

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

State and Non-State Cyber Actors and the Primacy of National Courts in Individual Criminal Accountability

YASHWANT S C*

ABSTRACT

The evolution of warfare and international criminality has increasingly moved into cyberspace, where state and non-state actors alike now possess the capability to inflict harm equivalent to that of traditional atrocity crimes: disabling hospital systems, crippling energy grids or destroying civilian infrastructure through purely digital means. The Rome Statute of the International Criminal Court, adopted in 1998, was drafted in an era of kinetic warfare and did not contemplate cyber conduct explicitly. Yet its framers drafted the instrument's core provisions, such as individual criminal responsibility, command and superior responsibility and the mental element, in technology-neutral terms capable, in principle, of extending to new means of commission. The Office of the Prosecutor's December 2025 Policy on Cyber-Enabled Crimes under the Rome Statute is the first formal confirmation by an international prosecuting authority that existing doctrine can be applied to cyberspace, covering conduct ranging from state-directed cyber units to hacktivist collectives and criminal proxies. Despite this doctrinal clarification, international criminal law faces a stark enforcement reality: no individual has yet been convicted by an international tribunal for a cyber-enabled international crime. This gap persists even as both state-sponsored and non-state cyber actors operate with increasing frequency. The paper distinguishes state from non-state cyber actors through the effective control test, the overall control test and the approach of the Tallinn Manual 2.0, and develops a multi-factor approach to cyber attribution built on factors such as institutional or organisational nexus, direction and control, object and target selection, and technical or forensic indicators. It argues that while the Rome Statute's liability doctrine is formally actor-neutral, its practical application diverges sharply between state and non-state cyber actors, driven by attribution difficulties and the non-membership of major cyber powers. It further examines how national courts, operating through both domestic criminal statutes and universal jurisdiction, are structurally better positioned than the ICC to close this accountability gap for both types of actor.

Keywords: *The Rome Statute, ICC Office of the Prosecutor's 2025 Policy, The State and Non-State Cyber Actor, Hacktivist, Domestic Criminal Statutes*

* Author is a Student at Shanmugha Arts, Science, Technology & Research Academy (SASTRA Deemed University), Thanjavur, Tamil Nadu, India.

I. INTRODUCTION

Cyberattacks targeting critical infrastructure produce cyber-physical effects, transforming digital disruption into immediate, dangerous and potentially fatal real-world consequences. In December 2015, for example, Russian military intelligence hackers known as Sandworm cut power to some 225,000 customers in Ukraine: they disabled backup power supplies, wiped system software and flooded call centres with telephone calls so that customers could not report the outages.¹ During the India-Pakistan hostilities of May 2025, in the course of Operation Sindoor, Pakistan-linked threat actors and hacktivist groups were reported to have launched waves of cyberattacks against Indian digital infrastructure.² The Rome Statute of the International Criminal Court (1998) created a permanent framework for prosecuting individuals for war crimes, crimes against humanity and genocide, but it was drafted with bombs, bullets and troops crossing physical borders in mind; the Office of the Prosecutor (OTP) of the International Criminal Court (ICC) has therefore issued a Policy on Cyber-Enabled Crimes setting out how that framework applies to conduct in cyberspace.³ Scholars such as Chaumette, van Sliedregt, Buchan and Tsagourias, Blank and Roberts, and the Tallinn Manual 2.0, treat cyber accountability gaps as one undifferentiated problem of attribution and jurisdiction. The Rome Statute itself follows an actor-neutral model: it does not differentiate among state actors, state-backed actors and non-state actors. Domestic courts, applying local laws and universal jurisdiction, are better equipped than the ICC to prosecute actors who hide behind national sovereignty, and to reach both types of actor. This paper begins by discussing legal attribution through the existing tests of international law, then designs a six-factor test and uses it to classify cyber actors as state actors, state-backed actors and non-state actors.

¹ ELEC. INFO. SHARING & ANALYSIS CTR. & SANS INDUS. CONTROL SYS., *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case* (Mar. 18, 2016), <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *Cyber-Attack Against Ukrainian Critical Infrastructure*, ICS Alert IR-ALERT-H-16-056-01 (Feb. 25, 2016), <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>; Press Release, U.S. DEP'T OF JUST., *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (Oct. 19, 2020), <https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>.

² Sameer Patil, *Operation Sindoor and India's Cyber Threat Landscape*, OBSERVER RSCH. FOUND. (May 28, 2025), <https://www.orfonline.org/expert-speak/operation-sindoor-and-india-s-cyber-threat-landscape>.

³ INT'L CRIM. CT., OFF. OF THE PROSECUTOR, *Policy on Cyber-Enabled Crimes under the Rome Statute* ¶¶ 1–5 (Dec. 2025), <https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf> [hereinafter OTP Cyber Policy]; see also Statement, INT'L CRIM. CT., *ICC Office of the Prosecutor Launches Policy on Cyber-Enabled Crimes under the Rome Statute to Address International Crimes in the Digital Era* (Dec. 3, 2025), <https://www.icc-cpi.int/news/icc-office-prosecutor-launches-policy-cyber-enabled-crimes-under-rome-statute-address>.

A. Statement of the problem

The paper examines how, although the Rome Statute's liability doctrine is formally actor-neutral, its practical application diverges sharply between state and non-state cyber actors: for the former because of attribution difficulties and the non-membership of major cyber powers, and for the latter because of gravity and admissibility thresholds and organisational diffuseness. It further examines whether national courts, operating through both domestic criminal statutes and universal jurisdiction, are structurally better positioned than the ICC to close this accountability gap for both types of actor.

B. Research methodology

This paper adopts a doctrinal and comparative methodology. The doctrinal component analyses the Rome Statute's modes of liability, jurisdictional provisions and crime definitions, read alongside the ICC Office of the Prosecutor's 2025 Policy on Cyber-Enabled Crimes, and examines case studies. The comparative component examines the prosecutorial frameworks of other jurisdictions, namely India, the United States and the European Union, for individual criminal responsibility.

C. Research proposition

Cyber actors can be distinguished by a test built from the existing standards of attribution in international law. Should national courts, rather than the ICC, be the primary forum for deciding individual criminal accountability for international cyber crimes committed by state, state-backed and non-state cyber actors alike?

II. LITERATURE REVIEW

A. Chaumette (2018)

Anne-Laure Chaumette, in *International Criminal Responsibility of Individuals in Case of Cyberattacks* (2018), identifies attribution and the fragmented nature of cyberspace as obstacles to individual criminal responsibility for cyberattacks.⁴ She notes that attribution is hard and that cyberspace does not respect borders in the way that traditional international crimes do.

