European Journal of Risk Regulation (2025), **16**, 498–513
doi:10.1017/err.2025.31

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Cybersecurity and the Fight against Cybercrime: Partners or Competitors?

Laura Bartoli

Department of Legal Studies, University of Bologna, Bologna, Italy
Email: laura.bartoli2@unibo.it

Abstract

In the early 2000, cybersecurity breaches were classified as "Internet crimes" and therefore managed through the tools of the criminal justice system. The Budapest Convention on Cybercrime forged new incriminating provisions and new procedural guidelines, updating the categories of criminal law and criminal procedure for the digital age. This style, unfortunately, has proved to be insufficient. To face the growing number of threats, the EU has shifted towards a much more preemptive, administrative-law-based approach to cybersecurity, with a view to protect critical infrastructure and industries from disruptive attacks. The criminal layer, however, has not been replaced: the relevant, international instruments are still there, and they have been recently extended to cover more ground. The essay will examine the new wave of legislation on cybercrime such as the United Nations Cybercrime Treaty, trying to identify the interactions and the frictions between two different contrast strategies to abusive cyber operations.

Keywords: Cybercrime; Cybersecurity; UN Convention on Cybercrime

I. Introduction

An ever-increasing number of threats come from the digital world, which influences everyone's life off-screen. Critical infrastructure can be sabotaged digitally[1]; communication systems can be shaken through cyberattacks[2]; elections can be manipulated by cyber-espionage[3]; land attacks can be aided by remotely sabotaging the alert systems.[4] The impact of digital malfeasance is impressive: in 2024, the global cost of cybercrime will reach 9,5 trillion $, making it the third global economy after the United States and China.

[1] See SK Venkatachary, J Prasad, A Alagappan, LJB Andrews, RA Raj and S Duraisamy, "Cybersecurity and Cyber-Terrorism Challenges to Energy-related Infrastructures – Cybersecurity Frameworks and Economics – Comprehensive Review" (2024) 45 International Journal of Critical Infrastructure Protection, <https://www.sciencedirect.com/science/article/abs/pii/S1874548224000180> (last accessed 14 April 2025).

[2] D Antonov and A Osborn, "Hacker Attack Disrupts Russian State Media on Putin's Birthday," 8 October 2024 <https://www.reuters.com/technology/cybersecurity/russian-state-media-company-hit-by-unprecedented-cyberattack-kremlin-says-2024-10-07/> (last accessed 14 April 2025).

[3] G Thrush and DE Sanger, "U.S. Charges Iranians with Hacking Trump Campaign," 27 September 2024, available at <https://www.nytimes.com/2024/09/27/us/politics/iran-hacking-trump-campaign.html> (last accessed 14 April 2025).

[4] M Schwirtz, "U.S. Indicts 2 Linked to Oct. 7 Cyberattack on Israeli Warning System," 18 October 2024, available at <https://www.nytimes.com/2024/10/18/world/middleeast/anonymous-sudan-cyberattack-indictment.html#:~:text=Linked%20to%20Oct.7%20Cyberattack%20on%20Israeli%20Warning%20System,as%20the%20Hamas%20attack%20unfolded> (last accessed 14 April 2025).

According to the same estimate, the impact is projected to rise by 15% per year, reaching 10,5 trillion $ by 2025.[5]

This increase and the variety of threats prompted a shift in the institutional response. The European Union in particular has taken up a prominent role in the fight for cybersecurity, aiming at reducing disparities across the digital single market and reaching a common, high standard of security for institutions, infrastructure, companies, and individuals. To achieve these results, the EU has issued a growing number of directives and regulations: it has given a clear, permanent mandate for ENISA,[6] and it has imposed a set of security requirements for products with digital elements.[7] It has proposed schemes to issue cybersecurity certificatins to products and services,[8] as well as a joint solidarity structure to prevent, analyze, and respond to attacks.[9] All these initiatives have been based on the need to reduce fragmentation among EU Member States, to perfect the single market (Article 114 TFEU), and to ensure the competitiveness of European companies (Article 173 TFEU).

This recent wave has left aside a traditional tool in the fight against cyber threats: criminal law and the criminal justice system at large. Even repressive policies have been moving away from the traditional, criminal punishment, as the European Union has come to impose sanctions on individuals allegedly responsible for cyber-attacks.[10] And yet, almost every conceivable cyber threat[11] is described by an incriminating provision and has the potential to trigger a criminal investigation.

This essay will examine the interplay between the two tiers of legislation, starting with a historical perspective on the emergence and development of criminal law in the digital domain. It will then delve into the reasons why the criminal justice system has ceased to be the preferred option when it comes to countering cyber threats and, finally, it will examine some new instruments and strategies aimed at revamping its effectiveness. I will finally articulate a proposal aimed at creating stronger synergies between the two domains.

II. From punch card attacks to the Budapest convention

As new technologies emerge, misuse soon follows, and the history of ICT is no exception. With a means of accessing more and more information, malign actors figured out ways to

[5] Cybersecurity Ventures, "2023 Annual Cybercrime Report," available at <https://www.esentire.com/resources/library/2023-official-cybercrime-report > (last accessed 14 April 2025).

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L151/15 (also known as "Cybersecurity Act").

[7] Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) n. 168/2013 and (EU) 2019/1020, and Directive (EU) 2020/1828 [2024] OJ L 2024/2847 (also known as Cyber Resilience Act).

[8] Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services COM(2023) 208.

[9] Proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents COM(2023) 209, currently under negotiations between the EU Parliament and Council.

[10] See Y Miadzvetskaya, "EU Sanctions in Response to Cyber-Attacks as Crime-Based Emergency Measures" (2024) 54 in Computer Law & Security Review, <https://www.sciencedirect.com/science/article/abs/pii/S0267364924000773> (last accessed 14 April 2025). For an overview beyond the EU see A Moiseienko, "Crime and Sanctions: Beyond Sanctions as a Foreign Policy Tool" (2024) 25 German Law Review 17, which argues that the target sanctions, as used today, are "a criminal justice tool in everything but the name" (p 18).

[11] The Cybersecurity Act defines "cyber threat" as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons": Article 2 n. 8, Cybersecurity Act.

use networks to their advantage. Abusive operations started as soon as the technology existed, and they evolved together: the first cyberattack dates back to 1962, and it was performed via punch card to (successfully) steal all the passwords that would grant access to the MIT computer system.[12] In the first manual on computer crime, published in 1979, the concern is palpable: in the span of the previous 8 years, the reported cases were already 669,[13] but the majority of incidents would not be reported to the authorities. Back then, prosecutors would "frequently refuse to accept the cases for a variety of reasons, including their lack of understanding of the technology [...]. On the other hand, prosecutors and investigators indicate that victim's records and documentation of crimes associated with computers in the business community are inadequate for effective prosecution."[14]

The first laws and guidelines to fight "cybercrime" were developed in that environment, with two main aims: reducing "the incidence of any type of crime in which a knowledge of computer technology is needed to understand the intentional acts that result in losses"; and successfully prosecuting the perpetrators.[15] This new avenue for antisocial behavior required new incriminating provisions, new methods of investigation, and a specific trial strategy. In the late 1970s and during the 1980s, a growing number of states criminalized conduct such as illegal access to data; illicit interception; damaging of data; and forgery of digital records. Some old notions, such as documents, where refurbished and newly defined to include also their digital counterparts[16]. Criminal law, however, was the "weapon of choice": it was perceived as being the proper tool to update and extend, to contain the phenomenon.

