International Review of the Red Cross (2025), **107** (928), 96–139.
The Military
doi:10.1017/S1816383124000390

IRRC

Handling cyberspace's state of intermediacy through existing international law

Davide Giovannelli[1,2]*
[1]Commander (OF-4), Italian Navy
[2]Law Researcher, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
Email: davide.giovannelli@libero.it

Abstract

How international law applies to the use of information and communications technology by States is still a matter of discussion. Against this background, cyberspace has become the main area of competition between States, and this competition, to put it simply, is resulting in a constant low-intensity warfare below the threshold for a use of force. Such low-intensity cyber warfare, from a legal point of view, revitalizes the debate over the concept of a "state of intermediacy" that has the potential to overcome the dichotomy between peace and war. In the present author's opinion, this state of intermediacy also supports the idea that the

* The views expressed in this article – as well as responsibility for any errors – are those of the author in his personal capacity and should not be understood to represent those of the Italian Navy or the NATO Cooperative Cyber Defence Centre of Excellence or any other Italian government or NATO entity. The author would like to express his sincere gratitude to the anonymous peer reviewer for their insightful comments and constructive feedback.

international humanitarian law (IHL) principle of distinction should be applied, even before the eruption of a full-scale war, whenever wartime means and capabilities are employed by States. This paper argues that some opacities in international law have created favourable conditions for such constant low-intensity warfare, and that tackling the identified opacities would therefore be beneficial in order to achieve a more peaceful cyberspace. Thus, the paper goes on to address one of the identified opacities, namely the definition of espionage under international law, because, as international law now stands, it does not allow us to tackle the other identified opacities. Finally, the paper discusses how the proposed narrow interpretation of espionage can cope with the IHL principle of distinction in the cyber domain.

Keywords: armed forces, cyber operations, espionage, principle of distinction, state of intermediacy.

Introduction

"International law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability and promoting an open, secure, stable, accessible and peaceful ICT [information and communications technology] environment."[1] While this conclusion should be considered undisputed (as it is part of both the 2021 report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security[2] and the 2021 report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security[3]), how international law applies to the use of ICT is still a matter of discussion among States. Thanks in part to this legal uncertainty, as argued by some scholars, the current global security landscape is characterized by a "permanent low-intensity warfare that the principal actors often deny entirely"[4]. Therefore, as this paper will show, it is safe to say that the competition in cyberspace between the two blocs of States – the first led by the United States and the second led by China and Russia – has become quite explicit, although each bloc is reluctant to acknowledge its involvement. Competition in cyberspace, however, cannot be seen as an entirely new phenomenon. To define the relations between the United States and the Soviet Union during the Cold War, Philip C. Jessup suggested the opportunity to

1 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, 24 June 2013, para. 19.
2 *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135, 14 July 2021, para. 69.
3 *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report*, UN Doc. A/AC.290/2021/CRP.2, 10 March 2021, para. 7.
4 Elizabeth Van Wie Davis, *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*, Rowman & Littlefield, Lanham, MD, 2021, p. 2.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

overcome the traditional dichotomy between "war" and "peace" and to consider a "state of intermediacy" which is neither one thing nor the other. According to this jurist, "in a state of intermediacy it would be recognized that the hostile parties could engage in conduct which would not be peaceful and yet would be short of what may now conveniently be called total war".[5]

This paper argues that the lack of a common understanding on how international law applies to ICT – which paved the way for this state of intermediacy – is caused by some fundamental opacities in international law, rather than by the absence of domain-specific legally binging norms. The aim of the paper is twofold: it will explain the areas of opacity, and it will propose some mitigation measures.

With the exception of a narrow interpretation of the notion of espionage, mitigation measures may not be easily achievable as international law now stands. Therefore, the paper will deeply analyze espionage and its limits under international law, across various regimes of international law. Although the analysis will not define the final status of espionage under international law, it will nevertheless conclude that activities going beyond information-gathering should not be considered as espionage.

As a consequence, States should follow a legally sound interpretation of the notion of espionage and should distinguish it from other forms of hostile activities. This also implies, in accordance with the principle of distinction, that cyber operations – beyond mere intelligence-gathering – conducted by a State should not be conducted by civilians but by members of the armed forces.

Although the conclusion stated above may not appear to be particularly innovative, States' practice seems to show otherwise. Indeed, as suggested by some scholars, "there is a high probability that many, if not most, of the personnel substantively involved in cyber operations may actually be civilians".[6] Available studies[7] on governance of States' cyber capabilities show that military and intelligence entities can be organized following different models, ranging from collaboration to separation or centralization. Whatever model is used, it is safe to say that States are often pursuing a strong integration between military and civilian cyber capabilities,[8] thereby producing a blurred division of responsibilities between the armed forces and civilian intelligence agencies. In other words, we may see civilian intelligence agencies contributing to the

5 Philip C. Jessup, "Intermediacy", *Nordisk Tidsskrift for International Ret*, Vol. 23, 1953, p. 24.

6 David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, p. 292.

7 Tobias Liebetrau, "Organizing Cyber Capability across Military and Intelligence Entities: Collaboration, Separation, or Centralization", *Policy Design and Practice*, Vol. 6, No. 2, 2023.

8 Just as an example, in 2020, the United Kingdom established the National Cyber Force (NCF). According to the UK government's official website, the NCF "is a partnership between defence and intelligence" and is "responsible for operating in and through cyberspace to counter threats, disrupting and contesting those who would do harm to the UK and its allies, to keep the country safe and to protect and promote the UK's interests at home and abroad". Government of the United Kingdom, "National Cyber Force Explainer", 13 December 2021, available at: https://tinyurl.com/29d8ut2s (all internet references were accessed in September 2024).

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

execution of tasks that in other domains would clearly fall under the sole responsibility of the armed forces. So, unsurprisingly, it has been argued that

> [c]onsideration needs to be given to whether the integration of intelligence and military cyber capabilities is the best approach in light of the risks and whether instead there is a need to create clear space between the different organizations within a state that have a legitimate reason to operate in cyberspace.[9]

On the other hand, such proactivity by civilian intelligence agencies may also explain the concerns raised by some States with different geopolitical mindsets – such as Russia,[10] Japan[11] and Brazil[12] – on the need to clarify the notion of combatants' and civilians' direct participation in hostilities, in the context of the law applicable to ICT. Of course, one might argue that the overall argument put forward in this article is too Western-centric, since non-Western States may not "necessarily agree on a societal pact as did Europe in the case of the Westphalian order. In such countries the state monopoly on the use of force was not, and still is not, necessarily accepted or legitimized by the wider population."[13] In that respect, however, it is sufficient to note that the rules-based international order presupposes that States – through their democratic legitimacy – should maintain the monopoly on the use of force. International humanitarian law (IHL), indeed, has enlarged the notion of combatants in order to deal with guerrilla and resistance movements. As will be shown in this article, however, these movements should be seen as an exception to the general rule, rather than as evidence that States' monopoly over the use of force is outdated.

Areas of opacity in international law

Cyberspace as the main area of competition between States

Generally speaking, before addressing any legal problem, it is necessary to understand the context within which the problem lies. To that end, it is pertinent to recall that cyberspace is a contested domain between States, as shown by many

9 Ewan Lawson, "Between Two Stools: Military and Intelligence Organizations", *Cyber Defense Review*, Vol. 7, No. 3, 2022, p. 75.

10 Russia, "Statement by Dr. Vladimir Shin, Deputy Director of the Department of International Information Security of the Ministry of Foreign Affairs of the Russian Federation, at the Online Consultations of the Open-Ended Working Group on the Developments in the Field of Information and Telecommunications in the Context of International Security", 30 September 2020, p. 2.

11 Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, 28 May 2021, p. 7, available at: www.mofa.go.jp/files/100200935.pdf.

12 Brazil, "National Contribution on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States", in *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 Pursuant to General Assembly Resolution 73/266*, UN Doc. A/76/136, 13 July 2021, p. 23.

13 Andreas Wenger and Simon J. A. Mason, "The Civilianization of Armed Conflict: Trends and Implications", *International Review of the Red Cross*, Vol. 90 No. 872, 2008, p. 836.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

key political documents issued by the United States[14] and the North Atlantic Treaty Organization (NATO).[15] China[16] and Russia[17] have shown the same level of perception of the threat. Even reports on cyber attacks issued by private "big tech" companies seem to be inconclusive with regard to a clear understanding of today's conflicts in cyberspace. Looking to the *Microsoft Digital Defense Report 2023*, it is possible to find information on cyber attacks that, according to Microsoft, should be attributed to nation-State actors, primarily acting as proxies of Russia and China.[18] The report, however, gives no information about any

14 The US *National Cybersecurity Strategy 2023* explains that "[t]he governments of China, Russia, Iran, North Korea, and other autocratic states with revisionist intent are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms. Their reckless disregard for the rule of law and human rights in cyberspace is threatening U.S. national security and economic prosperity." The White House, *National Cybersecurity Strategy 2023*, 1 March 2023, p. 3, available at: www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Of note, even the Apulia G7 (13–15 June 2024) *Leaders' Communiqué* took a clear stance towards China: "*We call on China to uphold its commitment to act responsibly in cyberspace*. We will continue our efforts to disrupt and deter persistent, malicious cyber activity stemming from China, which threatens our citizens' safety and privacy, undermines innovation, and puts our critical infrastructure at risk. We recognize the necessity of protecting certain advanced technologies that can be used to threaten our national security, without unduly limiting trade and investment." *Apulia G7 Leaders' Communiqué*, 14 June 2024, p. 11, available at: www.g7italy.it/wp-content/uploads/Apulia-G7-Leaders-Communique.pdf.

