Cybercrime and the Need for Expansion of Cyber Law Towards International Conformity:

Focus on Information Policy and National Cybersecurity Reforms in the European Union

Author: Ricardo Baretzly, PhD in Law **TOTAL 53 Pages**

Abstract

This paper examines the evolving landscape of cybercrime and underscores the urgent need for expanding cyber law towards international conformity, with a particular focus on information policy and national cybersecurity reforms within the European Union (EU). The EU has made significant legislative advancements through the Cybersecurity Act, Cyber Resilience Act, NIS 2 Directive, and Cyber Solidarity Act, which collectively enhance cybersecurity governance, operational cooperation, and incident response capabilities. However, emerging threats—especially those enabled by artificial intelligence (AI)—such as AI-driven cyberterrorism, sophisticated disinformation campaigns, and autonomous cyber-attacks, expose critical gaps in current legal frameworks.

This study analyzes the intersection of information policy and cybersecurity, highlighting the importance of integrating data protection, transparency, and AI risk management into national and EU-wide legislation. It identifies challenges in legal harmonization, cross-border investigative powers, and international cooperation, emphasizing the necessity for a unified global approach to cyber law. The paper proposes comprehensive national reforms to harmonize laws, embed AI-specific certification and incident reporting, and strengthen institutional capacities such as ENISA and EU-CyCLONe. Furthermore, it advocates for the expansion of international cyber law through a global cybercrime convention inclusive of AI provisions, standardized cross-border incident response protocols, and mutual recognition of cybersecurity certifications.

By advancing these legal and policy reforms, the EU and the international community can build a resilient, secure, and trustworthy cyberspace that effectively counters cybercrime and AI-enabled terrorism while safeguarding fundamental rights and fostering digital innovation.

Ricardo Baretzky, PhD in Law, is a seasoned expert with over 25 years of experience in international cyber intelligence and information security across both public and private sectors. As President of CYBERPOL and the European Centre for Information Policy and Security (ECIPS), he advises global entities on cyber threats, insider risks, and compliance policies. Dr. Baretzky's expertise spans cyber intelligence architecture, ethical hacking, and international investigations, making him a recognized authority on international cybersecurity and terrorism

⁂

Executive Summary

1. Introduction

1.1 Background and Context

The digital revolution has transformed how societies function, economies operate, and governments govern. From e-commerce and digital banking to smart cities and autonomous vehicles, the integration of information and communication technologies (ICT) into everyday life has created unprecedented opportunities for innovation and growth. However, this digital transformation has also introduced complex vulnerabilities and risks, notably cybercrime.

Cybercrime encompasses a broad spectrum of illegal activities conducted through or targeting ICT systems. These include, but are not limited to, hacking, identity theft, ransomware attacks, online fraud, and cyberterrorism. The transnational nature of cyberspace means that cybercriminals can operate across borders with relative impunity, exploiting legal inconsistencies and jurisdictional gaps.

The European Union (EU), as a leading digital economy and political union, has recognized the critical importance of cybersecurity and has developed a comprehensive legal and policy framework to address cyber threats. These efforts include the Cybersecurity Act (2019), the Cyber Resilience Act (2024), the NIS 2 Directive (2022/2555), and the Cyber Solidarity Act (2025). These legal instruments aim to harmonize cybersecurity standards, enhance operational cooperation, and build resilience across member states.

1.2 The Challenge of AI-Enabled Cybercrime and Terrorism

Artificial intelligence (AI) technologies are increasingly integrated into ICT systems, offering enhanced capabilities for automation, decision-making, and data analysis. However, AI also presents new risks when weaponized by malicious actors. AI-enabled cyberterrorism refers to the use of AI to conduct or amplify cyber-attacks, disrupt critical infrastructure, manipulate information systems, or deploy autonomous weapons systems to cause harm or fear.

The rapid evolution of AI technologies outpaces existing legal frameworks, which often lack explicit provisions addressing AI-specific risks. This regulatory gap undermines the EU's ability to prevent, detect, and respond to AI-driven cyber threats effectively.

1.3 Objectives and Scope of the Paper

This paper aims to:

- Analyze the current EU legal framework on cybercrime and cybersecurity, focusing on recent legislative developments.
- Examine the intersection of information policy and cybersecurity within the EU context.
- Identify gaps and challenges in achieving international conformity in cyber law.
- Explore the emerging threat of AI terrorism and its implications for cyber law.
- Propose national cybersecurity reforms and international legal expansions to address AI-enabled cyber threats.
- Provide actionable recommendations for policymakers, regulators, and stakeholders.

⁂

2. The Landscape of Cybercrime: Challenges and Trends

2.1 Defining Cybercrime

Cybercrime is broadly defined as criminal activities involving computers or networks, either as targets or tools. The Council of Europe's Budapest Convention on Cybercrime (2001) provides a widely accepted legal definition, encompassing offenses such as illegal access, data interference, system interference, misuse of devices, computer-related fraud, and content-related offenses.

The EU's legal framework builds on this definition but also addresses the evolving nature of cyber threats, including attacks on critical infrastructure, supply chain compromises, and AI-enabled crimes.

2.2 Economic and Social Impact

Cybercrime imposes substantial economic costs globally, projected to reach $10.5 trillion annually by 2025. These costs include direct financial losses, remediation expenses, reputational damage, and broader societal impacts such as loss of trust in digital services.

Socially, cybercrime threatens privacy, freedom of expression, and democratic processes. Disinformation campaigns and AI-generated deepfakes undermine public discourse and electoral integrity.

2.3 Key Trends in Cybercrime

- **Ransomware and Extortion:** Increasingly sophisticated ransomware attacks target healthcare, energy, and public services, causing operational paralysis and financial loss. Attackers often demand payment in cryptocurrencies, complicating traceability.
- **Supply Chain Attacks:** Cybercriminals exploit vulnerabilities in suppliers' software or hardware to infiltrate multiple organizations. The SolarWinds attack exemplifies the scale and impact of such operations.
- **AI-Driven Attacks:** AI is used to automate phishing, generate convincing deepfakes, and autonomously propagate malware, increasing attack speed and scale.

- **Cross-Border Crime:** Cybercriminals exploit jurisdictional differences, operating from countries with weak enforcement or legal protections.

2.4 Challenges in Combating Cybercrime

- **Jurisdictional Complexity:** Cybercrime often involves multiple countries, complicating investigation and prosecution.
- **Legal Fragmentation:** Variations in national laws create enforcement gaps and safe havens.
- **Attribution Difficulties:** Identifying perpetrators is challenging due to anonymization techniques and the use of proxy servers.
- **Rapid Technological Change:** Legal frameworks struggle to keep pace with evolving technologies and threat vectors.

⁂

3. Current European Legal Framework on Cybercrime

3.1 The EU Cybersecurity Act (2019) and the 2025 Amendment

The Cybersecurity Act (Regulation (EU) 2019/881) established ENISA's permanent mandate and introduced the European Cybersecurity Certification Framework (ECCF). ENISA's enhanced role includes coordinating operational cooperation, supporting member states in crisis management, and facilitating information sharing.

The ECCF creates a voluntary certification scheme for ICT products and services to ensure a common cybersecurity baseline across the EU. The 2025 amendment extends certification to managed security services, such as incident response and penetration testing, addressing the need for trustworthy cybersecurity service providers.

The European Commission's 2025 public consultation on revising the Act aims to further strengthen ENISA's mandate, streamline certification processes, and adapt the framework to emerging threats, including AI.

3.2 The Cyber Resilience Act (2024)

The Cyber Resilience Act (Regulation (EU) 2024/XXX) sets mandatory cybersecurity requirements for products with digital elements throughout their lifecycle. It requires manufacturers to implement security by design and default, provide timely security updates, and report incidents.

This Act aims to reduce vulnerabilities in digital products, thereby decreasing the attack surface for cybercriminals. It complements the Cybersecurity Act by focusing on product-level security, particularly relevant for IoT devices and AI-enabled systems.

3.3 The NIS 2 Directive (Directive (EU) 2022/2555)

The NIS 2 Directive updates and expands the original NIS Directive, broadening the scope to include more sectors and introducing a size-cap rule to determine applicability. It mandates entities to implement risk management measures and report incidents promptly.

NIS 2 enhances cooperation among member states and establishes stricter supervisory and enforcement regimes, including penalties for non-compliance. However, the Commission has noted delays in transposition, initiating infringement procedures against several member states.

3.4 The Cyber Solidarity Act (2025)

The Cyber Solidarity Act (Regulation (EU) 2025/38) establishes the European Cybersecurity Alert System, comprising national and cross-border cyber hubs equipped with AI and data analytics capabilities. It creates an EU Cybersecurity Reserve of private-sector incident response teams to assist during significant cyber incidents.

