SIOI
UNA Italy
OSSERVATORIO
sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana

Taking cyberattacks seriously: the (likely) Albanian cyber aggression and the Iranian responsibility

Annita Larissa Sciacovelli
Ricercatrice di Diritto internazionale, Università degli Studi di Bari Aldo Moro

1. ***The cyber aggression on Albania***. – There has been a great talking about the Islamic Republic of Iran during last years, starting from the stall of the nuclear deal, till the terrible and bloody repression of Iranian people protesting the Ayatollahs' regime. But few are the comments on the Iranian responsibility for the cyber-State attacks against Albania, a North Atlantic Treaty Organization (NATO) country.

The destructive cyber-attacks, launched on the 15th of July 2022 and in September 2022, were claimed on Telegram by two of the four groups of cyber criminals, *HomeLand Justice* and *APT42*, presumably acting from the Islamic Republic of Iran[1]. They cyberattacked Albanian government digital services and websites to disrupt, destroy, and leak government data. Their aim was to extract intelligence data, steal intellectual property, and imped military activities, as reported in the NATO statement of 8th September 2022[2]. Therefore, NATO and Albanian Government did not exclude "a possible collective response" towards Iran, applying Article 5 of the NATO Treaty on collective self-defense[3].

The digital forensic activity to attribute these attacks was conducted by Albania with the US Federal Bureau of Investigation (FBI), the US Cybersecurity and Infrastructure Security Agency (CISA), and two of the biggest private security companies, *Mandiant* and *Microsoft*[4]. The latter affirmed with a "moderate confidence" that the attackers were acting in support of Tehran's anti-dissident efforts *because APT42* is an Iranian State-sponsored cyber group pursuing the Iranian governmental interests[5].

Probably, the reason of Iranian cyber-attacks can be traced in the presence in Albania of 3,000 members of the opposition People's Mujahedeen of Iran (Mujahedeen-e-Khalq, MEK), which are hosted at the request of US Government and of the United Nations (UN)[6]. Teheran considers MEK a terrorist organization that, before the cyber-attacks, was planning to hold in Albania the 'Free Iran World Summit'. The event was cancelled because of the cyber-attacks.

The latter have been defined by the Albanian Prime Minister, Mr. Edi Rama, a State cyber aggression orchestrated and sponsored by Iran through the engagement of cyber

[1] https://www.cisa.gov/uscert/ncas/alerts/aa22-264.
[2] https://www.nato.int/cps/en/natohq/official_texts_207156.htm.
[3] https://www.nato.int/cps/en/natohq/official_texts_17120.htm.
[4] https://www.mandiant.com/media/17826.
[5] https://industrialcyber.co/threat-landscape/cyber-espionage-group-apt42-uses-spear-phishing-surveillance-operations-in-support-of-irans-strategic-priorities/.
[6] https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285.

groups[7]. Shocked by the stir of chaos and of insecurity in the country, the Albanian Government declared the Iranian embassy personnel *persona non grata*, obliging them to leave immediately the country[8]. For the White House spokesman these attacks "set(s) a troubling precedent for cyberspace"[9].

The Albanian case highlights the importance of cybersecurity as a new paradigm of *national* and *international* security in the wider threat landscape of malicious activities conducted in cyberspace by States also through non-State actors. For instance, in May 2022 Costa Rica was the target of a massive ransomware of the Russian cybergang *Conti*. The Government had to declare the state of emergency because the criminal hackers accessed many government agencies working for essential services, plunging the country into chaos[10]. Moreover, Member States of the European Union (EU), and especially Italy, have been targeted by cyber-criminal groups, probably acting from Russia. Hence, the decision of EU to develop the *European* Cyber Defense Policy to be better prepared for and respond to *cyberattacks*[11].

Specifically, criminal cyber gangs seem to have dual motivations: criminal motivation derived by economic profit and political motivations following the interests of States tolerating and sponsoring their malicious actions, despite their role of guarantors of the respect for international law.

Moreover, digital intrusion and disruption has become part of *modern warfare*, as demonstrated by the Russian Federation launch of massive cyberattacks against Ukrainian strategic infrastructures, short before the physical attack of February 2022[12]. The same happened in 2014 during the Crimean war and, going back in time, in 2008 against Georgia and in 2007 against Estonia, only to cite a few[13].