The effort was welcome, but not sufficient. As computers started to enter private homes and the World Wide Web started to be more and more available, the devices were set to be ever more connected and numerous, multiplying the opportunity for digital misbehavior.[17] Cybercrime changed accordingly: a growing number of individuals had first-hand access to computers, hence the number of potential targets increased, and technical ability ceased to be the only relevant factor. Social engineering became a key component of the first organized phishing campaigns, that targeted the vulnerabilities of the users as well as those of the machines. Such operations became the most common and the most profitable in less than a decade, bringing danger to every doorstep.

On the legal front, the difficulties multiplied. The number of incidents was growing, but the investigation was becoming more difficult: an internet connection was enough to elude borders and complicate the inquiry. The need for a shared dictionary and better coordination emerged soon, and the Council of Europe was the first institution to rise to the challenge. In 1997, its Committee of Ministers established the Committee of Experts on Crime in Cyberspace (PC-CY), which received the mandate to draft an international convention on the subject. From its initial stages, the project was meant to be more than a regional agreement. The United States of America, Canada, Japan, and South Africa were

[12] For a richer story of the most notable early threats, see European Commission, Joint Research Center, *Cybersecurity, Our Digital Anchor. A European Perspective* (Luxembourg, Publications Office of the European Union 2020) 13 ff.

[13] U.S. Department of Justice, "Computer Crime. Criminal Justice Resource Manual" (1979) 3 available at <https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crime-criminal-justice-resource-manual> (last accessed 14 April 2025).

[14] Ibid., p 2.

[15] Ibid, p 2.

[16] For a detailed analysis of the early legislation on computer related crimes see: S Schjølberg, *The History of Cybercrime: 1976–2016* (Norderstedt, Books on Demand 2017) 23 ff.

[17] For more details, see G Stratton, A Powell and R Cameron, "Crime and Justice in Digital Society: Towards a 'Digital Criminology'?" (2017) 6 II International Law Journal of Crime Justice and Social Democracy 19.

also called to the negotiating table: the global dimension of cybercrime was emerging, and broadening the scope as much as possible seemed like an essential trait of a functioning agreement.[18]

The Budapest Convention on Cybercrime was adopted in 2001 and has been an important milestone. It has been drafted to be flexible enough to serve as a widespread guideline – the Convention has currently seventy-six parties[19] – and it has been a fundamental tool to harmonize criminal law and to raise awareness on topics that were still seen as somewhat unusual, such as the correct gathering and handling of digital evidence.

The Convention contains a set of substantive law provisions, addressing the need for a common understanding of what conducts should be criminalized in the cyber realm. The provisions cover four main areas. The first one details the offences against the confidentiality, integrity and availability of computer data and systems, which the explanatory report to the Convention calls "the basic threats"[20] such as illegal access, data interference, system interference and misuse of devices. These infringements have become the "ground zero" of cybercrime: they are indeed the first situations that have been criminalized across borders, and they are the most relevant also in the domain of cybersecurity, as they aim to preserve the integrity of all ICT systems.[21]

The other areas respond to a different logic, at least in part. They do not focus on the integrity of information and systems *per se*, but on "ordinary" crimes that could find a new dimension online. The second one addresses the most widespread "computer-related crimes": computer-related forgery and computer-related fraud. The drafters of the Budapest convention were fully aware that most States had already criminalized such behaviors, online or offline: the added value of these provisions did not reside in their novelty but in their capability to provide a blueprint for harmonization. The Convention then moves to the criminalization of offences related to child pornography, which are defined as a "content-related" offence. The fight against the sexual exploitation of children online has been a signature issue, as technology has made victims more accessible to predators and has made it easier for criminals to groom or persuade children under false pretenses – i.e.: reaching out to them online by pretending to be a young girl in search of new friends[22] – and has simplified the circulation of illicit material. Lastly, the convention focuses on the offences related to the infringement of copyright, aimed at protecting

[18] For a full account of the drafting procedure and for first-hand testimonies see: Council of Europe, *Convention on Cybercrime. Special Edition Dedicated to the Drafters of the Convention (1997–2001)* (Document and Publication Production Department 2022) available at <https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e> (last accessed 14 April 2025).

[19] With twenty more states invited to sign, or being already signatories: the full list is available at <https://coe.int/en/web/cybercrime/parties-observers> (last accessed 14 April 2025).

[20] Council of Europe, "Convention on Cybercrime. Protocol on Xenophobia and Racism. Second protocol on Enhanced Co-operation and Disclosure of Electronic Evidence – Explanatory Reports and Guidance Notes" (2023) forty-four available at <https://rm.coe.int/prems-105223-gbr-2023-convention-cybercrimininalite-a5-web-4-/1680ae7118> (last accessed 14 April 2025).

[21] For the EU Member States, the criminalization of these actions has been reaffirmed by the legislative choices of the Union: see Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. The directive is explicitly tied to the Budapest convention by recital n. 15, which states that the incriminating provisions of the text intend to build on the Convention, and that "completing the process of ratification of that Convention by all Member States as soon as possible should be considered to be a priority."

[22] For instance, see the case of Alexander McCartney, a UK national that impersonated a 13-year-old girl on social media to befriend young girls all over the world of an average age of 10 to 12 years of age. After having established a friendship with his victims, he would ask for nude pictures and, upon receipt, blackmail the victims into producing more pornographic material that he would record and share. McCartney has been convicted thanks to the evidence found in 64 devices; he has been sentenced to life in prison. See F Murray and C Campbell, "Catching the Catfish Killer: Phone Calls and 64 Seized Devices Snared Child Sex Abuser," 26 October 2024 available at <https://www.bbc.com/news/articles/crejr8grr01o> (last accessed 14 April 2025).

intellectual property in an age of increasing importance of intangible goods – and increasing ease in appropriating and sharing them illicitly.[23]

The other two sections of the Budapest Convention on Cybercrime contain procedural provisions focused on the correct gathering and handling of digital evidence and the mutual legal assistance (MLA) procedures needed to ensure the repression of cybercrime across borders.