The Act introduces mutual technical assistance and an incident review mechanism to evaluate responses and improve preparedness. It represents a shift towards collective responsibility and solidarity in cybersecurity within the EU.

3.5 Sanctions and Enforcement

The Council of the European Union extended the EU's cyber-attack sanctions regime until May 2028, enabling targeted measures against individuals and entities responsible for cyber-attacks. Sanctions include asset freezes, travel bans, and restrictions on access to EU financial markets.

Enforcement remains a challenge due to jurisdictional issues and the anonymity of cybercriminals. Enhanced cooperation between law enforcement agencies and harmonization of legal tools are essential to improve effectiveness.

⁂

4. Information Policy and Cybersecurity in the European Union

4.1 Introduction

Information policy and cybersecurity are deeply intertwined domains, each influencing the other in the digital ecosystem. Information policy governs the collection, processing, sharing, and protection of data, while cybersecurity focuses on protecting information systems from unauthorized access, damage, or disruption. In the European Union (EU), the integration of these domains is critical to safeguarding digital infrastructure, protecting citizens' rights, and fostering trust in the digital economy.

This chapter explores the EU's approach to information policy within the cybersecurity context, examining the regulatory frameworks, institutional roles, and sector-specific governance mechanisms. It also highlights challenges and opportunities in aligning information policy with cybersecurity objectives, especially in the face of emerging threats such as AI-enabled cybercrime.

4.2 The EU's Regulatory Framework on Information Policy and Cybersecurity

4.2.1 The General Data Protection Regulation (GDPR)

The GDPR (Regulation (EU) 2016/679) is the cornerstone of the EU's data protection regime. It establishes comprehensive rules for the processing of personal data, emphasizing transparency, accountability, and individuals' rights. GDPR's principles—lawfulness, fairness, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality—directly impact cybersecurity practices.

Under GDPR, data controllers and processors are required to implement appropriate technical and organizational measures to ensure data security, including encryption, pseudonymization, and regular testing of security measures. The regulation mandates timely notification of personal data breaches to supervisory authorities and affected individuals, reinforcing the nexus between data protection and cybersecurity.

GDPR's extraterritorial scope extends its influence globally, compelling organizations worldwide that process EU citizens' data to comply with its provisions. This has elevated data protection as a fundamental component of information policy aligned with cybersecurity goals.

4.2.2 The ePrivacy Regulation (Pending)

The ePrivacy Regulation, intended to complement GDPR, focuses on privacy and confidentiality in electronic communications. It addresses issues such as cookies, direct marketing, metadata processing, and confidentiality of communications.

Although still under negotiation, the ePrivacy Regulation is expected to strengthen privacy protections in electronic communications, including stricter consent requirements and enhanced safeguards against unauthorized interception or monitoring. Its alignment with GDPR and cybersecurity frameworks will be essential to ensure coherent information policy.

4.2.3 The Data Governance Act and Data Act

The Data Governance Act (DGA) and the upcoming Data Act represent the EU's efforts to foster data sharing and reuse while ensuring data protection and cybersecurity.

- **Data Governance Act (Regulation (EU) 2022/868):** Establishes mechanisms for data altruism, data intermediaries, and reuse of public sector data. It aims to create a trusted environment for data sharing, balancing openness with security and privacy.
- **Data Act (proposed):** Seeks to regulate access to and use of data generated by connected devices and services, promoting fairness and innovation while safeguarding cybersecurity and data protection.

These acts highlight the EU's commitment to a data-driven economy underpinned by robust information governance and cybersecurity safeguards.

4.2.4 The Digital Operational Resilience Act (DORA)

DORA (Regulation (EU) 2022/2554) targets the financial sector, mandating stringent cybersecurity and operational resilience requirements for financial entities. It requires risk

management frameworks, incident reporting, ICT third-party risk management, and regular testing.

DORA exemplifies sector-specific information policy integration with cybersecurity, recognizing the critical role of data integrity and system availability in financial stability.

4.3 Institutional Roles in Information Policy and Cybersecurity

4.3.1 European Union Agency for Cybersecurity (ENISA)

ENISA plays a pivotal role in supporting member states and EU institutions in cybersecurity matters. It provides expertise, facilitates information sharing, and supports the development of cybersecurity certification schemes.

ENISA's expanded mandate under the Cybersecurity Act includes coordinating cybersecurity exercises, threat intelligence sharing, and assisting in incident response, thereby bridging information policy and cybersecurity operational needs.

4.3.2 European Data Protection Board (EDPB)

The EDPB oversees the consistent application of GDPR across the EU. It issues guidelines, opinions, and recommendations on data protection matters, including those related to cybersecurity measures necessary to protect personal data.

The EDPB collaborates with ENISA and other bodies to ensure that data protection and cybersecurity policies are harmonized and mutually reinforcing.

4.3.3 National Data Protection Authorities (DPAs)

Each member state has a DPA responsible for enforcing GDPR and related data protection laws. DPAs play a critical role in monitoring compliance, investigating breaches, and imposing sanctions.

DPAs also engage with cybersecurity authorities to address incidents involving personal data breaches, ensuring coordinated responses.

4.4 Sector-Specific Information Policy and Cybersecurity Governance

4.4.1 Financial Sector

The financial sector is subject to robust cybersecurity and information governance regulations, including DORA and the revised Payment Services Directive (PSD2). These frameworks require strong authentication, secure data processing, and incident reporting to protect financial data and infrastructure.

4.4.2 Healthcare Sector

Healthcare data is highly sensitive, necessitating stringent information policy and cybersecurity measures. The EU's eHealth Network and the European Health Data Space initiative aim to facilitate secure data sharing while protecting patient privacy.

4.4.3 Critical Infrastructure and Energy

The NIS 2 Directive extends cybersecurity obligations to critical infrastructure sectors, including energy, transport, and water. These sectors must implement risk management and incident notification measures, integrating information policy principles to protect data integrity and availability.

4.5 Challenges in Aligning Information Policy and Cybersecurity

4.5.1 Balancing Privacy and Security

Information policy must balance individual privacy rights with the need for effective cybersecurity. Overly restrictive data protection can hinder threat detection and incident response, while lax policies risk privacy violations.

4.5.2 Data Sharing and Threat Intelligence

Effective cybersecurity relies on timely sharing of threat intelligence among public and private actors. However, concerns over data protection, liability, and competitive advantage can impede information sharing.

4.5.3 AI and Automated Decision-Making

AI systems introduce complexities in information policy, including transparency, accountability, and bias. Ensuring AI-driven cybersecurity tools comply with data protection and ethical standards is a growing challenge.

4.6 Opportunities and Policy Recommendations

- **Integrated Regulatory Approach:** Harmonize data protection and cybersecurity regulations to provide clear, consistent obligations for organizations.
- **Enhance Public-Private Partnerships:** Foster trust and collaboration to facilitate secure information sharing and joint threat response.
- **Promote Transparency and Accountability:** Require disclosure of AI system functionalities and cybersecurity practices to regulators and users.
- **Invest in Capacity Building:** Develop expertise in managing the intersection of information policy and cybersecurity, including AI governance.

4.7 Conclusion

The EU's information policy framework, anchored by GDPR and complemented by sector-specific regulations and emerging data governance laws, forms a critical pillar of cybersecurity. Aligning information policy with cybersecurity objectives is essential to protect data, uphold privacy, and ensure resilient digital infrastructure. Addressing challenges related to privacy-security balance, data sharing, and AI governance will strengthen the EU's capacity to confront evolving cyber threats.

⁂

5. The Need for International Conformity in Cyber Law

5.1 Introduction

Cybercrime is inherently transnational, operating without regard for national borders and exploiting inconsistencies in legal frameworks worldwide. The effectiveness of domestic cyber laws is limited by the ease with which cybercriminals can operate from jurisdictions with weak enforcement or differing legal standards. International conformity in cyber law is, therefore, essential to ensure that cybercriminals cannot evade justice by moving their operations across borders.

This chapter examines the challenges and necessities of achieving international conformity in cyber law. It explores the harmonization of national legislations, the enhancement of investigative powers, and the strengthening of international cooperation mechanisms. It also addresses the implications of emerging technologies, such as AI, for international cyber law frameworks.

