Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2026, n. 2

EDITORIALE SCIENTIFICA

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies" www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2026, n. 2

Editoriale

Saggi, Articoli e Commenti

FOCUS

The EU as a Global Security Provider: Countering Transnational Crime and New Cooperation Architectures

Collected Papers of the Jean Monnet Module (2023-2026) Transnational Crime & EU Law: Towards Global Action against Cross-border Threats to Common Security, Rule of Law and Human Rights (EU-GLOBACT) – (Coordinator: Prof. Dr. Anna Oriolo)

THE EU'S CROSS-BORDER CYBERCRIME ENFORCEMENT AND THE LIMITS OF EXTRATERRITORIAL JURISDICTION

Heybatollah Najandimanesh *

SUMMARY: 1. Introduction. – 2. Jurisdictional Foundations and Their Structural Limits. – 3. The EU's Internal Enforcement Architecture. – 4. External Dimension and Normative Projection. – 5. Functional Extraterritoriality and Private Intermediaries. – 6. Enforcement Jurisdiction and the Problem of Consent. – 7. Sovereignty in the Digital Legal Order. – 8. Normative Evaluation: Between Effectiveness and Legal Constraint. – 9. Conclusion.

1. Introduction

The legal regulation of cybercrime has become one of the most structurally challenging domains of contemporary international law[1]. The difficulty does not lie merely in the increasing volume and sophistication of cyber offences, but rather in the fact that cyberspace fundamentally disrupts the spatial and conceptual assumptions upon which classical jurisdictional doctrines were historically constructed[2]. Traditional international law is grounded in territoriality, presuming a relatively stable alignment between conduct, actors, and consequences within identifiable sovereign spaces[3].Cyber operations, by contrast, fragment this alignment by dispersing digital conduct across distributed infrastructures, multiple legal orders, and transnational networks of actors in ways that resist clear localisation or singular jurisdictional attribution[4]. This structural disaggregation of territoriality generates persistent uncertainty as to where jurisdiction begins, how far it extends, and under what conditions it may be legitimately exercised.

Within this fragmented legal geography, the European Union has developed a particularly sophisticated and increasingly integrated regulatory and operational

* Associate Professor of International Law, Allameh Tabatabaei University, Tehran. E-mail: hnajandimanesh@gmail.com.

[1] C. KUNER, *Transborder Data Flows and Data Privacy Law*, Oxford, 2013.

[2] M.N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, II ed., Cambridge, 2017, pp. 22-24.

[3] J. CRAWFORD, *Brownlie's Principles of Public International Law*, IX ed., Oxford, 2019, pp. 456-459.

[4] C. RYNGAERT, *Jurisdiction in International Law*, II ed., Oxford, 2015, pp. 5-9.

framework for cybercrime enforcement[5]. This framework is characterised by a combination of substantive harmonisation, procedural integration, and expanding transnational cooperation mechanisms. On the substantive level, Directive 2013/40/EU on attacks against information systems establishes minimum rules concerning the criminalisation of core cyber offences, thereby reducing divergences among Member States and facilitating mutual recognition in criminal matters[6]. On the procedural level, the Union has progressively moved toward more direct mechanisms for cross-border access to electronic evidence, most notably through the proposed European Production and Preservation Orders, which aim to enable judicial authorities to address service providers across jurisdictions without reliance on traditional mutual legal assistance channels[7]. In parallel, operational cooperation has been significantly strengthened through EU agencies such as Europol and Eurojust, which function as coordination nodes for intelligence sharing, joint investigations, and judicial cooperation in cross-border cases[8]. Taken together, these developments reflect a gradual but discernible shift toward a more vertically and horizontally integrated model of cybercrime enforcement within the Union's legal order.

At the same time, the external dimension of this emerging enforcement architecture raises complex and unresolved questions under general international law. While the internal consolidation of EU cybercrime governance enhances effectiveness and coherence within the Union, its outward-facing components increasingly engage with third states, transnational service providers, and global digital infrastructures in ways that challenge established limits of extraterritorial jurisdiction. In particular, the expansion of cross-border evidence-gathering mechanisms, combined with direct regulatory engagement with private intermediaries, raises questions regarding the extent to which enforcement effects may be produced beyond EU territory without the explicit consent of affected third states. These developments intersect with foundational principles of international law, including territorial sovereignty, non-intervention, and consent-based limits on enforcement jurisdiction, thereby situating the EU's cybercrime framework at the boundary between lawful jurisdictional extension and potential functional overreach[9]. This tension reflects not only a doctrinal issue but also a broader structural transformation

[5] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2023*, 19 October 2023, pp. 12-15.
[6] Directive 2013/40/EU of the European Parliament and of the Council, *on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*, of 12 August 2013, in OJ L218, 14 August 2013, arts. 3-7.
[7] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 17 April 2018, COM/2018/225 final.
[8] Regulation (EU) 2016/794 of the European Parliament and of the Council, *on the European Union Agency for Law Enforcement Cooperation (Europol)*, of 11 May 2016, in OJ L135, 24 May 2016, pp. 12-14; Regulation (EU) 2018/1727 of the European Parliament and of the Council, *on the European Union Agency for Criminal Justice Cooperation (Eurojust)*, of 14 November 2018, in OJ L295, 21 November 2018, pp. 10-12.
[9] J. CRAWFORD, *Brownlie's Principles*, cit., pp. 465-468.

in contemporary global governance, where territorially bounded jurisdiction increasingly interacts with networked and decentralised regulatory systems.

The growing reliance on transnational cooperation structures, regulatory harmonisation, and private intermediary compliance further complicates this picture. As digital infrastructures are increasingly governed through globally networked private actors, enforcement is no longer exclusively mediated through inter-state channels but is also operationalised through corporate compliance systems embedded within transnational service architectures[10]. This shift contributes to the emergence of a hybrid enforcement space, in which the distinction between domestic and international enforcement becomes progressively blurred. Within such a configuration, regulatory authority is increasingly exercised through distributed compliance mechanisms rather than exclusively through territorial jurisdiction or formal interstate cooperation. As a result, the European Union not only regulates within its territorial boundaries but also projects normative and operational effects outward through interconnected legal, institutional, and technological mechanisms.

Against this background, this article examines the European Union's external dimension in the cross-border fight against cybercrime and assesses its compatibility with the limits of extraterritorial jurisdiction under general international law. It asks how the EU's evolving enforcement architecture should be understood within the doctrinal framework of international jurisdiction, and whether its operational logic can be reconciled with established principles of sovereignty, non-intervention, and consent. The analysis is based on a doctrinal legal methodology, relying on the interpretation of international jurisdictional principles, relevant jurisprudence, and EU legislative and cooperative instruments governing cybercrime enforcement. Accordingly, the study is grounded in a legal-dogmatic approach focused on normative interpretation rather than empirical investigation.

