Davide Giovannelli
DOI:10.33179/BSV.99.SVI.11.CMC.24.2.3

ZUNAJOZEMELJSKA PRISTOJNOST ZA KIBERNETSKO VOHUNJENJE: NOV TREND V MEDNARODNEM PRAVU ALI LE PRIMER UPORABE PRAVA KOT OROŽJA

EXTRATERRITORIAL JURISDICTION OVER CYBER ESPIONAGE: A NEW TREND IN INTERNATIONAL LAW OR JUST AN EXAMPLE OF LAWFARE

Povzetek Praksa v državah kaže, da obveščevalne agencije ne izvajajo le vohunjenja, temveč tudi druge, manj plemenite dejavnosti, kot je hibridno vojskovanje. Mednarodno pravo tradicionalno dopušča vohunjenje, domače kazensko pravo pa navadno omogoča njegov pregon. Ne glede na to se nestabilno ravnovesje zaradi rasti kibernetskega vohunjenja, ki omogoča učinkovitejše izvajanje, spreminja. Ni presenetljivo, da se povečuje zanimanje za prakso držav, saj so bili sprejeti novi pravni instrumenti za izvajanje zunajozemeljske pristojnosti nad kibernetskim vohunjenjem. V članku poskušamo oceniti, ali je treba nove pravne instrumente obravnavati kot nov pojav v mednarodnem pravu ali kot občasno uporabo prava kot orožja.

Ključne besede ***Zunajozemeljska pristojnost, kibernetsko vohunjenje, uporabo prava kot orožja , neprimerno tuje vplivanje, ekonomsko vohunjenje.***

Abstract States' practice shows that intelligence agencies have carried out not only espionage, but also other, less noble activities, such as hybrid warfare. Traditionally, international law tolerates espionage, while domestic criminal law generally allows its prosecution. However, this precarious equilibrium is changing due to the growth in cyber espionage, which allows espionage to be carried out more effectively. Not surprisingly, there is increasing interest in States' practice, as new legal instruments for exercising extraterritorial jurisdiction over cyber espionage have been adopted. This article tries to assess whether these new legal instruments should be considered a new trend in international law, or a sporadic exercise of lawfare.

Key words ***Extraterritorial jurisdiction, cyber espionage, lawfare, improper foreign influence, economic espionage.***

Introduction

As shown in this article, »traditional« espionage, as well as hybrid threats[1] and economic espionage, are not new practices. States have carried out such activities for centuries. However, the real game-changer of recent decades has been the impact of Information and Communications Technologies (ICT). ICT, indeed, is allowing more and more States to carry out espionage in all its forms more effectively. As we shall see in this article, this new situation leads to a change in the applicable legal framework in order to react more effectively towards these new threats.

This article aims to analyze this phenomenon, focusing on situations other than an armed conflict. First, the article will analyze what cyber espionage is. It will show that a comprehensive analysis cannot be limited only to what is legally considered espionage, but instead it is vital to also consider other clandestine activities that may be carried out by intelligence agencies from time to time. Secondly, espionage and other clandestine activities will be considered from international and domestic criminal law perspectives. Thus, this article will deepen understanding of how ICT has influenced and modified espionage and other clandestine activities. Finally, the article will address the emerging trends in criminal and administrative law to tackle such cyber threats, and it will try to measure their effectiveness in order to assess whether these are new trends in international law, or just an example of lawfare (i.e. the use of law to achieve national security objectives).

1 WHAT CYBER ESPIONAGE REALLY IS

In order to begin this analysis, it is opportune to define what is traditionally considered as espionage. It is helpful to recall the following passage from Oppenheim's book on International Law of 1905:

»*Spies are secret agents of a State sent abroad for the purpose of obtaining clandestinely information in regard to military or political secrets. Although all States constantly or occasionally send spies abroad, and although it is neither morally nor politically and legally considered wrong to send spies, such agents have, of course, no recognised position whatever according to International Law, since they are not agents of States for their international relations. Every State punishes them severely when they are caught committing an act which is a crime by the law of the land, or expels them if they cannot be punished. And the spy cannot legally excuse himself by pleading that he only executed the orders of his Government. The latter, on the other hand, will never interfere, since it cannot officially confess to having commissioned a spy*« (Oppenheim, 1905, pp 490-491).

Oppenheim's extract clearly shows that espionage is a common practice in international relations, and it gives some valuable features to shape its definition:

[1] *We will consider the following definition of 'hybrid threat': a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.*

1. From a material point of view, this activity is committed abroad (and quite obviously clandestinely);
2. Its purpose/intent is to obtain information with regard to military or political secrets;
3. It is not morally or politically and legally considered wrong by States, but those who carry out such activity (i.e. spies) can be prosecuted or expelled by the State in which the espionage is committed.

However, it would be naive to think that espionage is limited to this legal definition of espionage. States' practice, indeed, shows that intelligence agencies have been constantly used even for other less noble activities, even though States are – quite obviously – reluctant to admit it. It may not be unreasonably denied that sometimes States have been involved in some illegal – or at least regrettable – activities, such as the abduction of people from the territory of another State[2], or disinformation campaigns (Selvage, 2019; Geissler & Sprinkle, 2013).

At the beginning of the Cold War, a US Department of State Policy Planning Staff Memorandum pointed out that »*Political warfare is the logical application of Clausewitz's doctrine in time of peace. In the broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (such as ERP—the Marshall Plan), and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states*« (National Archives and Records Administration, 1948). Looking at the other side of the barricade, already in the 1960s there was a clear awareness among NATO Nations of the threat posed by the clandestine activities of the Soviet Union (NATO-wide co-operation and coordination in the field of psychological warfare – proposal by the Federal Republic of Germany, 1960). It goes without saying that parallel forms of intervention have been carried out by Western States (US *in primis*) also *vis-à-vis* their Allies, as frankly admitted by a reliable former CIA officer[3].

---

[2] *Without considering the most recent US practice of 'extraordinary rendition', it is worth recalliyng the following cases, already quoted by the UN International Law Commission:*

- *The abduction, from Switzerland to Italy, in 1928, of Cesare Rossi, by people probably acting by agreement with the Italian police;*
- *The abduction, from Switzerland to Italy, in 1935, of Berthold Jacob, by people employed for this task by the German Gestapo;*
- *The abduction, from Argentina to Israel, in 1960, of war criminal Adolf Eichmann, by a group of Israeli nationals in a suburb of Buenos Aires;*
- *The abduction, from Germany to France, on 1961, of ex-Colonel Argoud, one of the leaders of the OAS, by unknown individuals.*

Yearbook of the International Law Commission, 1971, Vol. II, Part One, pp 265-266.

[3] *Shane, 2018, where a former CIA officer – referring, among other things, to the CIA's activity in support of Italian candidates – admitted the following: »We've been doing this kind of thing since the CIA was created in 1947,« said Mr. Johnson, now at the University of Georgia. »We've used posters, pamphlets, mailers, banners — you name it. We've planted false information in foreign newspapers. We've used what the British call 'King George's cavalry': suitcases of cash«.*

Thus, it should be clear that not all activities carried out by intelligence agencies can be labelled as espionage. In other words, a clandestine activity carried out by an intelligence agency does not mean that it necessarily falls within the legal definition of espionage.