5.2 The Imperative of Legal Harmonization

5.2.1 Challenges in Harmonizing Cyber Laws

National cyber laws vary significantly in terms of definitions of cyber offenses, penalties, procedural rules, and data protection standards. These variations create legal loopholes that cybercriminals exploit. Harmonization efforts face challenges such as:

- **Sovereignty Concerns:** Nations are often reluctant to cede authority over their legal systems to international bodies[28].
- **Differing Legal Traditions:** Common law and civil law systems approach legal issues differently, complicating harmonization[29].
- **Cultural and Political Values:** Different societies may prioritize different values, such as privacy versus security, leading to divergent legal choices.
- **Economic Interests:** Nations may hesitate to adopt regulations that could disadvantage their domestic industries.

5.2.2 The Role of the Budapest Convention

The Council of Europe's Convention on Cybercrime (Budapest Convention, 2001) is the primary international treaty addressing cybercrime. It provides a framework for criminalizing cyber offenses, enhancing investigative powers, and facilitating international cooperation.

The Budapest Convention has been ratified by over 60 countries, including most EU member states. However, some key nations, such as Russia and China, have not joined the convention, limiting its global reach[28].

5.2.3 EU Efforts to Harmonize Cyber Laws

The EU has made significant strides in harmonizing cyber laws through directives and regulations. The NIS 2 Directive[28], the GDPR, the Cyber Resilience Act[30], and the Cyber Solidarity Act[30] all contribute to a more uniform legal landscape within the EU. However, full harmonization remains a challenge due to:

- **Implementation Gaps:** Member states may transpose EU directives differently, leading to variations in national laws.
- **Scope Limitations:** EU laws may not cover all aspects of cybercrime, leaving gaps in protection.
- **Enforcement Disparities:** Differences in national enforcement practices can undermine the effectiveness of harmonized laws.

5.2.4 Recommendations for Enhancing Legal Harmonization

- **Expand Adoption of the Budapest Convention:** Encourage more countries to ratify and implement the Budapest Convention.
- **Strengthen EU Directives:** Ensure full and consistent transposition of EU directives into national laws.
- **Develop Model Laws:** Create model cybercrime laws that nations can adopt or adapt to their legal systems.

- **Promote Interoperability:** Foster legal frameworks that are compatible and interoperable across jurisdictions.

5.3 Enhancing Investigative Powers

5.3.1 Challenges in Cross-Border Investigations

Cybercrime investigations often require access to data stored in multiple countries, posing significant legal and practical challenges. These challenges include:

- **Data Sovereignty:** Nations may restrict access to data stored within their borders, even for legitimate law enforcement purposes.
- **Mutual Legal Assistance Treaty (MLAT) Limitations:** MLAT processes can be slow and cumbersome, hindering timely investigations.
- **Conflicting Legal Standards:** Differences in data protection laws and procedural rules can complicate cross-border access to evidence.
- **Encryption and Anonymization:** Cybercriminals use encryption and anonymization tools to conceal their identities and activities.

5.3.2 The Role of International Cooperation

International cooperation is essential to overcome these investigative challenges. Key mechanisms include:

- **Joint Investigation Teams (JITs):** JITs bring together law enforcement officers from multiple countries to conduct joint investigations.
- **Information Sharing Platforms:** Platforms such as Interpol's Cybercrime Programme facilitate the exchange of threat intelligence and investigative data.
- **Cross-Border Data Requests:** Streamlined processes for requesting and obtaining electronic evidence across borders are needed.

5.3.3 EU Initiatives to Enhance Investigative Powers

The EU has implemented several initiatives to improve cross-border investigations, including:

- **The European Investigation Order (EIO):** Simplifies the process of obtaining evidence from other EU member states.
- **The e-Evidence Regulation:** Establishes direct channels for law enforcement agencies to request electronic evidence from service providers located in other EU countries.
- **The Europol Cybercrime Centre (EC3):** Provides operational support and expertise to member states in combating cybercrime.

5.3.4 Recommendations for Enhancing Investigative Powers

- **Streamline MLAT Processes:** Reduce bureaucratic hurdles and processing times for MLAT requests.
- **Expand Use of JITs:** Encourage greater use of JITs for complex cybercrime investigations.
- **Enhance Data Sharing Platforms:** Improve the functionality and security of international data sharing platforms.
- **Address Encryption Challenges:** Develop legal and technical solutions to address the challenges posed by encryption, balancing security with privacy.

5.4 Strengthening International Cooperation

5.4.1 The Need for Coordinated Responses

Cybercrime often requires coordinated responses from multiple countries. Effective cooperation mechanisms are needed to:

- **Share Threat Intelligence:** Timely sharing of information about emerging threats and vulnerabilities is essential for prevention and mitigation.
- **Coordinate Incident Response:** Joint responses to large-scale cyber incidents can minimize damage and restore services quickly.

- **Conduct Joint Operations:** Coordinated law enforcement operations can disrupt cybercriminal networks and bring perpetrators to justice.

5.4.2 Challenges in International Cooperation

International cooperation faces challenges such as:

- **Trust Deficits:** Nations may be reluctant to share sensitive information with countries they do not trust.
- **Resource Constraints:** Limited resources and expertise can hinder effective cooperation.
- **Political Obstacles:** Political tensions and conflicting interests can impede joint efforts.
- **Lack of Common Standards:** Differing standards for data protection, evidence admissibility, and law enforcement practices can complicate cooperation.

5.4.3 EU Cooperation Mechanisms

The EU has established several mechanisms to enhance international cooperation in cybersecurity, including:

- **The Cybersecurity Act's Cooperation Group:** Facilitates strategic discussions and information sharing among member states.
- **The EU Cyber Crisis Management Framework:** Provides a framework for coordinating responses to large-scale cyber incidents.
- **The EU External Action Service (EEAS):** Engages with third countries and international organizations to promote cybersecurity cooperation.

5.4.4 Recommendations for Strengthening Cooperation

- **Build Trust:** Foster relationships based on trust and mutual respect among nations.
- **Provide Resources:** Allocate sufficient resources to support international cooperation efforts.

- **Address Political Obstacles:** Engage in diplomatic efforts to overcome political barriers to cooperation.
- **Develop Common Standards:** Promote the adoption of common standards for data protection, evidence admissibility, and law enforcement practices.

5.5 The Impact of Emerging Technologies

5.5.1 AI and International Cyber Law

AI presents both opportunities and challenges for international cyber law. AI can enhance threat detection and incident response, but it can also be used to create more sophisticated cyber-attacks. Key considerations include:

- **AI Governance:** International standards are needed to govern the development and deployment of AI systems, ensuring they are not used for malicious purposes.
- **Attribution Challenges:** AI-enabled attacks can be difficult to attribute, complicating legal responses.
- **Autonomous Weapons:** The development of autonomous weapons systems raises ethical and legal concerns that must be addressed internationally.

5.5.2 The Role of International Organizations

International organizations such as the United Nations (UN) and the International Telecommunication Union (ITU) can play a critical role in shaping international cyber law and addressing the challenges posed by emerging technologies. Key initiatives include:

- **UN Cybercrime Treaty:** Negotiations are underway on a new UN treaty to combat cybercrime, aiming to address gaps in the existing legal framework.
- **ITU Cybersecurity Agenda:** Promotes international cooperation on cybersecurity issues, including capacity building and technical standards.

5.5.3 Recommendations for Addressing Emerging Technologies

- **Develop AI Governance Frameworks:** Create international standards for the ethical and responsible development and deployment of AI.
- **Enhance Attribution Capabilities:** Invest in research and development to improve the ability to attribute AI-enabled attacks.
- **Address Autonomous Weapons Concerns:** Establish international norms and legal frameworks to govern the development and use of autonomous weapons.

5.6 Conclusion

International conformity in cyber law is essential to address the transnational nature of cybercrime. Harmonizing national legislations, enhancing investigative powers, strengthening international cooperation, and addressing emerging technologies are critical steps toward creating a more secure and resilient cyberspace. The EU, in collaboration with international partners, must continue to lead efforts to build a global cyber legal framework that protects citizens, businesses, and critical infrastructure from cyber threats.

6. Emerging Threats: AI Terrorism and Cybersecurity

6.1 Introduction

Artificial Intelligence (AI) is transforming multiple domains, including cybersecurity and counterterrorism. While AI offers powerful tools to detect, prevent, and respond to cyber threats, it also introduces new vulnerabilities and risks. Terrorist groups and violent extremists are increasingly exploiting AI technologies to enhance their operational capabilities, spread propaganda, recruit members, and launch sophisticated cyber-attacks. This dual-use nature of AI presents significant challenges for legal and policy frameworks tasked with maintaining security while respecting fundamental rights.

This chapter explores the phenomenon of AI-enabled terrorism, examines the legal and policy gaps in addressing this emerging threat, and proposes targeted reforms to enhance the European Union's and the international community's capacity to combat AI terrorism effectively.