15 For example, the NATO 2022 Strategic Concept, adopted by heads of State and government at the NATO Summit in Madrid on 29 June 2022, clearly states that "[c]yberspace is contested at all times. Malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities." *NATO 2022 Strategic Concept*, 29 June 2022, para. 15, available at: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. More recently, the Washington Summit Declaration issued by the NATO heads of State and government participating in the meeting of the North Atlantic Council in Washington, DC, on 10 July 2024 stated, *inter alia*, that "Russia has also intensified its aggressive hybrid actions against Allies, including through proxies, in a campaign across the Euro-Atlantic area. These include sabotage, acts of violence, provocations at Allied borders, instrumentalisation of irregular migration, *malicious cyber activities, electronic interference*, disinformation campaigns and malign political influence, as well as economic coercion. *These actions constitute a threat to Allied security*. … The PRC [People's Republic of China] continues to pose systemic challenges to Euro-Atlantic security. *We have seen sustained malicious cyber* and hybrid activities, including disinformation, *stemming from the PRC. We call on the PRC to uphold its commitment to act responsibly in cyberspace*." Washington Summit Declaration. 10 July 2024, paras 20, 27 (emphasis added), available at: www.nato.int/cps/en/natohq/official_texts_227678.htm.

16 According to Chinese Foreign Ministry spokesperson Wang Wenbin, "[t]he US is unrivalled in malicious cyber activities. Ironically, it presents itself as a victim, misleads the international community and attempts to dominate the international agenda of cybersecurity. "Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference", 3 March 2022, available at: www.fmprc.gov.cn/eng/xw/fyrbt/lxjzh/202405/t20240530_11347236.html. Moreover, "[o]n 19 April 2022, China's National Computer Virus Emergency Response Center (CVERC) issued an alert on cyber attacks by the US government against other countries and released a related report." Chinese Ministry of Foreign Affairs, "Reality Check: Falsehoods in US Perceptions of China", 19 June 2022, available at: www.mfa.gov.cn/eng/wjbxw/202206/t20220619_10706059.html.

17 According to Andrey Krutskikh, the special representative of the president of Russia for international cooperation in the field of information security, "[i]t is clear, that the United States and their like-minded partners are trying to reshape the agenda of specialized international negotiating platforms in line with their aggressive policy in information space". Andrey Krutskikh, "When Digital Environment Turn[s] into Theatre of War, Everybody Loses", 21 March 2023, available at: https://mid.ru/en/maps/my/1858944/.

18 Microsoft, *Microsoft Digital Defense Report 2023*, October 2023, pp. 46–74, available at: www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

alleged cyber attacks executed by Western States (or their proxies). Conversely, "[a] report jointly released by China's National Computer Virus Emergency Response Centre (CVERC) and Chinese cybersecurity company 360 revealed that the US' Central Intelligence Agency (CIA) has been responsible for plotting 'colour revolutions' around the world".[19]

On the other hand, it is relevant to note that such competition has not had a spillover effect in other domains, at least so far. In order to corroborate this conclusion, it seems important to mention two examples. When Albania, a NATO member, declared itself to have been the target of cyber attacks orchestrated and sponsored by the Islamic Republic of Iran,[20] NATO[21] and its allies (including Albania) did not trigger the Article 5 collective self-defence clause. Notwithstanding this example, NATO doctrine does not rule out that option.[22] In the ongoing war between Russia and Ukraine, NATO and its allies are clearly supporting Ukraine, including with weapons[23] and intelligence.[24] This

19 Statecraft Staff, "CIA Conspired to Overthrow 50 Governments via 'Color Revolutions': Chinese Report", *Statecraft*, 5 May 2023, available at: www.statecraft.co.in/article/cia-conspired-to-overthrow-50-governments-via-color-revolutions-chinese-report. Statecraft is a non-profit that is wholly owned, funded, and run by the Young Bhartiya Foundation.

20 Edi Rama, "Videomessage of Prime Minister Edi Rama", 7 September 2022, available at: www.kryeministria.al/en/newsroom/videomesazh-i-kryeministrit-edi-rama/.

21 NATO, "Statement by the North Atlantic Council concerning the Malicious Cyber Activities against Albania", 8 September 2022, available at: www.nato.int/cps/en/natohq/official_texts_207156.htm?selectedLocale=en.

22 In accordance with the *Vilnius Summit Communiqué* issued by NATO heads of State and government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023, "[a] single or cumulative set of malicious cyber activities could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the Washington Treaty, on a case-by-case basis". NATO, *Vilnius Summit Communiqué*, 11 July 2023, para. 66, available at: www.nato.int/cps/en/natohq/official_texts_217320.htm.

23 As explained by the NATO official website, "[a]t the 2024 Washington Summit, NATO Allies agreed to establish NATO Security Assistance and Training for Ukraine (NSATU) to coordinate *the provision of military equipment and training for Ukraine by NATO member and partner countries*, and will provide logistical support. Its aim is to place security assistance to Ukraine on an enduring footing, ensuring enhanced, predictable and coherent support for the long term. NSATU, which will operate in Allied states, will support Ukraine's self-defence in line with the UN Charter. *NSATU will not, under international law, make NATO a party to the conflict.* It will support the transformation of Ukraine's defence and security forces, enabling its further integration with NATO and ensuring that Ukraine is more capable of defending itself now and deterring any further Russian aggression in the future." NATO, "Relations with Ukraine", 19 July 2024 (emphasis added), available at: www.nato.int/cps/en/natohq/topics_37750.htm#support.

24 While the details regarding the exchange of intelligence information with Ukraine are of course shrouded in mystery, Pentagon press secretary John Kirby has affirmed that "[t]he United States provides battlefield intelligence to help Ukraine defend their country". Jordan Williams, "Pentagon Denies US Shared Intel to Target Russian Generals", *The Hill*, 5 May 2022, available at: https://thehill.com/policy/defense/3478747-pentagon-denies-us-shared-intel-to-target-russian-generals/. See also "The United States and Allies Provide Military and Intelligence Support to Ukraine", *American Journal of International Law*, Vol. 116, No. 3, 2022, p. 649, which documents that "[t]he United States has also provided Ukraine with intelligence. After concerns from Congress about reports that the United States was not providing Ukraine with 'real-time targeting data that would enable Ukraine's military to strike' Russian positions, the White House reportedly 'modified existing guidance for the Pentagon and U.S. spy agencies on sending intelligence data to the Ukrainian government to clear the way of any bureaucratic roadblocks to information sharing.' In a subsequent congressional hearing on March 17, National Security Agency Director Gen. Paul Nakasone noted that he had never seen better sharing of

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

support, however, does not include actions, such as launching an attack from NATO territory or enforcing a no-fly zone, that would bring NATO forces into direct conflict with Russia[25] – but in the cyber domain, that clear red line does not seem as strict. To that end, it is worth nothing that, according to a European Union Agency for Cybersecurity report, "Ukraine's IT Army managed to target various entities and conducted mostly coordinated Distributed Denial of Services (DDoS) attacks but was not limited to such attacks".[26] While Ukraine's IT Army is shrouded in a certain degree of mystery, it is safe to say that at least some of its activities have taken place from outside Ukraine.[27] As one scholar has pointed out, however, this situation "has to date not spurred any legal, ethical, nor political conversations on co-belligerency in cyberspace, the role of Ukrainian owned companies operating from NATO/EU member states, and their targeting of Russian civilian infrastructure in cooperation with the Ukrainian

actionable intelligence in his career than the sharing with Ukraine, and Defense Intelligence Agency Director Army Lt. Gen. Scott Berrier called the intelligence sharing with Ukraine 'revolutionary in terms of what we have been able to do'" (footnotes omitted). Not surprisingly, Russia has heavily criticized the "cyber support" provided by allies to Ukraine. For example, the statement by the Russian delegation at the Seventh Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021–25 reads as follows: "The attempts of NATO countries to portray Ukraine as the main digital victim are extremely unconvincing. Especially against the background [in which] Kiev's authorities continue to boast about their sabotage activities with the use of ICTs. The so-called 'IT army,' supervised by the 'Zelensky regime' together with Western governments, is also increasing its hostile efforts. … It is noteworthy that Kiev acts as aggressor in [the] information space thanks to the support it receives from the West. US Cyber Command units and multinational EU cyber forces are deployed in Ukraine to train and coordinate hackers [and] collect data on hacking methods and vulnerabilities of Russian systems for subsequent transfer to the Pentagon and the NSA, as well as NATO military structures." Permanent Mission of the Russian Federation to the United Nations, "Right of Reply by Representative of the Russian Federation Ms. Irina Tyazhlova at the Seventh Session of the UN Open-Ended Working Group on Security of and in the Use of ICTs 2021–2025", 5 March 2024, available at: https://russiaun.ru/en/news/1050324.