As for the procedural provisions, they were conceived as a much-needed update to investigation techniques. As ICT was being used to perpetrate crimes, investigators needed to keep up, hence the Convention provided the basic notions and tools for an accurate digital investigation. Article 19 distinguished between data and physical storage for searches and seizures. It also provided for rules on the expedited preservation and disclosure of content and traffic data (Articles 16 and 17), on production orders (Article 18), on the live monitoring of traffic data, and on the interception of content data (Articles 20 and 21). This apparatus had the immediate effect of elevating forensically sound interventions to "best practice": the somewhat mixed approaches of the past were not swept away,[24] but the Budapest Convention was instrumental in raising awareness on the correct handling of digital material.

The heftier part of the Convention, however, deals with MLA (Articles 23–45), to regulate cooperation among different nations' law enforcement agencies, prosecution services, and judiciaries. The transnational aspects of cybercrime, after all, were one of the main reasons to resort to an instrument such as an international treaty in the first place: it is only natural that the final text was specially devoted to ensuring smooth and swift cross-border cooperation.[25] The text provides for a comprehensive set of general principles on MLA – including principles on extradition – as well as specific provisions that regulate the duty to help preserve, intercept, and access data abroad. Finally, the Convention sets up a 24/7 network, a system of national contact points that should ensure continuous and immediate assistance to foreign investigators, to build a permanent, reliable structure to fast-track cybercrime cases and quickly obtain aid from other nations. Among these provisions, Article 32 stirred controversy. It allows a party to access information that is either publicly available or stored in foreign territory without the authorization of other parties. Russia took issue with the provision, claiming it would infringe on state sovereignty by allowing unauthorized cross-border investigations. On these grounds, Russia has always refused to join the Budapest Convention.[26]

III. Mismatch of notions?

The Budapest Convention on Cybercrime has served as a watershed: it has harmonized legal frameworks, raised awareness of innovative investigation techniques, and underlined

[23] On the importance of copyright and child pornography related offences for the development of case law and jurisprudence on "cybercrime" see A Monti, "Rules of (Digital) Evidence and Prosecution's Actual Needs. When the Law Falls Behind Technology" in A Armando, R Baldoni and R Focardi (eds), *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*, (Italy, Venice 2017) p 167.

[24] Ibid, p 17, points out that the Convention generated "hype in the computer forensics community," but did not transform daily practice. Italian courts continued accepting forensically unsound evidence and did not produce specific exclusionary rules to ensure the reliability of digital material.

[25] As stated in the preamble, the drafters acted in the belief that "an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters."

[26] See "Russia Unveils Bid to Fight Cyber Crime and Samsung Pay Faces Patent Issue," 30 July 2021 available at <https://tass.com/pressreview/1320973> (last accessed 14 April 2025). For a western perspective see: M Page, "The Hypocrisy of Russia's Push for a New Global Cybercrime Treaty', 7 March 2022 available at <https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty> (last accessed 14 April 2025).

the need for close and quick cooperation almost a decade before the acknowledgment of cybersecurity as a forefront issue, at least for the European Union. Moreover, it has been at the center of countless activities held by the Council of Europe's Cybercrime Programme Office, which has been hosting capacity-building programs and assisting countries in strengthening legislation, training, and policies related to cybercrime, as defined by the Budapest Convention. To make a long story short, the Budapest convention is widespread, highly regarded, and well-supported.

And yet, despite its success, its impact on cybersecurity has been marginal. Cyberattacks have been multiplying; their impact – economic and societal – has been growing, and it is projected to rise further. The situation might appear paradoxical, but it finds both theoretical and practical explanations.

Firstly, the Budapest Convention on Cybercrime is somewhat of a general tool, too unfocused to be effective from a cybersecurity perspective. The international instrument – and the national provisions that derived from it – is concerned with a multitude of problems: it is aimed at bridging an awareness gap on a wide variety of harmful behaviors that could manifest differently, or at a different intensity, thanks to the developments in communication technology.[27] In other words, its scope is much broader than the strict "cybersecurity" area, hence: it is not specifically concerned with the question of how to preserve confidentiality, integrity, and the availability of information, which is the main essence of cybersecurity.[28] "Cybercrime" has to cover a somewhat vaster, vaguer area, as the notion is not clearly defined[29]; it encompasses a whole range of harmful situations, that have been classified in countless ways by criminologists: according to one account, cybercrime should be classified into at least three categories.[30] The first one encompasses the so-called "crimes against the machine," such as unauthorized access to computer systems or information. The second one provides for the crimes committed "using the machine," such as fraud, theft and extortion. The last one includes the "crimes in the machine," which corresponds to the "content-related" section of the Budapest Convention: it includes extreme content such as child pornography, hate speech and radical material, eg, terrorist propaganda. Other authors have proposed different arrangements,[31] and the classifications are bound to grow ampler and more complex, but they do not seem to converge with the categories that are employed to classify cybersecurity threats.[32] As an increasing number of

[27] The issue of whether technology impacts the quality or only the quantity of certain criminal activities in a controversial one. For a recent reconstruction, see M David, *Networked Crime. Does the Digital Make a Difference?* (Bristol, Bristol University Press 2023).

[28] Such is the definition of information security according to the standard ISO/IEC 27000:2018, which is also referred to by the standard ISO/IEC 27032:2023 in the definition of internet security. According to the previous version of the guidelines, the "preservation of confidentiality, integrity and availability of information in the cyberspace" was the very definition of cybersecurity (ISO/IEC 27032:2012). For a brief critique of the definition, see European Commission, Joint Research Center, "Cybersecurity, Our Digital Anchor" (12) 16, which states that "it is impossible to address cybersecurity in absolute terms."

[29] So much so that according to DS Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2nd ed., Cambridge, Polity 2024) 13, the term "cybercrime" is "largely an invention of the media," deprived of "any specific reference in point of law." The view highlights the vagueness of the notion, but it is not entirely correct: both the Budapest Convention and the draft UN Convention finalized in July 2024 (A/AC.291/L.15) have the term in their title. It does not have a specific, legally defined significance, but it is also not entirely unrelated to the legal world.

[30] DS Wall, *Cybercrime* (27) 53 ff.

[31] See for instance of A Lavorgna, *Cybercrimes. Critical Issues in a Global Context* (London, Macmillan-Red Globe Press 2020) which suggests a more articulated division. She categorizes cybercrimes in: (1) crime against devices; (2) crimes against persons; (3) crimes of deception and coercion; (4) market-based crimes and crimes against property; (5) political offences. Another one can be found in the Crown Prosecution Service's, "Cybercrime – Prosecution Guidance" last updated on 15 July 2024 available at <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> (last accessed 14 April 2025).

[32] See ENISA, *ENISA Threat Landscape 2024* (September 2024) available at <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (last accessed 14 April 2025) 10, which uses labels such as "threats against

human activities display a digital component, as technology changes, the very same notion of "cybercrimes" is bound to change, encompassing more reproachable conducts and stigmatizing new digital harms. The same goes for the investigation techniques, that were once used in a small fraction of cases, where the digital dimension was inevitable. Nowadays, it is rare to encounter a criminal case that does not require the forensic copy of a computer; the decryption of a cellphone; or the authentication of some messages. Unexpectedly, the Budapest convention has done more to raise awareness of the investigation techniques deployed in the everyday work of law enforcement than for cybersecurity in a stricter sense.