The article proceeds from the hypothesis that the EU's cybercrime governance reflects an emerging form of functional extraterritoriality embedded within its external action in the field of criminal justice. This concept captures a mode of regulatory projection in which enforcement effects extend beyond territorial boundaries not through formal assertions of jurisdiction, but through the operational architecture of transnational legal and technological networks. While certain elements of this framework may be justified under established bases of prescriptive jurisdiction in international law, such as the effects doctrine and the protection of essential interests, other practices raise concerns where they generate de facto enforcement effects beyond EU territory without a sufficiently clear consent basis. In this sense, the EU's cybercrime enforcement model not only contributes to the consolidation of global cyber governance structures, but also exposes deeper structural tensions within the architecture of international jurisdictional law, particularly regarding the evolving balance between effectiveness, sovereignty, and legal legitimacy.

[10] C. KUNER, *Transborder Data Flows*, cit., pp. 102-105.

In terms of structure, the article is organised as follows. The second section examines the doctrinal foundations of jurisdiction in international law and the structural limits imposed by territorial sovereignty and consent. The third section analyses the internal enforcement architecture of the European Union in the field of cybercrime. The fourth section addresses the external dimension of EU cybercrime governance and its normative projection beyond Union borders. The fifth section develops the concept of functional extraterritoriality with particular attention to private intermediaries. The sixth section examines enforcement jurisdiction and the problem of consent. The seventh section situates these developments within the broader framework of sovereignty in the digital legal order. The eighth section provides a normative evaluation of the EU model between effectiveness and legal constraint. The final section concludes the article.

2. Jurisdictional Foundations and Their Structural Limits

The regulation of cross-border cybercrime presents one of the most significant jurisdictional challenges confronting contemporary international law. The traditional law of jurisdiction developed within a legal order structured around territorially defined sovereign states, identifiable actors, and geographically ascertainable conduct. The architecture of cyberspace, by contrast, is characterized by the simultaneous dispersal of actors, infrastructure, data flows, and harmful consequences across multiple jurisdictions. As a result, the legal principles historically used to allocate regulatory authority among states increasingly encounter structural limitations when applied to cyber activities. Although the traditional jurisdictional bases of territoriality, nationality, protective jurisdiction, passive personality, and universality remain formally valid under international law, their practical application in cyberspace has become increasingly complex and contested[11]. The territorial principle has long occupied a central position within the international law of jurisdiction. As an incident of sovereignty, states possess authority to prescribe, adjudicate, and enforce legal rules with respect to conduct occurring within their territory. Territorial jurisdiction enjoys near-universal acceptance because it reflects the fundamental premise that a sovereign state exercises exclusive authority within its territorial domain. Historically, the territorial principle has offered a relatively clear and predictable basis for the allocation of jurisdictional competence. Where criminal conduct occurs wholly within the territory of a state, questions concerning jurisdiction rarely arise.

Difficulties emerge, however, when different components of an offence occur in different jurisdictions. International law has traditionally responded through the development of subjective and objective territoriality. Under the doctrine of subjective territoriality, jurisdiction may be exercised by the state in which the conduct constituting the offence commenced. Under objective territoriality, jurisdiction may be exercised by

[11] J. CRAWFORD, *Brownlie's Principles*, cit., pp. 457-462.

the state in which the offence was completed or where its harmful effects materialized. Both doctrines are widely accepted and permit concurrent jurisdiction in circumstances where transnational conduct spans multiple states[12].

The development of these doctrines is illustrated in several important judicial decisions. In Treacy v DPP [1971] AC 537, the House of Lords upheld jurisdiction over a blackmail scheme initiated in England but directed toward a victim located in Germany[13]. Similarly, in DPP v Doot [1973] AC 807, English courts exercised jurisdiction over a conspiracy formed abroad because significant elements of the criminal enterprise were intended to be implemented within the United Kingdom[14]. More significantly, the modern judicial trend has moved away from rigid attempts to identify a single territorial situs of a crime. In Somchai Liangsiriprasert v Government of the United States [1991] 1 AC 225, the House of Lords emphasized that jurisdiction may properly be exercised whenever a substantial part of the criminal conduct occurs within the forum state, unless considerations of international comity strongly indicate otherwise[15]. This evolution reflects a growing recognition that contemporary transnational conduct cannot easily be reduced to a single geographical location.

These challenges become considerably more pronounced in cyberspace. Digital communications routinely pass through multiple jurisdictions, data may be stored simultaneously in several states, and harmful consequences may materialize in locations far removed from both the perpetrator and the relevant technological infrastructure. In such circumstances, identifying the territorial location of conduct becomes increasingly artificial. A cyber intrusion directed from one state, routed through servers in several others, and producing effects in multiple jurisdictions may simultaneously satisfy several competing territorial claims. The result is a substantial increase in overlapping jurisdictional assertions and the corresponding risk of regulatory fragmentation.

The difficulties associated with territoriality are closely connected to broader debates concerning the legal characterization of cyberspace itself. Traditional jurisdictional analysis presupposes the existence of a geographically identifiable space in which conduct occurs[16]. Yet cyberspace challenges precisely this assumption. Scholars have long observed that cyberspace appears simultaneously everywhere and nowhere, existing through globally distributed technological infrastructure while remaining functionally detached from traditional territorial boundaries[17]. Johnson and Post famously argued that cyberspace should be understood as a distinct regulatory environment requiring legal approaches that differ from those developed for territorially bounded activities[18]. Some

[12] M.N. SHAW, *International Law*, IX ed., Cambridge, 2021, pp. 534-537.
[13] House of Lords, *Treacy v Director of Public Prosecutions*, judgment of 15 December 1971, [1971] AC 537.
[14] House of Lords, *Director of Public Prosecutions v Doot*, judgment of 21 March 1973, AC 807 (HL).
[15] House of Lords, *Somchai Liangsiriprasert v Government of the United States of America*, judgment of 02 July 1990, 1 AC 225 (PC).
[16] C. RYNGAERT, *Jurisdiction in International Law*, cit., pp. 1-3.
[17] C. KUNER, *Transborder Data Flows*, cit., pp. 45-47.
[18] D.R. JOHNSON, D. POST, *Law and Borders - The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, n. 5, pp. 1367-1370.

scholars have gone further, suggesting that cyberspace resembles other international spaces such as the high seas, Antarctica, or outer space, and should therefore be approached through analogous jurisdictional frameworks[19]. While such proposals have not gained widespread acceptance, they underscore the extent to which traditional territorial assumptions are strained by the digital environment.