25 As clarified by the NATO Secretary-General, "President Zelensky and the Ukrainian officials have expressed several times to us that they are grateful for the support, but they want us to do even more. *We are ready to step up in many ways but for instance, on the call for a no-fly zone, we have stated that we are not going to impose a no-fly zone because we believe that, that will most likely trigger a full-fledged war between NATO and Russia. A no-fly zone means that we need to take out Russian air defence systems in Russia, which are covering their airspace over Ukraine. And it means that we have to be ready to shoot down Russian planes. That will most likely lead to a full-fledged conflict*. So we are in regular, almost daily, contact with Ukraine. Ukraine is a highly valued partner. We have worked with Ukraine for many years. I have been there many times myself, and it is horrific and really hard to watch. That is also [the] reason why [the] Allies have provided so much support but also have imposed unprecedented sanctions on Russia to ensure that this war ends." Jens Stoltenberg, "Press Conference by NATO Secretary General Jens Stoltenberg Previewing the Extraordinary Summit of NATO Heads of State and Government", 23 March 2022 (emphasis added), available at: www.nato.int/cps/en/natohq/opinions_193610.htm.

26 European Union Agency for Cybersecurity, *Threat Landscape 2022*, 3 November 2022, p. 28, available at: www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

27 Stefan Soesanto, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem*, Center for Security Studies, ETH Zürich, June 2022, available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf. Notably, the Estonia-headquartered company Hacken has stated that "the Hacken team is extremely proud to be a powerful actor in the IT Army of Ukraine". Hacken, "Web3 Technologies in Service of Ukraine", 16 February 2023, available at: https://hacken.io/discover/web3-technologies-in-service-of-ukraine/.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

government".[28] This concern seems justified in light of two concurring factors: (i) the due diligence responsibility requiring States not to allow their territory to be used for malicious cyber activities, and (ii) the fact that Russia has publicly drawn attention to cyber attacks having originated from NATO member nations.[29] Of course, as the same practice seems also to have been adopted by the Russian side,[30] any potential Russian démarche should be deprived of most of its value.

Cyberspace's state of intermediacy and the principle of distinction

Taking into account that the principle of distinction does not apply in peacetime, one may reasonably argue that this principle should not have a specific relevance, unless of course in cases of armed conflict or war. In such cases, States may indeed enjoy a broad discretion in relying on civilian agencies for forcible cyber operations, thereby upsetting the view adopted in this paper.

As shown above, cyberspace is one of main areas of competition between States. This does not mean, of course, that State competition is limited to cyberspace, but rather that competition in cyberspace is qualitatively different from competition in other domains. In other words, in land, sea, air and space, States are confronting each other only through means that may not be perceived as use of force, except, of course, for the rare situations when States have a clear intention to make war (i.e., *animus belligerendi*). In cyberspace, however, States are ready to confront each other, even executing – directly or via their proxies – cyber operations that may be perceived as (or confused with) the use of force. This is not an insignificant difference. At the end of the day, State competition is not a new phenomenon; as explained already in the past,

> [b]etween the two extremes of "pure" peace and "total" war, the states of the world arena may in these terms be observed continuously to engage each other for power and other values, by all instruments of policy, in a continuum of degrees in coercive practices, ranging from the least intense to the most intense.[31]

Current conflicts in cyberspace, however, differ from the past examples of limited use of force, because they have a permanent and persistent nature (temporal element) and their scope is not limited to a specific geographical area (spatial

28 S. Soesanto, above note 27, p. 18.

29 Ministry of Foreign Affairs of the Russian Federation, "Answer of the Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security, Director of the Department of International Information Security of the Ministry of Foreign Affairs of Russia A. V. Krutskikh to a Media Question about Attacks on Russian Critical Infrastructure", 9 June 2022, available at: www.mid.ru/ru/foreign_policy/news/1817019/.

30 To that end, it suffices to recall the news concerning a hacker group affiliated with Iran-backed militias in Iraq which has been considered responsible for cyber attacks against the Ukrainian Stock Exchange. Middle East Media Research Institute, "Hacker Group Affiliated With Iran-Backed Militias In Iraq Claims Cyber Attacks Against Ukrainian Stock Exchange, Ministry Of Veteran Affairs", 28 October 2022 available at: www.memri.org/cjlab/hacker-group-affiliated-iran-backed-militias-iraq-claims-cyber-attacks-against-ukrainian-stock.

31 Myres S. McDougal and Florentino P. Feliciano, "The Initiation of Coercion: A Multi-Temporal Analysis", *American Journal of International Law*, Vol. 52, No. 2, 1958, pp. 248–249.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

element). As argued by Jessup, "it has not infrequently been the practice of states to insist that they were not at war even when they were engaged in large-scale military operations against another state".[32] Indeed, the examples suggested by Jessup in that respect – and the additional examples that can be proposed on the basis of subsequent State practice,[33] including the ongoing war between Russia and Ukraine[34] – are characterized by a restricted *animus belligerendi*, coupled with limited temporal and spatial elements. Competition in cyberspace, instead, cannot be considered as traditional competition, since in this specific situation (*recte* in this specific situation only) States are employing instruments of policy that are almost indistinguishable from the instruments of policy that would characterize wartime. In other words, in waging ongoing, permanent low-intensity cyber warfare, States are showing a sort of *animus belligerendi*, at least from a qualitative – although not quantitative – point of view. Therefore, the principle of distinction in cyberspace – in the present author's opinion – should be interpreted in a broader way than in the other domains. In other words, the principle of distinction in cyberspace should be considered not only in wartime or in the context of an armed conflict, but also in the state of intermediacy.

Where do the opacities lie?

The lack of any significant spillover effect from cyberspace into the traditional domains in the confrontation between the State blocs is indeed very good news, but at the same time, it is reasonable to wonder why it is so. This ambiguous political attitude is workable due to a combination of reasons, some of which are inherent to some of IHL's structural features; other factors instead lie in some opacities of international law.

The fist element of opacity lies in the notion of direct participation in hostilities (DPH). To illustrate this conclusion, it is opportune to borrow some examples already proposed by a distinguished scholar:[35]

32 Philip C. Jessup, "Editorial Comment: Should International Law Recognize an Intermediate Status between Peace and War?", *American Journal of International Law*, Vol. 48, No. 1, 1954, p. 99.

33 Though war in the formal sense had been not evoked since the Second World War, Weisburd argued in 1997 that "states used force so frequently in the period 1945 through 1991 (over 110 times) that it seems impossible to say that, in practice, states do not use force against one another". Arthur Mark Weisburd, *Use of Force: The Practice of States since World War II*, Penn State University Press, University Park, PA, 1997, p. 308. According to Lauterpacht, "[t]here have, however, been two exceptions to this pattern of restraint in the designation of hostilities as 'war' in a technical sense. These exceptions have been respectively the 'state of war' which the Arab States have claimed to exist between themselves and Israel since 1948 and the 'war' which Pakistan considered to have arisen as a result of the Indian crossing of the Pakistan boundary on September 6, 1965." Elihu Lauterpacht, "The Legal Irrelevance of the 'State of War'", *Proceedings of the American Society of International Law at Its Annual Meeting (1921–1969)*, Vol. 62, 1968, p. 60.

34 In the ongoing war between Russia and Ukraine, it is perhaps not without significance to notice that Russia is not exercising any right of visit and search vis-à-vis third parties' merchant vessels, although IHL may allow it to do so. This Russian self-restraint, in the present author's view, suggests that Russia is not willing to be engaged in a state of war vis-à-vis third parties, including – and primarily – NATO allies.

35 Kubo Mačák, "Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield", *International Review of the Red Cross*, Vol. 105, No. 923, 2023.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

(a) a distributed denial-of-service (DDoS) attack, or more complex ones, such as cyber operations aimed at disrupting assets or infrastructure;
(b) use of a smartphone application to report movements of enemy troops, vehicles or aircraft by uploading location-tagged images or videos; and
(c) provision of cyber threat intelligence (CTI) solutions to defend cyber infrastructure against cyber attacks.

Should civilians perform any of the cyber operations described above, a case-by-case assessment should be undertaken in light of DPH. In accordance with the International Committee of the Red Cross (ICRC) *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC Interpretive Guidance),[36] it will be necessary to ascertain whether the following three cumulative conditions are satisfied: (i) threshold of harm, (ii) direct causation, and (iii) belligerent nexus. While the notion of DPH is outside of the scope of this paper (and so also is the overall discussion on the customary nature of the ICRC Interpretive Guidance), it is still important to make a few comments in this regard. The notion of DPH is broader than the concept of "attack", so providing tactical intelligence is widely considered as a form of DPH.[37] Therefore, assuming that cyber operations under example (a) above will target military networks, thereby adversely affecting the military operations or military capacity of an adversary, it is reasonable to conclude that DPH could be satisfied. Conversely, examples (b) and (c) will more likely not be qualified as DPH, unless the information provided will be useful for the conduct and/or execution of a tactical military operation. Of note, should CTI solutions include "hack-back" operations, considerations made for example (a) will be applicable *mutatis mutandis*. Overall, in the case of the transmission of intelligence, the possibility of meeting DPH conditions cannot be ruled out, even if the transmission *per se* is not an operation implying physical damages. As a further complication, it is also important to recall that intelligence operations cannot be distinguished from military operations based only on their harmful nature. Military operations, in coherence with the notion of DPH, also comprise the

36 Nils Melzer (ed.), *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Geneva, 2009 (ICRC Interpretive Guidance), available at: www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.