B. Ambos (2016)

Kai Ambos, in *Individual Criminal Responsibility for Cyber Aggression* (2016), a contribution to the *Journal of Conflict and Security Law*'s special issue on non-state actors and responsibility

⁴ Anne-Laure Chaumette, *International Criminal Responsibility of Individuals in Case of Cyberattacks*, 18 INT'L CRIM. L. REV. 1 (2018), <https://doi.org/10.1163/15718123-01801004>.

in cyberspace, examines cyber conduct under Article 8 bis of the Rome Statute.⁵ His finding is narrow: aggression can be committed only by a state, and it is a leadership crime. The law therefore targets the people giving the orders, not the people who actually press the button.

C. Van Sliedregt (2016)

Elies van Sliedregt, in *Command Responsibility and Cyberattacks* (2016), published in the same special issue, tests command responsibility, that is, whether a commander can be held liable for what subordinates do, against three cyberattack scenarios.⁶ She finds that the doctrine works best when the attacker is part of a formal military cyber unit, becomes shakier when the operation is outsourced, and breaks down almost entirely when there is no link between the commander's subordinates and the hackers.

D. Katagiri (2021)

Nori Katagiri, in *Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks* (2021), finds that international law was built around states as the main actors, so that it has no real teeth against non-state actors such as individual hackers and private groups.⁷

E. Tallinn Manual 2.0 (2017)

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, edited by Michael N. Schmitt, is a manual written by an international group of legal experts explaining how existing rules of international law apply to cyber operations.⁸

F. Roberts (2014)

Shaun Roberts, in *Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors* (2014), argues that if a state cannot or will not stop a non-state actor from launching cyberattacks from its territory, the victim state should be allowed to respond regardless.⁹

⁵ Kai Ambos, *Individual Criminal Responsibility for Cyber Aggression*, 21 J. CONFLICT & SEC. L. 495 (2016), <https://doi.org/10.1093/jcsl/krw010>.

⁶ Elies van Sliedregt, *Command Responsibility and Cyberattacks*, 21 J. CONFLICT & SEC. L. 505 (2016), <https://doi.org/10.1093/jcsl/krw012>.

⁷ Nori Katagiri, *Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks*, 7 J. CYBERSECURITY tyab009 (2021), <https://doi.org/10.1093/cybsec/tyab009>.

⁸ TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt gen. ed., 2d ed. 2017), <https://doi.org/10.1017/9781316822524> [hereinafter TALLINN MANUAL 2.0].

⁹ Shaun Roberts, *Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors*, 41 N. KY. L. REV. 535 (2014).

G. Blank (2013)

Laurie R. Blank, in *International Law and Cyber Threats from Non-State Actors* (2013), studies how the law of armed conflict applies when non-state actors are involved in cyber conflict.¹⁰ She warns that when governments loosely call an event a cyber war or a cyber attack without its meeting the strict legal definition, they open the way to responses outside formal legal channels instead of actual prosecution.

H. Bo (2021)

Marta Bo, in *Autonomous Weapons and the Responsibility Gap in Light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute* (2021), examines the mental element of the war crime of attacking civilians in attacks carried out with semi-autonomous weapons or with AI-supported targeting.¹¹ She shows that Rome Statute doctrine strains when no human actor holds the requisite knowledge of the consequences, and argues that risk-taking mental elements such as *dolus eventualis* and recklessness would better capture such conduct, though only in specific circumstances, since in most human-machine teaming scenarios even these lower standards would not be met.

I. Milanovic (2026)

Marko Milanovic, in *AI and the Commission and Facilitation of International Crimes: On Accountability Gaps and the Minab School Strike* (2026), finds that existing international criminal law is largely adequate for present-day AI systems and argues that much of the literature overstates the accountability gaps that AI creates.¹²

The existing scholarship thus treats cyber accountability as a single, undifferentiated problem of attribution and jurisdiction. It does not ask whether state and non-state actors evade accountability for structurally distinct reasons, or whether the victim state has jurisdiction to prosecute.

¹⁰ Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, 89 INT'L L. STUD. 406 (2013), <https://digital-commons.usnwc.edu/ils/vol89/iss1/7/>.

¹¹ Marta Bo, *Autonomous Weapons and the Responsibility Gap in Light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute*, 19 J. INT'L CRIM. JUST. 275 (2021), <https://doi.org/10.1093/jicj/mqab005>.

¹² Marko Milanovic, *AI and the Commission and Facilitation of International Crimes: On Accountability Gaps and the Minab School Strike*, EJIL: TALK! (Mar. 9, 2026), <https://www.ejiltalk.org/ai-and-the-commission-and-facilitation-of-international-crimes-on-accountability-gaps-and-the-minab-school-strike/>.

III. ATTRIBUTION AND INDIVIDUAL CRIMINAL LIABILITY UNDER THE ROME STATUTE

A. The Rome Statute's actor-neutral model

The Rome Statute is the international treaty that established the International Criminal Court (ICC).¹³ It was adopted on 17 July 1998, entered into force on 1 July 2002 and serves as the governing legal framework for prosecuting individuals accused of the world's most egregious atrocities. The Court's jurisdiction is complementary to that of national courts: it acts only where a state is unwilling or unable genuinely to carry out an investigation or prosecution itself. The Statute sets out four core international crimes, namely genocide, crimes against humanity, war crimes and the crime of aggression.

Article 25 of the Rome Statute governs individual criminal responsibility.¹⁴ The ICC has jurisdiction over natural persons, and a person who commits a crime within the jurisdiction of the Court is individually responsible and liable for punishment. Article 25(3) provides several modes of liability to hold high-level orchestrators, accomplices and accessories accountable. Article 25(4) expressly separates individual guilt from state responsibility, providing that no provision of the Statute relating to individual criminal responsibility affects the responsibility of states under international law.

Article 28 deals with the responsibility of commanders and other superiors.¹⁵ It codifies the doctrine of command responsibility and bridges the gap where a leader did not directly order or execute a crime but allowed it to happen under his or her watch. It imposes liability in two categories. Under Article 28(a), a military commander, or a person effectively acting as one, is criminally responsible for crimes committed by forces under his or her effective command and control where the commander knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes, and failed to take all necessary and reasonable measures within his or her power to prevent or repress them or to submit the matter to the competent authorities. Under Article 28(b), a non-military (civilian) superior, such as a political leader or the head of a government agency, is criminally responsible for crimes committed by subordinates under his or her effective authority and control where the superior knew, or consciously disregarded information which clearly indicated, that the subordinates were committing or about to commit such crimes, the crimes concerned activities

¹³ Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 3, <https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf> [hereinafter Rome Statute].