From a cybersecurity perspective, this can lead to particularly dysfunctional consequences: the early warnings of potential cyberattacks come from crimes such as illicit access or misuse of data, that tend to be treated as minor cases (if they are treated at all). They can occur at distressing rates, but, on their own, they do not seem to be so harmful to take priority over other infringements. From the observatory of law enforcement agencies, phenomena like the sexual exploitation of children or big frauds deserve to be treated with the utmost urgency – and understandably so. Chances are that the mere crimes "against the machines" risk being left behind by the criminal justice system until they have been brought to more severe consequences, which would make them impossible to ignore.[33]

IV. A crisis of effectiveness

Let us assume that a cybercrime has occurred and that it has been harmful enough to be caught by the authorities' radar. Let us assume it has been duly investigated and that there is a reasonable assumption regarding the identity of the perpetrator. Normally, the authorities would go forward with the process, formalizing charges and/or arresting the suspect according to the legal framework that the investigators are operating under.

If the accused happens to be on the territory of the state, the law enforcement agencies will be perfectly self-sufficient. One example will suffice: an Italian 24-year-old has been recently placed in precautionary detention, as he is accused of having repeatedly hacked the servers of the Italian Ministry for Justice, as well as almost fifty individual accounts of public prosecutors. He was allegedly able to exfiltrate dossiers and to directly follow the development of the case that was being built against him, so much so that the lead prosecutor declared that the investigative team started communicating only with handwritten notes: the old-fashioned paper letters were much harder for a skilled hacker to intercept.[34] The investigators, eventually, identified the hacker; they discovered where

availability" to describe attacks such as DDoS and ransomwares; and "threats against data" to describe "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" – borrowing the definition from the GDPR notion of personal data breach as defined in Art 4, n 12. Other categories include information manipulation (such as misinformation campaigns), social engineering, and malwares.

[33] This issue is known in criminology as the "*de minimis* trap": if the harm provoked by an online, illegal conduct is not perceived as intense enough, the authorities could be tempted to let the case slide, as time and resources could be better spent on other fronts. The cumulative or long-term impact of these infringements, though, could be huge: gaining access to one account might *per se* be practically innocuous, but if the user connects to a wider net – which is almost always the case – the harm could escalate fast: on the topic see DS Wall, *Cybercrime* (27), p 177: "the problem with cybercrime is that, despite the dramatic media image, at the end of the day, like fraud, cybercrime "does not bang, bleed or shout" and does not grab the political agenda enough to also grab the funding." A Lavorgna. *Cybercrimes* (29) ch 9: "modern policing institutions have been designed to deal effectively with low-volume, high-impact crime and are profoundly hampered when it comes to processing cybercrimes, which are often high volume (even if low impact)."

[34] N. Piantadosi, "Hacker buca il Ministero della giustizia, rubati dati Segreti," 2 October 2024 available at <https://www.ansa.it/campania/notizie/2024/10/02/hacker-buca-ministero-giustizia-rubati-dati-segreti_45e37ce9-3ae3-474c-9311-f8f4e274644d.html> (last accessed 14 April 2025).

he lived and followed through as they would have in any other case: upon the authorization of a judge, they arrested the suspect, searched the premises and they seized all relevant material that they could find – in this case: several terabytes of digitally stored information, as well as millions of digital assets. The suspect in this case has been formally charged and he will stand trial in Italy.

Often, however, things are not so easy. The nature of networks, and the internet in particular, makes it all too easy to attack systems that are located outside the nation, hence, outside the jurisdiction, beyond the physical reach of the law enforcement agency that has investigated the crime. At that point, the law enforcement agencies encounter two different types of hurdles. First, the investigation can be hindered, and the precise responsibility of an individual can become more difficult to ascertain. According to the 2024 ENISA Threat Landscape, 34 per cent of threats can simply not be attributed[35] – not to an individual, a company, or a group.

Even when investigators manage to at least identify the area from which the attack came, cooperation is not always smooth. LEAs, at that point, could require the help of at least one foreign authority that should assist in locating the suspect, and in preserving all potential evidence connected to the case. The complexity of the inquiry, hence, raises, and with it the time that it requires: bringing in another authority and asking for cooperation is not necessarily a speedy process, and it does not necessarily yield results in a short time. First of all, the foreign authority must show the political will to cooperate with the investigation of another country. Within the EU, the point does not normally pose issues, but the landscape of threats is much wider than that, and the rising international tensions do not help to ensure smooth cooperation. The principal sources of the detected cyber threats are the so-called "state-nexus actors"[36]: they are organized groups, connected to nation-states, that are normally well-organized and well-financed. They are supposed to do their government's bidding; hence, they enjoy a good level of protection from prosecution: they can operate with the relative certainty that they will never be surrendered to a foreign authority. The criminal justice system, in such cases, simply cannot work, which does not mean that the perpetrators – if identified – must go unpunished. Where this expression of state sovereignty fails, others could fill in: states can react with a wide variety of tools, including targeted sanctions on the individuals deemed responsible[37] for a state-sponsored cyber-counter-strike[38]; it is the fast-evolving realm of cyber-diplomacy[39] and cyber-warfare.[40]

[35] ENISA, *ENISA Threat Landscape 2024* (30), p 21.

[36] Ibid, p 22 ff., with a group of hackers connected to Russia, NoName057, single-handedly providing for 30 per cent of cyber-threats.

[37] For a framework, see A Moiseienko and S Hufnagel, "Targeted Sanctions, Crimes and State Sovereignty' (2015) 6 *European Journal of Criminal Law* 351; A Moiseienko, "Crime and Sanctions" (10) 17; Y Miadzvetskaya, "EU Sanctions in Response to Cyber-Attacks as Crime-Based Emergency Measures" (10). For a recent example, see U.S. Department of Treasury, "Treasury Sanctions Iranian Regime Agents Attempting to Interfere in U.S. Election," 27 September 2024, available at <https://home.treasury.gov/news/press-releases/jy2621> (last accessed 14 April 2025).

[38] In Italy, the power is expressly recognized and further regulated by Art 7-*ter* d.l. 30 October 2015, n 174, converted into law 11 December 2015, n 198. Nation States could even adopt automatic hack back systems as a form of active defense; on this topic, and the delicate issues it raises, see S Haataja, "Cyber Operations and Automatic Hack Backs under International Law on Necessity" (2024) 53 Computer Law & Security Review 105992.

[39] See G Christou, "Cyber Diplomacy: From Concept to Practice" (2024) Tallin paper n 14, CCDCOE, 2024, available at <https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf> (last accessed 14 April 2025).