2 INTERNATIONAL LAW PERSPECTIVE

In essence, scholars' opinion over (traditional) espionage can be divided in the following three ways (A. J. Radsan, 2007, pp 601-607):

a) Espionage is not illegal (Oppenheim's view);

b) Espionage is illegal;

c) Espionage is neither legal nor illegal.

Followers of options A and C give weight to the judgement of the Permanent Court of International Justice in the Lotus case, where it was stated that: »*International law governs relations between independent States. Therefore, the rules of law binding upon States emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed*«.

Therefore, as specified by a scholar: *»According to the principle stated in the Lotus Case it is for those who assert the existence of the rule of law restricting state activity to show that such a restrictive rule exists. Moreover, in any case, it is not a self-evidently sound approach to the newish problems of peacetime espionage to assume that it must be unlawful unless it can be justified on some specific grounds. In the face of such rapid technological, strategic, and psychological change, it seems to be particularly important to approach the matter by asking whether there are any principles manifest in the practice of states that evidence any existing restrictive rules, or any sufficiently close analogies. With the greatest respect, I can at present find none«* (Stone, 1962, p 33).

On the other hand, case law presents cases that support the option that espionage is considered illegal. According to the Canadian Federal Court, *»the intrusive activities … are activities that impinge upon the principles mentioned above of territorial sovereign equality and non-intervention and are likely to violate the jurisdiction's laws where the investigative activities are to occur*« (Federal Court, Blanchard J., Ottawa, April 24, 27, June 14, 2007).

Thus, without wishing to enter into the controversial question of which of the three options should be preferable, even assuming as the most appropriate option B

(i.e. espionage is illegal), the illegality of espionage is sustainable only as far as a violation of territorial sovereignty and non-intervention occurs. Such a conclusion is also consistent with the undisputed practice of passive intelligence reconnaissance towards a foreign State, exercised by another State from its territory, the high seas or even outer space[4].

Additionally, the said conclusion also appears to be corroborated by the most recent case law of the International Court of Justice (ICJ). As convincingly pointed out in a comment to the ICJ order granting provisional measures in the case Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia): »*At present, it seems difficult to argue that a rule of customary international law, based on widespread state practice accepted out of a sense of legal obligation, provides that the interception of a foreign state's communications is either lawful or unlawful. But it can certainly be argued that such activities by an established state (here, one that belongs to an intelligence alliance with other intelligence powers) carried out against a small, newly established state create an unfair and unethical balance in international dispute settlement and negotiations*« (Bettauer, 2014, p 768).

In laymen's terms, the ICJ found that in such a situation (i.e. the Timor Sea International Arbitration between the Democratic Republic of Timor-Leste and Australia), »*a State has a plausible right to the protection of its communications with counsel relating to an arbitration or negotiations, in particular, to the protection of the correspondence between them, as well as to the protection of confidentiality of any documents and data prepared by counsel to advise that State in such a context*« (Timor-Leste v. Australia, Provisional Measures, Order of March 3 2014, ICJ Reports 2014, paragraph 27). Therefore, by a process of *a contrario* reasoning, it seems logical to conclude that ICJ opinion supports the idea that espionage should be considered, *per se*, as unlawful or illegal. Even the ICJ judgement in the case of Jadhav (India v. Pakistan) does not contradict this view. Indeed, the ICJ's recognition that the safeguards provided for in Article 36 of the Vienna Convention on Consular Relations of April 24 1963 are applicable even in the case of allegation of espionage activities can support only the (undisputed) rule that espionage can be punished by domestic criminal law. However, it does not allow the consideration of espionage *per se* as a breach of international law.

In order to analyze hybrid warfare in the light of the principle of foreign intervention, it is essential to recall the ICJ judgement in the case of Contras v. Nicaragua. In short, this judgement emphasized that:

[4] *In the past, the USSR attempted to qualify observation from space to collect intelligence as illegal (see: Soviet Statement in the General Assembly, First Committee, 17th Session, 1298th Meeting, December 3 1962). States' practice, however, has not followed the USSR's point of view.*

– Each State is permitted, by the principle of State sovereignty, to freely decide the choices of a political, economic, social and cultural system and the formulation of foreign policy;
– Foreign intervention is wrongful when it uses methods of coercion with regard to such choices;
– The element of coercion, which defines and indeed forms the very essence of prohibited intervention, is particularly obvious in the case of an intervention which uses force.

The above implies that foreign intervention could be considered wrongful only as far as methods of coercion are used. Thus, it is necessary to understand what coercion means and whether foreign intervention relying on ICT can be considered coercive. In this regard, as pointed out by a scholar: »*although 'coercion' arguably has never been adequately defined and is still an indistinct concept, the Nicaragua dictum remains the leading case on the issue*« (Lahmann, 2020, p 197). Thus, unless the threshold for qualifying a cyber-operation as use of force is met, it would be problematic to qualify a foreign intervention through ICT means as coercive.

Additionally, even the possibility of relying on other international law provisions to qualify a foreign intervention through ICT means as wrongful is hardly disputed. There is no consensus on the possibility of relying on the principle of sovereignty, even within Western countries. In this regard, it is sufficient to recall that »*The United Kingdom does not consider that the general concept of sovereignty provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention«* (UN Official Compendium, 2021). Through an innovative approach, other scholars have tried to rely on the right to self-determination. Ohlin, for example, argued that »*foreign interference is a violation of the membership rules for political decision-making, i.e., the idea that only members of a polity should participate in elections—not only concerning voting but also concerning financial contributions and other forms of electoral participation. Outsiders are free to express their opinions but covertly representing themselves as insiders constitutes a violation of these political norms, which are constitutive of the notion of self-determination, just as much as covertly funnelling foreign money to one candidate«* (Ohlin, 2021). However, even this proposal, to date, seems not to be supported by a significant States' practice and thus lacks the *opinio juris* to rise as a customary rule of international law. To corroborate this conclusion, we refer to and concur with the in-depth survey of States' practice already carried out by Lahmann (2020). Additionally, along the same lines, the UN Official Compendium of Voluntary National Contributions to the subject of how international law applies to the use of information and communications technologies shows that States are worried about foreign influence, mainly for malicious cyber activities targeting foreign elections, but they have maintained a cautious attitude on this topic and avoided considering any form of foreign influence as unlawful *per se*.

Therefore, as already pointed out by the legal doctrine, »*to date, States appear by and large to have maintained a posture of constructive ambiguity when it comes to the international lawfulness of influence operations – via cyber means or otherwise – that do not directly alter votes as they were cast*« (Chimène, 2021, p 193). Even another distinguished author argued that »*beyond the few unequivocally wrongful cases, multiple fault lines in the international law governing cyber activities could hinder definitive characterisation of particular election interference as unlawful*« (Schmitt, 2021, p 764).

3 DOMESTIC CRIMINAL LAW PERSPECTIVE

Concerning criminal law, the possibility of prosecuting espionage and other forms of coercive foreign intervention if the illicit conduct is carried out in the territory of the targeted State is undisputed[5].

