ZOOM IN

The question:

An International Agency for the Attribution of Malicious Cyber Operations?

Introduced by Emanuele Cimiotta[*]

As the globe becomes more interconnected and reliant on digital technologies, cyber attacks are dramatically proliferating (taking the form of phishing, malware, ransomware, distributed denial of service, just to name a few of them). They may come from States, State-sponsored actors and non-state entities alike and target institutions, governments, essential service providers – including those in the fields of transport, education, healthcare, finance, defence, communication, energy – as well as single individuals and corporations. The global cyber crime costs are also increasing considerably, reaching several trillion USD per year.[1] These costs include, among others, disruption to the normal business and service operations, destabilization of government networks, theft of money, intellectual property, personal and financial data, lost productivity and restoration of hacked data and systems.

The significant harmful effects of malicious cyber activities tend to reverberate on international relations, thus resulting in reciprocal accusations possibly leading to international instability. Consider for example the large-scale cyber attack that in 2019 destabilized many websites and servers of governmental agencies, State bodies, media outlets as well as

[*] Associate Professor of International Law, Sapienza University School of Law (emanuele.cimiotta@uniroma1.it).

[1] C Ene, '10.5 Trillion Reasons Why We Need A United Response To Cyber Risk' Forbes (22 February 2023) <https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/>.

commercial and private financial companies in Georgia, and the international response that followed, which attributed the attack to the Russian military intelligence service.[2]

One of the main concerns related to international law is attribution, that is the process by which States victims of malicious cyber operations make judgments about the source or origin of the attack and the damage suffered. This aims at identifying the authors of the attack and their sponsors as well as holding them responsible under international law.

Yet attribution in cyberspace raises a number of legal, technical and political challenges. Some of them are also encountered by the international law on State responsibility in general (consider the determination of legal criteria for ascribing conducts of non-state actors to a State and of common standards on the sufficiency of the evidence supporting an accusation) whereas others are specific to cyber attribution (consider the difficulty in investigating cyber incidents and collecting evidence due to the anonymity, default secrecy and multi-layer nature of cyber attacks, as well as the ensuing need for capacity and information sharing).

Various proposals have been put forward to address these challenges. A major dilemma arises from the possibility of centralizing attribution in cyberspace in place of the decentralized cyber attribution efforts (both individual and multilateral) that have been made so far. Do some of the above-mentioned concerns fade if the technical, political, and legal attribution is less decentralized and more centralized?

Through the years calls for some sort of collective action to address State and State-sponsored cyber-operations have multiplied, especially receiving industry and academic support. Nonetheless, it is not entirely clear if an independent international attribution mechanism for State-sponsored cyber operations could avoid some of the difficulties, at least for the benefit of less technologically developed States and private industry. More specifically, the question that arises is what features and role this mechanism should possess: should it be a full-fledged international

[2] G Nakashidze, 'Cyberattack against Georgia and International Response: emerging normative paradigm of "responsible state behavior in cyberspace"?' EJIL: Talk! (28 February 2020) <https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative-paradigm-of-responsible-state-behavior-in-cyberspace/>.

court aimed at conducting investigations on certain cyber activities, collecting evidence, and identifying the wrongdoers – or alternatively a less utopian agency?

The two authors of this Zoom-in are very well-renowned experts in the application of international law to cyberspace. François Delerue explores the fascinating idea of constituting a cyber-related international organization open to States and non-state actors alike, on the footprints of the Permanent Court of Arbitration (PCA). Its main goal would not be to publicly attribute cyber operations to States or adjudicate disputes, but to develop common standards of proof and evidentiary practices, as well as to promote capacity building and norms compliance. Nicholas Tsagourias is however skeptical about the viability and effectiveness even of a PCA-like accountability mechanism for cyber operations, given that, among other reasons, States claim attribution as a sovereign prerogative and wish to maintain their freedom if, when and how to attribute.