These attacks pose urgent complex questions that will briefly be analyzed in this paper and be widely exposed in the next future. The questions deal with: the cyber operations State-sponsored that may be categorize as an aggression; the problems of digital forensic in the process of attribution of these operations; the quasi-governmental role played in technical attribution by the high-tech companies and the need for an international investigation framework respectful of public law values.

---

[7] https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07.

[8] https://english.aawsat.com/home/article/3862471/iranian-diplomats-leave-embassy-albania-after-expulsion?amp.

[9] US statement of the 7th September 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/.

[10] https://www.wired.com/story/costa-rica-ransomware-conti/

[11] EU Strategic Compass for Security and Defence, 2022, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

[12] M. ORENSTEIN, *Russia's Use of Cyberattacks: Lessons from the Second Ukraine War*, in *Foreign Policy Research Institute*, 2022, https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/.

[13] F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, pp. 11-12.

2. A legal analysis of cyber aggression. – The debate whether the Albanian cyber-attack effectively consist of a State aggression (as defined by Albanian Prime Minister) should starts facing the longstanding lack of the notion of cyber-attack under Article 2(4) of the UN Charter. This norm prohibits the threat and the use of armed force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the UN.

The question is in which case a State-sponsored cyber operation may amount to this legal threshold and, more in depth, whether it is necessary that the attack brings injuries and physical damages, or whether it is sufficient the total or partial destruction or disruption of public and private Information and Communication Technology (ICT) systems[14].

It is well known that cyber operations that harm, in a tangible or intangible way, software, hardware, or data can significantly damage and impact government systems, financial services, and Critical Infrastructures services such as electricity, water, food and medicine supply, medical services or transportation and security systems[15].

There is no international convention directly addressing computer networks attacks or referring to the use of ICTs in the context of international security, because these legal provisions are designed for conventional weapons of *kinetic* nature. Indeed, Critical Infrastructures (like electric and nuclear power plants, railways, airports) have been defined *dual use targets* whose destruction can indirectly cause injury to human beings and material damages, as the *Stuxnet* operation showed[16]. They might also have cascading domestic, regional, and global effects of a great magnitude that are comparable to kinetic attacks, including the risk of violent escalation in cyberspace and can threaten international peace and security.

The problem is the lack of an international convention directly addressing computer networks attacks or referring to the use of ICTs in the context of international security, because the existing international treaties are designed only for conventional weapons of *kinetic* nature.

To fill this gap the UN Group of Governmental Experts in the field of Information and Telecommunications in the Context of International Security (UNGGE) and the UN Open-ended Working Group on Developments (OEWG) in their reports (2013, 2015 and 2021) recognize the applicability of international law principles and norms to State activities in cyber space, including the principle of the prohibition of the threat and the use of force[17]. Moreover, the OEWG last Report was negotiated and endorsed by all UN

[14] T. DIAS, A. COCO, *Cyber Due Diligence in International Law*, Oxford, 2022, p. 47 ff.

[15] For information on cyber operations affecting adversely States in recent decades see M. FINNEMORE, D. HOLLIS, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, in *The European Journal of International Law*, 2020, p. 970.

[16] In the *Stuxnet* case USA and Israel are believed to be responsible for physically destroying nuclear centrifuges in Iran in 2010 thanks to a piece malicious software they created, D.B. Hollis, *Could Deploying Stuxnet Be a War Crime?*, in *OpinioJuris.org*, 2011. On the legal definition of computer viruses as cyber weapons see S. LA PISCOPÌA, *Necessità di una definizione delle armi cibernetiche*, in *Eurasia* 2022, p. 37 f.

[17] See UN Group of Governmental Experts on the development in the field of information and telecommunication in the context of international security, Report of 24 June 2013, A/68/98, para. 19, UN General

States Members, giving a clear sign of the universal commitment to the UN Charter principles[18].

Both UN Groups propose voluntary, non-binding normative framework of responsible State behavior based on the 'due diligence principle' to strengthen international peace and security through building trust, confidence, and mutual international assurance in cyberspace[19]. Also, the EU, in its strategy for a cybersecure digital transformation in a complex threat environment, has adhered to the UN norms and principles of responsible State behavior[20]. Specifically, on this topic, a group of prominent scholars affirm that "in the cyber context, it is not the instrument of used to determines whether the use of force threshold has been crossed", but rather "its scales and effects" as far as it is comparable to a non-cyber operation raising the level of a use of force" (Rule 69 of Tallinn Manual 2.0 on international law applicable to cyber operation)[21]. This rule follows the *Nicaragua* judgment of the International Court of Justice on the 'scale and effects' paradigm, that is helpful to distinguish acts that qualify as use of force from those that do not[22].