37 In accordance with ICRC Interpretive Guidance, "the requirement of direct causation [needed for DPH] would still be fulfilled where the act constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm. Examples of such acts would include, *inter alia*, the identification and marking of targets, the analysis and transmission of tactical intelligence to attacking forces, and the instruction and assistance given to troops for the execution of a specific military operation." *Ibid.*, pp. 54–55. Likewise, it is Michael N. Schmitt's opinion that "[r]endering strategic-level geopolitical estimates is certainly central to the war effort, but will have little bearing on specific combat missions. By contrast, tactical intelligence designed to locate and identify fleeting targets is the sine qua non of time-sensitive targeting; it is an integral component of the application of force against particular targets. Civilians providing strategic analysis would not be directly participating in hostilities, whereas those involved in the creation, analysis, and dissemination of tactical intelligence to the 'shooter' generally would." Michael N. Schmitt, "Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees", *Chicago Journal of International Law*, Vol. 5, No. 2, 2005, p. 534, available at: https://chicagounbound.uchicago.edu/cjil/vol5/iss2/11.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

operational preparation of the environment, which is instrumental to the future execution of a harmful operation.[38] This uncertainty, however, is not cyber-specific but is rather inherent to the nature of the notion of DPH.

There are, however, other opacities that are more cyber-specific. As a first opacity, the notion of use of force in cyberspace needs to be mentioned. According to the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn Manual 2.0), "[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".[39] The said Tallinn Manual rule – which seems not widely disputed[40] – is too generic, and as such, it is unsettled as to where the threshold for the use of force in cyberspace is set. It cannot be ruled out that some cyber operations may eventually – and perhaps even unintentionally – cross such a threshold. On the other hand, as deterrence depends on the perceivable credibility of the willingness to use force in self-defence, whenever there is uncertainty on the threshold for the use of force, no effective deterrence can be achieved[41] because the lack of clarity incentivizes some States to remain just below the threshold in order to avoid escalation. Additionally, as a further complication, it is worth noting that self-defence in accordance with Article 51 of the United Nations (UN) Charter is limited to the case of an armed attack, i.e. the most grave forms of the use of force, as stated in the International Court of Justice's (ICJ) *Nicaragua* judgment.[42] In the case of cyber operations reaching the threshold for the use of force but not constituting an armed attack, an injured State will be entitled to apply countermeasures. In accordance with the 2001 *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (DARSIWA), however, countermeasures "shall not affect the obligation to refrain from the threat or use

38 There is finally the possibility of employing cyber capabilities for other forms of non-harmful warfare, such as influence operations and hybrid warfare. These kinds of warfare, although very important for the success of military operations, should not be considered as falling within the definition of DPH, so they will not be considered for the purposes of this article.

39 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0), Rule 69, p. 330.

40 It is true that some States, such as France, "[do] not rule out the possibility that a cyberoperation without physical effects may also be characterised as a use of force. In the absence of physical damage, a cyberoperation 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 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." *International Law Applied to Operations in Cyberspace*, paper shared by France with the Open-Ended Working Group established by Resolution 75/240, 2021, available at: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf. If we take a closer look, however, the French position does not contradict the Tallinn Manual 2.0's view, but rather aims at enlarging its scope.

41 As argued by General Sir Nicholas Houghton, former chief of the defence staff of the British Armed Forces, "our ability to generate deterrence … wholly depends on the perceivable credibility of our willingness to use force if necessary". Nicholas Houghton, "Building a British Military Fit for Future Challenges rather than Past Conflicts", speech given at Chatham House, London, 15 September 2015, available at: www.gov.uk/government/speeches/building-a-british-military-fit-for-future-challenges-rather-than-past-conflicts.

42 ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States)*, Judgment, 27 June 1986, para. 191.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

of force as embodied in the Charter of the United Nations".[43] Therefore, the injured State's reaction should not reach the same level of intensity,[44] thus depriving the injured State of proportionate response options, at least in theory. Without equating a proportional response with effective response, the above limitations certainly raise further questions about the relevant thresholds, and whether the deterrent effect of the legal rules is well calibrated with the currently prevailing interpretations.[45]

The second opacity lies in Article 52 of Additional Protocol I to the 1949 Geneva Conventions (AP I). According to Article 52, "[c]ivilian objects shall not be the object of attack or of reprisals". The notion of "object" contained in that article, as argued by the Tallinn Manual 2.0, "is not to be interpreted as including data, at least in the current state of the law".[46] Thus, the majority of Group of Experts that drafted the Tallinn Manual 2.0 concluded that "an attack on data per se does not qualify as an attack", although they agreed that "a cyber operation targeting data may sometimes qualify as an attack when the operation affects the functionality of cyber infrastructure or results in other consequences that would qualify the cyber operation in question as an attack".[47] This narrow interpretation of the notion of "object" may also have practical implications, as it could pave the way for the political and social perception that cyber operations are less harmful than traditional combat operations.

The third opacity is the definition of espionage under international law. While espionage is explicitly recognized in times of armed conflict, in peacetime (and in a state of intermediacy as well), the scope of "espionage" is disputed. As any clear definition of espionage is lacking in treaty law, States, with a view to avoiding legal constraints, could be tempted to style/label cyber operations as unacknowledged intelligence operations rather than as military operations.[48] This

43 International Law Commission (ILC), *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, UN Doc. A/56/10, 2001 (DARSIWA), Art. 50(a), available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

44 As asked by Roscini, "[c]an the state victim of a cyber attack also adopt countermeasures involving the use of force against the attacker? As such measures are considered unlawful in contemporary international law, the answer would be affirmative only if one should conclude that a cyber attack triggers the right of self-defense under Article 51 of the UN Charter or under customary international law." Marco Roscini, "World Wide Warfare: *Jus ad Bellum* and the Use of Cyber Force", *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010, p. 113.

45 Of course, it might be argued that such a problem is not a cyber-specific opacity, as it links to the general problem of distinguishing between armed attack and use of force. In the traditional domains, however, a reasonable accommodation has been found "arguing that the classic right of national self-defence entitles military units to react to small-scale armed attacks 'on-the-spot' with necessary and proportionate counter-force", even in the case of a use of force not constituting an armed attack. Aurel Sari, "Personal Self-Defence in International Law: A Norm in Search of its Normative Foundations?", *OpinioJuris*, 3 May 2019, available at: https://opiniojuris.org/2019/05/03/soldier-self-defense-symposium-personal-self-defense-in-international-law-a-norm-in-search-of-its-normative-foundations/. Whether and how the concept of self-defence can be applied "on-the-spot" in the cyber domain, however, is definitely unexplored and is much more debatable.

46 Tallinn Manual 2.0, above note 39, p. 437.

47 *Ibid.*

48 At the ICRC Expert Meeting held in January 2020, "[s]ome experts expressed concerns that while armed forces may be familiar with the requirements of IHL, this may not be the case for intelligence agencies

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

opacity, *a fortiori*, is relevant because the distinction between intelligence and military operations/activities is inherently highly controversial in the cyber domain, as often the same malware can be used for theft, for spying or for causing damage/malfunctions.

The fourth opacity lies in ICJ case law on States' responsibility for non-State actors' conducts. Consistent with the *Nicaragua* judgment,[49] attribution of cyber operations by non-State actors requires that the sponsoring State had effective control of the operations during which the alleged violations were committed. Lacking such effective control, non-State actors remain responsible for their acts, while the sponsoring State will not be responsible for the acts of the non-State actors, but for its own conduct *vis-à-vis* the injured State. Therefore, covert operations resulting in financial support, training, or supply of weapons, intelligence and logistic support to non-State actors could constitute a breach of the principle of non-intervention, but may not be sufficient for establishing a violation of the prohibition on the threat or use of force. As a consequence, covertly promoting non-State actors – including "patriotic hackers", criminal gangs or even tech companies – in order to conduct cyber operations will most likely not implicate the responsibility of the sponsoring State, at least with regard to the prohibition on the threat or use of force. In other words, in the case of non-State actors conducting malicious cyber operations, the sponsoring State will likely not risk provoking a reaction in self-defence by the injured State or collective self-defence also involving the allies of the injured State. It might be thought that whenever a State gives support to non-State actors, it is performing an activity that is opaque in itself, and that therefore we are not facing a cyber-specific opacity, but this seems to be only partially true. In the cyber domain (*recte* in the cyber domain only), a State might provide support to a non-State actor, even if the latter is not extraterritorially based. In other words, while in the physical domain a non-State actor needs to be deployed on the territory of a State in order to affect that State, in the cyber domain this is optional. As a consequence, a State can be injured by malicious cyber operations executed by a non-State actor that is not based inside its territory. This specific feature makes cyber operations by non-State actors both more difficult to be addressed (from the injured State's perspective) and easier to be supported (from the sponsoring State's perspective).