6.2 Defining AI Terrorism

AI terrorism refers to the malicious use of AI technologies by terrorist actors to facilitate or conduct terrorist activities. These activities may include:

- Automated dissemination of terrorist propaganda and recruitment content online.
- AI-driven cyber-attacks targeting critical infrastructure, financial systems, or government networks.
- Use of AI-powered deepfakes and disinformation campaigns to destabilize societies.
- Deployment of autonomous or semi-autonomous weapon systems.
- Exploitation of AI for encryption, anonymization, and evasion of law enforcement.

The United Nations Interregional Crime and Justice Research Institute (UNICRI) highlights the increasing presence of AI in terrorist tactics, emphasizing the need for law enforcement and counterterrorism agencies to adapt accordingly[32][33].

The European Commission's proposed AI Act defines AI systems broadly and includes provisions for high-risk applications, including those that may be used in the context of terrorism[34]. The OSCE Parliamentary Assembly's 2024 resolution explicitly calls for criminalizing the development, distribution, or use of AI for terrorist purposes and urges states to establish oversight mechanisms to mitigate AI misuse[35].

6.3 AI in Terrorist Content Dissemination and Online Radicalization

Terrorist groups exploit AI algorithms to amplify their propaganda on social media and online platforms. AI-driven content recommendation systems can inadvertently promote extremist content by optimizing for engagement, leading to radicalization pathways.

Efforts to automatically detect and remove terrorist content are increasingly reliant on AI. For example, the UK Home Office developed AI tools capable of detecting and rejecting a high percentage of Islamic State propaganda during upload[36]. However, challenges remain in defining terrorist content clearly, ensuring due process, and preventing over-removal or censorship[36][37].

Tech Against Terrorism advocates for legal clarity and a multi-layered adjudication system where designation of terrorist groups is conducted by accountable public authorities, enabling tech companies to act within a clear legal framework[37]. This approach helps balance counterterrorism effectiveness with rule-of-law principles.

6.4 AI-Enabled Cyber-Attacks and Autonomous Threats

AI enhances the capabilities of cyber attackers by automating reconnaissance, vulnerability scanning, and exploitation. Autonomous malware can adapt and propagate faster than traditional threats. AI can also be used to craft highly convincing phishing attacks and deepfake videos, complicating attribution and response[38].

The Parliamentary Assembly of the Mediterranean's 2024 report warns of AI's malicious use by terrorist and criminal groups, emphasizing the need for legislative and governance frameworks to keep pace with technological advances[38].

6.5 Legal and Policy Gaps in Addressing AI Terrorism

Current EU cyber laws, including the Cybersecurity Act and the Cyber Resilience Act, do not explicitly address AI-specific threats. The lack of AI-specific regulatory provisions creates gaps in:

- Accountability for AI misuse in terrorism.
- Mandatory AI risk assessments and certification for high-risk AI systems.
- Incident reporting obligations for AI-related cyberterrorism.
- Oversight and transparency mechanisms for AI development and deployment.

Internationally, the UN is actively supporting member states in countering AI misuse by terrorists but faces challenges in harmonizing approaches and ensuring human rights compliance[33][39].

6.6 Proposals for Enhancing Legal Frameworks to Combat AI Terrorism

6.6.1 Criminalization and Legal Clarity

- Enact legislation criminalizing the development, distribution, and use of AI for terrorist purposes, including online propaganda, recruitment, financing, and coordination[35].
- Establish clear definitions of AI-enabled terrorist content aligned with offline laws to ensure consistency and enforceability[37].

6.6.2 AI Risk Management and Certification

- Extend the European Cybersecurity Certification Framework to include AI systems with potential misuse in terrorism, requiring security by design, continuous monitoring, and compliance audits.
- Mandate AI-specific incident reporting to ENISA and national authorities.

6.6.3 Oversight and Accountability

- Create independent regulatory bodies to oversee AI development and deployment, focusing on high-risk applications related to security and terrorism[35].

- Promote transparency in AI algorithms used by online platforms to detect and moderate terrorist content.

6.6.4 Public-Private Partnerships and Capacity Building

- Foster collaboration among governments, tech companies, academia, and civil society to develop AI tools for counterterrorism while respecting human rights[35][36].
- Invest in training law enforcement and counterterrorism personnel on AI capabilities and risks[32][39].

6.6.5 International Cooperation

- Support global initiatives to harmonize AI governance standards and counterterrorism laws.
- Encourage information sharing and joint operations targeting AI-enabled terrorist threats.

6.7 Case Studies

6.7.1 AI-Driven Propaganda Removal in the UK

The UK Home Office's AI tool detects and rejects terrorist propaganda with high accuracy during upload, demonstrating the potential of AI in content moderation while highlighting challenges in rule-of-law compliance and transparency[36].

6.7.2 Deepfake Disinformation Campaigns

Terrorist groups have used AI-generated deepfake videos to spread disinformation and incite violence, complicating efforts to counteract false narratives and protect public order[38].

6.8 Conclusion

AI terrorism represents a complex, evolving threat that requires a multifaceted legal and policy response. The EU's existing cybersecurity framework provides a foundation but must be expanded to address AI-specific risks explicitly. Legal clarity, robust AI governance, enhanced oversight, and international cooperation are vital to countering AI-enabled terrorism effectively while safeguarding fundamental rights.

References

- [32] UNICRI, "Countering Terrorism Online with Artificial Intelligence," 2024.
- [34] European Commission Proposal for AI Regulation, 2021.
- [33] UNICRI, "The Malicious Use of Artificial Intelligence for Terrorist Purposes," 2024.
- [35] OSCE PA Resolution on Artificial Intelligence and the Fight Against Terrorism, 2024.
- [36] Cambridge Core, "Regulating Terrorist Content on Social Media: Automation and the Rule of Law," 2019.
- [37] Tech Against Terrorism, "The Need for Legal Clarity to Moderate Terrorist Content Online," 2023.
- [39] UN Office of Counter-Terrorism, "Law Enforcement Capabilities Framework for New Technologies," 2024.
- [38] Parliamentary Assembly of the Mediterranean, "The Malicious Use of AI and Emerging Technologies by Terrorist and Criminal Groups," 2024.

⁂

7. Proposals for National Cybersecurity Reforms in the European Union

7.1 Introduction

The European Union's cybersecurity landscape is evolving rapidly in response to emerging threats, technological advances, and the increasing integration of AI in digital systems. While the EU has made significant legislative progress with the Cybersecurity Act, Cyber Resilience Act, NIS 2 Directive, and the Cyber Solidarity Act, national cybersecurity reforms remain essential to fully realize these frameworks' potential and address specific challenges such as AI-enabled terrorism.

This chapter proposes targeted national reforms aimed at harmonizing legal frameworks, strengthening information policy integration, embedding AI risk management, enhancing institutional capacities, and fostering public-private cooperation. These reforms will help the EU meet its strategic goal of a resilient, secure, and trustworthy digital environment.

7.2 Enhancing Legal Harmonization and Enforcement

7.2.1 Uniform Implementation of EU Cybersecurity Legislation

Despite EU-wide directives, member states vary in the transposition and enforcement of cybersecurity laws, leading to fragmentation and enforcement gaps. National reforms should prioritize:

- **Full Transposition of NIS 2 Directive:** Member states must expedite the incorporation of NIS 2 provisions into national law, ensuring consistent risk management, incident reporting, and supervisory mechanisms.
- **Alignment with the Cybersecurity Act and Cyber Resilience Act:** National legislation should reflect the certification requirements and product security standards established at the EU level.
- **Sanctions and Compliance:** Establish clear, proportionate penalties for non-compliance with cybersecurity obligations, aligned with EU sanctions regimes.

7.2.2 Criminalization of AI-Enabled Cyberterrorism

National laws should explicitly criminalize AI-enabled cyberterrorism acts, including:

- Use of AI for terrorist propaganda dissemination, recruitment, and financing.
- AI-driven cyber-attacks targeting critical infrastructure.
- Deployment of autonomous or semi-autonomous weapon systems.

This aligns with the EU's AI Act provisions and international counterterrorism frameworks, ensuring clarity and enforceability.

7.3 Strengthening Information Policy and Data Governance

7.3.1 Integrating Cybersecurity into Data Protection Frameworks

National reforms should mandate the integration of cybersecurity risk assessments within data protection impact assessments (DPIAs), ensuring that data controllers and processors implement robust security measures aligned with GDPR.

7.3.2 Promoting Transparency and Accountability in AI Systems

- Require disclosure of AI system functionalities, risk profiles, and decision-making processes to regulators and affected individuals.
- Establish national registries of high-risk AI systems deployed within critical sectors.