States' practice concerning »pure« espionage committed in the territory of the »Victim State« instead shows that expulsion as *persona non grata* is often preferred over criminal prosecution[6]. Municipal law, however, seems not to preclude prosecution, even in the case of espionage committed abroad (i.e. out of the territory of the »Victim State«) by a foreigner, although the *actus reus* is not forbidden by the offender's national law[7].

With regard to improper foreign influence on elections or political systems, almost every legal system has provided regulation on the financing of political parties to prohibit – or at least regulate transparently – contributions from foreigners. The relevant case law on this topic is minimal, although, for example, the Soviet Union's massive transfer of financial resources to the Italian Communist Party (PCI) is documented (Drake, 2004). Finally, concerning economic espionage, it is worth starting from the G7 Declaration (2017) on responsible state behaviour in cyberspace. This document recalled the following non-binding norm of State behaviour during peacetime: »*No country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, to provide competitive advantages to companies or commercial sectors*«. However, as

---

[5] *See the High Court of Auckland judgment of November 22 1985 (concerning the sabotage of a Greenpeace ship – which resulted in the death of a Dutch citizen and the sinking of the ship – carried out in New Zealand by two agents of the French Directorate General of External Security) and the Italian Court of Cassation judgement of March 11 2014, No. 39788 (concerning the abduction and illegal transfer abroad of a person, carried out in Italy by some U.S. CIA officials).*

[6] *US memorandum giving detailed information on the illustrative list of Soviet espionage agents apprehended in the United States since the death of Marshal Stalin, attached to the Letter dated 60/05/24 from the Permanent Representative of the United States of America to the Secretary-General, UN document S/4325.*

[7] *According to the US judgment in the United States v. Zehe, 601 F. Supp. 196 (D. Mass. 1985), »the Court finds that the [Espionage] Act may be applied extraterritorially to both citizens and noncitizens because of the threat to national security that espionage poses«. Even the German Federal Constitutional Court in the Espionage Prosecution Case (Espionage Prosecution Case (Case No 2 BGs 38/91), Bundesgerichtshof [BGH][Federal Court of Justice] Jan. 30, 1991, 94 International Law Reports [ILR] 68, 70, 1994 (Ger.) took this view. For a deep analysis see Krizek, 1988.*

highlighted by some scholars (Hemmings and Swire, 2019), economic espionage is still in the background of the debate on the mechanism allowing law enforcement authorities of different States to request e-evidence directly from a cloud service provider abroad. Regardless of the substance of that concern (and the additional concern over privacy protection in the US), it is to be noted that the negotiation between the EU and the US for an agreement on facilitating access to e-evidence is still ongoing. Thus, absolute mutual trust has not been achieved even between Western States. So it is not surprising that national law in every legal system provides two levels of protection against economic espionage. On the one hand, National Government maintains the right to authorize (or deny) certain transactions involving foreign investment in strategic sectors, whenever the effect of such transactions would undermine the national security of the State concerned. To that end, we can recall Regulation (EU) 2019/452 of the European Parliament and of the Council of March 19 2019, establishing a framework for the screening of foreign direct investments into the Union, as well as the US Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). Additionally, some Nations also have a dedicated legislation on trade secret theft. The US, for example, pursuant to the Economic Espionage Act of 1996 (EEA), has considered two forms of trade secret theft as a criminal offence: (i) theft for the benefit of a foreign entity (economic espionage), and (ii) theft for pecuniary gain (theft of trade secrets).

4 THE IMPACT OF ICT

In order to assess the impact of ICT on the different forms of espionage, we should start by acknowledging that it is not limited to »traditional« espionage, but rather it also affects hybrid warfare and economic espionage. This implies that all these activities, compared with the past, now require a more limited presence of spies in the targeted State's territory and less financial effort. In other words, cyber espionage is dependent mainly on States' availability (directly or by proxy) of ICT technologies; such technologies, however, are not too expensive and so easily obtainable. This new paradigm is not without consequences, as ICT technologies are no longer limited to a few Nations but, on the contrary, they are available to many Nations and criminal groups as well. Additionally, with specific reference to hybrid warfare, social media and new technologies have allowed everyone to deliver their message to a broad target audience. In the past, conversely, mainstream media groups were the only ones able to do that[8]. Not surprisingly, therefore, social media and new technologies have become instruments for foreign influence operations and disinformation. Moreover – even if the question of international lawfulness of influence operations

[8] *The European Court of Auditors pointed out that »disinformation has been present in human communication since the dawn of civilisation and the creation of organised societies. However, what has changed in recent years is its sheer scale and the speed with which false or misleading information can reach its intended and unintended audiences through social media and new technologies. This may cause public harm«. See: Special Report No 09/2021 from the European Court of Auditors »Disinformation Affecting the EU: Tackled but not Tamed«, April 27 2021. Available at: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf.*

has not yet been solved – it is worth noting that nowadays Western democracies seem more vulnerable to foreign influence, while in the past it was East communist regimes that suffered more from such types of influence. This turnaround favouring authoritarian regimes should be considered an unintended consequence of the said ICT technologies.

However, the above alone is not deemed sufficient to explain the increasing threat posed by the impact of ICT. The fact that more States are potentially able to carry out cyber espionage is not sufficient to explain why there is also more willingness to carry out such activities. After all, resorting to cyber espionage could be rewarding, but it could also be dangerous. Therefore, it is a matter of how States perceive the reward-cost calculus. Among the many possible considerations, some elements seem to tip the balance towards a more aggressive posture in applying ICT to carry out cyber espionage. On the one hand, in the case of ICT exploitation, strategic deterrence – i.e. the combination of denial and punishment – does not work correctly. Unlike nuclear weapons, which are not meant to be used due to the mutual assurance of destruction (MAD) of both the attacker and the defender, cyber operations are frequently conducted, since no MAD is applicable. On the other hand, difficulties in determining the attribution to a State of ICT employment for cyber espionage is another incentive for such employment. Moreover, as cyber spies are seldom in the territory of the »victim« State, the latter will have almost no possibility of apprehending and prosecuting those responsible for such crimes. This situation entails an incentive to rely on cyber espionage, since a high sense of impunity is widely perceived. Additionally, the legal understanding of the threshold of cyber-attack for triggering the applicability of the law of armed conflict (LOAC) could also be relevant. To put it simply, the higher the threshold, the more States will be prepared to accept the costs – e.g. possible reputational damage – associated with cyber espionage, since they will not bear the risks of triggering an armed conflict.

Concerning the last point, it is worth noting States' opinions, as expressed in the UN official Compendium of Voluntary National Contributions to this topic[9]. Such opinions are in line with the view expressed in the Tallinn Manual 2.0 on International Law Applicable to Cyber Operations. It means, following the reasoning of the ICJ's Nicaragua judgement, that:

– »*A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force*« (Tallinn Manual – Rule 69);

[9] *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established according to General Assembly resolution 73/266. UN document A/76/136 dated July 13 2021. However, it is worth noting that the Netherlands affirmed the following partially nuanced position: »In the view of the government, at this time, it cannot be ruled out that a cyber operation with a severe financial or economic impact may qualify the use of force«.*

– »*A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects*« (Tallinn Manual – Rule 71).