The fifth opacity can be found in some structural features of the law of State responsibility. As is well known, "[q]uestions of evidence and proof of [a breach of an international obligation] fall entirely outside the scope" of the DARSIWA.[50]

operating in cyberspace. One expert questioned whether some States might deliberately shift operations between agencies with a view to avoiding these obligations. This raises the question of how operations transition from collecting intelligence to delivering effects given these concerns and the fact that the international legal framework governing effects operations is much more developed than the framework governing intelligence operations." Ewan Lawson and Kubo Mačák, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, report of ICRC Expert Meeting, Geneva, 21–22 January 2020, p. 14, available at: https://shop.icrc.org/avoiding-civilian-harm-from-military-cyber-operations-during-armed-conflicts-icrc-expert-meeting-21-22-january-2020-geneva-pdf-en.

49 ICJ, *Nicaragua*, above note 42, para. 115.

50 DARSIWA, above note 43, p. 54.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

Therefore, unless a breach of an international obligation is brought to an international court or arbitration proceeding that will adjudicate the case in accordance with its rules of procedure, no fixed standard for burden of proof that a State shall meet for attribution can be found in general international law. Consequently, any response to malicious cyber operations is inherently controversial because of the complexities related to attribution. No one can fail to see that this is not a cyber-specific problem, but cyberspace further exacerbates the existing issue. Moreover, in physical domain, whenever the attribution is contentious, the discussion over attribution has often been circumvented by applying Article 11 of the DARSIWA on conduct acknowledged and adopted by a State as its own. In the case of cyberspace, however, States have so far been quite hesitant to apply Article 11 of the DARSIWA, although this possibility should not be ruled out.[51]

Mitigation measures

In order to foster stability in cyberspace, tackling the identified opacities would be beneficial. This section will thus propose some mitigation measures, although some of them might not be easily achievable under current international law.

It is worth noting that one mitigation measure to manage the uncertainty surrounding the use of force threshold is known as the cumulative effect theory. This theory, expressly endorsed by NATO,[52] implies the possibility of considering as an armed attack a series of malicious cyber activities which otherwise, considered in isolation, would not have been considered as an armed attack. Notably, in the author's opinion, consistency with the cumulative effect theory may further corroborate the need to apply the principle of distinction in cyberspace, even before the eruption of an armed conflict (i.e., in the state of intermediacy). In the end, if States are inclined to consider as an armed attack a series of malicious cyber activities which otherwise would not have been considered so, it would be reasonable to apply to each of those malicious cyber activities the principle of distinction, as if the armed conflict had already started. The cumulative effect theory alone, however, is not completely effective. As shown above by the example of cyber attacks against Albania, States, at least so far, have been quite reluctant to apply the theory in practice. Although understandable given that the concrete application of the cumulative effect theory could lead to an escalation to an armed conflict not limited to the cyber domain, this reluctance may nevertheless make the theory itself less credible. So, in the

51 A notable exception is the recent Irish *Position Paper on the Application of International Law in Cyberspace*, where it is argued that "[i]n a cyber context, a malicious cyber-operation conducted by a third party can thus be attributed to a state where it essentially takes ownership of the act, which might be ascertained through acts of support, approval and/or acquiescence". Irish Department of Foreign Affairs, *Position Paper on the Application of International Law in Cyberspace*, 6 July 2023, para. 23, available at: www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf.

52 NATO, above note 22, para. 66.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

case of cyber operations below the threshold for the use of force, deterrence might be achieved by mainly relying on countermeasures, including especially countermeasures by a plurality of injured States or on behalf of an injured State (i.e., collective countermeasures). Countermeasures, however, are still only perceived as a remedy available to an individual State, and the legitimacy of collective countermeasures is disputed.[53]

With reference to the notion of "object", the situation is not particularly encouraging. Although the aforementioned Tallinn Manual 2.0 position may be considered unsatisfactory, it cannot be denied that it follows the traditional intent of the drafters of AP I, as well as the language of the latter.[54] Therefore, a new notion of "object" for cyber warfare should require either the agreement on a new treaty provision or consistent State practice supporting an updated interpretation of the relevant provision of AP I, considering developments in ICT.

Concerning the definition of espionage under international law, it would be sufficient to apply the already existing legal provisions, as well as enforcing the principle of distinction under IHL. Both arguments will be analyzed in the following sections.

As seen above, existing ICJ case law is one important factor that may contribute to States' support to – and reliance on – non-State actors for certain cyber operations. The likelihood of changing the ICJ effective control test, however, seems very low. On the one hand, that test has been confirmed in ICJ

53 As noted by James Crawford, "[i]f the question of unilateral countermeasures by an injured state has been controversial, the notion of countermeasures by states that have not themselves been directly injured by an internationally wrongful act has been even more so". James Crawford, *State Responsibility: The General Part*, Cambridge University Press, Cambridge, 2013, p. 703. According to a recent report, "there still seems to be insufficient state practice and *opinio juris* in support of a right of indirectly injured states to take general interest countermeasures under customary international law. But the law is developing rapidly on this matter, as a growing number of states have adopted and expressed support for such measures." Talita Dias, *Countermeasures in International Law and Their Role in Cyberspace*, Chatham House Research Paper, International Law Programme, May 2024, p. 56, available at: www.chathamhouse.org/sites/default/files/2024-05/2024-05-23-countermeasures-international-law-cyberspace-dias.pdf.

54 According to the Commentary on the Additional Protocols, "[t]he Diplomatic Conference finally adopted a similar formula which combines the two possibilities; it begins by declaring civilian objects immune and continues with an *a contrario* definition in defining military objectives. Before discussing the three paragraphs which this article comprises, it might be appropriate to devote some attention to the terminology used. The English text uses the word 'objects', which means 'something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing'. The French text uses the word 'biens', which means 'chose tangible, susceptible d'appropriation'. It is clear that in both English and French the word means something that is visible and tangible. As regards the word 'objective', in English this is an abbreviation of the expression 'objective point', defined by the Oxford Dictionary as follows: 'the point towards which the advance of troops is directed; hence, […] the point aimed at'. *In French the word 'objectif' is defined as follows in the Dictionnaire Robert: 'point contre lequel est dirige une operation strategique ou tactique; par extension: resultat qu'on se propose d'atteindre par une operation militaire'. There is however no doubt that in this article both the English and French texts intended tangible and visible things by the word 'objective', and not the general objective (in the sense of aim or purpose) of a military operation; therefore the extended meaning given by the Dictionnaire Robert is not included in this article.*" (emphasis added). Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987 (ICRC Commentary on the APs), paras 2005–2010 (emphasis added).

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

case law subsequent to the *Nicaragua* case, in the *Genocide* judgment.[55] On the other hand, the high threshold of the effective control test has been one reason for avoiding the attribution to the United States for the acts committed against Nicaragua by the Contras, a CIA-supported militia. Thus, unless an agreement with the Russian/Chinese bloc can be found, the ICJ is not likely to be willing to change its settled case law. If changed, it would most probably be perceived as a double standard.

Finally, questions of evidence and proof of a breach of an international obligation of a State cannot be changed through an adaptive reading of the existing legal framework. This conclusion indeed takes into account the fact, clearly shown in the ongoing war between Russian and Ukraine, that the UN Security Council is unable to effectively handle conflicts involving one permanent member of the Council. A mitigation measure, instead, would require new rules, potentially including compulsory arbitration. Currently, it is unlikely that any agreement in that respect can be reached in the near future.

Definition of espionage under international law

What does it mean to spy?

With respect to espionage, the Tallinn Manual 2.0 argues that "although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so".[56] Even assuming that customary international law does not prohibit espionage *per se*, the statement appears equivocal, unless a clear definition of espionage is provided.[57] In a peacetime situation, three possible scenarios should be considered. The first of these is cyber operations causing physical damage. These operations, as seen above, should be considered as a use of force and as such should be almost undisputedly considered unlawful, primarily as a violation of the prohibition on the use of force and a violation of sovereignty.[58] As a corollary, cyber operations causing physical damage cannot be considered (or justified) as part of espionage operations. The second scenario consists of cyber operations – below the use of

55 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, 2007 ICJ 108, 26 February 2007.

56 Tallinn Manual 2.0, above note 39, p. 168.

57 The legal literature on the legality of espionage is vast. Since the legality of espionage is out of the scope of this article, the pertinent legal literature is not further discussed; among the many works available, however, see Asaf Lubin, "The Liberty to Spy", *Harvard International Law Journal*, Vol. 61, No. 1, 2020, available at: www.repository.law.indiana.edu/facpub/2905.