Therefore, the '*Nicaragua approach*' can be applied in case where a State is arming (with malware) and training (for cyber operations) a group that is fighting against another State. In this case the supply and training should enable the group to conduct cyber operations that *amount* to the use of force, although it is very difficult to prove it for criminals in cyber space, also due to the invisible nature of cyber weapons[23].

In sum, it generally requires some degree of damage to physical objects or injury to human beings, but there is no common view among States. For instance, France, in its declaration on 'International Law Applied to Operations in Cyberspace' of 2019, affirms that it "does not rule out the possibility that a cyber operation without physical effects may also be characterized as a use of force. In the absence of physical damage, a cyber operation may be deemed a use of force against the yardstick of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the

Assembly resolution, Report of 22 July 2015, A/70/174, pp. 7-12. A. KASTELIC, *Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights*, 2021, https://unidir.org/publication/due-diligence-cyberspace-normative-expectations-reciprocal-protection-international.

[18] Report of the OEWG, 18 March 2021, A/75/816, para. 34; UN Secretary-General, Report on the Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behavior in the use of information and communications technologies, 2022, UN Doc. A/77/92, which collect the efforts taken by Member States at the national level to strengthen information security and promote international cooperation.

[19] UN General Assembly, Resolution 10 March 2021, Chair's Summary of the OEWG, A/AC.290/2021/CRP.3, paras. 1 and 11.

[20] EU Council Conclusions on the European Union's Cybersecurity Strategy for the Digital Decade, 22 March 2021, 7290/21.

[21] M. SCHMITT (ed.), *Tallinn Manual 2.0 on international law applicable to cyber operation*, Cambridge, 2017, p. 328 ff.

[22] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America), Merits, Judgment*, in *ICJ Reports*, 1986, p. 51, paras. 86 and 195.

[23] International Court of Justice, *Nicaragua Judgment*, cit., para. 228, M. SCHMITT (ed.), *Tallinn Manual*, cit., p. 332.

operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target" [24].

On this topic it is useful to remember the advisory opinion of the International Court of Justice on *Legality of the threat or use of nuclear weapons* which stated that the prohibition of the use of force applies "regardless of the weapons employed", and it is undeniable that computer viruses are cyber weapons[25].

Moreover, States hold the sovereign right to decide, on individual basis, whether they have been subjected to an armed attack that, depending on the extent of its intrusion and its effects, may violate the principles of sovereignty, of non-intervention or even the prohibition of the threat or the use of force[26].

In the light of what has been said up to now, and based on the technical attribution reported, it can be assumed that Albania has been target by a politically motivated cyberattacks, probably sponsored by Iran, that can be compared to an armed attack but that did not reach the threshold of an aggression. This position can be confirmed by the U.S. Cyber Command, operating with the Albanian Government, that reported that "a significant cyberattack" targeted Albania in 2022[27].

A similar problem was faced by Estonia in 2007 during *the first suspected incident of a State-sponsored cyberattacks. It was* conducted by a Kremlin-affiliated hacker group (*Killnet*) and it disrupted the vital computer systems of Estonia, caused a loss quantified at twenty-seven to forty million US dollars but did not create any physical damage, death, and destruction. *The Estonian* Prime Minister claimed the 'heavy attack' of the sovereign State, but he did not blame the Russian authorities directly, he just published a series of IP addresses originating from Russia [28]. This attack *was defined a* cyber malicious operation politically motivated[29].

Indeed, despite the exponential increase of this type of attacks, actually there is no practical cases of a State aggression attributable to governmental ICT services disruption and to digital data destruction. For *OEWG* "cyber operations are a reality of today's armed

---

[24] France, *International Law Applied to Operations in Cyberspace*, 2019, p. 3, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

[25] International Court of Justice, *Legality of the threat or use of nuclear weapons advisory opinion*, Advisory Opinions, in *ICJ Reports*, 1996, p. 226.

[26] M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014.

[27] US Cyber Command, *Committed Partners in Cyberspace": Following cyberattack, US conducts first defensive Hunt Operation in Albania*, in https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/, 2023.