The structural limitations of territoriality have contributed to the growing importance of the effects doctrine, often described as a form of objective territorial jurisdiction[20]. The effects doctrine permits a state to exercise jurisdiction over conduct occurring outside its territory where that conduct produces substantial effects within the state's territory[21]. Historically, the doctrine emerged as a response to increasing economic interdependence and the growing capacity of extraterritorial conduct to affect domestic markets and regulatory interests.

The intellectual origins of modern effects-based jurisdiction are often associated with the controversial decision in United States v Aluminium Co of America (Alcoa), 148 F.2d 416 (2d Cir. 1945)[22]. In that case, the United States Court of Appeals asserted jurisdiction over foreign conduct on the basis that it produced intended and substantial effects within the United States. The court suggested that states may impose legal consequences upon conduct occurring abroad where such conduct generates domestic effects that the state has a legitimate interest in regulating. Although the decision became highly influential, it also generated significant international criticism. Many states viewed the doctrine as an excessive assertion of extraterritorial authority capable of undermining sovereign equality and creating conflicts of jurisdiction.

Subsequent American jurisprudence sought to moderate the expansive implications of Alcoa. In Timberlane Lumber Co v Bank of America (1976), the court introduced a balancing approach requiring consideration of the interests of other states and the reasonableness of exercising jurisdiction in the circumstances[23]. This development reflected an emerging recognition that jurisdictional claims cannot be evaluated solely by reference to domestic effects but must also take account of broader principles of international comity and interstate accommodation.

Within Europe, analogous developments occurred in competition law. In Dyestuffs (ICI v Commission) (1972) and later in Woodpulp (Ahlström Osakeyhtiö v Commission) (1988), European institutions asserted jurisdiction over foreign undertakings whose

[19] D.C. MENTHE, *Jurisdiction in Cyberspace: A Theory of International Spaces*, in *Michigan Telecommunications and Technology Law Review*, 1998, no. 1, p. 83.
[20] M. VAGIAS, *The Effects Doctrine*, in M. VAGIAS (ed.), *The Territorial Jurisdiction of the International Criminal Court*, Cambridge, 2014.
[21] W. ESTEY, *The Five Bases of Extraterritorial Jurisdiction and the Failure of the Presumption against Extraterritoriality*, in *Hastings International and Comparative Law Review*, 1997, no. 1, pp. 186-190.
[22] U.S. Court of Appeals for the Second Circuit, *United States v Aluminium Co of America*, judgment of 12 March 1945, 148 F.2d 416.
[23] U.S. Court of Appeals for the Ninth Circuit, *Timberlane Lumber Co. v Bank of America*, judgment of 27 December 1976, 549 F.2d 597.

conduct produced effects within the European market[24]. Although the European Court of Justice sought formally to characterize its reasoning as an application of territoriality rather than an independent effects doctrine, the practical distinction remains difficult to sustain. The underlying rationale in both cases was that conduct occurring outside the territory of the European Community could nevertheless be regulated because of its significant impact upon the internal market. Consequently, the jurisprudence illustrates the continuing tendency of regulatory systems to expand jurisdictional claims in response to transnational economic activity.

3. The EU's Internal Enforcement Architecture

The European Union's response to cybercrime has evolved from a fragmented system of intergovernmental cooperation into an increasingly integrated enforcement architecture characterized by legal harmonization, institutional coordination, and the gradual centralization of enforcement capacities[25]. This transformation reflects a broader process of Europeanization in which regulatory authority, once exercised primarily by Member States, has increasingly been complemented by supranational mechanisms designed to ensure uniform implementation and effective enforcement across the Union. In the field of cybercrime, where offences frequently transcend territorial boundaries and involve multiple jurisdictions simultaneously, the development of a coherent internal enforcement framework has become a functional necessity.

At the substantive level, the foundation of the EU's cybercrime regime is provided by Directive 2013/40/EU on attacks against information systems. The Directive harmonizes the criminalization of core cyber offences, including illegal access to information systems, illegal system interference, illegal data interference, and the misuse of devices intended to facilitate such crimes[26]. By reducing divergences among national criminal laws, the Directive facilitates mutual trust and mutual recognition between Member States, both of which are indispensable for effective cross-border enforcement. Harmonization of substantive offences also diminishes the likelihood that cybercriminals can exploit regulatory disparities between jurisdictions, thereby strengthening the Union's capacity to respond collectively to transnational cyber threats.

The procedural dimension of EU cybercrime enforcement has undergone equally significant transformation. Traditionally, cross-border access to electronic evidence

[24] Court of Justice, judgment of 14 July 1972, *Imperial Chemical Industries Ltd v Commission of the European Communities (Dyestuffs)*, case 48/69; Court of Justice, Fifth Chamber, judgment of 31 March 1993, *Ahlström Osakeyhtiö and Others v Commission of the European Communities (Woodpulp)*, joined cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 and C-125/85 to C-129/85.

[25] I. MENDOZA GARCÍA, *Cybercrime and Its Evolution in the European and Spanish Regulatory Framework*, in *Review of International and European Economic Law*, 2026, n. 8, https://rieel.com/index.php/rieel/article/view/125.

[26] Directive 2013/40/EU of the European Parliament and of the Council, *on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*, cit., arts. 3-7.

depended upon mutual legal assistance procedures, which were often criticized for being slow, cumbersome, and ill-suited to the speed with which digital evidence may be altered, transferred, or deleted. In response to these limitations, the European Commission proposed the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, which seeks to allow judicial authorities in one Member State to issue binding requests directly to service providers located in another Member State without relying upon traditional intergovernmental channels[27]. This proposal reflects a broader shift within EU enforcement policy from indirect interstate cooperation toward direct regulatory engagement with private actors that control access to relevant digital information. Such developments illustrate the emergence of a model of enforcement that increasingly bypasses classical territorial intermediaries in favour of more immediate and technologically responsive mechanisms.

Institutionally, the effectiveness of the EU's cybercrime regime depends upon a network of specialized agencies that facilitate coordination among national authorities. In particular, Europol and Eurojust have become central nodes within the Union's enforcement architecture. Europol has evolved beyond its original role as an information-sharing platform and now functions as an operational hub supporting intelligence analysis, joint investigations, and real-time coordination among law-enforcement authorities. Its increasing engagement with private technology companies and digital service providers further reflects the growing interdependence between public enforcement institutions and private actors in cyberspace[28]. Eurojust complements these activities by facilitating judicial cooperation, coordinating prosecutions, resolving jurisdictional conflicts, and supporting the execution of cross-border investigative measures. Together, these institutions contribute to a networked enforcement model that transcends traditional forms of intergovernmental cooperation and enhances the operational capacity of Member States to address cybercrime collectively.