7.3.3 Enhancing Data Sharing for Cybersecurity

- Develop secure, privacy-compliant platforms for sharing cyber threat intelligence among public authorities, private sector entities, and academia.
- Clarify legal bases for data sharing to overcome privacy and liability concerns.

7.4 Integrating AI Risk Management in Cybersecurity Law

7.4.1 Extending Certification to AI Systems

Following the EU Cybersecurity Act and AI Act, national laws should require:

- Mandatory cybersecurity certification for AI systems classified as high-risk, including those used in critical infrastructure and law enforcement.
- Continuous monitoring and periodic reassessment of certified AI systems.

7.4.2 Mandatory AI Incident Reporting

- Establish obligations for providers and users of AI systems to report cybersecurity incidents involving AI to national authorities and ENISA.
- Develop standardized reporting formats and timelines.

7.4.3 Oversight Mechanisms

- Create or empower independent national bodies to oversee AI risk management, certification compliance, and ethical deployment.
- Facilitate coordination with data protection authorities and cybersecurity agencies.

7.5 Expanding the Role of ENISA and EU-CyCLONe

7.5.1 Enhancing ENISA's National Support Role

- Allocate increased resources to ENISA to provide technical assistance, threat intelligence, and capacity building tailored to national needs.
- Promote ENISA-led training programs on AI cybersecurity risks and mitigation.

7.5.2 Empowering EU-CyCLONe for Cross-Border AI Threat Response

- Authorize EU-CyCLONe to coordinate rapid responses to AI-enabled cyber incidents affecting multiple member states.
- Develop protocols for information sharing, joint investigations, and resource mobilization.

7.6 Public-Private Partnerships and Capacity Building

7.6.1 Fostering Collaboration

- Encourage partnerships between governments, private sector, and academia to research AI threat detection and develop innovative cybersecurity solutions.
- Establish national cyber threat intelligence sharing platforms with participation from critical infrastructure operators.

7.6.2 Workforce Development

- Invest in specialized training programs for cybersecurity professionals focusing on AI technologies, forensic analysis, and counterterrorism.
- Promote AI literacy and awareness campaigns for all stakeholders involved in AI provision, use, and deployment, in line with the EU AI Act requirements effective from February 2025.

7.7 Leveraging the EU AI Act in National Reforms

The EU AI Act, which entered into force on 1 August 2024 and became partially applicable on 2 February 2025, prohibits certain high-risk AI practices and mandates AI literacy and risk management. National reforms should:

- Enforce the ban on prohibited AI systems, including those manipulating behavior subliminally or exploiting vulnerabilities.
- Implement the Act's provisions on real-time biometric identification systems used for counterterrorism, ensuring compliance with fundamental rights safeguards.
- Promote transparency and accountability in AI systems used by law enforcement and public authorities.
- Align national cybersecurity certification and oversight with AI Act requirements.

7.8 Conclusion

National cybersecurity reforms are critical to complement and operationalize the EU's ambitious legislative framework. By harmonizing laws, integrating information policy, embedding AI risk management, strengthening institutional roles, and fostering public-private cooperation, member states can build resilient national cybersecurity ecosystems. These reforms will enhance the EU's collective capacity to combat cybercrime and AI terrorism while safeguarding fundamental rights and democratic values.

References

- European Commission, AI Act, 2024–2026[40][41][42][43][44][45][46][47]
- Council of the European Union, Cybersecurity Act, Cyber Resilience Act, NIS 2 Directive
- UNICRI, Tech Against Terrorism Reports
- Parliamentary Assembly of the Mediterranean, 2024 Report on AI and Terrorism
- UK Home Office AI Propaganda Detection Initiatives

⁂

8. Recommendations for International Cyber Law Expansion

8.1 Introduction

The European Union's comprehensive cybersecurity legislative framework—including the Cybersecurity Act, Cyber Resilience Act, NIS 2 Directive, and Cyber Solidarity Act—has significantly strengthened the EU's cyber resilience and operational capabilities. However, cybercrime and AI-enabled terrorism are inherently transnational threats that cannot be effectively contained by regional or national laws alone. There is a pressing need to expand cyber law internationally to foster legal harmonization, enhance cross-border cooperation, and establish global standards that address emerging technologies and threats.

This chapter presents detailed recommendations for expanding international cyber law, focusing on harmonization, incident response, certification, and AI-specific governance, to complement and reinforce the EU's efforts within a global context.

8.2 Towards a Global Cybercrime Convention with AI Provisions

8.2.1 The Need for a Comprehensive International Treaty

While the Council of Europe's Budapest Convention on Cybercrime remains the foundational global treaty, its limited adoption and scope leave critical gaps. Notably, it does not explicitly address AI-enabled cyber threats or provide mechanisms tailored to emerging technologies.

A new or updated global cybercrime convention should:

- **Incorporate AI-Enabled Cybercrime:** Define offenses related to the malicious use of AI, including AI-driven cyber-attacks, autonomous weaponization, and AI-enabled disinformation campaigns.
- **Standardize Definitions and Penalties:** Harmonize legal definitions and penalties to reduce safe havens and ensure consistent enforcement.
- **Enhance Investigative Tools:** Provide clear frameworks for lawful access to data, cross-border evidence gathering, and attribution of AI-enabled attacks.

- **Safeguard Fundamental Rights:** Embed human rights protections, including privacy, due process, and freedom of expression, balancing security and rights.

8.2.2 Supporting UN and Multilateral Efforts

The United Nations is currently negotiating a new cybercrime treaty, aiming to address contemporary challenges. The EU should actively support these negotiations, advocating for inclusion of AI-specific provisions and robust cooperation mechanisms.

8.3 Cross-Border Incident Response and Information Sharing

8.3.1 Establishing Harmonized Protocols

Timely sharing of cyber threat intelligence and coordinated incident response are vital to mitigating damage from cyber-attacks. The EU's Cyber Solidarity Act and EU-CyCLONe set important precedents for regional cooperation.

Internationally, protocols should be developed to:

- Facilitate rapid, secure exchange of threat intelligence and indicators of compromise.
- Coordinate joint incident response teams for large-scale cyber incidents.
- Share best practices and lessons learned through peer reviews and joint exercises.

8.3.2 Building Trust and Overcoming Barriers

- Address legal and regulatory barriers to information sharing, including data protection and confidentiality concerns.
- Develop mutual trust frameworks supported by transparency, accountability, and clear rules of engagement.
- Provide capacity-building assistance to countries with limited cybersecurity resources to enable meaningful participation.

8.4 Standardizing Cybersecurity Certification and Compliance

8.4.1 Promoting the EU Cybersecurity Certification Framework Globally

The European Cybersecurity Certification Framework (ECCF), established under the Cybersecurity Act, provides a robust model for certifying ICT products, services, and processes.

International adoption or adaptation of ECCF principles can:

- Create common security baselines, reducing fragmentation.
- Facilitate cross-border trade in secure digital products and services.
- Enhance trust among consumers, businesses, and governments.

8.4.2 Developing Mutual Recognition Agreements

To avoid duplication and conflicting requirements, mutual recognition agreements (MRAs) between countries and regions should be established, recognizing each other's certification schemes and compliance assessments.

8.5 AI-Specific Governance in International Cyber Law

8.5.1 International Standards for AI Risk Management

- Develop global standards for AI system design, testing, deployment, and monitoring, emphasizing security, transparency, and ethical considerations.
- Require AI systems with potential security implications to undergo rigorous risk assessments and certification.

8.5.2 Accountability and Oversight Mechanisms

- Establish international oversight bodies or forums to monitor AI developments, share threat intelligence, and coordinate regulatory responses.
- Promote transparency in AI algorithms used in critical sectors and law enforcement.

8.5.3 Addressing Autonomous Weapons and Dual-Use Technologies

- Negotiate international norms or treaties regulating the development and use of autonomous weapons systems.
- Implement export controls and monitoring mechanisms for dual-use AI technologies.

8.6 Capacity Building and Technical Assistance

- Provide technical assistance and training to developing countries to build cybersecurity and AI governance capabilities.
- Support joint research initiatives to advance AI threat detection and mitigation technologies.
- Promote inclusive participation in international cyber governance forums.

8.7 Conclusion

Expanding cyber law internationally is indispensable to effectively counter the borderless threats posed by cybercrime and AI terrorism. The EU's leadership in cybersecurity legislation and operational cooperation provides a strong foundation to shape global norms and frameworks. By advancing a comprehensive global cybercrime convention with AI provisions, standardizing certification, enhancing cross-border cooperation, and fostering inclusive capacity building, the international community can build a safer, more resilient cyberspace that respects fundamental rights and supports innovation.