¹⁴ Rome Statute, *supra* note 13, art. 25.

¹⁵ Rome Statute, *supra* note 13, art. 28.

within the superior's effective responsibility and control, and the superior failed to take all necessary and reasonable measures to prevent or repress them or to submit the matter for investigation and prosecution.

Article 30 deals with the mental element of intent and knowledge.¹⁶ It establishes the default threshold for conviction under the Statute: unless otherwise provided, a person is criminally responsible only if the material elements of the crime are committed with intent and knowledge.

The Rome Statute is technology-neutral. If a cyber operation satisfies the material, mental and contextual elements of a core international crime, it falls within the jurisdiction of the ICC. The OTP's Policy on Cyber-Enabled Crimes under the Rome Statute, issued on 3 December 2025, states that the provisions of the Statute, including those setting out the crimes within the Court's jurisdiction, "clearly apply to the commission or facilitation of these crimes by cyber means", and that the Statute "is technology-neutral in the terms in which it is written".¹⁷ Accordingly, crimes within the jurisdiction of the Court may be committed or facilitated by cyber means just as by physical means.

B. The attribution threshold

The OTP's Policy does not set out a framework for classifying cyber actors; it addresses attribution to a state only briefly, in the context of aggression committed through a non-state proxy.¹⁸ Sorting the actors is nonetheless significant for clarifying which legal provisions apply. Attribution does not itself create individual liability; rather, it determines which specific forms of liability the Prosecutor can legally pursue. The International Law Commission's (ILC) Articles on State Responsibility can serve as the primary tool for sorting these actors.

The Articles on Responsibility of States for Internationally Wrongful Acts (2001)¹⁹ provide secondary rules of state responsibility rather than rules of individual criminal liability. They are not a binding treaty, but many of them reflect customary international law, as international courts and the ILC's accompanying commentary have repeatedly affirmed.

Article 4 concerns *de jure* organs: it covers the conduct of formal state organs, whatever their position or function within the government hierarchy.²⁰ Article 5 concerns the conduct of persons or entities exercising elements of governmental authority, that is, individuals or private

¹⁶ Rome Statute, *supra* note 13, art. 30.

¹⁷ OTP Cyber Policy, *supra* note 3, ¶ 3; *see also id.* ¶¶ 4, 49.

¹⁸ OTP Cyber Policy, *supra* note 3, ¶ 102.

¹⁹ Rep. of the Int'l L. Comm'n, 53d Sess., Apr. 23–June 1, July 2–Aug. 10, 2001, U.N. Doc. A/56/10, GAOR, 56th Sess., Supp. No. 10, at 43 (2001) (Draft Articles on Responsibility of States for Internationally Wrongful Acts) [hereinafter ILC Draft Articles].

²⁰ ILC Draft Articles, *supra* note 19, art. 4.

entities that are not formal state organs but are empowered by domestic law to exercise elements of governmental authority.²¹ Examples include a state-sanctioned cyber unit launching a disruptive malware operation, or a licensed private IT contractor tasked by legislation with managing and securing critical state voting infrastructure.

Article 8 embodies the effective control test, governing conduct directed or controlled by a state.²² In the *Nicaragua* case the International Court of Justice (ICJ) set a high threshold of effective control for attribution under this standard: the state must have issued specific instructions or directed the precise operation in question, and general state funding, the provision of equipment and overarching political support for a rogue group are not enough.²³

Article 11 deals with conduct acknowledged and adopted by a state as its own. It triggers state responsibility when a government retrospectively embraces private conduct, for example where, after a successful campaign by an activist group, the state identifies the operation as its own and assumes responsibility for it, thereby transforming private cyber operations into an act of the state. Mere praise, verbal approval or general endorsement is not enough.²⁴

In the *Bosnian Genocide* case the ICJ rejected the overall control test as a standard for attributing conduct to a state.²⁵ The International Criminal Tribunal for the former Yugoslavia (ICTY) had applied this broader test in *Tadić* to classify an armed conflict as international; the ICJ accepted that the test might be suitable for that purpose but held it unsuitable for establishing state responsibility.²⁶

This paper proposes a six-factor test for identifying the attribution factors. It adapts overall control principles not as a rule of attribution but strictly as an evidentiary bar for evaluating circumstantial ties in cyber operations. The attribution factors draw on the Tallinn Manual 2.0,²⁷ which restates how the customary international law of state responsibility applies to cyber operations. Rule 15 reflects the core principle of Articles 4 and 5: cyber operations conducted by state organs, or by persons or entities empowered by domestic law to exercise elements of

²¹ ILC Draft Articles, *supra* note 19, art. 5.

²² ILC Draft Articles, *supra* note 19, art. 8.

²³ *Military and Paramilitary Activities in and against Nicaragua* (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27), <https://www.icj-cij.org/case/70>.

²⁴ ILC Draft Articles, *supra* note 19, art. 11 & cmt. ¶ 6.

²⁵ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶¶ 396–407 (Feb. 26), <https://www.icj-cij.org/case/91>.

²⁶ *Prosecutor v. Tadić*, Case No. IT-94-1-A, Judgment, ¶¶ 116–45 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999), <https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf>; Antonio Cassese, *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 EUR. J. INT'L L. 649 (2007), <https://www.ejil.org/pdfs/18/4/233.pdf>, <https://doi.org/10.1093/ejil/chm034>.

²⁷ TALLINN MANUAL 2.0, *supra* note 8, r. 15, at 87, r. 17, at 94, <https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf>.

governmental authority, are attributable to the state. Rule 17 aligns with Article 8 by attributing a non-state actor's cyber operations to a state where they are carried out on its instructions or under its direction or control, or where the state acknowledges and adopts them as its own.²⁸

C. The six-factor test and the three-tier table

Establishing state responsibility for cyber operations is a profound evidentiary challenge in international law. Direct proof that a state stood behind and instructed a private proxy operator is exceptionally rare in cyberspace, given the nature of digital infrastructure and the sophistication of the techniques used, so that Article 8 of the ILC Articles is difficult to apply in practice. To address this evidentiary gap, a six-factor framework is proposed to evaluate the circumstantial evidence of state involvement systematically, and so to identify who stands behind an operation. The framework is an analytical tool rather than a binding legal mechanism: the six factors are an academic proposal and do not constitute settled international law. They draw on the ILC Articles, the Tallinn Manual 2.0 and the concept of overall control articulated by the ICTY in *Tadić*.