In practice, these rules imply a pretty high threshold. As pointed out by some scholars, »*given that acts of cyber espionage result in the copying of confidential data and do not produce physical damage, they do not contravene the use of force prohibition*« (Buchan, 2018, p 68). Similarly, as the use of ICT for hybrid warfare does not produce any physical damage, it is deemed appropriate to conclude that it will not amount to the use of force. However, from an EU law perspective, it is worth noting that the Member States have a specific measure to apply in each of the two situations (i.e. below or over the threshold). As clarified by the Council: »*Article 42(7) TEU* [*i.e.* the EU collective self-defence clause] *can be invoked by a Member State in case of armed aggression on its territory*«, and cyberattack »*can constitute an armed aggression within the meaning of Article 42(7), under the relevant principles of public international law*«, while »*Article 222 TFEU* [i.e. the EU solidarity clause] *applies to a terrorist attack or a natural or man-made disaster affecting a Member State, which can be triggered by a cyberattack as well*« (Council of the EU – answer to question E-002456/21).

Additionally, some consideration should be given to the argument that the measures in response to cyber operations also comprise retorsion, countermeasures and measures taken based on necessity. A brief analysis of the positions expressed in the UN official Compendium of Voluntary National Contributions may provide some fascinating insight into the nexus between such measures and espionage.

Concerning retorsion, the Netherlands pointed out that *»a state may respond to a cyber operation by another state, for example, by declaring diplomats 'persona non grata', or by taking economic or other measures against individuals or entities involved in the operation. Another retorsion measure a state may consider is limiting or cutting off the other state's access to servers or other digital infrastructure in its territory, provided the countries in question have not concluded a treaty on mutual access to digital infrastructure in each other's territory*« (UN Official Compendium, 2021, p 62). Therefore, it seems reasonable to conclude that retorsion could not be a valid excuse for extraterritorial espionage activity violating international law.

Concerning countermeasures, instead, according to Germany: »*Due to the multifold and close interlinkage of cyberinfrastructures not only across different States but also across different institutions and segments of society within States, cyber countermeasures are specifically prone to generating unwanted or even unlawful side effects. Against this background, States must be extensive and prudent in examining whether or not the applicable limitation criteria to cyber countermeasures are met. A State may – a maiore ad minus – engage in cyber reconnaissance measures in order to explore options for countermeasures and assess the potential risk of*

side effects if such measures fulfil the requirements for countermeasures« (UN Official Compendium, 2021, p 42). Then, as sharply observed by another author, »*by suggesting this precautionary step, Germany necessarily acknowledges that espionage as such is not a violation of international law*« (Schmitt, 2021).

However, an extensive interpretation of the requirements allowing measures taken based on necessity might create an unexpected deterrence effect. In order to clarify this point, it is helpful to follow the German position expressed in the UN Official Compendium of Voluntary National Contributions. According to Germany, »*the wrongfulness of a State's cyber operation that contravenes its international obligations may be precluded by exception if that State acted out of necessity. It entails that a State may – under certain narrow circumstances – act against malicious cyber operations by resorting, for its part, to active counter-operations even in certain situations in which the prerequisites for countermeasures or self-defence are not met*« (UN Official Compendium, 2021, p 42). An extensive interpretation of the requirements for the measures taken based on necessity will somehow allow the circumvention of the limits that characterize countermeasures (it goes without saying, however, that the measures taken based on necessity will, in any event, have to comply with other requirements, including proportionality). It means that the interpretation of the concepts of *essential interest* and *grave and imminent peril* will be essential[10]. The margin for interpretation, however, seems to be narrow. Indeed, as convincingly pointed out by Schmitt, *»the critical point is that the mere fact that a hostile cyber operation has targeted a vital interest does not alone justify acting based on necessity; the peril must be grave. An example of failure to satisfy this element would be pure espionage involving critical infrastructure«* (Ibid.).

5 CRIMINAL AND ADMINISTRATIVE RESPONSE TO CYBER ESPIONAGE

The recent responses of the US and EU to cyber espionage will be now analyzed. As previous paragraphs have discussed, the analysis of cyber espionage phenomena will cover hybrid warfare, economic theft, and »traditional« espionage.

At first, the different approaches adopted by the US and EU on the question of attribution need to be mentioned. On the one hand, the US does not hesitate to

[10] *In this regard, according to the said position, »Germany holds the view that, in the cyber context, the affectedness of an 'essential interest' may, among other things, be explained by reference to the type of infrastructure actually or potentially targeted by a malicious cyber operation and an analysis of that infrastructure's relevance for the State as a whole. For example, the protection of certain critical infrastructures may constitute an 'essential interest'. It might likewise be determined by reference to the type of harm actually or potentially caused due to a foreign State's cyber operation. For example, protecting its citizens against serious physical harm will be an 'essential interest' of each State – regardless of whether critical infrastructure is targeted or not. Nevertheless, given the exceptional character of the necessity argument, an 'essential interest' must not be assumed prematurely«. Additionally, Germany pointed out also that »a case-by-case assessment is necessary to determine whether a peril is 'grave'. The more important an 'essential interest' is for the basic functioning of a State, the lower the threshold of the 'gravity' criterion should be. Germany agrees that a 'grave peril' does not presuppose physical injury but may also be caused by large-scale functional impairments«.*

attribute malicious cyber activities and irresponsible State behaviour to the People's Republic of China (White House, 2021), while the EU limits its assertion only to a lack of due diligence for allowing Chinese territory to be used for malicious cyber activities (Declaration by the High Representative, 2021).

On the contrary, concerning Russia's improper influence activities, we can find only a low-profile posture from the US (Statement by the President, 2016), notwithstanding the well-known Mueller Report has shown that »*in sum, the investigation established that Russia interfered in the 2016 presidential election through the »active measures« social media campaign carried out by the IRA, an organization funded by Prigozhin and companies that he controlled*« (Mueller Report, 2019, p 35). Apart from the sanctions regime concerning hybrid warfare which will be analyzed shortly, the US reacted against Russia's improper influence on the US election by the expulsion of some Russian diplomatic staff. This measure of retorsion, however, as already pointed out by Schmitt, »*involves acts that international law does not prohibit*« (Schmitt, 2021, p 762). Thus »*a State may engage in it without establishing that the underlying activities violate its international legal rights*«. Instead, the European Council did not miss the opportunity to »*condemn the illegal, provocative and disruptive Russian activities against the EU, its Member States and beyond«* (European Council 2021). Such European Council conclusions, moreover, should be read in conjunction with the subsequent Joint Communication (EU Commission and High Representative for Foreign Affairs and Security Policy) to the European Parliament, the European Council and the Council on EU-Russia relations, issued on June 16 2021, where it is clearly stated that »*the Russian leadership uses a variety of instruments to influence, interfere in, weaken or even seek to destabilise the EU and its Member States, as well as the Western Balkans and Eastern Partnership countries. As part of these efforts, it invests heavily in its ability to control and influence the information space inside and outside its borders«* (Joint Communication, 2021, p 1). In this regard, it is also relevant to highlight that the European Council had already invited the »*EU's High Representative for Foreign Affairs and Security Policy, in cooperation with the Member States and EU institutions, 'to develop an action plan on strategic communication to address Russia's ongoing disinformation campaigns'«* (European Council Conclusions, 2015)[11]. Therefore, the European External Action Service set up (Joint Communication, 2018, p 1)[12]:

– Specific strategic communication task forces to address disinformation and develop response strategies. In this regard, the flagship project named *EUvsDisinfo,* with the aims of providing a better forecast, address, and response to ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the shared neighbourhood, is of note;

[11] *European Council meeting (19 and 20 March 2015) – Conclusions – EUCO 11/15 (https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf).*

[12] *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan against Disinformation, 5 December 2018 JOIN(2018) 36 final (https://eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf).*

– A Rapid Alert System (RAS) to provide warnings on disinformation campaigns in real time through dedicated technological infrastructure.