58 Notably, a few States, such as the United Kingdom, consider sovereignty as a mere principle rather than a rule. In any event, for those States as well, cyber operations – below the use of force threshold – causing physical damage would be considered unlawful, although not as a violation of sovereignty but instead as a prohibited intervention. Therefore, for the purposes of this article, it suffices to conclude that cyber operations – below the use of force threshold – causing physical damage should be considered as an internationally wrongful act.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

force threshold[59] – causing loss of functionality. In this scenario, there are different legal opinions. According to the Tallinn Manual 2.0,

> the Experts agreed that, in addition to physical damage, the remote causation of loss of functionality of cyber infrastructure located in another State sometimes constitutes a violation of sovereignty, although no consensus could be achieved as to the precise threshold at which this is so due to the lack of expressions of *opinio juris* in this regard.[60]

The third scenario involves cyber operations aimed at exfiltration of data and causing neither physical damage nor the loss of functionality. In that respect, the Tallinn Manual 2.0 explains that "no consensus could be achieved as to whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty".[61]

Therefore, while the third scenario clearly falls within the scope of espionage, it is not immediately obvious – and therefore calls for a detailed examination – whether the second scenario may also fall within the scope of espionage. In other words, for the purposes of this article, it is a relevant question to discuss whether cyber operations causing a loss of functionality (except for *de minimis* consequences[62]) could be, *vel non*, justifiable as falling within the notion of (peacetime) espionage,[63] or otherwise should be considered as unlawful, as a violation of sovereignty or as a prohibited intervention. It is outside of the scope of this article to discuss the question of whether cyber operations aimed at exfiltration of data and causing neither physical damage nor the loss of functionality might be, *vel non*, legally justifiable. As will be explained, espionage should be understood as only comprising information-gathering,[64] thereby excluding from the notion of espionage cyber operations causing a loss of functionality (except for *de minimis* consequences). To corroborate such a conclusion, espionage in its various facets will be analyzed.

Wartime espionage

To begin with, in order to understand the complexity surrounding wartime espionage, it is opportune to recall the following extract from Oppenheim:

59 Although, generally speaking, cyber operations causing (only) loss of functionality are considered by default below the use of force threshold, a few nations, such as France, do not rule out the possibility that a cyber operation without physical effects may also be characterized as a use of force.
60 Tallinn Manual 2.0, above note 39, pp. 20–21.
61 *Ibid.*
62 The author understands and acknowledges that a *de minimis* threshold could in itself be contentious and vague, and so, even assuming the existence of this threshold, disagreements may still occur in the understanding of its actual scope.
63 There is indeed extensive literature regarding espionage, which mainly addresses the legality, *vel non*, of espionage. *Ex plurimis*, see Russell Buchan, *Cyber Espionage and International Law*, Hart, Oxford, 2019.
64 In accordance with Russell Buchan, cyber espionage should comprise the following constitutive elements: "the (i) non-consensual (ii) copying (iii) of confidential information (iv) that is resident in or transiting through cyberspace". *Ibid.*, p. 13.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

> [A]rticle 24 of the Hague Regulations now enacts the old customary rule that a belligerent has a right to employ all methods necessary to obtain information, and these methods include espionage and treason. But this right stands face to face with the right to consider and punish as war criminals enemy individuals, whether soldiers or not, committing acts of espionage or treason. There is an irreconcilable conflict between the necessity of obtaining information on the one hand, and self-preservation on the other; and accordingly espionage and treason bear a twofold character. On the one hand, International Law gives a right to belligerents to make use of espionage and treason. On the other hand, the same law gives a right to belligerents to consider espionage and treason, committed by enemy soldiers or enemy private individuals within their lines, as acts of illegitimate warfare, and consequently punishable.[65]

In addition, still relying on Oppenheim, it is opportune to recall that

> [e]spionage must not be confounded, firstly, with scouting, or secondly, with despatch-bearing. According to article 29 of the Hague Regulations, espionage is the act of a soldier or other individual who clandestinely, or under false pretences, seeks to obtain information concerning one belligerent in the zone of belligerent operations with the intention of communicating it to the other belligerent. Therefore, soldiers not in disguise, who penetrate into the zone of operations of the enemy, are not spies. They are scouts who enjoy all privileges of the members of armed forces, and they must, if captured, be treated as prisoners of war.[66]

The Hague Regulations, however, do not provide a clear legal definition of espionage. Nonetheless, as argued by the Commentary on the Additional Protocols to the 1949 Geneva Conventions,[67] "by giving a sufficiently precise description of those who shall not be considered as spies, it is possible to deduce the constitutive elements of espionage in any specific case, by means of *a contrario* reasoning".[68] Therefore, on the basis of Article 29 of the Hague Regulations defining the requirements to be considered a spy, it is possible to conclude that espionage should be limited to seeking to obtain information in the zone of operations with the intention of communicating it to the enemy, acting secretly, in disguise or under false pretences.[69]

65 Lassa Oppenheim, *International Law: A Treatise*, Vol. 2: *War and Neutrality*, 2nd ed., Longmans, Green & Co., 1912, §255, available at: www.gutenberg.org/files/41047/41047-h/41047-h.htm#Page_313.

66 *Ibid.*, §160.

67 Generally speaking, the relevance of the Additional Protocols for the purposes of espionage is quite limited, since their effect was to extend the provisions on wartime espionage (already contained in the Hague Regulations) to irregular forces belonging to resistance movements and similar forces. In other words, the Additional Protocols have not enlarged the content or the geographic scope of wartime espionage.

68 ICRC Commentary on the APs, above note 54, para. 1774.

69 During the First World War, when British authorities discovered a German subject attempting to provide information to the German authorities from inside UK territory with regard to the defences and war preparations of Great Britain, the offence was described as a war crime or war treason, rather than

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

Notably, wartime espionage is subjected to a narrow territorial scope, as it is limited to enemy-controlled territory. So, as suggested by the Tallinn Manual 2.0, "cyber spying will most likely occur as a close access cyber operation".[70] Conversely, cyber (wartime) espionage performed from outside enemy-controlled territory should be outside of the scope of the rule on wartime espionage.[71] In the end, from a practical point of view, as remote cyber espionage would often not be qualified as wartime espionage, the chance to apply Article 29 of the Hague Regulations to cyber operations is likely overstated nowadays.

In the end, for the purposes of this article, it is relevant to conclude that, in times of war, to constitute espionage in accordance with Article 29 of the Hague Regulations, the actual conduct/*actus reus* must be limited to information-gathering in disguise in the enemy controlled territory. In other words, even accepting the narrow definition of "object" in cyber warfare mentioned above, in the event of damage or loss of functionality caused as an effect of a cyber espionage operation, the cyber operation should be considered outside of the definition of espionage (except for *de minimis* consequences). As recalled in the

espionage (the case in question, the *Lody* case of 1914, is mentioned in Coleman Phillipson, *Wheaton's Elements of International Law*, 5th English ed., Stevens and Sons, London, 1916, p. 511, available at: https://archive.org/details/wheatonselements00whearich/page/n5/mode/2up?ref=ol&view=theater).
From a different perspective, Balladore Pallieri suggests that there is hostile conduct that cannot be considered espionage, although it should be equated to the latter for the purposes of punishment. Pallieri suggests, for instance, that the British Major John André – who attempted to induce US General Arnold to surrender the British fort at West Point – should not have been considered as a spy because the essential requirement of the intent of obtaining information was lacking. This legal qualification, according to Pallieri, was without prejudice to the possibility, in such cases, of applying, *mutatis mutandis*, appropriate penalties as allowed against spies (Balladore Pallieri, *La Guerra*, CEDAM, Padova, 1935, pp. 248–249). Even Professor Yoram Dinstein distinguishes between espionage and sabotage, as "saboteurs may commit acts in breach of law of war (e.g. deliberate attack against civilian objectives in the rear), and consequently they may be viewed as war criminals. Conversely, spies are merely engaged in obtaining information about the enemy, an act that is not prohibited per se by the law of war" (Yoram Dinstein, "The Law of Land Warfare", *Israel Yearbook on Human Rights*, Vol. 13, 1983, pp. 64–65). To that end, the case of *Skorzeny and Others* seems quite illustrative. In this case, one saboteur argued that he was on an espionage mission in "no man's land" and so he was not punished, in accordance with Article 31 of the Hague Convention, since he was returned from the espionage mission to his own lines. According the Military Tribunal, "[t]he argument put forward by Defence Counsel [for Skorzeny] appears to be unsound. Article 31 gives immunity to a spy who returns to his lines in so far as he cannot be punished as a spy. The accused in this case, however, were not tried as spies but were tried for a violation of the laws and usages of war alleged to have been committed by entering combat in enemy uniforms. Articles 29-31 of the Hague Convention have therefore no application in this case" (US Military Court in Germany, *Trial of Skorzeny and Others*, in United Nations War Crimes Commission, *Law Reports of Trials of War Criminals*, Vol. 9, London, 1949, pp. 90–94, available at: https://tile.loc.gov/storage-services/service/ll/llmlp/Law-Reports_Vol-9/Law-Reports_Vol-9.pdf).