1. *Institutional or organisational nexus*. Is the actor a formal state organ, such as a designated military or intelligence cyber unit, or does it operate independently of any state apparatus? This factor applies the de jure organ test of Article 4 of the ILC Articles directly to the cyber context.
2. *Direction and control*. Did a state organise, fund, train or coordinate the actor's general activity, even without directing a specific operation? This is a lower evidentiary bar than the ICJ's effective control standard in *Nicaragua*, which requires proof of control over the specific act in question;²⁹ it applies the ICTY's overall control standard from *Tadić*.³⁰
3. *Toleration versus active direction*. This factor distinguishes a state that merely harbours a criminal or hacktivist group from one that actively directs it. Toleration alone does not amount to acknowledgement and adoption under Article 11 of the ILC Articles, although it may still engage the state's separate responsibility on due diligence grounds.³¹

²⁸ Wieteke Theeuwen, *Attribution for the Purposes of State Responsibility*, MILITAIR RECHTELIJK TIJDSCHRIFT (2018), https://puc.overheid.nl/doc/PUC_248325_11/ (last visited Oct. 1, 2026).

²⁹ *Nicaragua*, *supra* note 23, ¶ 115.

³⁰ *Tadić*, *supra* note 26, ¶¶ 116–45.

³¹ ILC Draft Articles, *supra* note 19, art. 11 & cmt. ¶ 6; *see also* TALLINN MANUAL 2.0, *supra* note 8, r. 6, at 30.

4. *Object and target selection.* Does the target align with a state's strategic interest, such as critical infrastructure or government systems, or with a financial motive, such as ransomware directed at private companies? This factor is circumstantial but widely used in threat-intelligence attribution practice.
5. *Technical and forensic indicators.* Malware signatures, shared command-and-control infrastructure and operational patterns consistent with known state-linked advanced persistent threat (APT) groups stand in for the direct evidence on which attribution in traditional armed conflict relies.
6. *Post-hoc state conduct.* Does the state shield the individual, refuse extradition or publicly endorse the act after the fact? Such conduct is circumstantial evidence of a link; it amounts to attribution under Article 11 of the ILC Articles only where the state acknowledges and adopts the conduct as its own.

These six factors sort cyber actors into three tiers, each triggering a different subset of Rome Statute provisions.

Tier	Legal basis	Rome Statute consequence
State actor	Draft Arts. 4 or 5 satisfied	Arts. 25, 28 and 8 bis all potentially engaged
State-directed proxy	Draft Art. 8 satisfied (effective or overall control)	Art. 25 engaged; Art. 28 contested on the facts; Art. 8 bis generally unavailable
Non-state actor	None of Draft Arts. 4, 5 or 8 satisfied	Art. 25 only, most likely Art. 25(3) (d) common purpose given decentralised structure

Table 1: Three tiers of cyber actors and their Rome Statute consequences

D. Command responsibility under Article 28

As noted above, Article 28 of the Rome Statute imposes superior liability for crimes committed by subordinates under a superior's effective control. Command responsibility under Article 28 applies only when a crime within the jurisdiction of the Court under Articles 6 to 8 bis has been committed, that is, genocide, crimes against humanity, war crimes or the crime of aggression. Cyber operations serve merely as the means of committing those crimes, not as independent offences.

In law, effective control is the material ability to prevent or punish the conduct.³² Evidence of real control in the cyber context includes exclusive authority over access credentials, physical

³² *Prosecutor v. Delalić*, Case No. IT-96-21-A, Judgment, ¶ 256 (Int'l Crim. Trib. for the Former Yugoslavia Feb. 20, 2001), <https://www.icty.org/x/cases/mucic/acjug/en/cel-aj010220.pdf>; see also OTP Cyber Policy, *supra* note 3, ¶ 116.

or cloud-based servers and specialised malware tools. Superiors manifest their control through the formal approval of operational code deployments and the direct capacity to revoke access remotely and sever network connections. Proving a superior's knowledge, or failure to act, relies heavily on digital trails and operational metrics: evidence that a superior knew or should have known of illicit activity includes system access logs, internal briefing reports, automated forensic traces and patterns of repeated network activity. While the Trial Chamber in *Bemba* set broad standards for these duties, the ICC Appeals Chamber's 2018 reversal emphasised that a superior cannot be held to an impossible standard of compliance, requiring a realistic assessment of the measures actually available to a remote commander.³³

- *Tier One (state cyber units)*. Article 28(a) fits this tier well. A formal military or state chain of command exists, which makes it easier to establish both the legal duty and de facto control over state-employed operators.³⁴
- *Tier Two (contractors and proxies)*. Article 28(b) applies to these non-military relationships where an official or company head holds effective authority and control. Because digital proxy relationships are easily obscured, proving that control requires linking behaviour directly to the six factors set out above.
- *Tier Three (independent groups)*. Article 28 liability often fails at this level because external actors rarely maintain effective control over loose, decentralised networks. Article 25(3)(d) offers a more viable route, targeting individuals who contribute to the commission of a crime by a group of persons acting with a common purpose.³⁵

E. Why Article 8 bis is closed to non-state actors

Article 8 bis defines aggression as an act committed by a state, and confines individual liability to persons in a position effectively to exercise control over or to direct the political or military action of a state.³⁶ Ambos argues that even where the conduct itself satisfies the conditions of aggression, liability will likely fall on a state's commanding officials rather than on the individual operator who actually launched the attack, because aggression is by definition a leadership crime.³⁷ A non-state actor operating independently of any state cannot commit

³³ Press Release, INT'L CRIM. CT., *ICC Appeals Chamber Acquits Mr Bemba from Charges of War Crimes and Crimes Against Humanity* (June 8, 2018), <https://www.icc-cpi.int/news/icc-appeals-chamber-acquits-mr-bemba-charges-war-crimes-and-crimes-against-humanity> (last visited Oct. 1, 2026); see also Diane Marie Amann, *In Bemba, Command Responsibility Doctrine Ordered to Stand Down*, ICC FORUM (May 27, 2019), <https://iccforum.com/responsibility#Amann> (last visited Oct. 1, 2026).

³⁴ Rome Statute, *supra* note 13, art. 28(a); OTP Cyber Policy, *supra* note 3, ¶ 116; see van Sliedregt, *supra* note 6.

³⁵ Rome Statute, *supra* note 13, art. 25(3)(d).

³⁶ Rome Statute, *supra* note 13, art. 8 bis(1).

³⁷ Ambos, *supra* note 5.

aggression under this provision. A Tier Two proxy's operation could amount to an act of aggression only if it is attributable to the directing state, and even then individual liability would attach to that state's leaders rather than to the proxy's own operators.³⁸ This confirms a sharp doctrinal asymmetry: Tier One and, conditionally, Tier Two operations can engage the full range of Rome Statute crimes, while Tier Three conduct never engages aggression at all.