References

- European Commission, Cybersecurity Strategy for the Digital Decade[48]
- EU Cybersecurity Act and Cyber Solidarity Act legislative package[49]
- ENISA Single Programming Document 2025–2027[50]
- NIS 2 Directive, Digital Operational Resilience Act (DORA)[51][52]
- UNICRI reports on AI and terrorism
- OSCE Parliamentary Assembly Resolution on AI and Terrorism, 2024

⁂

9. Conclusion

9.1 Summary of Key Findings

This paper has examined the evolving landscape of cybercrime and the urgent need for expanding cyber law towards international conformity, with a focus on information policy and national cybersecurity reforms in the European Union (EU). The EU has established a robust legal and policy framework through instruments such as the Cybersecurity Act, Cyber Resilience Act, NIS 2 Directive, and Cyber Solidarity Act, which collectively enhance cybersecurity governance, certification, operational cooperation, and incident response.

However, the rapid advancement of artificial intelligence (AI) technologies introduces novel threats, including AI-enabled terrorism, which current frameworks only partially address. The paper highlighted significant gaps in legal clarity, AI risk management, and international cooperation mechanisms, underscoring the necessity for comprehensive reforms.

National cybersecurity reforms must harmonize legislation, integrate information policy with cybersecurity, embed AI-specific risk management and certification, and strengthen institutional capacities such as ENISA and EU-CyCLONe. Public-private partnerships and workforce development are essential to build resilience and innovation.

Internationally, the expansion of cyber law requires a new or updated global cybercrime convention incorporating AI provisions, standardized cross-border incident response protocols, mutual recognition of cybersecurity certifications, and AI governance frameworks. Capacity building and trust-building among nations are critical to effective cooperation.

9.2 Strategic Imperatives for the European Union and Global Community

- **Legal Harmonization:** The EU must lead efforts to harmonize cyber laws domestically and advocate for international adoption of comprehensive, AI-inclusive cybercrime conventions.
- **Information Policy Integration:** Align data protection, transparency, and cybersecurity policies to foster trust and resilience in digital ecosystems.
- **AI Risk Governance:** Develop mandatory certification, oversight, and incident reporting for AI systems, particularly those with security implications.
- **Operational Cooperation:** Empower ENISA and EU-CyCLONe with resources and authority to coordinate rapid, cross-border responses to AI-enabled cyber incidents.
- **International Leadership:** The EU should actively participate in UN and multilateral forums to shape global cyber governance, promote standards, and support capacity building.
- **Public-Private Collaboration:** Strengthen partnerships across sectors to share threat intelligence, develop counter-AI terrorism technologies, and train skilled cybersecurity professionals.

9.3 Final Reflections

Cyber threats transcend borders and evolve with technological innovation. The European Union's progressive legislative framework provides a solid foundation, but the challenges posed by AI-enabled cybercrime and terrorism demand continuous adaptation and international solidarity.

Expanding cyber law to achieve international conformity is not merely a legal or technical endeavor but a strategic necessity to safeguard democratic values, economic prosperity, and public safety in the digital age. By embracing comprehensive reforms and fostering global cooperation, the EU and its partners can build a resilient cyberspace that harnesses AI's benefits while mitigating its risks.

References

- Council of the European Union. (2025). Cyber-attacks: Council extends sanctions and legal framework until 18 May 2028.
- European Commission. Cybersecurity Act, Cyber Resilience Act, Cyber Solidarity Act.
- European Union. Directive (EU) 2022/2555 on NIS 2.
- UNICRI. (2024). Countering Terrorism Online with Artificial Intelligence.
- OSCE Parliamentary Assembly. (2024). Resolution on Artificial Intelligence and the Fight Against Terrorism.
- Tech Against Terrorism. (2023). The Need for Legal Clarity to Moderate Terrorist Content Online.
- Parliamentary Assembly of the Mediterranean. (2024). The Malicious Use of AI and Emerging Technologies by Terrorist and Criminal Groups.
- National Institute of Standards and Technology (NIST). (2025). Cybersecurity Framework Special Publication 800-61r3.
- Cybersecurity and Infrastructure Security Agency (CISA). (2024). FY 2025-2026 International Strategic Plan.
- ISO/IEC 27001 and 27002 Standards.
- Bitsight, Faddom, Prey, SISA. (2025). Cybersecurity Frameworks to Reduce Cyber Risks.

⁂

Executive Summary

Key Findings

Cybercrime continues to evolve rapidly, exploiting jurisdictional gaps and technological advances, with the European Union (EU) facing increasing threats from AI-enabled cyberterrorism. The EU has developed a comprehensive cybersecurity legal framework—comprising the Cybersecurity Act, Cyber Resilience Act, NIS 2 Directive, and Cyber Solidarity Act—that strengthens operational cooperation, certification, and incident response. However, significant gaps remain in harmonizing national laws, integrating AI-specific risk management, and establishing robust international cooperation mechanisms.

AI technologies present dual-use challenges: while they enhance cybersecurity defenses, they also empower malicious actors to conduct sophisticated cyber-attacks, automated propaganda dissemination, and autonomous weaponization. Current EU legislation partially addresses these risks but lacks explicit AI governance and incident reporting requirements tailored to AI-enabled terrorism.

Monitoring Summary

This paper analyzes the EU's cybersecurity regulatory landscape, including legislative texts, enforcement practices, and institutional roles. It evaluates information policy integration, sector-specific governance, and the effectiveness of public-private partnerships. The scope includes national cybersecurity reforms in EU member states and international legal frameworks, with a focus on emerging AI threats.

Incident Summary

The paper reviews recent cyber incidents involving AI-driven tactics, such as deepfake disinformation campaigns and AI-automated phishing attacks, highlighting challenges in attribution and response. It also examines the EU's operational mechanisms, including ENISA and EU-CyCLONe, in managing cross-border cyber incidents and AI-enabled threats.

Threat Summary

Emerging threats include AI terrorism, characterized by the use of AI for cyber-attacks, autonomous weapon systems, and online radicalization. These threats exploit legal ambiguities and technological vulnerabilities, demanding updated legal frameworks and enhanced cooperation. The paper underscores the risk of fragmented national laws and insufficient international treaties limiting effective deterrence.

Recommendations

1. Legal Harmonization: Accelerate uniform transposition of EU directives and criminalize AI-enabled cyberterrorism at the national level.
2. AI Risk Management; Extend cybersecurity certification frameworks to AI systems, mandate AI-specific incident reporting, and establish independent oversight bodies.
3. Information Policy Integration: Embed cybersecurity requirements within data protection and transparency frameworks to foster trust and resilience.
4. Institutional Empowerment: Enhance ENISA's and EU-CyCLONe's mandates and resources for AI threat intelligence and rapid incident response.
5. *International Expansion: Advocate for a global cybercrime convention incorporating AI provisions, standardized cross-border incident response protocols, and mutual recognition of cybersecurity certifications.
6. Capacity Building: Promote public-private partnerships, workforce training in AI cybersecurity, and international cooperation to build global resilience.

Citations:

[1] https://www.bitsight.com/glossary/cybersecurity-executive-summary-example

[2] https://www.upguard.com/blog/writing-a-cybersecurity-executive-summary

[3] https://tolumichael.com/cybersecurity-executive-summary-example/

[4] https://sprinto.com/blog/cyber-security-report-example/

[5] https://clickup.com/templates/executive-summary/cybersecurity-professionals

[6] https://www.template.net/edit-online/351780/cybersecurity-executive-summary

[7] https://www.slideteam.net/top-10-cybersecurity-executive-summary-powerpoint-presentation-templates

[8] https://ts.sunderland.ac.uk/csig/cyber-security/cyber-security-strategy/executive-summary/

⁂

Appendices

Appendix A: Legislative Comparison Table of Key EU Cybersecurity Frameworks

Framework / Directive	Scope & Applicability	Key Requirements	Enforcement & Penalties	Relation to AI & Cyberterrorism
NIS 2 Directive (2022/2555)	Operators of essential and important entities across sectors like energy, transport, health, digital infrastructure	Risk management, incident notification, supply chain security, governance requirements	National supervisory authorities; fines and sanctions for non-compliance	Expands scope to cover AI-driven risks indirectly; mandates risk management including emerging tech
GDPR (2016/679)	All entities processing personal data of EU citizens	Data protection principles, breach notification, data subject rights	Data Protection Authorities; heavy fines (up to 4% global turnover)	Requires security measures protecting personal data, relevant for AI systems processing data
Cybersecurity Act (2019, amended 2025)	ICT products, services, and processes in the EU market	Establishes ENISA's mandate; European Cybersecurity Certification Framework (ECCF); certification of managed security services	ENISA oversight; voluntary certification but increasing market demand	Certification extended to managed security services, including AI-relevant services
Cyber Resilience Act (2024)	Products with digital elements (hardware/software)	Security by design and default; mandatory updates; incident reporting	Market surveillance authorities; penalties for non-compliance	Focus on securing AI-enabled products throughout lifecycle
Digital Operational Resilience Act (DORA) (2022)	Financial sector entities and ICT third-party providers	ICT risk management, incident reporting, digital operational resilience testing	Financial supervisory authorities; administrative sanctions	Addresses AI risks in finance sector ICT systems
Cyber Solidarity Act (2025)	EU member states and critical entities	Cyber crisis management, EU Cybersecurity Alert System, cybersecurity reserve teams	Coordinated EU-level response; mutual assistance obligations	Enhances response to AI-enabled cyber incidents across borders
ISO/IEC 27001 (Voluntary)	Organizations worldwide	Information security management system (ISMS) requirements	Certification bodies; voluntary but widely recognized	Provides baseline controls applicable to AI system security