The development of this enforcement architecture must also be understood within the broader framework of EU compliance and enforcement theory. As identified in the literature, EU enforcement operates through three overlapping and mutually reinforcing approaches: legal enforcement, political persuasion, and managerial or capacity-building mechanisms[29]. Although these approaches apply across multiple policy sectors, they are particularly relevant to understanding how the Union seeks to ensure the effective implementation of cybercrime legislation and digital security measures.

The legal enforcement dimension is rooted in the European Commission's role as the "Guardian of the Treaties" under Article 17(1) of the Treaty on European Union. Member States remain primarily responsible for implementing and enforcing EU law, but the Commission is entrusted with monitoring compliance and ensuring uniform application

[27] European Commission, *Proposal for a Regulation*, cit.
[28] E. CASEY, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, IV ed., Amsterdam, 2021, pp. 233-236.
[29] O. TREIB, *Implementing and Complying with EU Governance Outputs*, in *Living Reviews in European Governance*, 2014, no. 1, pp. 21-24.

throughout the Union. To fulfil this responsibility, the Commission employs a variety of supervisory mechanisms, including conformity assessments, consultations with national authorities, implementation reviews, and ex post evaluations of legislative effectiveness. Where a Member State fails to comply with its obligations, the Commission may initiate infringement proceedings under Article 258 TFEU. The procedure begins with a letter of formal notice and may culminate in a reasoned opinion requiring compliance within a specified period. If the Member State persists in its non-compliance, the Commission may refer the matter to the Court of Justice of the European Union (CJEU), which may ultimately impose financial sanctions under Article 260 TFEU. In cases involving failure to transpose directives, financial penalties may be imposed at the stage of the Court's initial judgment pursuant to Article 260(3) TFEU. These mechanisms provide the legal foundation for ensuring the consistent implementation of cybercrime legislation throughout the Union.

Nevertheless, empirical evidence indicates that the Commission has increasingly relied less upon coercive legal enforcement and more upon cooperative mechanisms. The number of formal infringement actions has declined significantly over the past two decades, reflecting a broader institutional preference for engagement, dialogue, and negotiated compliance rather than adversarial enforcement. This trend is particularly important in highly technical and politically sensitive fields such as cybersecurity, where effective implementation often depends upon sustained cooperation between national authorities and EU institutions rather than purely judicial sanctions.

The political dimension of EU enforcement reflects this preference for persuasion over coercion. Rather than relying exclusively on legal proceedings, the Commission frequently seeks to secure compliance through deliberative engagement with Member States. Such dialogue aims not only to resolve implementation deficiencies but also to foster acceptance of common regulatory objectives and encourage national ownership of EU policies. The underlying assumption is that compliance is more likely to be durable when Member States perceive EU rules as legitimate and appropriate rather than merely obligatory. This approach is particularly relevant in cybersecurity governance, where national security concerns, resource disparities, and varying institutional capacities may complicate the implementation of common rules[30].

The managerial approach constitutes a third pillar of the EU's enforcement architecture. Recognizing that non-compliance often results from administrative limitations rather than deliberate resistance, the Commission has increasingly invested in capacity-building, technical assistance, training programmes, and financial support mechanisms. Through specialized networks of regulators, law-enforcement authorities, and judicial actors, the EU seeks to promote the exchange of expertise, harmonize operational practices, and cultivate a common professional culture among national enforcement bodies. Such networks have become a defining feature of contemporary EU governance and have played an important role in reducing implementation gaps across

[30] M. BALLESTEROS PERALS, *Monitoring the Implementation of EU Law: Tools and Challenges*, Brussels, January 2025, https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)769042.

multiple policy sectors. In the cybercrime context, these capacity-building initiatives enhance the ability of national authorities to investigate digital offences, preserve electronic evidence, and cooperate effectively with counterparts across the Union.

The broader trajectory of EU enforcement suggests an ongoing process of centralization driven by functional necessity. While implementation deficits continue to exist due to variations in national administrative capacities, political priorities, and legal cultures, scholars have observed a gradual transfer of enforcement authority from the national to the European level[31]. According to this view, the Europeanization of regulatory governance inevitably generates corresponding pressures for the Europeanization of enforcement. As regulatory responsibilities expand at the supranational level, effective implementation increasingly requires stronger coordinating institutions and, in some cases, direct enforcement powers for EU bodies. The emergence of powerful European agencies and enforcement networks can therefore be understood as a form of functional spillover accompanying deeper regulatory integration.

Recent policy developments further illustrate this trend. In April 2025, the European Commission introduced the ProtectEU Internal Security Strategy, which seeks to strengthen the Union's capacity to address terrorism, organized crime, cyber threats, and hybrid security challenges. The strategy emphasizes regular threat assessments, expanded operational capacities for agencies such as Europol and Eurojust, enhanced cybersecurity protections, greater resilience of critical infrastructure, and strengthened partnerships with third countries. It also envisages the development of a European Critical Communication System to facilitate secure information-sharing among national authorities and emergency responders. Collectively, these initiatives demonstrate the Union's commitment to constructing a more integrated and operationally capable internal security framework capable of responding to increasingly complex digital threats[32].

Viewed as a whole, the EU's internal enforcement architecture in the cybercrime domain reflects a sophisticated combination of legal harmonization, institutional coordination, political engagement, and managerial capacity-building. While Member States remain the primary actors responsible for criminal enforcement, the growing role of EU institutions and agencies demonstrates an unmistakable movement toward a more centralized and networked model of governance. This evolution has significantly enhanced the Union's ability to address transnational cybercrime within its internal legal order, while simultaneously laying the foundation for the increasingly assertive extraterritorial dimensions of EU cybercrime enforcement examined in the following sections.

[31] E. MASTENBROEK, *EU Compliance: Still a 'Black Hole'?*, in *Journal of European Public Policy*, 2005, n. 6, pp. 1103-1120.
[32] European Commission, *Commission Presents ProtectEU Internal Security Strategy*, 2025, available at: https://commission.europa.eu/news-and-media/news/commission-presents-european-internal-security-strategy-2025-04-01_en.

4. External Dimension and Normative Projection

The external dimension of EU cybercrime governance is structurally anchored in a combination of multilateral treaty frameworks, regulatory diffusion strategies, and capacity-building instruments that collectively extend the Union's influence beyond its formal jurisdiction. At the centre of this architecture lies the Council of Europe Convention on Cybercrime[33], which has emerged as the principal global reference point for the harmonisation of substantive and procedural cybercrime law[34]. Although the Convention is formally not an EU legal instrument, the European Union and its Member States have played a decisive role in its promotion, consolidation, and global diffusion. As Bartoli observes, the EU has consistently acted as a "norm entrepreneur" in the field of cybersecurity governance, actively encouraging third states to accede to the Convention and to align their domestic legal frameworks with its standards[35]. This engagement has been operationalised through a combination of diplomatic advocacy, technical assistance programmes, and structured cooperation frameworks, particularly in the context of EU external relations and enlargement policy.