[40] For a legal framing of cyber warfare, see MN Schmitt, *Tallin Manual 2.0 on the International Law Applicable to Cyber Warfare*, (2nd ed., Cambridge, Cambridge University Press 2017). A third edition is currently underway, prepared by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). For a strategic assessment of possible reactions see B Valk, "Escalation Roadmap: an Analysis Paper" (2023) CCDCOE, available at <https://ccdcoe.org/uploads/2023/07/Escalation-Roadmap-Final_version_13-06-2023-1.pdf> (last accessed 14 April 2025) that contains a

State-nexus actors are not the only ones who can benefit from this kind of de facto immunity from foreign prosecution. Also group of cyber-criminals, motivated by profit, can be based in states that routinely refuse cooperation, often on the grounds of geopolitical interests and alliances. The lack of cooperation can either make the investigation impractical – making it harder to identify the offending individual or confirm suspicions – or it can make the enforcement impossible. If a sovereign nation refuses to hand over the alleged perpetrator, the criminal justice system is practically toothless: in some jurisdictions, suspects can be tried *in absentia*[41] but, even if the criminal proceedings ended up in a conviction, it would be very difficult – if not straight out impossible – to see the sentence carried out. In the majority of cases, the wheels of the expensive criminal justice machine would have turned to no avail, which makes alternative approaches much more convenient. The imposition of administrative sanctions does not require a complex, contradictory proceeding that ensures all the guarantees that the criminal justice system should respect. Furthermore, it does not require the cooperation of any other subject: it is a unilateral decision that puts the state (or the regional entity, such as the EU) back in control of its response. The effectiveness of the two tools appears to be the same, but the latter comes faster and at a lower cost.

V. The UN convention on cybercrime: a step towards an improved international cooperation?

Against such a background, one might believe criminal law to be a semi-abandoned tool. The assumption, however, would be wrong. International and regional organizations are renewing and reshaping the tools of criminal law and criminal procedure, with a variety of initiatives that often differ in style and overall objectives.

Many European efforts, led by the Council of Europe and the European Union, have been focused on the relationship between state authorities and service providers with at least three significant instruments: the Second Protocol to the Budapest Convention, the Digital Service Act, and the e-Evidence package. All deal with the same issue: disciplining the direct relationship between LEAs and service providers to ensure the swift disclosure and exchange of electronic evidence.[42] These novelties largely mirror preexisting national or regional policies,[43] whereas other multilateral initiatives – which we will examine more closely – aim to face the global challenge of cyber threats with a worldwide, coordinated effort that should supersede national or regional initiatives. The endeavor is taking two, main roads: the proposal of a new international convention on cybercrime on the one hand, and the interest towards an international jurisdiction for cybercrime cases.

categorization of possible harms (p 11) and flowcharts detailing the appropriate response, given the legal background.

[41] For a comparative study on the topic, see S Quattrocolo and S Ruggeri (eds), *Personal Participation in Criminal Proceedings: A Comparative Study of Participatory Safeguards and in Absentia Trials in Europe* (Cham, Springer 2019).

[42] For a comprehensive analysis of the Second protocol to the Budapest Convention, see S Tosza, "Internet Service Providers as Law Eenforcers and Adjudicators. A Public Role of Private Actors" (2021) 43 Computer Law & Security Review, n 105614; for the analysis of the eEvidence package, see *Electronic Evidence* (2023) Eucrim, issue n 2, entirely devoted to Regulation (EU) 2023/1543 and to Directive (EU) 2023/1544. On the Digital Service Act (Regulation (EU) 2022/2065), and especially on its Article 10, see W Folkert, LK Saulius and PJ Loewehnthal, *The EU Digital Services Act. A Commentary* (Oxford, Oxford University Press 2024) p 101 ff.

[43] On the subject see P De Hert and A Aguinaldo, "Cybercrime Convention-Based Access to Personal Data Held by Big Tech: Decades of Council of Europe's Greenlighting Codified in a New Protocol" in H Matsumi, D Hallinan, D Dimitrova, E Kosta and P De Hert (eds), *Data Protection and Privacy. In Transitional Times* (Oxford, Hart 2023) p 185 ff.; L Bartoli, "Digital Evidence for the Criminal Trial: Limitless Cloud and State Boundaries" (2019) Eurojus, special issue, p 96 ff.

In 2019, the UN's General Assembly adopted a resolution that established an "open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes."[44] The action was led by Russia, soon followed by other states like China, North Korea, Syria and Belarus, to negotiate a new international instrument with the potential to overshadow the 2001 Budapest Convention both in scope and in political support. The negotiation at the UN level was bound to involve all countries that did not have a seat at the table in the drafting, the implementation, and the possible amendment of the European instrument, which has been criticized on multiple occasions for being more focused on countries that host ICT infrastructure – namely: the "first world" – rather than on nations that host potential victims, such as small and developing countries.[45] The push to develop a new global standard, however, was received with alarm,[46] fearing that the treaty could be used as a trojan horse by autocratic regimes: under the guise of fostering cooperation, they could introduce provisions aimed at hampering free speech, investigating dissidents, whistleblowers, researchers and journalists. To facilitate the negotiations, some actors suggested adopting a narrow focus: according to this perspective, the treaty should have concerned itself only with the illicit conducts that are most relevant to the cybersecurity domain, such as unauthorized access to data; unauthorized interference with the systems – with a specific aim at DDoS attacks; and unauthorized data interference, with a focus of phishing campaigns. Such a lens would have allowed the divide to be bridged between the Budapest Convention's notion of cybercrime and the concept of cybersecurity: the criminal law layer would have had a guideline specifically aimed at conceptualizing cyber-threats as crimes, developing a blueprint on how to cooperate to prosecute them globally. Moreover, such a concentrated effort would have allowed a content-neutral discussion: the differences on what constitutes inflammatory speech, hate speech or even extremist propaganda could have been avoided.[47] Although wise, this view has not prevailed at the negotiating table. The United Nations Convention on Cybercrime, adopted by the U.N. General Assembly on 24 December 2024, largely overlaps with the Budapest Convention.[48] The incriminating provisions also cover conducts such as fraud (Article 13); child pornography and online child abuse (Article 14); grooming, solicitation "or making any arrangement through an information and communications technology system for the purpose of committing a sexual offence against a child" (Article 15); non-consensual dissemination of intimate images (Article 16); laundering of the proceedings of crime (Article 17). This choice has made the treaty, once again, too broad to be an effective

[44] UN General Assembly, Resolution 74/247 Countering the use of information and communications technologies for criminal purposes (A/RES/74/247), 27 December 2019, p 3.

[45] For a version of this remark, see M Gercke, "Achievements and Failures of the Council of Europe's Instrument in the Fight against Internet-Related Crimes" (2011) 12 Computer Law Review International 145, which also relates on the previous calls to start a global debate on cybercrime within the UN. Furthermore, see S Schjølberg, *The History of Cybercrime* (16) 80 f.

[46] Before the vote on the resolution, the representative from the United States warned that it would "stifle global anti-cybercrime efforts": UN General Assembly, 74th session, 52nd meeting (resumed), GA/12235, 27 December 2019.