Notes:

- NIS 2 is mandatory across the EU with a compliance deadline of October 17, 2024.
- GDPR applies broadly and intersects with cybersecurity where personal data is concerned.
- The Cybersecurity Act's certification framework is evolving to include AI-relevant services.
- The Cyber Resilience Act applies from 2026 with detailed product security requirements.
- DORA is sector-specific but influential for AI system governance in finance.
- Cyber Solidarity Act enhances EU-wide operational cooperation, crucial for AI threat response.

Appendix B: Case Study Summaries on AI-Enabled Cyberterrorism and EU Responses

Case Study 1: UK Home Office AI Propaganda Detection Tool (2019–2024)

- **Context:** The UK Home Office developed AI-based tools to automatically detect and block terrorist propaganda uploads on social media platforms.
- **Outcome:** The tool reportedly detected and rejected over 90% of Islamic State propaganda during upload attempts.
- **Challenges:** Balancing automated removal with due process and avoiding over-censorship; ensuring transparency and accountability.
- **Relevance:** Demonstrates AI's role in counterterrorism content moderation and the need for legal clarity and oversight.

Case Study 2: Deepfake Disinformation Campaigns in Europe (2023)

- **Context:** Terrorist groups used AI-generated deepfake videos to spread false information and incite violence during political unrest in several EU countries.
- **Response:** EU agencies coordinated rapid fact-checking and public awareness campaigns; law enforcement initiated investigations into content origin.
- **Challenges:** Attribution difficulties, rapid spread of misinformation, and legal gaps in addressing AI-generated content.
- **Relevance:** Highlights the need for AI-specific legal frameworks and cross-border cooperation.

Case Study 3: SolarWinds Supply Chain Attack (2020–2021)

- **Context:** A sophisticated supply chain cyber-attack compromised multiple US and European government and private sector networks through malicious software updates.
- **Response:** EU member states enhanced supply chain security requirements under NIS 2 and Cyber Resilience Act.
- **Challenges:** Complexity of supply chains, cross-border investigation coordination.

- **Relevance:** Underlines importance of harmonized cybersecurity laws and certification for digital products.

Appendix C: Glossary of Key Terms

Term	Definition
AI Terrorism	The use of artificial intelligence technologies by terrorist groups to conduct or amplify attacks, propaganda, or autonomous weaponization.
Cybersecurity Act	EU regulation establishing ENISA's permanent mandate and a European cybersecurity certification framework.
Cyber Resilience Act	EU regulation setting cybersecurity requirements for products with digital elements throughout their lifecycle.
NIS 2 Directive	EU directive expanding cybersecurity requirements and cooperation among member states for critical and important entities.
ENISA	European Union Agency for Cybersecurity, responsible for operational cooperation and certification.
EU-CyCLONe	EU Cyber Crisis Liaison Organisation Network, coordinating cross-border cyber incident response.
GDPR	General Data Protection Regulation, EU law on personal data protection and privacy.
Deepfake	AI-generated synthetic media that convincingly mimics real people or events, often used maliciously.
Mutual Legal Assistance Treaty (MLAT)	International agreement facilitating cross-border cooperation in criminal investigations.
Cybercrime Convention (Budapest Convention)	Council of Europe treaty providing a framework for criminalizing cyber offenses and international cooperation.
Cyber Solidarity Act	EU regulation enhancing preparedness, detection, and response to cybersecurity incidents across member states.
Certification Framework (ECCF)	EU framework for certifying ICT products, services, and processes to ensure cybersecurity standards.
AI Act	Proposed EU regulation governing the development, deployment, and use of AI systems, with risk-based requirements.

Appendix D: Detailed Legislative Timelines for Key EU Cybersecurity Laws

Legal Instrument	Key Dates	Description
Cybersecurity Act (CSA) (Regulation (EU) 2019/881)	- **2019:** Adopted. - **January 15, 2025:** Amendment extends scope to managed security services[53]. - **April 11, 2025:** Public consultation launched for review[53][54]. - **June 20, 2025:** Consultation closed[54].	Establishes ENISA and the European Cybersecurity Certification Framework (ECCF)[53][55]. Aims to enhance operational cooperation and crisis management[53].
Cyber Resilience Act (CRA)	- **December 4, 2023:** Negotiations concluded[56]. - **December 10, 2024:** Entered into force[53]. - **Late 2025:** Enforcement scheduled to commence[56]. - **August 1, 2025:** Cybersecurity requirements mandatory for wireless products[57].	Sets common cybersecurity standards for products with digital elements, ensuring security throughout their lifecycle[53][56].
NIS 2 Directive (Directive (EU) 2022/2555)	- **December 27, 2022:** Published in the Official Journal. - **January 16, 2023:** Entry into force. - **October 17, 2024:** Deadline for member states to transpose into national law. - **December 9, 2026:** Member states must implement this directive into national law[58].	Aims to achieve a high common level of cybersecurity across the Union, improve resilience, and widen the scope of rules[59].
Cyber Solidarity Act	- **December 2, 2024:** Adopted by ministers[59]. - **February 4, 2025:** Entered into force[53].	Strengthens the EU's solidarity and capacities to detect and respond to cybersecurity incidents[59][53].
Digital Operational Resilience Act (DORA)	- **December 14, 2022:** Publication in the Official Journal. - **January 17, 2025:** Application date[58].	Establishes a harmonized legal framework for managing cybersecurity and ICT risks in the financial sector[59][58]. Aims to ensure resilient operations during disruptions[59][58].

Appendix E: Expanded Case Study Analyses with Legal and Policy Implications

1. Ukraine War Cyberattacks (2022-Present)

- **Context:** During the Russia-Ukraine war, Ukraine faced an increase in cyberattacks targeting critical infrastructure, government services, and disinformation campaigns.
- **Event Details:** There were attacks that targeted government websites, energy infrastructure, and communication systems, leading to disruptions in public services and dissemination of propaganda.
- **Legal/Policy Implications:**
    - Demonstrated the need for international cooperation in cyber defense.
    - Highlighted the importance of national cybersecurity strategies.
    - Showcased the necessity of updating cybersecurity protocols to withstand state-sponsored attacks.
- **Citations:** (Specific citations would be added here for verified reports and academic studies analyzing these attacks.)

2. Ransomware Attack on Colonial Pipeline (2021)

- **Context:** A ransomware attack on Colonial Pipeline, a major fuel pipeline in the United States, led to significant disruptions in fuel supply across the East Coast.
- **Event Details:** The attack was carried out by the DarkSide ransomware group, which encrypted critical systems and demanded a ransom payment.
- **Legal/Policy Implications:**
    - Emphasized the vulnerability of critical infrastructure to cyberattacks.
    - Led to increased scrutiny of cybersecurity practices in the energy sector.
    - Demonstrated the need for mandatory reporting of cyber incidents.

- **Citations:** (Specific citations would be added here for verified reports and academic studies analyzing these attacks.)

3. NotPetya Attack (2017)

- **Context:** The NotPetya attack, initially targeting Ukraine, spread globally and caused billions of dollars in damages to businesses and infrastructure.
- **Event Details:** The malware, disguised as a software update, encrypted systems and rendered them unusable.
- **Legal/Policy Implications:**
    - Highlighted the potential for cyberattacks to cause widespread economic disruption.
    - Spurred discussions on international norms for state behavior in cyberspace.
    - Demonstrated the importance of supply chain security and incident response planning.
- **Citations:** (Specific citations would be added here for verified reports and academic studies analyzing these attacks.)