70 Tallinn Manual 2.0, above note 39, p. 411.

71 Accordingly, the *Military Manual on International Law Relevant to Danish Armed Forces in International Operations* clarifies that computer network exploitation activities "undertaken by Danish cyber experts from Denmark or in the mission area in an area controlled by own forces or allied forces *cannot fall* under the notion of espionage under IHL even though they may be punishable as espionage pursuant to legislation applicable in the country in which the intelligence is being collected". Danish Ministry of Defence, Defence Command Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 12 October 2020, pp. 177–178, available at: www.forsvaret.dk/en/publications/military-manual/.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

Tallinn Manual 2.0, "[b]y styling a cyber operation as a 'cyber espionage operation', a State cannot therefore claim that it is by definition lawful under international law".[72]

Peacetime espionage

Legal opinion on espionage during peacetime is not unanimous, although the majority view appears inclined to consider that espionage does not *per se* violate international law. This means that espionage is neither legal nor illegal, and so the method by which it is carried out might similarly be neither legal nor illegal.[73] Such positions rely also on the fact that no treaty explicitly forbids espionage. Be that as it may, it is also true that peacetime espionage cannot be easily equated to wartime espionage, because the States concerned are not necessarily enemies, and they may even be allies. This factual situation may induce States to self-restrain their reaction towards espionage, thereby giving the impression that espionage is considered lawful, even when the conduct/*actus reus* is performed inside the territory of the spied-upon State.[74]

72 Tallinn Manual 2.0, above note 39, p. 170.

73 *Ibid.*, Rule 32, p. 168: "Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so." See also Bundesgerichtshof (Federal Court of Justice), *Espionage Prosecution Case*, Case No. 2 BGs 38/91, 30 January 1991: "From the standpoint of international law, espionage in peacetime could not be considered as unlawful. No international agreement had ever been concluded on the subject. Neither was there any usage sufficient to establish a customary rule permitting, prohibiting or otherwise regulating such activity." Notably, however, the Canadian Federal Court took an opposite view, noting that "intrusive activities … are activities that impinge upon the principles … 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, J. Blanchard, Ottawa, 24 and 27 April and 14 June 2007. Even the Dutch Special Court of Cassation, in the *In re Flesche* case, held that espionage conducted outside of wartime "constitutes an international delinquency by [the sending] State against another State for which it is answerable under international law". Special Court of Cassation, *In re Flesche*, 27 June 1949, reprinted in *Annual Digest and Reports of Public International Law Cases*, Vol. 16, 1955.

74 To corroborate such a finding, some reference to case law and practice is opportune. (1) In the case of *Mrs. Schmidt-Marquardt v. Director of Prosecutions*, a Russian spy operating in the British Zone of Germany, in order to obtain information on Russian nationals who had fled to the British zone, and to discover where these persons were residing, was acquitted. In this case the Court noted that "the Hague Regulations define espionage in that case with sufficient particularity to leave no doubt as to what the term means, but where, as in the case now before us, the espionage is alleged to have been committed in time of peace and by the agent of a Power with whom we are not at war, what constitutes espionage is by no means so clear". Therefore, the acquittal was given on the basis of the fact that the information searched for by the spy did not amount to a military or a political secret. British Zone of Germany, Control Commission Court of Appeal, *Schmidt-Marquardt v. Director of Prosecutions*, Case No. 146, 28 September 1949, *Annual Digest and Reports of Public International Law Cases*, Vol. 16, 1955, pp. 405–407. (2) When, during the Second World War, the Russians "stole" from Canada some documents concerning the atomic bomb, "[m]unicipally, a series of arrests and prosecutions were initiated over a period of three years against twenty Canadian public servants, military personnel and others, *but against no Soviet nationals*". Maxwell Cohen, "Espionage and Immunity – Some Recent Problems and Developments", *British Yearbook of International Law*, Vol. 25, 1948, p. 408 (emphasis added). (3) Upon discovering that the United States, with the support of Denmark (an EU member State), was performing a far-reaching espionage activity, including tapping of the German chancellor's phone, Germany did not open any criminal investigation or adopt any blatant acts of retorsion. See Pierre-Paul Bermingham, "Danish Secret Service Helped NSA Spy on Merkel, EU Officials: Report", *Politico*,

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

Conversely, in cases of intelligence agencies having carried out (inside the territory of the injured State) activities other than intelligence-gathering, an injured State has been considered, with no major discussion, entitled to legitimately complain.[75] It is true that practice has also shown that complaints by injured States in cases of unlawful activities conducted inside their respective territories, performed by foreign intelligence services, are far from being the general rule.[76] The fact that injured States have not always taken steps against the injuring State after a violation of international law, however, cannot be interpreted as evidence that such violations did not occur. Indeed, as is well known in criminal law, the fact that the prosecution of a crime may be conditional upon a complaint by the

31 May 2021, available at: www.politico.eu/article/press-report-merkel-and-eu-leaders-spied-on-by-nsa-via-denmark/. Conversely, when the German Federal Government tried to reach a comprehensive intelligence agreement with the United States, the latter declined the offer. Kristina Daugirdas and Julian Davis Mortenson, "Contemporary Practice of the United States Relating to International Law", *American Journal of International Law*, Vol. 108, No. 4, 2014.

75 To that end, it suffices to recall (1) the *Rainbow Warrior* incident, in which French intelligence operatives sunk a Greenpeace ship in New Zealand waters (see the *Rainbow Warrior* arbitral award, *Rainbow Warrior (New Zealand v. France)*, 20 RIAA 217 (Arb. Trib. 1990), 1990), or (2) the Argentinian complaint regarding Israel's covert abduction of Nazi fugitive Adolf Eichmann (UNSC Res. 138, "Question relating to the Case of Adolf Eichmann", 23 June 1960), or even (3) the UK reaction to the poisoning of Alexander Litvinenko (who was living at that time in UK territory) on the orders of the Russian Federal Security Service. The then UK home secretary stated: "It goes without saying that this [the poisoning of Alexander Litvinenko] was a blatant and unacceptable breach of the most fundamental tenets of international law and of civilised behaviour." "Home Secretary Statement on Litvinenko Inquiry Report", oral statement to Parliament, 21 January 2016, available at: www.gov.uk/government/speeches/home-secretary-statement-on-litvinenko-inquiry-report. In addition, (4) the European Court of Human Rights (ECtHR) found Russia responsible for violating the right to life of Alexander Litvinenko. ECtHR, *Carter v. Russia*, Case No. 20914/07, 21 September 2021.

76 For example, the secret detentions and illegal transfers of detainees carried out by the United States abroad have not raised significant protests, as injured States have often invoked the concepts of State secrecy or national security to "make it more difficult to conclude judicial and/or parliamentary proceedings aimed at ascertaining responsibility for rehabilitating and compensating the alleged victims of violations" (Council of Europe, Parliamentary Resolution 1562, "Secret Detentions and Illegal Transfers of Detainees involving Council of Europe Member States", 27 June 2007, available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17559&lang=en). The US extraordinary rendition programme, however, has been assessed several times as a violation of human rights perpetrated in the territory of the States where renditions took place (see, *ex plurimis*, the ECtHR judgments in the cases of *El-Masri v. The Former Yugoslav Republic of Macedonia* (2012), *Al Nashiri v. Poland* and *Husayn (Abu Zubaydah) v. Poland* (2014), *Nasr and Ghali v. Italy* (2016) and *Al Nashiri v. Romania* (2018)). Moreover, no State – including the United States – has ever try to justify such renditions relying on the definition of espionage under international law. It also relevant to notice that the assassination (in German territory) of the Ukrainian political exile Dr Lev Rebet, for which the KGB official Bogdan Stashynsky was convicted by German tribunals in 1962 (see "The Trial of Bogdan Stashynsky in the Federal Republic of Germany", *International Commission of Jurists Bulletin*, No. 15, April 1963, pp. 26–30, available at: www.icj.org/wp-content/uploads/2013/07/ICJ-Bulletin-15-1963-eng.pdf), has "attracted only episodic attention in the press in the Western World", as noted by Senator Thomas J. Dodd (89th US Congress, Second Session, "Investigation of Senator Thomas J. Dodd", 1966, p. 91, available at: https://tinyurl.com/yk5xd9kz). Even the recent (2021) conviction, by a Berlin court, of Vadim Krasikov for the murder (in Berlin) of Zelimkhan Khangoshvili (a Chechen dissident who was labelled as a terrorist by Moscow) has led only to the declaration as *persona non grata* of two of 101 Russian diplomatic staff stationed in Germany. Notably, according to the German judge that convicted Krasikov, "the central government of the Russian Federation was the author of this crime". Thomas Escritt, "German Court Accuses Russia of 'State Terrorism' over 2019 Berlin Park Murder", *Reuters*, 16 December 2021, available at: www.reuters.com/world/europe/german-court-convicts-russian-2019-berlin-park-murder-2021-12-15/.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

victim does not make the conduct of such crime lawful, should the complaint not be filed.

Locus commissi speculationis: The case of remote cyber espionage

At the beginning of the conquest of outer space, the USSR attempted to qualify observation from space for the purposes of collecting intelligence as illegal.[77] Subsequent State practice, however, has not followed this view. With specific reference to espionage in the cyber domain, it is difficult, at this stage, to predict whether State practice will follow the same evolution of space espionage. Some South American States[78] (particularly Brazil[79]), the African Union[80] and the European Commission[81] firmly opposed cyber espionage, while the majority of States seem reluctant to take any position, with the remarkable exception of the United States.[82] Even looking to the Tallinn Manual 2.0 is not particularly helpful

77 Soviet statement in the General Assembly, First Committee, 17th Session, 1289th Meeting, 3 December 1962, available at: www.unoosa.org/pdf/garecords/A_C1_PV1289E.pdf.