[47] This was the position of the International Chamber of Commerce, that participated to the negotiation in representation of businesses: see ICC, 'Annex to ICC Cybersecurity Issue Brief # 2' (2023), available at <https://iccwbo.org/wp-content/uploads/sites/3/2023/09/2023-icc-annex-icc-cybersecurity-issue-brief-2.pdf> (last accessed 14 April 2025).

[48] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, Resolution adopted by the General Assembly on 24 December 2024, A/RES/79/243 (hereinafter: the U.N. Convention).

guideline on cybersecurity, as it is not specifically concerned with its needs.[49] Moreover, including content-related infringements has made the negotiation more contentious: cultural standards on subjects such as intimate pictures vary widely, and countries such as Iran have pushed hard for stricter provisions against the firm objections of other parties.[50]

Moreover, the procedural provisions establish powers that, according to the private sector representatives participating in the negotiations, could actively harm national security, force companies to reveal vulnerabilities, and hamper cybersecurity research. The first worry arises from Articles 29 and 30, which regulate the real-time collection of traffic data and the interception of content data. They ask the adherent states to allow the convert collection of data – to be done directly or with the assistance of a service provider. These powers can be deployed only in the investigation of "serious crimes," and Article 24 of the U.N. Convention contains a general call to respect human rights and the principle of proportionality; to ensure the right to an effective remedy and judicial (or other independent) oversight; to establish rules to narrow the scope and the duration of the measures. However, Articles 29 and 30 do not provide for any specific guardrail: the text fails to establish a minimal common guideline in the exercise of such penetrating powers, which has led organizations such as Microsoft – as an ISP that would have to cooperate in these investigative measures – to ask for the elimination of the two articles, equating them

[49] Some of the negotiating parties would have extended the scope even more. The Russian Federation argued that also "offenses related to the transfer, processing and distortion of information using ICTs" should have been addressed, to counter phenomena such as "dissemination of terrorist and extremist ideas, Nazi appeals, information on human trafficking and illegal trafficking in weapons and drugs": "Statement by the Head of the Russian Delegation at the opening of the reconvened concluding session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes," 29 July 2024, available at <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/Statement_Head_of_Delegation_ENG_29_July_2024.pdf> (last accessed 14 April 2025). At the other end of the spectrum, the representatives of the private sector decried the vagueness of the final draft and plead for clearer language, as well as for a general alignment with the Budapest Convention's definitions: "Cybersecurity Tech Accord Statement to Reconvened concluding session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes," 30 July 2024, 2 available at <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_Statement_07.30_AHC7.13.pdf> (last accessed 14 April 2025): "we have an instrument so broad in scope that nobody in or outside of this room even knows what acts it covers"; on the same position, see also: International Chamber of Commerce, "Industry Perspectives Ahead of the Reconvened Concluding Session of the UN Ad Hoc Committee on Cybercrime" (June 2024) 3 available at <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/ICC_industry_perspectives_AHC_reconvened_concluding_session.pdf> (last accessed 14 April 2025); as well as Microsoft's submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (29 July–9 August 2024) 3 and 5 <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf> (last accessed 14 April 2025).

[50] A last push came at the very last session, when the Islamic Republic of Iran moved for the criminalization of the simple diffusion of intimate picture, even when consensual, remarking that it is not a matter of privacy only, but also of morals; moreover, Iran requested the criminalization of nude images of minors, that could have potentially led to the incrimination of "sexting" among adolescents (see "Concept note presented by the Islamic Republic of Iran on Articles 14 and 16 of the Draft Convention on Countering the Use of ICT for Criminal Purpose" (3 July 2024) available at <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/I.R.Iran-Explanation_of_Position-9_August_2024_NY.pdf> (last accessed 14 April 2025).

From a western point of view, such requests were simply outrageous, as mentioned – and not without some emphasis – during the final debate: "last – but definitely not least, we have an instrument that facilitates charging children as criminals subject to international law enforcement cooperation for their selfies – selfies, Madame Chair": Cybersecurity Tech Accord Statement, (45) 2, which mentions that the same concern was shared by Austria, Italy and Slovakia.

to a "*de facto* blessing" of "surveillance and intelligence collecting [. . .] under the guise of combating cybercrime."[51]

The broad definition of these investigative powers is much more worrying if one considers their scope: according to Article 23 of the draft, such procedural measures should apply not only to the offences established by the Convention, but also to other criminal offences "committed by means of an information and communications technology system," and, even more broadly, to the collection of electronic evidence.

The second red flag has been raised about Article 28(4), which prompts the states to "empower its competent authorities to order any person who has knowledge about the functioning of the information and communications technology system in question, the information and telecommunications network, or their component parts, or measures applied to protect the electronic data therein, to provide, as is reasonable, the necessary information" to search and seize electronic data. The provision would not only force the disclosure of access credentials; it has a much broader scope than that: it would require "any person" to share information on how an IT system works, how it is built, how it is balanced and, therefore, where it is vulnerable. From a cybersecurity perspective (and from an intellectual property viewpoint as well), the provision could not be more problematic, especially at a time when a good number of cyber threats come exactly from nation-states, that would be able to leverage the measures of the convention to their benefit.[52]

Finally, the text does not contain safeguards for "white hat" hackers and penetration testers, which – according to the Cybersecurity Tech Accord – are "aggressively targeted" in some jurisdictions.[53] The Convention does little to protect good-faith cybersecurity practitioners from criminal liability,[54] which has caused concerns: many companies rely on their efforts to identify and fix vulnerabilities, and some jurisdictions have carved specific safeguards in legal provisions[55] or prosecutorial guidelines.[56]

[51] Microsoft's submission to the Seventh Reconvened Session (45) 2.

[52] Microsoft's submission to the Seventh Reconvened Session (45) 4, contains a very explicit formulation of this argument. It calls for the suppression of Article 28(4) as it would allow "any state – including states who have conducted cyberattacks against critical infrastructure – to compel a company or government agency employee with special knowledge of a computer system to hand over" passwords and other sensitive information. According to the International Chamber of Commerce, the provision could also reduce the interest of investors and curb the economic expansion of the industry: sharing critical information could help replicas, making innovative products less profitable. See "Global Business Urges Governments to Reject New International Cybercrime Treaty" (13 August 2024) ICC <https://iccwbo.org/news-publications/news/global-business-urges-governments-to-reject-new-international-cybercrime-treaty> (last accessed 14 April 2025).

[53] The reference is to China. See "Cybersecurity Tech Accord Submission to the Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime" (January 2024) UNDOC 3 <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Multi-Stakeholders/Cybersecurity_Tech_Accord_-_7th_AHC_session_submission.pdf> (last accessed 14 April 2025).

[54] The sole mention of the problem is in Article 53 § 2 (e), which contains a list of preventive measures among which "Recognizing the contributions of the legitimate activities of security researchers when intended solely, and to the extent permitted and subject to the conditions prescribed by domestic law, to strengthen and improve the security of service providers' products, services and customers located within the territory of the State Party."