[28] Declaration of the Minister of Foreign Affairs of the Republic of Estonia, 1st May 2007, https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia. On April 27th 2007, after removing the Bronze soldier, a Soviet war memorial, from the center of Tallinn, the critical and essential infrastructures of the Estonian state was crippled by cyber attackers. Estonian institutions, ministries, parliament, media, banks, newspapers, telecommunications companies, came under sustained and coordinated cyberattack that lasted for weeks. S. HAATAJA, *The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwielL3-5cT9AhWJ2aQKHWD2B84QFnoECAwQAQ&url=https%3A%2F%2Fresearch-repository.griffith.edu.au%2Frest%2Fbitstreams%2Fe6e5408e-5ff9-5afb-bd29-e54ba1cc932b%2Fretrieve&usg=AOvVaw2yDxFAN8TQtuefVIbtJi9M

[29] https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007).

conflicts, and their use is likely to continue to grow in the future"[30]. The problem is twofold: many States are developing ICT capabilities for military purposes and have formed active-duty cyber forces within their military structures and some non-State actors "have used military cyber capabilities in the context of contemporary armed conflicts, at times as stand-alone operations, at times in co-ordination with kinetic operations"[31].

These types of malicious operations and the *cyberwar* in Ukraine by Russia demonstrate their capacity to initiate a kinetic conflict (or to develop parallel to it) and the importance of the respect of the principle of due diligence in cyber space.

The State targeted by cyberattacks can act in self-defense in accordance with Article 51 of the UN Charter and international law. Self-defense can be realized using three options: either it recurs to the military force, or to cyberweapons or to both launching a hybrid attack.

Lastly, in case of cyber malicious operation politically motivated, launched directly or through cyber criminals, the targeted State can act through diplomatic responses and countermeasures depending on the extent of the attack.

Actually, we can observe also a new activity in cyberspace called 'hunting forward' that is a defensive cyber operation conducted by a team of cyber operators from the U.S. Cyber Command in partnership with the State victim of cyberattacks. In cybersecurity the operations called 'hunting forward' is "a proactive cyber defense activity, to observe and mitigate threats that are undetected on a network or system" in which the "HFO [hunting forward operation] teams do not mitigate threats on partner networks, but they *enable* their counterparts to pursue and address the threats found"[32]. The question now is if they are a new type of 'preventive self-defense' activity in cyberspace especially in case it is activated against a State[33].

3. The problem of cyber malicious activities attribution. – The second issue to be examined in the Albanian cyberattacks deals with the tricky problem of their attribution because of the difficulty to understand quickly and accurately who launched and directed them. This process is essential because it forms the basis of legal determinations, and it underpins the international responsibility of its perpetrator. Without attribution there is no possibility to declare the perpetrator accountable.

Attribution is articulated in three distinct and intertwined aspects: factual or technical, legal, and political. Technical attribution is the process of forensic investigation of a malicious incident to origins it to a platform and to associate its tooling and infrastructure. The legal attribution is the determination of the author based on legal

[30] *OEWG*, Final Substantive Report, 10 March 2021, A /AC.290/2021/CRP.2.

[31] J. BLESSING, *The Global Spread of Cyber Forces, 2000–2018*, 2021, https://ccdcoe.org/uploads/2021/05/CyCon_2021_Blessing.pdf.

[32] US Cyber Command, *Committed Partners in Cyberspace": Following cyberattack, US conducts first defensive Hunt Operation in Albania*, in https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/, 2023.

[33] Y. DINSTEIN, *War, Aggression and Self-Defence*, 5th ed., Cambridge, 2011, p. 88.

criteria to ascribe its legal consequences. Lastly, the political attribution is the task of the executive branch of the government, or of political institutions in general, to publicly declare the perpetrator, i.e., "naming-and-shaming"[34].

In cyberspace attribution is challenging because of the almost complete anonymity of the actor, of the multi-stage nature of cyberattacks, and of the indiscriminate and invisible nature of cyber tools. Attribution requires specific human and technical resources, lengthy time scales, and associated investigatory to avoid misattribution. It is worth noting that misattribution facilitate an escalatory reaction to an ICT incident, especially in case of 'false flag', and it can threaten international peace and security[35].