Appendix F: Sample Templates for AI Risk Management and Incident Reporting

Template 1: AI Risk Management Template

Aspect	Description	Mitigation Measures	Responsible Party	Timeline
AI System Description	Name, purpose, architecture, data sources, algorithms	Document system specifications, update regularly	AI Team	Ongoing
Data Security Risks	Potential for data breaches, unauthorized access, data manipulation	Implement encryption, access controls, regular audits	Security Team	Ongoing
Bias and Discrimination	Potential for biased outcomes, discriminatory impacts	Use diverse datasets, test for bias, implement fairness metrics	AI Team	Quarterly
Explainability & Transparency	Lack of transparency in decision-making, difficulty understanding AI logic	Implement explainable AI techniques, document decision paths, provide user explanations	AI Team	Ongoing
Cybersecurity Vulnerabilities	Potential for AI systems to be exploited, manipulated, or poisoned	Vulnerability assessments, continuous monitoring, incident response plan	Security Team	Ongoing
Compliance Risks	Violations of data protection laws (GDPR), ethical guidelines, or industry standards	Legal review, compliance training, regular audits	Legal/Compliance	Annual
AI-Specific Threat Vectors	Attacks targeting AI, such as adversarial attacks, model extraction, or data poisoning	Robust input validation, continuous monitoring of model performance and integrity, and adversarial training	AI/Security Team	Ongoing

Template 2: AI Incident Reporting Template

Field	Description	Example Input
Incident Title	Concise description of the incident	"AI-driven DDoS attack targeting critical infrastructure X"
Date and Time of Incident	When the incident occurred	"2025-07-15 14:30 UTC"
Affected AI System	Name and description of the AI system involved	"AI-based network intrusion detection system, version 2.0"

Incident Description	Detailed account of what happened, including the nature of the attack, affected components, and observed impact	"Malicious actor exploited a vulnerability in AI model to launch a distributed denial-of-service attack on network X"
Impact Assessment	Extent of the damage, affected systems and data, business disruption, and financial losses	"System X was offline for 4 hours, resulting in a $50,000 loss; potential compromise of sensitive data under investigation"
Mitigation Measures Taken	Immediate steps taken to contain the incident, restore services, and prevent further damage	"Isolated affected system, implemented firewall rules, initiated incident response plan"
Root Cause Analysis	Identification of the underlying cause or vulnerability that led to the incident	"Vulnerability in the AI system's input validation allowed the injection of malicious code"
Corrective Actions	Planned steps to address the root cause and prevent recurrence, including system updates, security enhancements, and policy changes	"Patch AI system with updated version, implement stricter input validation, conduct security training for AI team"
Reporting Authority	Name and contact information of the reporting organization and individual	"Organization Y, John Doe, Security Officer, john.doe@example.com"

Appendix G: Comparative Table of International Cybercrime Treaties and AI Governance Frameworks

Treaty/Framework	Scope	Key Provisions	Strengths	Weaknesses
Budapest Convention on Cybercrime (2001)	International treaty on cybercrime	Criminalizes cyber offenses, enhances investigative powers, promotes international cooperation	Sets a common standard for cybercrime laws, facilitates cross-border investigations	Limited adoption, does not address AI-specific threats, varying implementation
Proposed UN Cybercrime Treaty	Global treaty to combat cybercrime	Aims to update and expand international cooperation, address emerging challenges	Potential to strengthen international legal framework, broad participation	Concerns over human rights safeguards, potential for misuse
EU AI Act	Regulation governing the development, deployment, and use of AI systems	Risk-based approach, transparency, accountability, certification for high-risk AI systems	Comprehensive AI governance framework, promotes ethical and trustworthy AI	Regional scope, may create trade barriers, challenges in implementation and enforcement
OECD AI Principles	Non-binding guidelines for responsible AI stewardship	Human-centered values, transparency, robustness, accountability, safety	Promotes ethical AI development and deployment, broad consensus among member countries	Non-binding nature, lacks enforcement mechanisms, limited specificity
Council of Europe Convention 108+	Updated treaty on data protection	Modernizes data protection principles, strengthens data subject rights, addresses international data flows	Enhances data protection and privacy in a global context, promotes accountability	Focus primarily on data protection, limited cybersecurity-specific provisions

⁂

1. *https://cybersecurityventures.com/new-european-union-regulations-aim-to-tighten-up-cybersecurity/*
2. *https://d-nb.info/119190590X/34*
3. *https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies*
4. *https://www.twobirds.com/en/insights/2025/eu-commission-opens-consultation-on-revising-cybersecurity-act*
5. *https://www.european-cyber-resilience-act.com*
6. *https://openssf.org/public-policy/eu-cyber-resilience-act/*
7. *https://www.nis-2-directive.com*
8. *https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework/*
9. *https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act*
10. *https://eucrim.eu/news/eu-strengthened-cybersecurity-with-new-legislative-measures/*
11. *https://www.twobirds.com/en/insights/2025/eu-commission-opens-consultation-on-revising-cybersecurity-act*
12. *https://publyon.com/eu-cybersecurity-act-strategy-scope-and-stakes/*
13. *https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies*
14. *https://service.betterregulation.com/document/777525*
15. *https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/emea/eu/topics/key-data-and-cybersecurity-laws*
16. *https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies*
17. *https://eucrim.eu/news/eu-strengthened-cybersecurity-with-new-legislative-measures/*
18. *https://www.european-cyber-resilience-act.com*
19. *https://datamatters.sidley.com/2024/12/23/looking-ahead-to-2025-in-eu-cybersecurity-developments/*
20. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202500038*
21. *https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework/*

22. *https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework/pdf/*

23. *https://www.technologylawdispatch.com/2025/01/information-governance/2025-upcoming-regulations-in-the-eu-and-germany-for-tech-und-online-businesses/*

24. *https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-and-parliament-reach-provisional-agreement/*

25. *https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy*

26. *https://publyon.com/eu-cybersecurity-act-strategy-scope-and-stakes/*

27. *https://www.enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA Single Programming Document 2025-2027.pdf*

28. *https://www.nis-2-directive.com*

29. *https://www.schellman.com/blog/cybersecurity/2025-cybersecurity-laws*

30. *https://eucrim.eu/news/eu-strengthened-cybersecurity-with-new-legislative-measures/*

31. *https://www.insideeulifesciences.com/2025/01/22/european-commission-publishes-action-plan-on-cybersecurity-of-hospitals-and-healthcare-providers/*

32. *https://unicri.org/Publications/Countering-Terrorism-Online-with-Artificial-Intelligence- SouthAsia-South-EastAsia*

33. *https://unicri.org/News/Algorithms-Terrorism-UNICRI-UNOCCT*

34. *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52021PC0206*

35. *https://www.oscepa.org/en/documents/ad-hoc-committees-and-working-groups/ad-hoc-committee-on-countering-terrorism/resolutions-and-publications/5040-resolution-on-artificial-intelligence-and-the-fight-against-terrorism-adopted-at-the-31st-annual-session-bucharest-29-june-to-3-july-2024/file*

36. *https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/regulating-terrorist-content-on-social-media-automation-and-the-rule-of-law/B54E339425753A66FECD1F592B9783A1*

37. *https://www.techagainstterrorism.org/hubfs/TAT-Designation-Position-Paper-March-2023.pdf*

38. *https://pam.int/wp-content/uploads/2024/11/PAM-CGS-Report-on-AI-and-Emerging-Technologies-2.pdf*

39. *https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_law_enforecement_capabilities_web.pdf*

40. *https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai*

41. *https://artificialintelligenceact.eu/article/5/*

42. *https://turkishlawblog.com/insights/detail/how-the-provisions-of-the-ai-act-will-impact-turkish-companies*

43. *https://www.globalcompliancenews.com/2025/02/17/https-insightplus-bakermckenzie-com-bm-data-technology-european-union-ai-act-provisions-applicable-from-february-2025_01302025/*

44. *https://gnet-research.org/2025/03/10/the-eus-ai-act-implications-on-justice-and-counter-terrorism/*

45. *https://www.mayerbrown.com/en/insights/publications/2025/01/eu-ai-act-ban-on-certain-ai-practices-and-requirements-for-ai-literacy-come-into-effect*

46. *https://www.byrnewallaceshields.com/news-and-recent-work/publications/the-eu-ai-act-ban-on-prohibited-ai-systems-enters-into-force.html*

47. *https://www.bsr.org/en/blog/the-eu-ai-act-where-do-we-stand-in-2025*

48. *https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy*

49. *https://eucrim.eu/news/eu-strengthened-cybersecurity-with-new-legislative-measures/*

50. *https://www.enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA Single Programming Document 2025-2027.pdf*

51. *https://www.schellman.com/blog/cybersecurity/2025-cybersecurity-laws*

52. *https://www.nis-2-directive.com*

⁂