Additionally, the EU Commission has issued a European democracy action plan (Communication from the Commission, 2020) which, *inter alia*, strengthens the fight against disinformation. Among the EU's different activities against disinformation, it is also essential to mention Special Report No. 09/2021 from the European Court of Auditors, »Disinformation Affecting the EU: Tackled but not Tamed«. The European Court of Auditors found that *»the EU action plan against disinformation was relevant but incomplete, and even though its implementation is broadly on track and there is evidence of positive developments, some results have not been delivered as intended«* (European Court of Auditors, 2021, p 4).

The US Department of Defence (DoD), instead, recently recalled that »*a core part of the DoD's mission to defend the US elections consists of defending against covert foreign government malign influence operations; targeting the US electorate*« (Ney, Jr., 2020). To that end, the DoD supported the idea of responding to malicious cyber activities carried out against the United States, including carrying out military cyber operations. According to the DoD, compliance with the right of free expression under the First Amendment of such cyber operations against covert foreign government malign influence is ensured »…*whether the operation is targeting the foreign actors seeking to influence US elections covertly rather than the information itself; the extent to which the operation may be conducted in a »content-neutral« manner; and, the foreign location and foreign government affiliation of the targeted entity … Accordingly, in assessing proposed operations related to elections, DoD lawyers pay particular attention to whether the proposed operation may be conducted consistent with legal and regulatory limits on the use of official positions to influence or affect the results of US elections or to engage in, or create the appearance of engaging in, partisan politics«* (Ibid.). However, of note is the fact that the DoD speaks only of the First Amendment, without mentioning international law on this topic. The absence of clear and manifest blame from the US for improper foreign influence is consistent with US jurisprudence. The Ninth Circuit Court of Appeals, among other things, affirmed that the Foreign Sovereign Immunities Act (FSIA) bars plaintiffs' claims against Qatar for allegedly hacking into their computer servers, stealing their confidential information, and leaking it to the media in a retaliatory effort to embarrass the plaintiff and thereby to neutralize their ability to continue to effectively criticize the Qatari regime and its alleged support of terrorism[13].

[13] *Broidy Capital Management v. the State of Qatar, No. 18-56256 (9th Cir. 2020). According to this judgement: »The alleged actions that Qatar took here have not been shown to violate either Qatari law or applicable international law. The parties do not dispute that, under Qatari law, the various criminal prohibitions against hacking, theft, or disclosure of trade secrets do not bind government agents acting following official orders. Indeed, it would perhaps be surprising if the domestic law of any country prohibited its government agents from engaging in covert cyber espionage and public relations activities aimed at foreign nationals in other countries. Nor have the specific forms of cyber espionage alleged here been shown to violate international law's judicially enforceable principles. The status of peacetime espionage under international law is a subject of vigorous debate. The parties have not pointed us to any sufficiently clear rule of international law that would impose a mandatory and judicially enforceable duty on Qatar not to do what it allegedly did here.«*

The US and EU have also developed a dedicated sanctions regime concerning hybrid warfare and economic theft.

In the US, Executive Order (EO) 13694, issued on April 1, 2015 authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities which result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. This EO was amended to allow for the imposition of sanctions on individuals and entities responsible for tampering, altering, or causing the misappropriation of information to interfere with or undermine election processes or institutions. Moreover, EO 13757, issued on December 28, 2016, allowed the Secretary of the Treasury (in consultation with the Attorney General and the Secretary of State) to impose sanctions on those determined to be responsible for or complicit in cyber-enabled activities under EO 13694. The US Department of State and other US government agencies work to identify individuals and entities whose conduct meets the criteria outlined in EO 13694, and designate them for sanction under the delegated authority of the Treasury's Office of Foreign Assets Control (OFAC). Those designated under this authority are added to OFACS's Specially Designated Nationals and Blocked Persons list. Of note, US-designated Russia-linked individuals have been included in OFACS's list for attempting to influence the US electoral process, while a debate is ongoing within the US Administration on whether and how to sanction China for ransomware attacks (Bertrand, Liptak and Fung, 2021). Additionally, OFAC recently resorts to EO 13694 in order to designate a Russia-based virtual currency exchange for its part in facilitating financial transactions for ransomware actors.

The EU, on the other hand, adopted the Council Decision (CFSP) 2019/797 and the Council Regulation (EU) 2019/796 on May 17 2019, concerning restrictive measures (such as travel bans, asset and funds freezes) against cyber-attacks threatening the Union or its Member States. Subsequently, these Acts have been amended to designate individuals and entities. Looking at the last consolidated version of the Acts, we can see the designation of both Chinese individuals and entities (neither of which, however, belong to the Chinese People's Liberation Army) and individuals and entities belonging to the Armed Forces of the Russian Federation. The designations of Russian individuals and entities are related to acts of hybrid warfare. In contrast, for the Chinese individuals and entities, the designation is related to cyber-attacks that had targeted multinational companies' information systems, including companies located in the Union, and had gained unauthorized access to commercially sensitive data, resulting in significant economic loss.

As already pointed out by Chachko, a significant difference between the US and EU sanction regimes is the standard of judicial review applied for delisting. The US judiciary shows a deferential attitude towards OFAC designations, and non-resident aliens without substantial connections to the United States are not entitled

to Fifth Amendment protections. On the other hand, the European Court of Justice (ECJ), under Kadi jurisprudence, shows a minor degree of deference towards EU designation and requests well-founded reasons supported by evidence. This means that disclosure of classified information could be necessary in the case of a request for judicial review of a designation. However, the ECJ jurisprudence also allows the disclosure of a summary outlining the information's content or that of the evidence in question (Chachko, 2019). Additionally, Article 105.8 of the General Court Rules of Procedure, in the case of information or material about the security of the Union or that of one or more of its Member States, even allows – after an assessment of strict necessity – the judgment to be delivered based on closed evidence not disclosed to the applicant even as a non-confidential summary[14]. Finally, concerning the EU's sanction regime, it is worth noting that Recital 9 of the Council Decision (CFSP) 2019/797 of May 17 2019 explicitly clarified that »*targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State«*. The latter understanding is consistent with that expressed by Germany[15] and it is in line with the US point of view. According to the US, *»It is crucial, however, to distinguish legal attribution from attribution in the technical and political senses* » (UN Official Compendium, 2021, p 142).