In the absence of international mandatory norms on State' cyber activities, UNGGE and OEWG affirmed that international responsibility under customary international law is extended to the State's use of ICTs. It means that it can be acknowledged responsibility for committing a malicious cyber operation directly or indirectly. In the last case State responsibility requires i) the use of proxies that act following its *instruction* or that are under its *control* (*de facto* agents), or ii) that the State acknowledged their act as its own, in accordance with Article 8, on the "Conduct directed or controlled by a State", of the UN Draft of 'Articles on Responsibility of States for Internationally Wrongful Acts'[36]. As cited in the *Nicaragua* judgment, the legal standard for attribution requests an effective control of the State on group or individual committing (cyber) attacks that is very difficult to be proved in cyberspace[37].

The difficulty is due to the invisible nature of cyber weapons and to the vast array of tools that cyber criminals can use to conceal and disguise them and to impersonate other computing systems (IP spoofing) and to anonymize communication through layers of encryption (onion routing).

In case of impossibility to attribute online disruptions for technical and legal reasons to a State, a useful solution is to consider the violation of the 'principle of due diligence' in cyberspace. It imposes to the State i) to ensure that its territory and ICTs systems are not used by non-State actor for acts contrary to international, and ii) to take all necessary measures to prevent the attack and the causing of significant harm[38].

Although States have divergent positions on whether the principle of 'due diligence' is a voluntary norm or a principle of international law imposing obligations,

---

[34] N. TSAGOURIAS, M.D. FARRELL, *Cyber Attribution: Technical and Legal Approaches and Challenges*, https://sites.tufts.edu/cilg/files/2018/09/attributiondraftsm.pdf,

[35] A. KASTELIC, *Non-Escalatory Attribution of International Cyber Incidents: Facts, International Law and Politics*, 2022, https://unidir.org/publication/non-escalatory-attribution-international-cyber-incidents.

[36] UN General Assembly, Resolution 10th March 2021, Chair's Summary of the OEWG, cit., para. 13; UN International Law Commission, Article 8 of the Draft of Articles on Responsibility of States for Internationally Wrongful Acts, UN General Assembly Resolution 56/83 of 12 December 2001, UN A/56/49(Vol. I)/Corr4; para. 7 of the commentary, UN General Assembly, Resolution A/56/10. See also Rule 17, *Tallinn Manual*, cit., p. 94; D. BROEDERS, E. DE BUSSER, F. CRISTIANO, T. TROPINA, *Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching Towards Lines in the Sand?*, in *Journal of Cyber Policy*, 2022, p. 108.

[37] International Court of Justice, *Nicaragua*, cit., pp. 62 and 64–65, paras. 109-115, 228.

[38] Report of the UNGGE, Note by the Secretary-General, A/70/174, 22 July 2015, para. 13 (c); M. SCHMITT (ed.), *Tallinn Manual*, cit., Rules 6 and 71, p. 339.

the International Court of Justice in the *Corfu Channel* decision affirmed clearly that States are obliged to make their best efforts to prevent use of their territory, and of areas on which they exercise jurisdiction, of which they are aware or should have been aware, that causes, or may cause, significant harm to another State[39].

However, it is important to bear in mind that it is quite difficult to collect digital evidence to prove that a cyberattack originated in a specific place, from a specific hardware, via a specific IP address executing a State order, due to the anonymity permitted by cyberspace and because of the absence of evidentiary international standards and rules.

All these critical issues limit the forensic capabilities, as clearly demonstrated in the Albanian case, where the technical evidence to declare 'Iranian State sponsorship' for the malicious use of ITCs by cybercriminals seems quite limited from the legal perspective, probably also due to security reasons.

Specifically, *Microsoft* declared "with high confidence" the Iranian responsibility based on evidence referring to the use of *similar* cyber tools by *other* cyber-Iranian criminals. For instance, the digital evidence "includes but is not limited to […] tools *previously* used by *other* known Iranian attackers"; it referred generally i) to targets *consistent* "with Iranian interests", ii) to the use of wiper code that was *previously used by a known Iranian actor*, and iii) to the use of "the same digital certificate used to sign *other* tools used by Iranian actors" (italics added)[40]. Lastly "[T]he messaging, timing, and target selection of the cyberattacks *bolstered [our] confidence* that the attackers were acting on behalf of the Iranian government".

Similarly, *Mandiant* "estimate(s) *with moderate confidence* that *APT42* operates on behalf of the Islamic Revolutionary Guard Corps' Intelligence Organization based on targeting patterns that align with the organization's operational mandates and priorities, which includes defending the [Iranian] regime against internal and external threats"[41].