IV. INSTITUTIONAL BARRIERS TO ACCOUNTABILITY FOR CYBERCRIMES

A. ICC barriers for state-linked cyber operators

Article 12 of the Rome Statute sets out the preconditions to the exercise of jurisdiction. A state that becomes a party to the Statute thereby accepts the jurisdiction of the Court over the crimes referred to in Article 5. Unless the Security Council refers the situation, the Court can exercise its jurisdiction only if the crime was committed on the territory of a State Party (or on board a vessel or aircraft registered in a State Party) or by a national of a State Party, or if the state concerned has accepted the Court's jurisdiction by declaration.³⁹ The ICC therefore lacks jurisdiction over state-linked cyber operators who are nationals of, and operate from, a state that is not a party to the treaty, unless their conduct takes effect on the territory of a State Party. Where cybercrime, cyberattacks and cyber warfare are driven by states operating outside this legal framework, a major structural barrier stands in the way of holding state-linked cyber operators individually accountable.

The three principal cyber powers outside the Rome Statute stand as follows.⁴⁰

1. Russia signed the Rome Statute on 13 September 2000 but on 30 November 2016 formally notified the UN Secretary-General of its intention not to become a party. It remains a non-party.
2. The United States signed the Rome Statute on 31 December 2000 under President Clinton, but on 6 May 2002, under President George W. Bush, notified the Secretary-General that it did not intend to become a party.

³⁸ OTP Cyber Policy, *supra* note 3, ¶ 102.

³⁹ Rome Statute, *supra* note 13, art. 12; *see also* Tracey Begley, Benjamin R. Farley & Sarah Harrison, *International Accountability for U.S. Crimes in the Caribbean and Pacific*, JUST SECURITY (May 27, 2026), <https://www.justsecurity.org/133689/accountability-us-crimes-caribbean-pacific/> (last visited Oct. 1, 2026).

⁴⁰ Rome Statute of the International Criminal Court: Status, U.N. TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtsg_no=XVIII-10&chapter=18 (last visited Oct. 4, 2026) (signatures of the Russian Federation and the United States, and notes 9 and 12).

3. China has neither signed nor ratified the Rome Statute. At the 1998 Rome Conference it was one of the seven states that voted against the adoption of the Statute.⁴¹

To circumvent the structural limits of Article 12, international prosecutors and states rely on specific legal workarounds to hold state-linked cyber operators accountable. Each alternative path, however, has significant legal and structural weaknesses and leaves a prominent accountability gap.

1. Article 13(b) of the Rome Statute empowers the UN Security Council, acting under Chapter VII of the UN Charter, to refer to the Prosecutor a situation in which crimes within the jurisdiction of the ICC appear to have been committed, even where the situation involves states that are not parties to the Statute.⁴² Such a referral, however, faces a veto whenever it touches a permanent member, which makes a referral directed at a permanent member's own state-linked cyber operators politically impossible.
2. An ad hoc declaration under Article 12(3) of the Rome Statute allows a state that is not a party to accept the Court's jurisdiction over a specific crime. A victim state may lodge one, as Ukraine twice did before it joined the Statute,⁴³ but a state whose own cyber operators are implicated will never willingly subject them to scrutiny in this way.

The territorial route offers a further basis. In the OTP's view, where a cyberattack originates in a non-member state but is completed in a State Party, the Court's territorial jurisdiction extends to it, and the Court can then prosecute the individuals responsible, including nationals of non-member states.⁴⁴ Ukraine became the 125th State Party to the Rome Statute on 1 January 2025, which gives the ICC territorial jurisdiction over international crimes committed within its borders, whatever the nationality of the perpetrator.⁴⁵

⁴¹ U.N. Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, *Summary Records of the Plenary Meetings*, 9th plen. mtg., ¶¶ 10, 36–40, U.N. Doc. A/CONF.183/13 (Vol. II), at 121–24 (July 17, 1998), https://legal.un.org/icc/rome/proceedings/e/rome%20proceedings_v2_e.pdf.

⁴² Rome Statute, *supra* note 13, art. 13(b).

⁴³ Rome Statute, *supra* note 13, art. 12(3); INT'L CRIM. CT., *Situation in Ukraine*, <https://www.icc-cpi.int/situations/ukraine> (last visited Oct. 4, 2026).

⁴⁴ OTP Cyber Policy, *supra* note 3, ¶¶ 42–43, 46.

⁴⁵ INT'L CRIM. CT., *ICC Welcomes Ukraine as a New State Party* (Jan. 2, 2025), <https://www.icc-cpi.int/news/icc-welcomes-ukraine-new-state-party>.

B. ICC bottlenecks for non-state actors

Non-state actors face operational and legal barriers different from those facing state actors. The OTP's Policy separates international crimes committed by cyber means from ordinary cybercrimes,⁴⁶ and the OTP's accompanying questions and answers state that the Court's jurisdiction does not extend to 'ordinary' cybercrimes prohibited under national laws, such as hacking, fraud or identity theft, unless those acts form part of or facilitate crimes already defined in the Rome Statute.⁴⁷ Article 5 confines the Court's jurisdiction to the most serious crimes of concern to the international community as a whole, and Article 17(1)(d) renders a case inadmissible if it is not of sufficient gravity to justify further action by the Court.⁴⁸ Low-level, decentralised and repeated small-scale cybercrimes struggle to pass this admissibility screen, and the Prosecutor must weigh the same gravity considerations when deciding under Article 53 whether to initiate an investigation. Prosecuting non-state actors also presents a formidable challenge under the definitions of the crimes. Crimes against humanity, for example, require a widespread or systematic attack against a civilian population pursuant to or in furtherance of a state or organisational policy under Article 7(2)(a), and a loose collective or decentralised hacker group may not qualify as an organisation. In its Article 15 decision on Kenya, Pre-Trial Chamber II held that the formal nature of a group and its level of organisation are not the defining criteria: the question is whether the group has the capability to perform acts that infringe basic human values, assessed case by case with reference to considerations such as whether it is under responsible command or has an established hierarchy, whether it has the means to carry out a widespread or systematic attack, and whether it exercises control over part of a state's territory.⁴⁹ The OTP's Policy likewise accepts that hacker groups may in principle qualify as organisations, especially where they form part of a wider entity such as an armed group.⁵⁰ A diffuse collective without command, hierarchy or means will nonetheless struggle to meet these criteria. War crimes under Article 8 require a clear nexus to an armed conflict, and an independent, profit-driven criminal group acting solely for financial gain lacks that link.

⁴⁶ OTP Cyber Policy, *supra* note 3, ¶¶ 5–6.