This process has produced a gradual but identifiable pattern of normative convergence, whereby non-EU jurisdictions increasingly adopt cybercrime legislation that mirrors the substantive offences and procedural tools embedded in the Budapest framework. Importantly, this convergence does not operate through classical forms of legal coercion or formal hierarchy. Instead, it is facilitated by institutional dependency relationships in which third states rely on EU-supported capacity-building, training programmes, and access to transnational investigative cooperation networks. As Bartoli further notes, the governance of cybercrime and cybersecurity is increasingly characterised by an intertwined ecosystem of actors in which regulatory alignment is incentivised through access to information-sharing mechanisms, operational cooperation, and technical expertise rather than through binding jurisdictional imposition[36]. In this sense, the EU's external influence is better understood as a structured form of regulatory attraction embedded within broader cooperation architectures, rather than as an exercise of traditional external sovereignty.

These dynamics can be conceptualised more precisely through the notion of normative externalisation, which captures the process by which legal and regulatory standards developed within the EU legal order acquire transnational regulatory effects without requiring the formal extension of EU jurisdiction. Unlike classical extraterritoriality, which presupposes the direct application of domestic law to conduct occurring abroad, normative externalisation operates through indirect diffusion mechanisms embedded in international cooperation regimes, mutual assistance

[33] Council of Europe Convention on Cybercrime, 23 November 2001, CETS n. 185.
[34] M. GERCKE, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, II ed., Geneva, 2012.
[35] L. BARTOLI, *Cybersecurity and the Fight against Cybercrime: Partners or Competitors?*, in *European Journal of Risk Regulation*, 2025, no. 2, pp. 498-513.
[36] *Ibid.*

frameworks, and regulatory interdependence. In the cybercrime context, this means that EU-originated standards - particularly those related to criminalisation thresholds, procedural safeguards for electronic evidence, and cross-border investigative cooperation - become embedded in third-country legal systems through iterative processes of alignment and institutional learning.

This form of externalisation is structurally sustained by the EU's broader external governance strategy, which links market access, operational cooperation, and technical assistance to the adoption of compatible regulatory frameworks. As a result, compliance with EU-aligned cybercrime standards often becomes a de facto condition for participation in transnational enforcement networks or for benefiting from EU-funded cybersecurity capacity-building initiatives. Over time, such mechanisms generate a form of regulatory convergence that is both incremental and path-dependent, reinforcing the global circulation of EU legal norms without requiring formal legal transplantation. Consequently, the EU's role in global cybercrime governance is not limited to participation in multilateral treaty regimes but extends to the subtle shaping of regulatory environments beyond its borders through sustained normative projection embedded in institutional practice[37].

5. Functional Extraterritoriality and Private Intermediaries

A defining feature of the contemporary EU cybercrime enforcement model is its structural reliance on private intermediaries as de facto enforcement conduits. In the context of digitally mediated offences, enforcement no longer operates exclusively through classical state-to-state cooperation or territorially bounded investigative action. Instead, it is increasingly channelled through global service providers - most notably cloud infrastructure companies, social media platforms, and communication service providers - that control access to data, metadata, and digital communications essential for criminal investigations. This institutional configuration has been significantly reinforced by the EU's evolving framework for cross-border electronic evidence, particularly the proposed Regulation on European Production and Preservation Orders, which enables judicial authorities to directly request data from service providers regardless of the Member State in which those providers are established[38]. The operational logic of this system is not dependent on physical enforcement within a territory, but rather on the compliance architecture of transnational corporate actors whose infrastructures are inherently global in scope.

Within this framework, enforcement is effectively operationalised through private governance systems rather than direct coercive state action. Once a production or preservation order is issued, compliance is implemented internally by the relevant service provider through its global data management and legal compliance units. This means that

[37] L. BARTOLI, *Cybersecurity*, cit.; M. GERCKE, *Understanding Cybercrime*, cit., pp. 12-15.
[38] European Commission, *Proposal for a Regulation*, cit.

an EU-originating legal request may produce effects across multiple jurisdictions simultaneously, insofar as the provider's internal systems are designed to ensure uniform compliance with legal obligations irrespective of the geographic location of the data subject or the servers involved. As a result, regulatory authority is indirectly projected beyond EU territory through the private ordering mechanisms of multinational digital firms. This development reflects a structural transformation in which states increasingly outsource operational aspects of enforcement to private actors that function as intermediaries in the governance of cyberspace. The effect is not merely procedural efficiency, but a deeper redistribution of enforcement capacity from public authorities to globally networked corporate infrastructures.

This institutional shift gives rise to what may be conceptualised as functional extraterritoriality, namely a form of regulatory projection in which legal effects extend beyond territorial boundaries not through formal assertions of jurisdiction, but through the operational logic of globally integrated private networks. Unlike traditional extraterritorial jurisdiction, which presupposes either territoriality-based exceptions or recognised principles such as nationality, effects doctrine, or universal jurisdiction, functional extraterritoriality does not depend on the legal classification of jurisdictional competence. Instead, it emerges from the structural position of private intermediaries as unavoidable gatekeepers of cross-border data flows. Because digital infrastructures are inherently transnational, compliance obligations imposed on a single corporate entity may generate cascading regulatory effects across multiple jurisdictions simultaneously, even in the absence of formal legal harmonisation among those jurisdictions.

The legal significance of this model lies in its hybrid nature. Enforcement is neither fully domestic—since the relevant data and affected individuals may be located outside the issuing state—nor fully international in the traditional sense, since there is no intergovernmental treaty-based enforcement mechanism mediating the process. Instead, it occupies an intermediate space in which private compliance structures function as operational extensions of public authority. This hybridity complicates established doctrinal distinctions between jurisdiction and enforcement, particularly in the context of cross-border data access and digital surveillance regimes. It also raises important questions regarding accountability, due process, and the allocation of regulatory authority in situations where enforcement outcomes are determined by private actors operating under multiple and potentially overlapping legal obligations.

Legal scholarship has increasingly recognised that such developments challenge the classical bifurcation between prescriptive and enforcement jurisdiction. As Kuner argues, data protection and cross-border digital regulation reveal the inadequacy of traditional jurisdictional categories when applied to globally networked information systems, particularly where enforcement is mediated through private compliance architectures rather than direct state coercion[39]. While prescriptive jurisdiction may remain defensible under established doctrines of territoriality and effects, the enforcement dimension

[39] C. KUNER, *Transborder Data Flows*, cit., pp. 102-105.

generated through private intermediaries introduces a qualitatively different set of legal problems. These include uncertainties regarding the locus of accountability, the fragmentation of procedural safeguards, and the potential circumvention of sovereign regulatory controls through corporate compliance harmonisation. Consequently, the increasing reliance on private intermediaries in EU cybercrime governance not only expands the functional reach of European regulatory standards but also destabilises conventional understandings of jurisdictional authority in international law.