The use of the term 'confidence' by the two private security companies in the technical attribution confirm the legal difficulties in attribution that cannot constitute a discretionary act. It is undeniable that to support a claim that a State has acted wrongfully, also for acts committed by non-State actor under its jurisdiction, legally requires credible evidence based on reliable factual elements, supplemented by circumstantial evidence and multiple sources.

Based on what has been said so far (and on open-source information) it is assumed that the Albanian cyber-attack was politically motivated and can be attributed to Iran for the lack of diligence for acts committed in its cyberspace, if not for its sponsorship.

---

[39] International Court of Justice, *Corfu Channel Case*, Judgment of April 9th 1949, in *I.C.J. Reports*, 1949, p. 4, para. 8; Italian Foreign Ministry, *International Law and Cyberspace*, 2021, p. 15, https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf.

[40] https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government.

[41] https://www.mandiant.com/media/17826, p. 12.

4. The role of private security companies in attribution: performing government-like roles? – The third issue in the Albanian case deals with the role of the two high-tech companies in the process of attribution. It shows the creation of a *de facto* system of 'public-private relationships' that on one side is necessary for the forensic analysis, because actually only high-tech private security companies possess the technologies to investigate that are needed by governments. On the other hand, this informal and complicated system of public-private relationships, that is characterized by the out-sourcing of governmental functions to private actors, *can* undermine public law values, such as accountability, transparency, and fairness in the attribution procedure, whose respect is not legally required[42]. These are public constraints that are usually applied to national intelligence systems, and from which are exempted private actors when they are performing *de facto* a *quasi-government role* on key cybersecurity issues.

The outcome is that they play the role of private-intelligence partnership without being held accountable of eventual mistake during the digital forensic activity. Hence, one should question about the legitimacy of private parties performing government-like actions, especially when discretionary policy choices can lead to misattribution especially in case of 'false flag', that is an operation designed to deflect attribution to an uninvolved party[43]. Hence, we express the need of legal tools for remediation also in case of abuse of power.

These complexities require solutions to safeguard public law values and to secure privacy: a solution that can be enhanced realizing digital autonomy, although it requires time and great investments, and it is almost difficult to realize.

5. Concluding remarks. – The complexity of the Albanian case reminds us of the universal relevance of sophisticated cyber threats and shows the urgent need to collectively address them and to develop evidentiary standards in international law. The lack of an international binding legal framework of responsible States' behavior in cyberspace results in a *grey area* that some States exploit being aware that the target States are uncertain about how they could react under international law. In the next future there might be a change in the legal doctrine of *jus ad bellum* by States to face the *shift* from a kinetic battlefield to a cyber one also using cybercriminals[44].

Therefore, it is urgent a regulatory response at the international level by the OEWG, that has always been cautious because of the different States approaches on the topic. In the meantime, some solutions can be proposed to face technical, legal, and political

[42] C. GUITTON, *Inside the Enemy's Computer: Identifying Cyber Attackers*, Oxford, 2017; S. ROMANOSKY, *Private-Sector Attribution of Cyber Attacks: A Growing Concern over the U.S. Government?*, 2017, https://www.lawfareblog.com.

[43] E.K. EICHENSEHR, *Public-Private Cybersecurity*, in *Texas Law Review*, 2017, p. 504. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847173.

[44] M.M. FOGT, *Legal Challenges Or "Gaps" By Countering Hybrid Warfare – Building Resilience In* Jus Ante Bellum, https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf.

complexities of the process of attribution assuming its pivotal role in the determination of international responsibility.

Specifically, States should avoid unilateral actions in case of cyberattacks that may escalate and endanger 'international cyber peace and security' and they should settle their disputes by peaceful means through consultation. To this end it will be useful that the UN and/or international regional organizations will: i) categorize cyberattacks and incidents that may amount to an aggression to differentiate them with other less grave, ii) institutionalize an international attribution mechanism, iii) introduce an *ad hoc* and common evidentiary regime with protocols for collecting and analyzing evidence, including the reversal of the burden of proof, and iv) standardize the methods of investigations to reduce concerns over the integrity of evidence.

These proposals can positively change the process of attribution because they aim to centralize this process at an international level; to limit the quasi-governmental role of private security companies and contribute to the creation of international investigation framework respectful of the principles of transparency and fairness.

Concluding, the Albanian case has been a wake-up call for the likely aggressive Iranian posture in cyberspace, also outside Middle East, but we must all be aware that cyber weapons race (by State and non-State actors) is a reality, and that international peace and security may be in danger also in cyberspace.

Marzo 2023