The hybrid threat of cyber-terrorist groups: critical gaps in the international legal framework

by **Matteo Pastorella**

Cyber conflict presents challenges beyond conventional security paradigms. A key blind spot is the use of non-state groups as state proxies.[1] The blurred distinction between state-sponsored and non-state-sponsored activities complicates attribution, weakening legal and strategic responses, and enabling aggression with impunity.

Cyber conflict is inherently asymmetric. By outsourcing operations to ideologically driven actors, states maintain plausible deniability,[2] complicating the application of international law on attribution and responsibility. Without a clear and direct state digital footprint, countermeasures become difficult, creating a permissive environment for malicious activities.

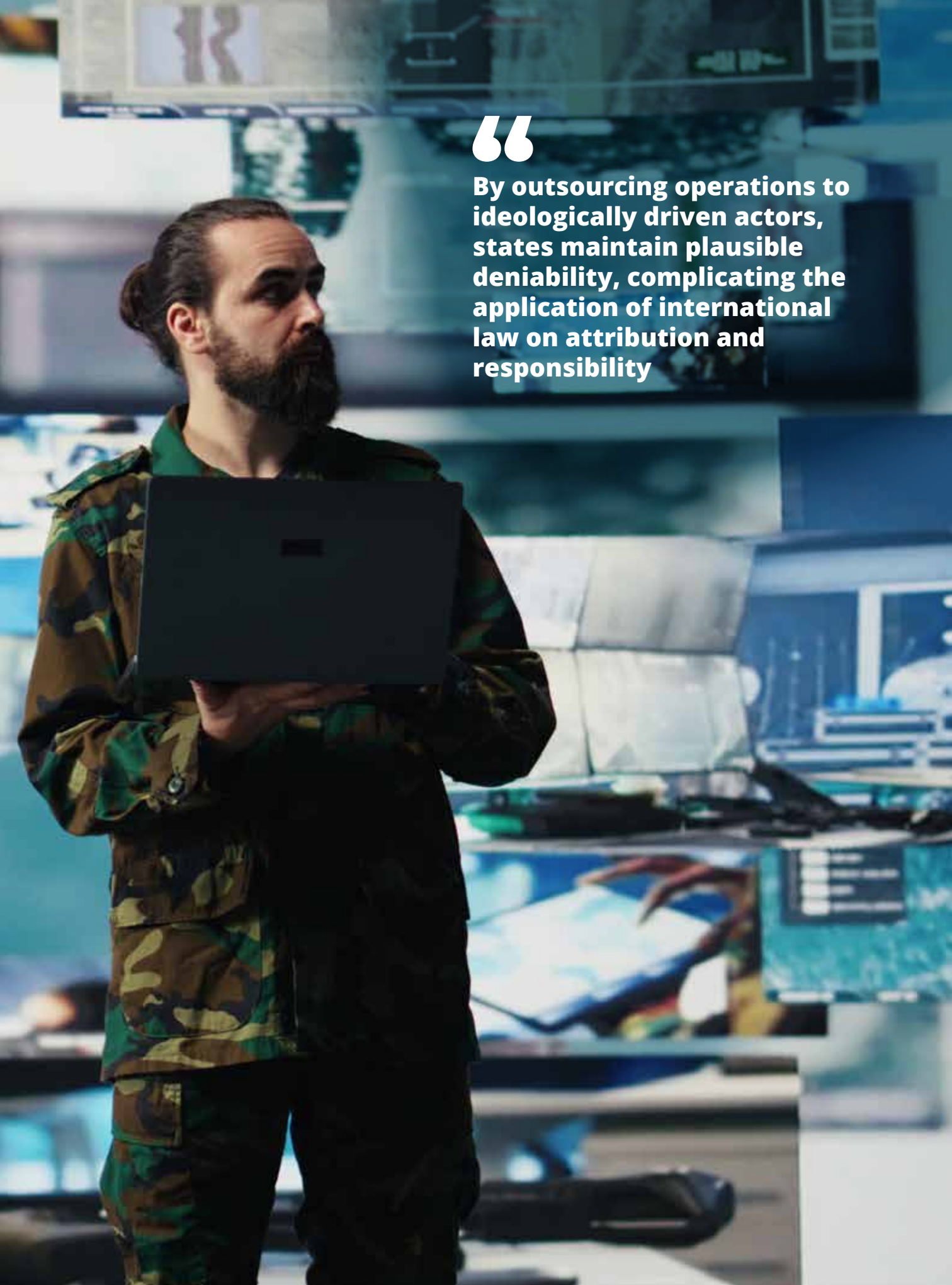
Hacktivist groups,[3] once decentralized and ideological, now access advanced capabilities through diverse levels of state sponsorship and support, carrying out malicious cyber activities as Advanced Persistent Threats (APTs) that rival military units. These APT campaigns are *advanced, deploying* logistical, technical and intelligence resources; *persistent, ensuring* long-term access; and a *threat, relying on* deliberate strategy with clear objectives. Unlike cyber-criminals seeking profit, cyber-terrorists pursue political aims, destabilizing societies and undermining security. This evolution requires re-categorizing cyber-terrorists within cyber threat intelligence: they are hacktivists with advanced capabilities whose campaigns must be treated as APTs.