6. Enforcement Jurisdiction and the Problem of Consent

A foundational principle of international jurisdictional law is that enforcement measures undertaken within the territory of another state require either the consent of that state or a clear treaty-based authorization. This principle reflects the broader structure of the international legal order, in which sovereignty operates as both a source of legal personality and a constraint on unilateral enforcement action. The International Court of Justice has repeatedly reaffirmed the centrality of territorial sovereignty as a limiting principle on extraterritorial enforcement, most notably in its consistent articulation of the idea that a state may not exercise its enforcement jurisdiction within the territory of another state without consent, subject to narrowly defined exceptions grounded in international agreement or established legal doctrine[40]. This understanding is deeply embedded in the classical Westphalian model of jurisdiction, which distinguishes between prescriptive jurisdiction (the authority to regulate conduct) and enforcement jurisdiction (the authority to implement and compel compliance), reserving the latter almost exclusively to the territorial state.

At a more foundational level, this consent-based structure reflects what Guzman conceptualises as the "consent problem" in international law, namely the structural difficulty of achieving legal evolution in a system where binding obligations depend on unanimous or near-universal state consent[41]. While consent provides robust protection for state autonomy by allowing each state to opt out of legal change that is perceived as contrary to its interests, it simultaneously generates a systemic status quo bias that inhibits regulatory adaptation. In areas such as cybercrime, where technological developments evolve rapidly and generate transnational externalities, this rigidity becomes particularly pronounced. The result is a structural tension between the efficiency demands of global regulatory problems and the consent-based architecture of international legal obligation.

The EU's emerging cybercrime enforcement framework complicates this traditional model of jurisdiction by introducing forms of indirect enforcement that do not rely on physical presence within foreign territory. Mechanisms such as cross-border production and preservation orders directed at private service providers enable EU judicial or investigative authorities to obtain electronic evidence held or processed outside the Union

[40] J. CRAWFORD, *Brownlie's Principles*, cit., pp. 465-468.
[41] A.T. GUZMAN, *Against Consent*, in *Virginia Journal of International Law*, 2011, no. 4, pp. 747-790.

without necessarily engaging in classical inter-state mutual legal assistance procedures. Although formally addressed to private actors rather than foreign states, such measures may nonetheless produce enforcement effects within the territory of third states, insofar as they require compliance with EU-originating legal obligations that affect data located abroad or subject to foreign regulatory regimes. In this sense, enforcement is operationalised through transnational corporate infrastructures rather than through direct sovereign action, thereby altering the functional distribution of jurisdictional authority in practice.

This development raises significant questions regarding the principle of consent in international law. Traditionally, enforcement action affecting the sovereign domain of another state is legitimate only where it is grounded in that state's consent, typically expressed through treaties governing mutual legal assistance or other forms of judicial cooperation. The EU model, however, increasingly relies on direct engagement with private intermediaries, thereby potentially bypassing the procedural mediation role of the territorial state. While mutual legal assistance frameworks remain formally available, the operational preference for direct requests to service providers may in practice reduce the centrality of inter-state consent as the primary mechanism governing cross-border evidence gathering. This shift does not necessarily constitute a formal violation of international law in each individual case; rather, it reflects a gradual structural reconfiguration of enforcement pathways that may weaken the practical salience of consent-based constraints.

From a functional perspective, such mechanisms are often justified on grounds of necessity, efficiency, and evidentiary volatility. Digital evidence is inherently mutable, easily transferable, and frequently stored across multiple jurisdictions, which makes traditional mutual legal assistance procedures comparatively slow and potentially ineffective in time-sensitive investigations. However, even where these pragmatic justifications are compelling, the normative implications remain contested. The concern is not primarily that EU measures are categorically unlawful under existing doctrine, but that they contribute to a gradual erosion of the inter-state mediation model that has historically underpinned international legal cooperation. As Guzman's analysis of the consent problem suggests, international law already struggles with the tension between consensual legitimacy and functional effectiveness, and the expansion of non-consensual or semi-consensual regulatory mechanisms may further destabilise this balance[42]. In this respect, the EU's cybercrime enforcement architecture illustrates a broader transformation in enforcement jurisdiction, in which the formal requirement of consent is increasingly complemented—and in some contexts partially displaced—by operational systems of compliance embedded in transnational private governance networks. The resulting legal landscape is characterised not by the disappearance of consent, but by its functional relativisation, as enforcement outcomes become increasingly dependent on

[42] A.T. GUZMAN, *Against Consent*, cit.

institutional arrangements that operate alongside, rather than strictly within, traditional consent-based frameworks of international law.

7. Sovereignty in the Digital Legal Order

The contemporary debate on digital sovereignty within the European Union reflects a broader conceptual and structural transformation in the meaning of sovereignty under conditions of technological interdependence and regulatory fragmentation. As Czerniawski argues, the EU's recent political initiatives, including the Berlin Declaration on European Digital Sovereignty, signal a growing awareness of the need to reduce strategic dependencies and enhance autonomous digital capacity, yet they simultaneously reveal a persistent gap between aspirational sovereignty and enforceable regulatory authority[43]. While the Declaration emphasises technological capability, infrastructural investment, and strategic autonomy, it insufficiently integrates the enforcement dimension of sovereignty, namely the capacity to ensure the effective application of EU law vis-à-vis powerful non-EU technology companies that structure the digital environment within the Union. This omission is particularly significant given that sovereignty, in its classical legal sense, is not merely the ability to regulate but the ability to ensure compliance through effective and credible enforcement mechanisms.

Within EU legal scholarship, this tension has been conceptualised as part of a broader regulatory paradigm in which legislative ambition increasingly outpaces enforcement capacity. Von Ditfurth demonstrates that the EU's recent digital legislative framework, including the General Data Protection Regulation, the Digital Services Act, the Digital Markets Act, the Data Governance Act, and the Artificial Intelligence Act, constitutes an integrated regulatory architecture designed to project European standards both internally and externally[44]. These instruments are not merely internal market regulations; rather, they function as components of a broader sovereignty project aimed at shaping global digital governance through what is often described as "Brussels effect" dynamics. However, the effectiveness of this regulatory projection depends critically on the Union's ability to enforce compliance, including against transnational digital platforms whose operational infrastructures lie partially or entirely outside EU territory.