In addition to the sanctions regime, the US – but not the EU or any of its Member States – is fighting relentlessly against economic espionage through means belonging to criminal law. To that end, we can mention the Department of Justice's (DoJ) China Initiative, which aims to identify and prosecute those engaged in trade secret theft, hacking, and economic espionage, as well as protecting US critical infrastructure against external threats through foreign direct investment and supply chain compromises, and combating covert efforts to influence the American public and policymakers without proper transparency. This initiative, of course, is not limited to the cyber threat, but the latter was clearly included. Within the framework of this initiative, the DoJ has also obtained several indictments against Chinese cyber spies, including some belonging to the Chinese People's Liberation Army (Department of Justice, February 10, 2020). This type of judicial activism of the DoJ, however, has not been limited to Chinese PLA personnel, as other indictments have been issued against personnel belonging to the Russian Federal Security Service (Department of Justice, 2017). Moreover, the DoJ issued a criminal complaint charging North Korean citizens for their involvement in a conspiracy to conduct multiple destructive cyberattacks around the world, and alleging the DPRK government's support in those malicious cyber actions (Department of Justice, 2018). Additionally, to pull the rug

[14] *For more details on the EU General Court Rules of Procedure, see Abazi, V., & Eckes, C., 2018.*

[15] *See: UN Official Compendium, 2021. According to the German view, »attribution in the context of State responsibility must be distinguished from politically assigning responsibility for an incident to States or non-State actors: generally, such statements are made at the discretion of each State and constitute a manifestation of state sovereignty«.*

from under the cybercriminals' feet (including but not limited to those potentially hired for cyber espionage), the DoJ obtained an indictment against a darknet-based cryptocurrency laundering service for the charge of conducting money transmission without a licence (Department of Justice, February 13, 2020).

As already pointed out by Chimène (2019), this attribution through criminal indictment had at least three audiences: (i) Chinese (or Russian) authorities and potential hackers; (ii) the US domestic audience; and (iii) an international audience comprised of other foreign states and individuals. Concerning the latter, however, it seems opportune to draw a distinction. On the one hand, such indictments are an occasion to encourage law enforcement cooperation, mainly with like-minded States. On the other hand, however, if we look to States dissenting from the US, the indictments are essential to assert that cyber espionage should be considered unlawful even when carried out by State officials. The latter consideration is not of small importance, as the legal framework on cyber espionage is far from clear (Chimène, 2019).

Finally, concerning »traditional« espionage, it is worth recalling Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016, concerning measures for a typically high level of security of network and information systems across the Union. Although public administration entities that carry out activities in public security, law enforcement, defence or national security are explicitly excluded from the scope of its application, this legislation sets significant and detailed standards of cyber security measures. Consequently, *de facto*, Directive (EU) 2016/1148 produced a spill-over effect implying the application of its standard (at least as a minimum standard) even to other areas, including defence or national security. With regard to EU Member States' practice in the case of »traditional« espionage, it is only worth noting that after the 2014 expulsion of US personnel from Germany due to allegations of spying, no prosecution of US personnel was attempted by Germany (Patrick, 2015). Instead, Germany asked the US to reach a comprehensive intelligence agreement. The US, however, declined the request (Daugirdas, 2014).

6 US MILITARY RESPONSE TO CYBER ESPIONAGE: CLANDESTINE MILITARY ACTIVITY OR OPERATION IN CYBERSPACE

While the US diplomatic response to improper influence activities by Russia has been limited, US legislation has been significantly modified.

First, it should be mentioned that the provision allows active cyber defence operations against attacks in cyberspace by the Russian Federation, the People's Republic of

China, the Democratic People's Republic of Korea, and the Islamic Republic of Iran[16]. Moreover, US Congress also affirmed the authority of the Secretary of Defense to »*conduct military operations, including clandestine operations, in the information environment to defend the United States, allies of the United States, and interests of the United States, including in response to malicious influence activities carried out against the United States or a United States person by a foreign power*«[17].

Additionally, Title 10 of the USC (United States Code) § 394 was amended to allow the Armed Forces to conduct cyber activities or operations in cyberspace, including clandestine military activities. The latter authority includes »*the conduct of military activities or operations in cyberspace short of hostilities or in areas in which hostilities are not occurring, including for the preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States*«. Of note is the fact that the Title 10 authority to carry out clandestine military activities or operations in cyberspace is additional to Title 50 of the US Code statutory authority for intelligence activities. In other words, even before the new Title 10 authority, Armed Forces could carry out clandestine activities, including in cyberspace, under Title 50 of the US Code statutory authority. The new USC § 394 has not created an additional category of permissible secret cyberspace operations, but rather it has established a dedicated Congressional oversight of clandestine cyber activities.

Conclusion

Espionage is commonly symbolized by the Roman god Janus, represented by a double-faced head. It is related to the root ambivalence that characterizes espionage, where no foreign State, even the tightest Ally, can be deemed an absolute friend. From the legal point of view this ambivalence is also confirmed, as espionage is not illegal *per se* for international law, but it can be prosecuted as a crime by domestic law.

The impact of ICT on espionage is significant since, today, more and more States can carry out espionage in all its facets more effectively. This new situation is creating a circle that keeps turning since more and more States, echoing the German position on the application of international law in cyberspace, may *»engage in cyber reconnaissance measures in order to explore options for countermeasures and assess the potential risk of side effects if such measures fulfil the requirements for countermeasures*« (UN Official Compendium, 2021, p 42). The new Title 10

---

[16] *According to the fiscal year (FY) 2019, the National Defense Authorization Act (NDAA): »In the event that the National Command Authority determines that the Russian Federation, the People's Republic of China, the Democratic People's Republic of Korea, or the Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes, the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks under the authority and policy of the Secretary of Defense from conducting cyber operations and information operations as traditional military activities« (John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 1642(a), 132 Stat. 1636, 2132 (2018).*

[17] *Section 1631 of the National Defense Authorization Act for Fiscal Year 2020, amending USC (United States Code) § 391.*

authority allowing Armed Forces to conduct clandestine cyber military activities is one example that confirms this conclusion.

It implies that espionage should not be accepted whenever it aims at foreign influence or economic theft. On the contrary, »pure« cyber-espionage committed by a foreigner abroad through ITC means should not be punishable by the criminal law of the »Victim State«, as the intelligence-gathering activities were legal by the law of the country where they took place, as well as »tolerable« for the international community.

A high threshold for triggering the Law of Armed Conflict (LOAC) in the case of cyber operations resulted in the proliferation of cyber espionage, particularly in hybrid warfare and economic theft. This suggests an opportunity for radical change in the appraisal of traditional espionage. The latter, in some ways, should be seen as a measure aimed at preventing and reacting to the use of ICT means for hybrid warfare and economic theft. »Traditional« espionage should indeed be seen as the lesser evil, to avoid a possible uncontrolled escalation in the case of cyber operations. Failing to do so could sooner or later open Pandora's Box, i.e. accept the risk of triggering a full-scale armed conflict in reaction to cyber operations; a situation that is not desirable because not all the possible consequences and effects can be predicted.