[55] It is the case in Belgium, where "white-hat hackers" enjoy the same protections as whistleblowers under the law 28 November 2022, n. 2022042980. For a quick overview on the topic, see C Somers, K Vranckaert and L Drechsler, "Belgium Legalises Ethical Hacking: A Threat or an Opportunity for Cybersecurity?"(2023) KU Leuven CiTiP Blog <https://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity> (last accessed 14 April 2025).

[56] DOJ Policy for Charging Cases under the Computer Fraud and Abuse Act (19 May 2022), p 4 no 8, available at <https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act#:~:text=The%20new%20policy%20states%20explicitly,and%20availability%20of%20information%20stored> (last accessed 14 April 2025).

Despite the last-minute calls for its rejection,[57] the Convention has now been adopted and is currently open for signature: it requires forty instruments of ratification by 31 December 2026 to enter into force.[58] According to the first declaration, the final text is a compromise that does not fully satisfy the interests of liberal democracies, which see the potential threats to fundamental rights; nor does it satisfy states such as the Islamic Republic of Iran, which objected repeatedly to the provisions that it deemed too lax. The ratification process will probably mirror the concerns of individual nations: many countries will reasonably try to minimize exposure, limiting the provisions that could be used as trojan horses while concluding bilateral treaties with nations they can trust.[59] The space for cooperation with foreign authorities will reasonably be restricted to protect national interests, such as its security and the protection of human rights. In other words, this multilateral effort will depend on the unilateral willingness to cooperate, and given the heightened international tension, it is unrealistic to assume that this tool, alone, could mark a decisive improvement in cooperation.

VI. An international criminal court for cybercrimes?

Another set of proposals has stemmed from the need for transnational cooperation: if cyberthreats and cybercrimes are organized on a global playfield, some scholars have advocated for an *ad hoc* international institution, ie, an International Criminal Court for Cyberspace.[60] The proposal is for sure authoritative and fascinating: such an institution, run effectively, could at least coordinate and direct investigations in an independent way, acting as a global watchdog rather than as the guardian of one individual nation. If taken seriously, such an effort could help reign in the "state-nexus" actors or at least provide an independent, authoritative account of the phenomenon. This new international tribunal, according to its proponents, should work as a new, additional permanent organism; it should have its statute and its jurisdictional perimeter; in other words: it should not be a mere expansion of the International Criminal Court (ICC) and its Rome Statute. The suggestion is captivating, but it does not seem feasible, at least in the short term.[61]

Another similar avenue, however, has been studied for years and has recently shown some interesting developments. In particular, the discussion has been focusing on the International Criminal Court of the Hague and its mandate: can it already adjudicate cybercrime cases? At what conditions? The Rome Statute limits the scope of the ICC to "the most serious crimes of concern to the international community as a whole" (Article 5), leaving the "minor" episodes to the national authorities. Moreover, the jurisdiction only regards a narrow list of crimes: genocide, crimes against humanity, war crimes, and crimes of aggression. On the one hand, according to some scholars, the provisions can be interpreted in such a way to include cyberattacks: to all intents and purposes, they are an essential part of modern warfare, and they can be construed as "use of force," and therefore they should be evaluated by the competent international authority.[62] Other

[57] International Chamber of Commerce, "Global Business Urges Governments to Reject New International Cybercrime Treaty" (48).

[58] Recital n 2 and Article 65 of the Convention.

[59] See G Priyandita and B Hogeveen, "The UN Cybercrime Convention: A Victory for State Sovereignty," 16 August 20254, available at <https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/> (last accessed 14 April 2025).

[60] S. Schjølberg, *The History of Cybercrime* (16) p 184 ss., with a draft statute of an International Court for Cyberspace at p 210 ff.

[61] International Chamber of Commerce, "Global Business Urges Governments to Reject New International Cybercrime Treaty" (48).

[62] On cyberattacks as war crimes, hence included in Article 8 of the Rome Statute, see: K Ambos, "Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?" (2022) ICC Forum

voices, on the other hand, argue for an amendment of the statute: cyberattacks can have devastating effects and they should be included in the list of crimes that fall under the Court's scope. Doing it without modifying the statute would mean adding a crime through case law: even if cyberattacks are undoubtedly part of modern warfare, their adjudication by the court would be "a novelty,"[63] infringing upon the *nullum crimen sine lege* principle established by Article 22 of the Statute. A third position strikes quite a realistic balance: it argues that cybercrimes could already be conceived as war crimes as defined by the Statute, but this simple acknowledgment would not automatically bring results in terms of deterrence. Building a solid case would require an unshakable attribution, as well as a precise assessment of the consequences of the cyberattack: it should always clear the gravity threshold set by Article 5 and be so severe to constitute a "concern to the international community as a whole." These two requirements are typically not easy to satisfy, which would hamper the dissuasive power of the entire system.[64] Moreover, prosecutors could focus on different, "easier" cases rather than on an investigation that could be long, complex, and expensive, and that could very well lead to uncertain attribution.[65]

The theoretical inquiry could soon be tested. After some encouraging statements by the ICC's prosecutor,[66] the Berkeley Law's Human Rights Center has filed an Article 15 communication with the ICC prosecutor's office asserting the occurrence of cyber war crimes perpetrated by Russia on Ukraine's critical infrastructure.[67] The communication appears to be based on a Grand Jury Indictment unsealed in 2020 by the U.S. Department of Justice, which leveled charges against six Russian military intelligence officers allegedly responsible for a series of cyberattacks.[68] The case, hence, could benefit from a previous investigation, carried out by a single nation, that has arrived to a precise attribution; of course, it is for the ICC prosecutor's office to evaluate the credibility of all information that they receive, but the information has been shared, and the question has been formally

<https://iccforum.com/cyberwar> (last accessed 14 April 2025): his analysis is mainly focus on the label of war crimes; M Roscini, "Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute' (2022) ICC Forum <https://iccforum.com/cyberwar> (last accessed 14 April 2025). On cyberattacks as crime of aggression, hence covered by Art 8 *bis* of the Rome Statute, see: OA Hathaway, "To What Extent and Under What Conditions Might Cyber Operations or Cyberwarfare Constitute Crimes Specified in the Rome Statute?" (2022) ICC Forum <https://iccforum.com/cyberwar> (last accessed 14 April 2025).

[63] D Scheffer, "Amending the Rome Statute to Cover Cyberwarfare as Aggression" (2022) ICC Forum <https://iccforum.com/cyberwar> (last accessed 14 April 2025); for more details, see: Id, "The Missing Pieces in Article 8 bis (Aggression) of the Rome Statute" (2017) 58 Harvard International Law Journal 84.

[64] GD Brown, "Some Nondestructive State Cyber Operations Probably Constitute the Crime of Aggression under the Rome Statute, but Attribution Difficulties and State Practice Make Effective Deterrence Unlikely" (2022) ICC Forum <https://iccforum.com/cyberwar> (last accessed on 14 April 2025).