The rise of transnational cyber enforcement mechanisms therefore reflects a deeper structural reconfiguration of sovereignty itself. Rather than being exclusively territorially bounded, sovereignty increasingly operates through participation in interconnected governance networks that include supranational institutions, national regulators, and private intermediaries. As von Ditfurth further notes, the EU's pursuit of digital

[43] M. CZERNIAWSKI, *EU's Digital Sovereignty and the Rights-Based Imperative: Linking Enforcement, Competences and Fundamental Rights*, 3 December 2025, available at: https://verfassungsblog.de/digital-sovereignty-and-the-rights/.
[44] L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act: Eine Analyse der europäischen Regulierung von B2B-Datenvermittlungsdiensten*, Berlin/Boston, 2024.

sovereignty should be understood not as a return to classical Westphalian autonomy, but as an attempt to reconfigure regulatory authority within a globally networked environment in which legal control is exercised through a combination of legislative reach, market access conditions, and compliance-based governance mechanisms[45]. In this sense, sovereignty becomes relational and infrastructural rather than purely territorial, embedded in the capacity to shape and coordinate transnational regulatory ecosystems.

In the EU context, this relational model of sovereignty is institutionalised through a partial pooling of authority among Member States and a partial externalisation of regulatory functions through cooperative and transnational regimes. Enforcement of key digital regulatory instruments, including data protection and platform governance rules, relies heavily on national supervisory authorities that operate within a multi-level governance structure. As Czerniawski emphasises, this fragmentation generates structural constraints on the EU's ability to act as a fully sovereign digital actor, particularly where enforcement depends on uneven administrative capacities and divergent political priorities among Member States[46]. At the same time, the EU's external projection of regulatory authority depends on structured reciprocity and consent-based cooperation mechanisms, including international agreements, adequacy decisions, and regulatory dialogues with third countries. Where such consent-based frameworks are absent or weakened, the legitimacy and effectiveness of enforcement actions become increasingly contested.

The digital environment further intensifies these tensions by embedding regulatory compliance within privately governed infrastructures that operate transnationally. Enforcement is increasingly mediated through platform governance systems, cloud service architectures, and data processing infrastructures controlled by multinational corporations, which function as de facto regulatory intermediaries. As a result, sovereignty is no longer exclusively challenged by other states within a classical interstate system, but is also continuously negotiated within corporate governance structures that operate across multiple jurisdictions simultaneously[47]. This development complicates traditional doctrinal understandings of sovereignty, as regulatory authority becomes dependent on the compliance decisions of private actors whose operational logic is shaped by overlapping legal regimes and risk management strategies rather than by a single sovereign command structure. Within this framework, legitimacy concerns become particularly acute when enforcement mechanisms extend beyond structured consent frameworks. The relational model of sovereignty presupposes a baseline of institutional reciprocity, legal coordination, and shared normative commitments. However, when enforcement is exercised through extraterritorial regulatory reach or through private intermediary compliance structures without clear consent from affected jurisdictions, the foundational assumptions of international legal order are placed under strain. Czerniawski highlights that without effective enforcement capacity, including vis-à-vis non-EU digital

[45] *Ibid.*
[46] M. CZERNIAWSKI, *EU's Digital Sovereignty*, cit.
[47] L. DENARDIS, *The Global War for Internet Governance*, New Haven, 2014, pp. 127-145.

actors, the EU's claims to digital sovereignty risk remaining declaratory rather than operational, thereby undermining both its regulatory credibility and its constitutional commitments under Article 2 TEU and the Charter of Fundamental Rights[48]. Consequently, digital sovereignty in the EU legal order must be understood as a multidimensional construct that integrates legislative competence, enforcement capacity, and normative legitimacy. It is not sufficient for the Union to articulate comprehensive regulatory frameworks; it must also ensure their effective and consistent application within a transnational digital environment characterised by infrastructural interdependence and private governance authority. As von Ditfurth concludes, the EU's digital sovereignty project is ultimately an exercise in regulatory constitution-building within a globalised technological order, in which sovereignty is measured not only by formal competence but by the practical ability to shape and enforce the conditions under which digital actors operate[49].

8. Normative Evaluation: Between Effectiveness and Legal Constraint

The European Union's cybercrime enforcement model exhibits a pronounced normative ambivalence that reflects a structural tension at the heart of contemporary transnational governance. On one level, the EU has developed a highly sophisticated enforcement architecture capable of addressing the inherently cross-border nature of cybercrime, which routinely eludes territorially confined investigative and prosecutorial systems. Instruments such as harmonised substantive criminal law under Directive 2013/40/EU, coupled with emerging mechanisms for cross-border access to electronic evidence and the operational coordination of Europol and Eurojust, significantly enhance the Union's capacity to respond to digitally mediated criminal activity[50]. From a functional perspective, this architecture represents a necessary adaptation to the structural characteristics of cyberspace, where data flows, perpetrators, victims, and infrastructures are dispersed across multiple jurisdictions simultaneously. In this sense, the EU model can be interpreted as a pragmatic response to the inadequacies of classical territorially bounded enforcement systems. However, this functional effectiveness comes at a normative cost. The increasing reliance on extraterritorial effects, direct cross-border data requests, and private intermediary compliance mechanisms risks stretching established jurisdictional doctrines beyond their conceptual and doctrinal limits. As Kuner has observed in the context of global data governance, the evolution of digital regulation increasingly challenges the traditional separation between prescriptive and enforcement jurisdiction, particularly where regulatory effects are produced through distributed

[48] M. CZERNIAWSKI, *EU's Digital Sovereignty*, cit.
[49] L. VON DITFURTH, *Datenmärkte*, cit.
[50] Directive 2013/40/EU of the European Parliament and of the Council, *on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*, cit., arts. 3-7; E. CASEY, *Digital Evidence*, cit.

technological infrastructures rather than direct sovereign action[51]. In the EU cybercrime context, this tension becomes particularly visible where enforcement outcomes are generated without physical enforcement action in the territory of another state, but nonetheless produce legal and practical consequences that extend beyond EU borders. The result is a form of regulatory projection that is difficult to categorise within conventional jurisdictional frameworks, thereby raising questions about doctrinal coherence and systemic legitimacy.

The legitimacy of extraterritorial legal effects in international law ultimately depends on a careful balance between functional necessity and structural restraint. International law has historically accommodated limited forms of extraterritoriality through recognised doctrines such as nationality jurisdiction, effects-based jurisdiction, and universal jurisdiction in exceptional circumstances. However, these exceptions remain embedded within a broader normative architecture grounded in sovereignty, non-intervention, and consent. As Guzman argues in his analysis of the "consent problem," the international legal system is fundamentally structured around state consent, which both enables legal stability and constrains regulatory evolution[52]. While this consent-based structure may generate inefficiencies in addressing collective action problems such as cybercrime, it remains a core legitimating principle of international law. Any expansion of extraterritorial enforcement must therefore be assessed against its compatibility with these foundational constraints, rather than solely on the basis of functional effectiveness.