With regard to foreign influence, it is hoped that hybrid confrontation will drop in intensity. To reach this goal, Western countries, which are currently those more affected by this type of warfare, might not exclude *a priori* the possibility of having a frank and open discussion with China and other non-Western countries. Such negotiation should increase transparency rather than limit human rights. A fair balance on this sensitive issue is opportune. One should keep in mind that the fight against disinformation should not lead to the creation of a sort of Orwellian Ministry of Truth[18].

Concerning economic espionage, a clear understanding of this topic has not been reached so far; US and EU activism on this side is critical. Even though some criticism can be reasonable[19], it is vital to seize every opportunity to hamper

---

[18] *It is worth mentioning the following extract from the remarks of EU Vice-President Vera Jourová: »I am thrilled that our response to disinformation is maturing with every step we take. I need to say one thing from the outset. We will not regulate the removal of disputed content. We do not want to create a Ministry of Truth. Freedom of speech is essential, and I will not support any solution that undermines it«.*

European Democracy Action Plan: Remarks by Vice-President Vera Jourová, December 3 2020 (https://ec.europa.eu/commission/presscorner/detail/en/speech_20_2308).

[19] *For example, Stefan Soesanto (2020) argued that »as far as tangible evidence goes, there is no proof that sanctions deter anyone, shame anyone, nor impose costs or restrict an adversary's ability to conduct their malicious campaigns. The very notion that cyber sanctions (for example, travel bans) might work because Russian military intelligence officials are longing for a house on the French Riviera and want to visit the Colosseum in Rome is built on fragile ice. Similarly, it is highly doubtful that any intelligence front companies nor individual cyber operatives own any funds subject to EU jurisdiction. It is not known whether the EU has frozen any assets of individuals and entities listed under the EU cyber sanctions regime so far. Given this discrepancy, EU cyber sanctions are largely symbolic, and their prime utility seems to signal red lines, political intent and EU unity«.*

those who may have the idea to carry out cyber-attacks for economic theft. In the same vein, as the DoJ has done, it seems even more helpful to chase and block virtual currency exchange providers involved in facilitating financial transactions for ransomware actors. To that end, even domestic criminal law could be helpful. While cybercriminals – even more so when belonging to the armed forces of foreign countries – will rarely be prosecuted for extraterritorial offences, domestic criminal law offences can still be helpful. Taking into account that each sanctions regime can be applied only to a limited number of situations (due to the need for specific and robust evidence), in order to achieve a significant deterrent effect, domestic criminal law could fill the gap by indicting virtual currency exchange providers of conducting money transmission without a licence. Indeed, this *modus operandi* could break the business model of those involved in economic theft by seizing assets that otherwise would have been available to the cybercriminals. Although it may be true that in the case of State-led theft of confidential information this kind of criminal approach is not enough, it could play an essential role in dissuading criminal gangs from acting as a proxy for States' intelligence agencies.

Above all, however, within the ongoing strategic competition between Western and non-Western countries, the actual match is the ongoing development of international law applicable to cyber operations. Western countries' attempt to shape international law to effectively tackle hybrid warfare and economic theft. On the contrary, other actors are exploiting the loopholes of the actual contradictory legal regime on these matters.

As highlighted in this article, different forms of cyber espionage are currently in grey areas of international law. Consequently, on the current stage, it appears not to be possible to conclude whether the new legal measures adopted by the US and EU will become a new trend in international law. Nevertheless, these legal measures still play an essential part in reaching that desired trend.

Bibliography

1. *Abazi, V., and Eckes, C., 2018. Closed evidence in EU courts: Security, secrets and access to justice. Common Market Law Review, 55(3), 753-782. http://www.kluwerlawonline.com/abstract.php?area=Journals&id=COLA2018069.*
2. *Bertrand, N., Liptak, K., Fung, B., 2021. Biden administration debating whether and how to sanction China for ransomware attacks, www.cnn.com 20 July 2021. https://edition.cnn.com/2021/07/19/politics/china-biden-ransomware/index.html.*
3. *Bettauer, R. J., 2014. Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia). Provisional Measures Order, The American Journal of International Law, Vol. 108, No. 4 (October 2014), pp 763-769.*
4. *Buchan, R., 2018. Cyber Espionage and International Law, Hart Publishing.*
5. *Chachko, E., 2019. Due Process Is in the Details: US Targeted Economic Sanctions and International Human Rights Law, 113 AJIL Unbound 157-162.*

6. *Cheng, B., Properly Speaking, Only Celestial Bodies Have Been Reserved for Use Exclusively for Peaceful (Non-Military) Purposes, but Not Outer Void Space, International Law Studies – Volume 75 (2000) – International Law Across the Spectrum of Conflict: Essays in Honour of Professor L.C. Green On the Occasion of His Eightieth Birthday. Michael N. Schmitt (Ed.).*
7. *Chimène, K., 2021. Foreign Election Interference and International Law In: Duncan B. Hollis and Jens David Ohlin (Eds.), Defending Democracies. Oxford University Press.*
8. *Chimène, K., 2019. Attribution by Indictment. UC Hastings Research Paper No. 316. https://ssrn.com/abstract=3322943, 9 January 2019.*
9. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – On the European Democracy Action Plan, 3 December 2020 COM (2020) 790 Final.*
10. *Council of the EU, Parliamentary Question, Answer to Question E-002456/21, 22 September 2021. https://www.europarl.europa.eu/doceo/document/E-9-2021-002456-ASW_EN.html.*
11. *Daugirdas, K., and Mortenson, D. J., 2014. Contemporary practice of the United States relating to international law. The American Journal of International Law, Vol. 108, No. 4, [American Society of International Law, Cambridge University Press], 2014, pp 783-842. https://doi.org/10.5305/amerjintelaw.108.4.0783.*
12. *Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory, 19 July 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/.*
13. *Department of Justice – Office of Public Affairs, Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax, 10 February 2020. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.*
14. *Department of Justice – Office of Public Affairs, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, 6 September 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.*
15. *Department of Justice – Office of Public Affairs, Ohio Resident Charged with Operating Darknet-Based Bitcoin »Mixer,« which Laundered Over $300 Million, 13 February 2020, https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million.*
16. *Department of Justice – Office of Public Affairs, US Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts, 15 March 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.*
17. *Drake, R., 2004. The Soviet Dimension of Italian Communism [Review of Oro da Mosca: I Finanziamenti Sovietici al PCI dalla Rivoluzione d'Ottobre al Crollo dell'URSS; L'Oro di Mosca: La Verità sui Finanziamenti Sovietici al PCI Raccontata dal Diretto Protagonista. 2nd Ed., by V. Riva & G. Cervetti. Journal of Cold War Studies, 6(3), 115-119. https://www.jstor.org/stable/26925390.*
18. *European Council (19 and 20 March 2015) – Conclusions.*
19. *European Council (24 and 25 May 2021) – Conclusions.*
20. *European Court of Auditors Special Report No 09/2021, Disinformation Affecting the EU: Tackled but not Tamed.*
21. *Fiore, P., 1837-1914; Borchard, E. M., 1884-1951, International Law Codified and its Legal Sanction: Or, The Legal Organization of the Society of States.*