⁴⁷ INT'L CRIM. CT., OFF. OF THE PROSECUTOR, *Questions and Answers: The ICC Office of the Prosecutor's Policy on Cyber-Enabled Crimes under the Rome Statute*, q. 5, <https://www.icc-cpi.int/about/otp/questions-and-answers-the-icc-office-of-the-prosecutors-policy-on-cyber-enabled-crimes-under-the-rome-statute> (last visited Oct. 1, 2026).

⁴⁸ Rome Statute, *supra* note 13, arts. 5(1), 17(1)(d), 53(1).

⁴⁹ *Situation in the Republic of Kenya*, ICC-01/09-19, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, ¶¶ 90, 92–93 (Pre-Trial Chamber II Mar. 31, 2010), <https://www.legal-tools.org/doc/338a6f/>, <https://www.refworld.org/jurisprudence/caselaw/icc/2010/72797> (last visited Oct. 1, 2026); *cf. id.* (dissenting opinion of Judge Hans-Peter Kaul) ¶ 51 (requiring that an organisation partake of some characteristics of a State).

⁵⁰ OTP Cyber Policy, *supra* note 3, ¶ 68.

Non-state cyber operations are therefore bottlenecked by statutory gravity, organisational requirements and the frequent absence of a conflict context. These legal gaps shift the responsibility for prosecuting non-state cyber actors from international tribunals toward national courts.

C. Complementarity: deliberate design or institutional inadequacy

Under Article 17 of the Rome Statute a case is inadmissible if a state with jurisdiction is genuinely investigating or prosecuting it; the Court acts only when the state is unwilling or unable to do so.⁵¹ Unwillingness under Article 17(2) involves proceedings undertaken to shield a person from criminal responsibility, unjustified delay, or a lack of independence or impartiality, whereas inability under Article 17(3) arises from a total or substantial collapse or unavailability of the national judicial system. The OTP's Policy on Cyber-Enabled Crimes deliberately leaves ordinary domestic cybercrime to national legal systems while reserving the Court's jurisdiction for the core international crimes.⁵² The preceding analysis suggests that this residual role is not primarily an institutional failure. For state actors, national courts, through indictment practice and universal jurisdiction, are often the only forum capable of generating public attribution at all, given the ICC's own membership and referral constraints. For non-state actors, national statutes such as Section 66F of India's Information Technology Act reach conduct that the OTP's gravity threshold and the organisational requirement exclude by design. Complementarity therefore functions less as a fallback than as a structural allocation of labour: national courts absorb the volume of cyber-enabled prosecutions for both types of actor, while the ICC is reserved for cases of exceptional gravity and for standard-setting through instruments such as the 2025 Policy itself.

V. COMPARATIVE INSTITUTIONAL ANALYSIS

A. India

Section 66F of the Information Technology Act, 2000 creates the offence of cyber terrorism in India.⁵³ Under Section 66F(1)(A), the offence is committed by whoever, with intent to threaten

⁵¹ Rome Statute, *supra* note 13, art. 17; Sarah M. H. Nouwen, *The Rome Statute: Complementarity in Its Legal Context*, in SARAH M. H. NOUWEN, COMPLEMENTARITY IN THE LINE OF FIRE: THE CATALYSING EFFECT OF THE INTERNATIONAL CRIMINAL COURT IN UGANDA AND SUDAN 34 (2013), <https://www.cambridge.org/core/books/complementarity-in-the-line-of-fire/rome-statute-complementarity-in-its-legal-context/5FE71ABC0EB78FEE8BA94559E23B0F45>, <https://doi.org/10.1017/CBO9780511863264.006> (last visited Oct. 1, 2026).

⁵² OTP Cyber Policy, *supra* note 3, ¶¶ 5–6, 44.

⁵³ Information Technology Act, No. 21 of 2000, § 66F, INDIA CODE (2000), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited Oct. 1, 2026).

the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people:

- denies or causes the denial of access to any person authorised to access a computer resource;
- attempts to penetrate or access a computer resource without authorisation or by exceeding authorised access; or
- introduces or causes to be introduced any computer contaminant (such as malware or a virus),

and by such conduct causes or is likely to cause death or injury to persons or damage to or destruction of property, or disrupts, or knows that it is likely to cause damage to or disruption of, supplies or services essential to the life of the community, or adversely affects critical information infrastructure.

Under Section 66F(1)(B), the offence is also committed by whoever knowingly or intentionally gains unauthorised access to restricted information, data or a computer database with reason to believe that it may be used to injure the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order, or to the advantage of any foreign nation or group of individuals. Under Section 66F(2), whoever commits or conspires to commit cyber terrorism is punishable with imprisonment which may extend to imprisonment for life.⁵⁴

The Act also has extraterritorial reach. Under Section 1(2), it extends to the whole of India and applies also to any offence or contravention under it committed outside India by any person. Section 75 provides that the Act applies to an offence committed outside India by any person, irrespective of nationality, if the act or conduct constituting the offence involves a computer, computer system or computer network located in India.⁵⁵

The Information Technology Act, 2000 functions as a domestic national security and cyber-offence statute rather than as a law on core international crimes, and it has no structural or legal link to Articles 6 to 8 bis of the Rome Statute. India is not a State Party to the Rome Statute and, apart from the Geneva Conventions Act, 1960, which punishes grave breaches of the Geneva Conventions,⁵⁶ has no domestic legislation criminalising the core international crimes.

⁵⁴ Information Technology Act, *supra* note 53, § 66F(1)(B), (2).

⁵⁵ Information Technology Act, *supra* note 53, §§ 1(2), 75.

⁵⁶ Geneva Conventions Act, No. 6 of 1960, § 3, INDIA CODE (1960).