This raises important challenges in the application of international law to cyber conflict. The reliance of states on APT actors is facilitated by a highly fragmented legal framework. Cyberspace is not in a legislative vacuum; it is governed by treaty and by customary norms applicable to the physical realm, including the United Nations Charter.

1 Katharina Kiener-Manu, Cybercrime Module 14: Key Issues – Cyberwarfare, *UNODC (n.d)*.

2 Justin Key Canfil, The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay, *Journal of Cybersecurity*, vol. 8, No. 1 (2022).

3 Check Point Software Technologies, What is Hacktivism? *Check Point Cyber Hub* (n.d.).



By outsourcing operations to ideologically driven actors, states maintain plausible deniability, complicating the application of international law on attribution and responsibility

"The central issue is not whether international law applies to cyberspace but how it should be applied."

Legally, the two concepts of attribution and the prohibition on the use of force (UN Charter, Article 2[4])[4] remain among the most contentious in defining a cyber-attack. Before attribution, it must be determined whether a cyber-attack is malicious – that is, a cyber operation breaching the prohibition on the use of force – since only that would justify proportional countermeasures.

As affirmed in the International Court of Justice's 1996 advisory opinion, Legality of the Threat or Use of Nuclear Weapons,[5] core legal principles apply regardless of the weapons employed – including cyber means and methods. Consequently, a cyber-attack may trigger the right of self-defence under Article 51[6] of the UN Charter and, theoretically, under Article 5 of NATO's North Atlantic Treaty. The 2007 Estonia cyber-attack[7] illustrated this possibility. Furthermore, the 2021 NATO Summit[8] confirmed that cyber-attacks could trigger a NATO response[9], thereby supporting an effect-based approach[10] that assesses consequences such as infrastructure destruction or loss of life to determine equivalence to traditional military attacks.

Once a cyber operation has been determined to be malicious, attribution is then analyzed across three independent dimensions: technical, legal, and political. Technical forensic analysis relies on indicators of compromise[11] and tactics, techniques, and procedures[12] of malicious actors. Yet, APT proxies and cyber techniques, such as Internet Protocol (IP) spoofing, hinder technical attribution. Consequently, legal attribution under international law is equally complex. Of the three dimensions, political attribution often takes precedence, limiting responses to media statements and diplomatic measures.

"While malicious acts – especially against critical infrastructure – are widely condemned, so-called naming and blaming often leads to uncertain results in today's polarized context."

Modern cyber conflict requires merging legal frameworks with new governance tools. Article 2[4] of the UN Charter, along with the principles of attribution, provides a legal basis but remains insufficient. For instance, although the Tallinn Manual[13] offers valuable guidance, it lacks binding enforcement mechanisms; similarly, the Schmitt Test,[14]

4 United Nations, Repertory of Practice of United Nations Organs: Supplement No. 7, *Volume I, Article 2(4)*.

5 International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, ICJ Reports 1996.

6 United Nations, Charter of the United Nations, *Chapter VII, San Francisco, 1945*.

7 Eneken Tikk, Kadri Kaska and Liis Vihul, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,Tallinn: Cooperative Cyber Defence Centre of Excellence, 2008.

8 North Atlantic Treaty Organization, Brussels Summit Communiqué, *NATO* (14 June 2021).

9 Tomas Minarik, *Cyber Attacks and Article 5: A Note on a Blurry but Consistent Position of NATO*, Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010.

10 Henry Farrell and Charles L. Glaser, The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine, *Journal of Cybersecurity*, vol. 3, No. 1 (March 2017), pp. 7–17.

11 Microsoft, What Are Indicators of Compromise (IoC)? *Microsoft Security* (n.d.).

12 National Institute of Standards and Technology, Tactics, Techniques and Procedures, *NIST Computer Security Resource Center* (n.d.).

13 NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, Tallinn: NATO CCDCOE, 2013.

14 James E. McGhee, Cyber Redux: the Schmitt Analysis, Tallinn Manual and US cyber policy, *Journal of Law and Cyber Warfare*, vol. 2, No. 1 (2013), pp. 64–103.

which assesses whether a cyber operation constitutes the use of force, exposes persistent ambiguities in attribution and response mechanisms.

Beyond legal instruments, cyber diplomacy plays a vital role in mitigating escalation risks and fostering international cooperation. The EU Cyber Diplomacy Toolbox[15] promotes multilateral cyber norms, deterrence, and responsible state behaviour, helping to mitigate geopolitical cyber destabilization. Meanwhile, confidence-building measures,[16] pioneered by the Organization for Security and Co-operation in Europe, enhance transparency and trust. In parallel, the UN Group of Government Experts outlined 11 voluntary, non-binding norms[17] for state behaviour in cyberspace, reinforcing existing standards against the misuse of information and communication technologies.