22. *Geissler, E., and Hunt Sprinkle, R., 2013. Disinformation Squared: Was the HIV-from-Fort-Detrick Myth a Stasi Success? Politics and the Life Sciences, Vol. 32, No. 2, Association for Politics and the Life Sciences, pp. 2-99. http://www.jstor.org/stable/43287281.*
23. *Hemmings, J., Swire, N., 2019. The Cloud Act Is Not a Tool for Theft of Trade Secrets, 23 April 2019, https://www.lawfareblog.com/cloud-act-not-tool-theft-trade-secrets.*
24. *Joint Communication to the European Parliament, the European Council and the Council on EU-Russia relations – Push Back, Constrain and Engage, dated 16. June 2021 – JOIN (2021) 20 Final.*
25. *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan against Disinformation, 5. December 2018 JOIN (2018) 36 Final.*
26. *Krizek, M. B., 1988. The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal 6, No. 2 (Fall 1988): pp 337-360.*
27. *Lahmann, H., 2020. Information Operations and the Question of Illegitimate Interference under International Law (June 2020). Israel Law Review, Volume 53, Issue 2, pp 189-224 36, June 2020.*
28. *Lotrionte, C., 2014. Countering State-Sponsored Cyber Economic Espionage under International Law, 40 – NC. J. INT'L L. 443.*
29. *Lubin, A., 2018. Cyber Law and Espionage Law as Communicating Vessels (March 17, 2018). Proceedings of the 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2018), Available at SSRN: https://ssrn.com/abstract=3099769.*
30. *Mueller Report – US Dep't of Justice, Report On The Investigation Into Russian Interference In The 2016 Election Vol. I, 1-5 (2019), p 35.*
31. *National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2. Top Secret. No drafting information appears in the source text. An earlier, similar version, 30 April, in Ibid., RG 59, Records of the Department of State, Policy Planning Staff Files 1944-47: Lot 64 D 563, Box 11.*
32. *NATO-wide co-operation and coordination in the field of psychological warfare – proposal by the Federal Republic of Germany, 1960. Available at: https://archives.nato.int/nato-wide-co-operation-and-co-ordination-in-field-of-psychological-warfare-proposal-by-federal-republic-of-germany.*
33. *Navarrete, I., and Buchan, R., 2019. Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions, Cornell International Law Journal: Vol. 51: No. 4, Article 4.*
34. *Ney, Hon. P. C. Jr., 2020. DOD General Counsel Remarks at US Cyber Command Legal Conference – 2 March 2020. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.*
35. *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established according to General Assembly resolution 73/266. UN document A/76/136 dated 13 July 2021.*
36. *Ohlin, J. D., 2021. Election Interference: A Unique Harm Requiring Unique Solutions, 1 November 2018. Defending Democracies: Combating Foreign Election Interference in a Digital Age (Oxford University Press, 2021), Cornell Legal Studies Research Paper No. 18-50. https://ssrn.com/abstract=3276940 or http://dx.doi.org/10.2139/ssrn.3276940.*
37. *Oppenheim, L., 1905. International Law Vol. 1, 1905. https://archive.org/details/in.ernet.dli.2015.24439/page/n529/mode/2up?q=spy.*

38. *Orde F. K., 2016. Lawfare – Law as a Weapon of War, Oxford University Press 2016.*
39. *Patrick, T. C. R., 2015. »Absolute Friends«: US Espionage against Germany and Public International Law. In: Revue Québécoise de Droit International, Volume 28-2, 2015. pp 173-203. https://www.persee.fr/doc/rqdi_0828-9999_2015_num_28_2_2188.*
40. *Pompeo, M. R., 2019. U. S. Secretary of State, Why Diplomacy Matters (Questions and Answers), 15 April, 2019. From the official US State Department transcript. https://2017-2021.state.gov/remarks-at-texas-am-wiley-lecture-series/index.html.*
41. *Quint, P. E., 1997. The Imperfect Union: Constitutional Structures of German Unification. Princeton University Press, 1997, pp 213-214.*
42. *Radsan, A. J., 2007. The Unresolved Equation of Espionage and International Law, 28 MICH. J. INT'L L. 595.*
43. *Schmitt, M., 2021. Foreign Cyber Interference in Elections. Vol. 97, International Law Studies 2021.*
44. *Schmitt, M., 2021. Germany's Positions on International Law in Cyberspace Part I. https://www.justsecurity.org/, 9 March 2021.*
45. *Selvage, D., 2019. Operation »Denver«: The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985-1986 (Part 1). Journal of Cold War Studies 2019; 21 (4): 71-123. https://doi.org/10.1162/jcws_a_00907.*
46. *Shane, S., 2018. NEWS ANALYSIS – Russia Is not the Only One Meddling in Elections. We Do It, Too, The New York Times, 17 February 2018.*
47. *Soesanto, S., 2020. Europe Has No Strategy on Cyber Sanctions, November 20, 2020. https://www.lawfareblog.com/, https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions.*
48. *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, 29 December 2016. In that statement, President Obama attributed to Russia (only) the violation of »established international norms of behaviour«, but not the violation of international law. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.*
49. *Stone, J.,1962. Legal Problems of Espionage in Conditions of Modern Conflict, Essays on Espionage and International Law. OHIO State University Press 1962.*
50. *Strawbridge, J., 2016. The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation, 47 GEO. J. INT'l L. 833.*
51. *Tondini, M., 2019. Espionage and International Law in the Age of Permanent Competition. Military Law and the Law of War Review Vol. 57, No. 1, 2018-2019.*
52. *Van Wie Davis, E., 2021. Shadow Warfare: Cyberwar Policy in the United States, Russia and China, Rowman & Littlefield Publishers.*
53. *Whitehouse Statements and Releases – The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, 19 July 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.*
54. *Yearbook of the International Law Commission, 1971, Vol. II, Part One, pp 265-266.*

e-mail: davide.giovannelli@ccdcoe.org

e-mail: davide.giovannelli@ccdcoe.org

Davide Giovannelli je magistriral iz prava na univerzi v Pisi in na univerzi LUISS. Končal je italijansko mornariško akademijo v Livornu in leta 2004 pridobil čin poročnika korvete. Trenutno je kapitan fregate. Avgusta 2021 je začel delati v Natovem centru odličnosti za kibernetsko obrambo kot raziskovalec v Sektorju za pravne zadeve. Pred tem je služboval na številnih vojaškopravnih funkcijah, med drugim kot pravni svetovalec v mednarodnih operacijah (NATO Allied Provider in Unified Protector, Unifil v Libanonu ter EU Atalanta in Sophia), v italijanski mornarici in na generalštabu obrambnih sil.

Davide Giovannelli has a master's degree in Law from Pisa University and a LLM from LUISS University. He attended the Italian Naval Academy in Livorno and was commissioned to the rank of Ensign in 2004. Currently, he is a Commander (OF-4). He joined the CCDCOE in August 2021 as Researcher in the Law Branch. Prior to assuming his current position, he served in many areas of military legal counselling, including Legal Advisor in several operations (NATO Allied Provider and Unified Protector, United Nations Interim Force in Lebanon, EU Naval Operations ATALANTA and SOPHIA), the Navy and the Defence General Staff.