At the same time, the International Court of Justice has consistently reaffirmed that territorial sovereignty constitutes a central limiting principle on unilateral enforcement action, reinforcing the idea that enforcement jurisdiction cannot be exercised within the territory of another state without consent or a recognised legal basis[53]. This doctrinal baseline underscores the importance of maintaining a clear distinction between lawful regulatory effects and impermissible encroachments on sovereign authority. The challenge posed by the EU cybercrime model is not that it explicitly rejects these principles, but that it operates in a regulatory space where enforcement effects are increasingly decoupled from territorial presence, thereby rendering the application of traditional sovereignty-based constraints more complex and, at times, less determinate.

The EU's approach thus illustrates both the transformative potential and the institutional fragility of legal adaptation in the digital age. On the one hand, it demonstrates that effective cybercrime governance increasingly depends on transnational coordination structures that integrate supranational institutions, national authorities, and private intermediaries into a single operational ecosystem. On the other hand, it reveals that the normative foundations of these structures remain only partially articulated within existing frameworks of international law. While instruments such as the Budapest Convention provide an important baseline for cooperation and harmonisation[54], they do

[51] C. KUNER, *Transborder Data Flows*, cit., pp. 102-105.
[52] A.T. GUZMAN, *Against Consent*, cit.
[53] International Court of Justice, *Corfu Channel (United Kingdom v. Albania)*, judgment of 9 April 1949.
[54] M. GERCKE, *Understanding Cybercrime*, cit., pp. 12-15.

not fully resolve the deeper tensions between effectiveness, sovereignty, and consent that arise in contemporary enforcement practice. As Bartoli notes in her analysis of cybersecurity governance, the increasing interdependence between cybersecurity and cybercrime enforcement further complicates institutional coherence, as overlapping regulatory agendas generate both synergies and jurisdictional ambiguities[55]. Consequently, the EU's cybercrime enforcement model should be understood as a transitional legal formation situated between traditional sovereignty-based enforcement and emerging networked governance structures. Its normative strength lies in its capacity to respond to technologically complex and transnational threats; its normative vulnerability lies in the partial disembedding of enforcement from classical principles of territorial sovereignty and consent. The central challenge for international law is therefore not merely to accommodate new forms of effectiveness, but to develop a more explicit and coherent account of the conditions under which such effectiveness can be reconciled with the structural constraints that continue to define the legitimacy of the international legal order.

9. Conclusion

This article has examined the European Union's external dimension in the cross-border fight against cybercrime and assessed its compatibility with the limits of extraterritorial jurisdiction under general international law. It has demonstrated that cybercrime, as a structurally transnational phenomenon, destabilises traditional jurisdictional assumptions by dispersing perpetrators, victims, and evidentiary infrastructures across multiple legal orders. In response, the European Union has progressively developed an increasingly integrated framework for cross-border criminal cooperation in cyberspace, encompassing mechanisms for the preservation and cross-border access to electronic evidence, enhanced operational coordination between EU and third-state law-enforcement authorities, and the external projection of EU regulatory and procedural standards in cybercrime investigation and judicial cooperation. The analysis has shown that these developments reflect an emerging model of functional extraterritoriality embedded within the EU's external action in the field of criminal justice. Rather than relying exclusively on classical forms of territorial enforcement or formal intergovernmental cooperation, the EU increasingly operates through hybrid mechanisms that combine regulatory harmonisation, direct engagement with private intermediaries, and structured cooperation frameworks with third states. This configuration enables enforcement effects to extend beyond EU territory in ways that are not always reducible to traditional categories of prescriptive or enforcement jurisdiction. While certain dimensions of this framework may be accommodated within established bases of international jurisdiction, including the effects doctrine and the protection of

[55] BARTOLI, *Cybersecurity*, cit.

essential interests, its operational logic frequently relies on indirect enforcement pathways that do not neatly correspond to conventional jurisdictional paradigms.

At the same time, the study has highlighted that the increasing reliance on such mechanisms raises important legal and normative questions under general international law. In particular, where cross-border access to electronic evidence and cooperation with private service providers generate de facto enforcement effects beyond EU territory without the explicit consent of affected third states, concerns arise regarding the preservation of sovereignty and the procedural integrity of inter-state cooperation. As international law remains fundamentally structured around consent-based limitations on enforcement jurisdiction and the principle of territorial sovereignty, these developments expose tensions between the operational demands of cybercrime control and the doctrinal constraints of the existing legal.

Against this background, the article concludes that the European Union has become a central actor in shaping the emerging global architecture of cybercrime enforcement. Through its internal legal integration and external normative projection, the EU significantly contributes to the development of transnational standards and practices in cybercrime governance. However, this expanding cross-border reach simultaneously reveals unresolved structural tensions between the effectiveness of transnational crime control and the legal limits imposed by state sovereignty and consent under international law. The EU model thus occupies an ambivalent position: it is both a driver of functional innovation in global cybercrime enforcement and a site where the doctrinal boundaries of extraterritorial jurisdiction are increasingly tested and reconfigured.

ABSTRACT: This article examines the European Union's external dimension in the cross-border fight against cybercrime and assesses its compatibility with the limits of extraterritorial jurisdiction under general international law. Cybercrime, as a structurally transnational phenomenon, challenges traditional jurisdictional doctrines due to the fragmentation of offenders, victims, and digital infrastructures across multiple legal orders. In response, the European Union has developed an increasingly integrated framework for cross-border criminal cooperation in cyberspace. This framework includes mechanisms for the preservation and cross-border access to electronic evidence, enhanced operational cooperation between EU and third-state law enforcement authorities, and the external projection of EU standards in cybercrime investigation and judicial cooperation. The article argues that these developments reflect an emerging form of functional extraterritoriality embedded within the EU's external action in the field of criminal justice. While certain measures may be justified under established bases of prescriptive jurisdiction in international law, such as the effects doctrine and the protection of essential interests, other practices raise concerns where they generate de facto enforcement effects beyond EU territory without clear consent of affected third states. Methodologically, the analysis is based on doctrinal interpretation of international

jurisdictional principles and relevant EU legislative and cooperative instruments. The article concludes that the EU has become a central actor in shaping global cybercrime enforcement architecture, yet its expanding cross-border reach exposes unresolved tensions between effective transnational crime control and the constraints of state sovereignty under international law.

KEYWORDS: Cybercrime enforcement – European Union – Extraterritorial Jurisdiction – Sovereignty in International Law – Transnational Criminal Cooperation.