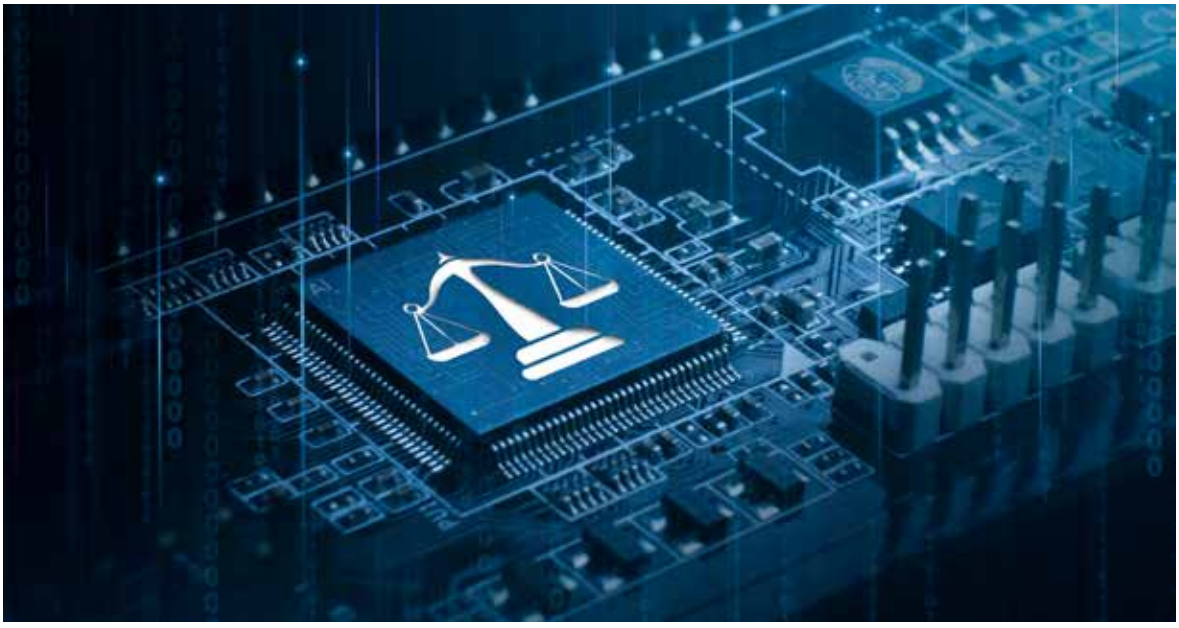
The systematic use of APTs remains a blind spot. Without effective attribution, state-sponsored aggression continues, undermining stability and sovereignty. The absence of a universal definition of cyber-terrorism – as seen by its omission in the 2001 Budapest Convention on Cybercrime[18] – complicates responses. Deterrence requires refining legal instruments, clarifying responsibility, and building enforcement. Without these measures, cyber aggression will persist, eroding security frameworks and destabilizing order.

[15] European Union, Cyber Diplomacy Toolbox, *European External Action Service* (n.d.).

[16] United Nations Office for Disarmament Affairs, Military Confidence-building Measures, *UNODA* (n.d.).

[17] United Nations General Assembly, *Resolution 70/237,* Developments in the Field of Information and Telecommunications in the Context of International Security, 23 December 2015.

[18] Council of Europe, *Convention on Cybercrime* (Budapest Convention), ETS No. 185, 23 November 2001.



About the Author

Matteo Pastorella is an advisor in international relations and cybersecurity. He holds several degrees, including degrees in Political Science, International Relations, and European Union Studies from LUISS Guido Carli and the University of Salzburg, as well as a Master's degree in Defence and Security from the University of Palermo. He has conducted research on defence and cybersecurity at specialized think tanks and parliamentary study centres, and has managed international projects at the Embassy of Colombia in Italy and the Italian Cultural Institute in Lima, Peru. He previously served within the Cybersecurity Unit of the Italian Ministry of Foreign Affairs and as a Cybersecurity Advisor in the framework of the G7 Task Force under the Italian Presidency of the Council of Ministers. He currently contributes to the Cyber Capacity Building Task Force at the Italian Ministry of Foreign Affairs. He has spoken at high-level institutional forums, including the Italian Parliament and the European Affairs Committee of the Chamber of Deputies, addressing issues related to cybersecurity, innovation, and European technological sovereignty. He is the author of several publications on cyber capacity building, hybrid threats, European strategic autonomy, and Latin American political processes, contributing to think tanks such as *Opinio Juris*, the Centro Studi Internazionali (CeSI), and the Istituto Affari Internazionali (IAI).

DECODING TRANSPARENCY

How to Foster Public Trust in Responsible AI Innovation in Law Enforcement

Public trust is the bedrock of legitimate, effective law enforcement. Its importance grows when law enforcement agencies adopt AI systems. Public attitudes towards AI in policing remain cautious, and trust in law enforcement agencies can strongly influence whether the public accepts new technologies. Therefore, it is up to law enforcement agencies to act effectively and, above all, fairly when making decisions about whether, when and how to adopt and implement AI systems.

DOWNLOAD THE PUBLICATION