University of Georgia Press; 2016.

[41] Goodwin CF, Nicholas JP. Developing a National strategy for CyberSecurity. Foundation for Security Growth and Innovation. 2013 Oct.