B. United States

In the United States, federal law at 18 U.S.C. § 1030, commonly known as the Computer Fraud and Abuse Act (CFAA) and enacted in 1986, punishes fraud and related activity in connection with computers. It protects “protected computers”, a term that extends to any computer used in or affecting interstate or foreign commerce or communication and so reaches most internet-connected devices, including smartphones and tablets.⁵⁷ The principal charges brought against international cyber actors are domestic offences, including:

- computer fraud and abuse under 18 U.S.C. § 1030;
- conspiracy under 18 U.S.C. § 371;
- wire fraud under 18 U.S.C. § 1343; and
- economic espionage under 18 U.S.C. § 1831.⁵⁸

United States courts can reach cyber conduct that occurred abroad when it affects US computers, victims or infrastructure, and the Department of Justice (DOJ) has consistently asserted extraterritorial jurisdiction through prominent indictments:

1. *2018 GRU election intrusions*. On 13 July 2018, a federal grand jury indicted twelve officers of Russia’s Main Intelligence Directorate (GRU) for conspiracy to commit computer intrusion offences, aggravated identity theft and conspiracy to launder money, in connection with interference in the 2016 US presidential election.⁵⁹
2. *Sandworm and NotPetya*. On 15 October 2020, a federal grand jury indicted six officers of GRU Unit 74455 (known as the Sandworm Team) for deploying destructive malware, including NotPetya, which disrupted computer systems worldwide and caused nearly US\$1 billion in losses to the three victims identified in the indictment alone.⁶⁰
3. *2014 PLA Unit 61398*. On 19 May 2014, the DOJ announced an unprecedented indictment of five officers of Unit 61398 of the Chinese People’s Liberation Army

⁵⁷ 18 U.S.C. § 1030(e)(2) (2018), <https://www.law.cornell.edu/uscode/text/18/1030> (last visited Oct. 1, 2026).

⁵⁸ U.S. DEP’T OF JUST., *Justice Manual* § 9-48.000 (Computer Fraud and Abuse Act), <https://www.justice.gov/jm/jm-9-48000-computer-fraud> (last visited Oct. 1, 2026).

⁵⁹ Press Release, U.S. DEP’T OF JUST., *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election* (July 13, 2018), <https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>.

⁶⁰ Press Release, U.S. DEP’T OF JUST., *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, *supra* note 1.

(PLA) for computer hacking and economic espionage directed at US commercial interests.⁶¹

This framework works best against state-linked operators, as indictments publicly unmask individuals hidden deep within state intelligence and military organs. The tool is not, however, confined to state organs: it also reaches non-state actors, such as the ransomware operators discussed in the LockBit and Colonial Pipeline (DarkSide) case studies below. The United States is not a State Party to the Rome Statute.

C. European Union

The European Union (EU) has no single prosecutor for core international crimes. The legal pathway to prosecuting these atrocities instead runs through the domestic laws and national judicial systems of individual member states. Germany is the leading example of this decentralised enforcement. Its Code of Crimes against International Law (Völkerstrafgesetzbuch, VStGB) establishes unconditional universal jurisdiction: under Section 1, the Code “applies to all criminal offences against international law designated herein; for offences under sections 6 to 12, it applies even when the offence was committed abroad and bears no relation to Germany.” German courts can therefore try individuals for genocide, crimes against humanity and war crimes regardless of the nationality of the perpetrator or the victim, or of where the act took place.⁶²

Directive 2013/40/EU harmonises national rules on attacks against information systems (covering illegal access, illegal system interference, illegal data interference and illegal interception), but it does not create international crimes.⁶³ It addresses transnational cybercrime rather than the *jus cogens* violations that ground universal jurisdiction. The national prosecution route is structurally suited to non-state actors who are physically present in an EU member state, since presence is typically what allows a domestic prosecution to go forward. The mechanism is significantly weaker against state-linked actors, who seldom come within reach, though it can succeed when one does. In the landmark Koblenz judgment of 13 January 2022, the Higher Regional Court of Koblenz convicted Anwar Raslan, a former colonel in the Syrian intelligence

⁶¹ Press Release, U.S. DEP’T OF JUST., *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014), <https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>; COUNCIL ON FOREIGN RELS., *Indictment of PLA Officers*, Cyber Operations Tracker (May 2014), <https://www.cfr.org/cyber-operations/indictment-of-pla-officers> (last visited Oct. 1, 2026).

⁶² Völkerstrafgesetzbuch [VStGB] [Code of Crimes Against International Law], June 26, 2002, BUNDESGESETZBLATT I at 2254, § 1, as amended, https://www.gesetze-im-internet.de/englisch_vstgb/englisch_vstgb.html (last visited Oct. 1, 2026).

⁶³ 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, arts. 3–6, 2013 O.J. (L 218) 8, <https://eur-lex.europa.eu/eli/dir/2013/40/oj>.

services, of crimes against humanity and sentenced him to life imprisonment for his co-perpetration of torture, murder and sexual violence in Damascus.⁶⁴

VI. CASE STUDIES

A. State actors

China: Volt Typhoon and APT41 (Double Dragon). Volt Typhoon is assessed by US and allied agencies to be a state-sponsored actor of the People's Republic of China (PRC) that has pre-positioned itself inside US critical infrastructure networks, including in the energy and water sectors, for likely future disruptive use rather than for espionage alone.⁶⁵ APT41 combines state-sponsored espionage with financially motivated intrusion, which itself tests the boundary between Tier One and Tier Two.⁶⁶ Target selection directed at critical infrastructure, together with the attribution by US and allied agencies, places Volt Typhoon in Tier One.

Russia: APT28 (Fancy Bear) and APT29 (Cozy Bear). APT28 and APT29 are publicly attributed to Russia's military intelligence service (the GRU) and to its Foreign Intelligence Service (the SVR) respectively.⁶⁷ Institutional nexus and post-hoc conduct, including Russia's refusal to extradite individuals named in US indictments, satisfy Tier One classification, engaging Article 28 in principle even though non-membership makes ICC prosecution unavailable except through the territorial route.

North Korea: Lazarus Group. Lazarus Group, which the US Treasury identifies as a state-sponsored group subordinate to North Korea's Reconnaissance General Bureau, combines espionage, sabotage and large-scale theft, including cryptocurrency theft, that funds state programmes.⁶⁸ Its financial nexus to state objectives, rather than to personal enrichment,

⁶⁴ Maria Pia Grizzuti, *Koblenz Court Issues Verdict in the Case of Anwar Raslan*, COMM'N FOR INT'L JUST. & ACCOUNTABILITY (Jan. 13, 2022), <https://www.cijonline.org/news/koblenz-court-issues-verdict-in-the-case-of-anwar-raslan> (last visited Oct. 1, 2026).

⁶⁵ CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY ET AL., *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Cybersecurity Advisory AA24-038A (Feb. 7, 2024), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

⁶⁶ Nalani Fraser et al., *APT41: A Dual Espionage and Cyber Crime Operation*, MANDIANT (Aug. 7, 2019), <https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation>.

⁶⁷ CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY ET AL., *Russian GRU Targeting Western Logistics Entities and Technology Companies*, Cybersecurity Advisory AA25-141A (May 21, 2025), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a> (identifying GRU military unit 26165 as APT28 and Fancy Bear); Fact Sheet, THE WHITE HOUSE, *Imposing Costs for Harmful Foreign Activities by the Russian Government* (Apr. 15, 2021), <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/> (naming the SVR, also known as APT29 and Cozy Bear); see also Press Release, U.S. DEP'T OF JUST., *Grand Jury Indicts 12 Russian Intelligence Officers*, *supra* note 59.