[65] M Roscini, "Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes" (2019) Criminal Law Forum 269.

[66] KAA Kahn, "Technology Will Not Exceed Our Humanity" (2023) Digital Front Lines <https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity> (last accessed 14 April 2025): "international criminal justice can and must adapt to this new landscape. While no provision of the Rome Statute is dedicated to cybercrimes, such conduct may potentially fulfill the elements of many core international crimes as already defined."

[67] For a legal exam of the submission, see L Freeman, A. Ghahremani and S Lombardo, "The Gravity of Russia's Cyberwar against Ukraine," 19 April 2023 available at <https://opiniojuris.org/2023/04/19/the-gravity-of-russias-cyberwar-against-ukraine> (last accessed 14 April 2025).

[68] For the connection between the two actions, see L Freeman, "Russian Cyberattacks Need an International Criminal Court Response," 19 July 2022 <https://cepa.org/article/russian-cyberattacks-need-an-international-criminal-court-response> (last accessed 14 April 2025).

asked. Reportedly, the Prosecutor's office is considering the label of "war crimes" for the cyber-attacks against civilian infrastructure in the Russia–Ukraine war.[69]

Whatever conclusions it will reach, the investigation will surely be groundbreaking for the assessment of cyber-attacks as war crimes. From a practical point of view, however, the problem of effectiveness would not change much: a full investigation requires time; attribution and the gravity threshold pose serious issues, and, finally, even if the process would end in a conviction by the ICC, the question of enforcement would remain open. The decision would have a huge symbolic value, but it could be less significant in terms of concrete deterrence.

VII. Conclusions

Despite all its flaws, and all the hurdles of mutual legal assistance, the criminal justice system is still a sought tool in the fight against cyber threats, and for good reasons. It can neutralize criminals by detaining them while protecting the accused through all the procedural rights that a criminal trial guarantees – and that could be practically eluded by bestowing administrative sanctions. At the same time, the perspective of being caught and having to face real-life consequences can be much more dissuasive than receiving another kind of sanction. A functional criminal justice system, hence, is a very valuable device also from a strict cybersecurity perspective. For the partnership to be profitable, though, the effectiveness gap needs to be bridged.

A first, useful step could consist in the abandonment of the label "cybercrime," as it frames the discussion in a somewhat unhelpful way. In the beginning, it was conceived to focus the attention on those illicit acts that required the "knowledge of computer technology [...] to understand the intentional acts."[70] Nowadays, the investigation and the ascertainment of any crime needs some degree of ability – or, at least, of awareness – when it comes to digital technologies: that criterion cannot be productively used to identify a class of similar situations, that share methods, investigative needs, legal and operative problems. It is time to unpack the notion of "cybercrime," which would allow us to focus more on the issues to solve (and on the possible solutions) rather than on the technology alone.

This simple change of perspective could lead to significant changes in policy. The organization of LEAs, for instance, would follow a different path. Instead of having units of specialists devoted to "cybercrimes" – ranging from IP theft to cyberbullying, from cyberattacks to child pornography – the police forces would set a baseline of digital skills that should be common to every unit, as they are a necessary tool of daily practice. Some units, at that point, could specialize by subject: some would work on child pornography, some on international terrorism, but some would comprehensively work on the offences that tend to be more significant from a cybersecurity perspective.

The reporting system would change accordingly: it would not lump together all "cybercrimes," but it would distinguish the type of scenario from the beginning. Similar models already exist: F.B.I., for instance, provides a good example of a similar structure. Its Internet Crime Complaint Center (IC3) has such a "narrow" scope. Its website clearly explains its mission to the public and allows them to file a report; at the same time, the opening page makes clear that the IC3 does not deal with terrorism, child pornography, or sources of imminent danger: it indicates the proper channels for each of these possibilities, but it explicitly declines to treat with those affairs. The United Kingdom

[69] A Deutsch, S van den Berg and J Pearson, "ICC Probes Cyberattacks in Ukraine as Possible War Crimes, Sources Say," (*Reuters*, 14 June 2024) <https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14> (last accessed 14 April 2025).

[70] U.S. Department of Justice, "Computer Crime" (13) p 2.

offers a similar service with the National Fraud & Cyber Crime Reporting Center: its website contains information on the most widespread types of online fraud and presents a simple and transparent way to report phishing, fraud, and other cybercrime-related incidents.[71]

If such structures were widespread, adequately equipped and funded,[72] citizens would have a clear reference point to report facts that are normally perceived as *minutia*, not severe enough to investigate or even to relate to the police. Having a dedicated unit would signal to the public that identity theft and system interference are not facts to be taken lightly, or circumstances that the authorities would not even bother to review. The victims would know who to address. They could talk with someone who understands the harm they have received, and who has all the background information that one needs to appreciate the gravity of the occurrence. Individuals would probably report more incidents, allowing LEAs to paint a granular picture of cyber threats.

The shift would reinforce communication between investigators and individuals, creating public trust. At the same time, it would generate a stream of information that would be crucial in mapping ongoing threats: there would be more data points to reconstruct, investigate and prosecute them. The proposal, of course, would not solve all issues. For instance, it would not do much to prosecute effectively foreign state-nexus actors: in that scenario, the available countermoves would still be referring the case to intelligence services, or imposing administrative crime-based sanctions as discussed above. The investigation, however, would be more accurate: attribution could be more precise and definitive, providing a better indication of what could constitute a proportionate response. Moreover, data would also be crucial from a preemptive point of view: cybersecurity strategies are as good as the knowledge they are based on, and having a more precise idea of the threat landscape would help improve them.

Funding statement. This paper stems from a research conducted in cooperation with EcoCyber-SERICS, a project funded by MUR National Recovery and Resilience Plan funded by the European Union - NextGeneraionEU - Mission 4 Component 2, Investment 1.3 "Parternariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca", MUR notice n. 341, 15 March 2022, proposal: PE00000014, CUP: J33C22002810001, funded by MUR decree n. 1556, 11 October 2022.

Competing interests. The author has no conflicts of interest to declare.

[71] The page dedicates a specific section to businesses and a hotline to individual citizens <https://www.actionfraud.police.uk/> (last accessed 14 April 2025).

[72] This does not seem to be the case, now, in Europe. The Europol web page for reporting cybercrime online links to the national police forces' websites <https://www.europol.europa.eu/report-a-crime/report-cybercrime-online> (last accessed 14 April 2025). Sometimes, the link connects to pages that are concerned with extreme content online (it is the case for France) or to the page of the generic "tech unit" (as it is for Italy). In other cases, the website refers generically to the website of the police (Germany, Spain).

Cite this article: L Bartoli (2025). "Cybersecurity and the Fight against Cybercrime: Partners or Competitors?" *European Journal of Risk Regulation* **16**, 498–513. https://doi.org/10.1017/err.2025.31