⁶⁸ Press Release, U.S. DEP'T OF THE TREASURY, *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups* (Sept. 13, 2019), <https://home.treasury.gov/news/press-releases/sm774>.

engages the object and target selection factor cleanly and supports Tier One classification despite its criminal methods.

Iran: APT42 and Peach Sandstorm. Mandiant assesses with moderate confidence that APT42 operates on behalf of the Intelligence Organization of Iran's Islamic Revolutionary Guard Corps and conducts surveillance of opponents of the regime, including dissidents abroad; Microsoft tracks Peach Sandstorm as an Iranian nation-state actor that has targeted the satellite, defence and pharmaceutical sectors.⁶⁹ Both are Tier One actors whose exposure under the Rome Statute remains theoretical, given the non-membership barriers.

B. Non-state actors

Cybercriminal and ransomware gangs: LockBit, BlackCat and DarkSide. DarkSide's 2021 ransomware attack on Colonial Pipeline disrupted the US fuel supply and shows that financially motivated non-state actors can inflict harm on a Tier One scale without state direction.⁷⁰ LockBit and BlackCat were disrupted by coordinated law-enforcement action, and the LockBit indictments charge individual Russian nationals by name, confirming that national indictment practice, not ICC process, has been the operative accountability mechanism.⁷¹

Hactivists: Anonymous, Anonymous Sudan and pro-Iranian units. These groups are decentralised and generally lack a responsible command or an established hierarchy, which count among the considerations for whether a group is sufficiently organised, whether as an organised armed group within the meaning of *Tadić* or as an organisation under Article 7(2)(a) of the Rome Statute.⁷² Anonymous Sudan's claimed state sympathies test the toleration-versus-direction factor at its most ambiguous, since claimed alignment alone does not satisfy Article 8 of the ILC Articles without proof of instruction, direction or control.

⁶⁹ MANDIANT, *APT42: Crooked Charms, Cons, and Compromises* (Sept. 7, 2022), <https://cloud.google.com/blog/topics/threat-intelligence/apt42-charms-cons-compromises>; MICROSOFT THREAT INTEL., *Peach Sandstorm Password Spray Campaigns Enable Intelligence Collection at High-Value Targets* (Sept. 14, 2023), <https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/>.

⁷⁰ Press Release, U.S. DEP'T OF JUST., *Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 7, 2021), <https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.

⁷¹ Press Release, U.S. DEP'T OF JUST., *U.S. and U.K. Disrupt LockBit Ransomware Variant* (Feb. 20, 2024), <https://www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant> (announcing the unsealing in the District of New Jersey of an indictment charging Artur Sungatov and Ivan Kondratyev); Press Release, U.S. DEP'T OF JUST., *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant* (Dec. 19, 2023), <https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant>.

⁷² *Prosecutor v. Tadić*, Case No. IT-94-1-AR72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995), <https://www.icty.org/x/cases/tadic/acdec/en/51002.htm>; *Situation in the Republic of Kenya*, *supra* note 49, ¶ 93; see generally Blank, *supra* note 10.

Volunteer cyber armies: the IT Army of Ukraine. Formed in response to the Ukrainian government's public call for volunteers, yet operating as a decentralised network without formal command, the IT Army sits on the boundary between Tier Two and Tier Three.⁷³ It shows that the six-factor test does not always yield a clean answer and that the toleration-versus-direction factor requires case-specific evidentiary judgment.

C. Grey-zone actor

NSO Group, an Israeli firm that develops the Pegasus spyware and supplies it to government clients, does not fit cleanly into any tier.⁷⁴ It is not a state organ under Article 4 of the ILC Articles, yet its product functions as an instrument of state surveillance once licensed to a government client, which engages the institutional nexus and toleration-versus-direction factors simultaneously. On the six factors, NSO Group's own conduct in developing and selling the tool sits closer to Tier Three, since the company acts independently of any single state's direction or control, while a client government deploying Pegasus against a target may itself be classified as Tier One for that specific act. This split outcome, in which the same underlying conduct yields different tier classifications for the developer and for the deploying state, is the clearest illustration in this paper's case studies of why a rigid three-tier model needs a fourth, hybrid category for commercially enabled state proxies, a refinement left for future work.

VII. SUGGESTIONS

1. *Implement the attribution framework as an operational tool.* Prosecutors at the ICC and in national systems can rely on Article 8 of the ILC Articles as the legal test and on the six factors as an evidentiary checklist. The framework has not yet been applied by any court and needs to be tested in actual cases.
2. *Create a standing cooperation agreement between the ICC and national authorities.* Such an agreement would allow evidence-sharing and joint investigations even in the absence of a referral. It depends on willing states, since states may refuse to share intelligence.

⁷³ Giulia Gabrielli, *Individual Criminal Responsibility of Non-State Actors Operating in Cyberspace for War Crimes under the ICC Statute*, 7 EU & COMPAR. L. ISSUES & CHALLENGES SERIES 286 (2023), <https://doi.org/10.25234/eclic/28268>.

⁷⁴ AMNESTY INT'L, *Forensic Methodology Report: How to Catch NSO Group's Pegasus* (July 18, 2021) (peer-reviewed by the Citizen Lab), <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>; Press Release, U.S. DEP'T OF COM., *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), <https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list>.

3. *Adopt model national legislation for cyber-enabled core crimes.* The model text should be actor-neutral and give guidance on charging such crimes by reference to the six factors, for adaptation by each state to its own legal system.
4. *Establish an evidentiary standard for private-sector attribution reports.* Courts need a standard for weighing the attribution reports published by companies such as Mandiant and Microsoft, on which several of the case studies above rely.

VIII. CONCLUSION

This paper set out to test whether national courts, rather than the ICC, are the primary forum for individual criminal accountability for cyber-enabled international crimes, for both state and non-state actors, though for different reasons. The doctrinal and comparative analysis supports this proposition. State actors evade ICC jurisdiction primarily through non-membership and the difficulty of attribution, while non-state actors are excluded primarily by the gravity threshold and by the organisational requirement for crimes against humanity under Article 7. National courts, through indictment practice, universal jurisdiction and domestic statutes such as Section 66F, have in practice absorbed the accountability function for both. The ICC's residual role under complementarity is best read as deliberate institutional design rather than failure, reserved for standard-setting and for cases of exceptional gravity. The three-tier classification and six-factor test developed here offer a transferable diagnostic tool, though the NSO Group case study shows that a hybrid fourth category for commercially enabled proxies remains an open question for further research.