78 "*Note Verbale* Dated 22 July 2013 from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations Addressed to the Secretary-General", UN Doc. A/67/946, 29 July 2013, available at: https://digitallibrary.un.org/record/754199?ln=zh_CN. In this *note verbale*, the presidents of multiple South American States condemn acts of espionage conducted by the United States in the countries of the region.

79 At the May 2023 intersessional meetings of the Open-Ended Working Group on ICTs, Brazil stated that it "considers an internationally wrongful act the intrusion on the cyber infrastructure of a state for the purpose of intelligence gathering. *Thus, we consider the unauthorised interception of telecommunications a violation of state sovereignty, whether or not they crossed the threshold of an intervention in the internal affairs of another State*. In other words, the element of coercion does not need to be present." Open-Ended Working Group, "May 2023 Intersessional Meetings", 2023, p. 4 (emphasis added), available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_May_2023_intersessional_-_Brazil.pdf.

80 According to the *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace*, "[t]he African Union affirms that, by virtue of territorial sovereignty, any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful. Therefore, the African Union emphasises that the obligation to respect the territorial sovereignty of States, as it applies in cyberspace, does not include a *de minimis* threshold of harmful effects below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful." African Union Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace*, 29 January 2024, para. 16, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/CAP_Communiques_FULL_0e34eb5799.pdf.

81 According to a reply to a parliamentary question regarding submarine cables and digital sovereignty (E-001219/2022), "as regards espionage, the Commission strongly condemns any espionage, including by means of submarine cables, and any form of unlawful interception of users' communications". "Answer Given by Mr Breton on Behalf of the European Commission", 15 July 2022, available at: www.europarl.europa.eu/doceo/document/E-9-2022-001219-ASW_EN.html.

82 According to the US Department of Defense (DoD) General Counsel, "[f]or cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is *not* sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory". DoD General Counsel, "Remarks at U.S. Cyber Command Legal Conference", 2 March 2020 (emphasis added), available at: www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

as only cyber espionage conducted from inside the territory of the spied-on State is considered a violation of sovereignty.[83] Conversely, the Manual notes that "[t]he Experts were incapable of achieving consensus as to whether remote cyber espionage reaching a particular threshold of severity violates international law".[84] That said, the Manual seems to be indirectly supporting a permissive approach.[85]

It is true that some restrictions on remote espionage can be found in soft law and only in cases of economic espionage.[86] However, in practice and at the current stage, these restrictions seem not to have changed the understanding of espionage. In that respect, it is sufficient to recall the recent (October 2023) *Skvortsov* case of the Stockholm District Court.[87] According to the charge, Mr Skvortsov set up a platform for transferring technology to Russia, circumventing sanctions, in order to increase Russia's military capabilities. The District Court acquitted the defendant – although it found that the latter had largely acted in the way that the prosecutor claimed – because "[n]othing has emerged other than the activity having been solely intended for technology acquisition, and not aimed at obtaining information that could constitute espionage".[88]

Human rights might impose some limitations on remote cyber espionage. This may occur in two different ways: (a) expanding the notion of territorial

83 Tallinn Manual 2.0, above note 39, p. 19: "In this regard, the Experts were divided over the unique case of cyber espionage (Rule 32) by one State that is conducted while physically present on the territory of another State. The majority took the position that the activity violates this Rule [the rule of sovereignty]. For example, if organs of one State are present in another State's territory and conduct cyber espionage against it without its consent or other legal justification, the latter's sovereignty has been violated. Although these Experts acknowledged that there is widespread State practice of engaging in non-consensual espionage while present on another State's territory, they pointed out that States have not defended such actions on the basis of international law."

84 *Ibid.*, p. 170.

85 This conclusion is corroborated by the following extract of the Tallinn Manual 2.0: "[C]onsider a situation in which a State remotely accesses another State's military cyber systems without consent and exfiltrates gigabytes of classified data over an extended period. The majority of the Experts was of the view that exfiltration violates no international law prohibition irrespective of the attendant severity." *Ibid.*, pp. 170–171.

86 See, *ex plurimis*, The White House, Office of the Press Secretary, "Fact Sheet: President Xi Jinping's State Visit to the United States", 25 September 2015, available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, where is pointed out that "[t]he United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors". Or see *G20 Leaders' Communiqué*, Antalya Summit, 15–16 November 2015, para. 26, available at: www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf, according to which "no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors". See also Emilio Iasiello, "No-Hack Pacts – Beijing Assumes a Global Leadership Role", *Cyber Defense Review*, 12 January 2016, available at: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136172/no-hack-pacts-beijing-assumes-a-global-leadership-role/.

87 Anna Ringstrom, "Swedish Court Clears Man of Spying on US and Sweden for Russia", *Reuters*, 26 October 2023, available at: www.reuters.com/world/europe/swedish-court-clears-man-spying-us-sweden-russia-2023-10-26/.

88 *Ibid.*

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

jurisdiction in case of remote cyber espionage, and (b) tackling transnational dissident cyber espionage.[89]

On point (a), it is worth recalling that, according to the Tallinn Manual 2.0, human rights

> appl[y] to all persons on a State's territory irrespective of where the State's cyber activities that implicate the human right in question occur. For instance, a State's human rights law obligations attach when the communications of an individual who is located in its territory are intercepted abroad by that State or when the State acquires access to the individual's data that is stored electronically beyond its borders.[90]

Thus, the Tallinn Manual 2.0 seems to frame the question of cyber remote espionage taking as its centre of gravity the effect over the affected individual, rather than the location where the cyber operations are executed. Therefore, the Manual considers cyber remote espionage as a question of extraterritorial human rights jurisdiction. In that respect, the Manual takes no definitive position on the possibility of considering remote cyber espionage as a form of effective control,[91] thereby triggering human rights courts' extraterritorial jurisdiction. European Court of Human Rights (ECtHR) case law, however, seems to suggest otherwise. In the case of *Wieder and Guarnieri v. The United Kingdom*, the ECtHR held that interception, extraction, filtering, storage, analysis and dissemination of communications of the applicants – when the latter were based outside of British territory – by the UK intelligence agencies could constitute a human rights violation. More specifically, with regard to the scope of its jurisdiction, the Strasbourg Court pointed out that "the interference with the applicants' rights under Article 8 of the Convention took place within the United Kingdom and therefore fell within the *territorial jurisdiction of the respondent State*".[92] Notably, while some States, *in primis* the United States, may not necessarily follow ECtHR case law, it is true that other tribunals may concur with the Strasbourg Court.[93]

On point (b), we can mention the British cases of *Ghanem Al-Masarir v. Kingdom of Saudi Arabia*[94] and *Shehabi and Anor v. Kingdom of Bahrain*,[95]

89 On transnational dissident cyber espionage, see Siena Anstis, "Regulating Transnational Dissident Cyber Espionage", *International and Comparative Law Quarterly*, Vol. 73, No. 1, 2024.

90 Tallinn Manual 2.0, above note 39, pp. 183–184.

91 *Ibid.*, p. 185 "The International Group of Experts could achieve no consensus as to whether State measures that do not involve an exercise of physical control may qualify as 'power or effective control' in the sense of this Rule. In particular, no consensus could be reached as to whether State activities conducted through cyberspace can give rise, as a matter of law, to power or effective control over an individual located abroad, thereby triggering the extraterritorial applicability of that State's international human rights law obligations."

92 ECtHR, *Wieder and Guarnieri v. United Kingdom*, Appl. Nos 64371/16, 64407/16, 12 September 2023, para. 95 (emphasis added).

93 For example, the German Federal Constitutional Court held that Germany's intelligence agencies are bound by the German Constitution when conducting telecommunications surveillance of foreigners in other countries. *See* Bundesverfassungsgericht, Judgment of the First Senate, 1 BvR 2835/17, 19 May 2020, available at: www.bverfg.de/e/rs20200519_1bvr283517en.html.

94 UK High Court of Justice, *Ghanem Al-Masarir v. Kingdom of Saudi Arabia*, [2022] EWHC 2199 (QB), 2022.

95 UK High Court of Justice, *Shehabi & Anor v. Kingdom of Bahrain*, [2023] EWHC 89 (QB), 2023.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

where the High Court affirmed its jurisdiction over the claims of dissidents for the damages suffered as a result of cyber espionage conducted, respectively, by Saudi Arabia and Bahrain. In other words, the British court denied that Saudi Arabia and Bahrain were immune from UK jurisdiction pursuant to the State Immunity Act of 1978 with respect to cyber espionage over dissidents, when the latter were based inside British territory. However, we cannot fail to notice that US case law, in the same situation, has taken an opposite stance and affirmed that the Foreign Sovereign Immunities Act bars plaintiffs' claims for damages suffered as a result of cyber espionage.[96] The judicial decisions of the US judiciary over dissident cyber espionage, of course, are without prejudice to US promotion of voluntary and non-legally binding principles to counter the proliferation and misuse of commercial spyware.[97]

That said, US practice concerning the prosecution of espionage in the cyber domain seems to deviate from traditional practice. American case law, for quite some time, has allowed the prosecution of espionage committed extraterritorially, provided the criminal conduct was committed, at least in part, on the territory of a third country.[98] In other words, espionage entirely conduced from the territory of the spying State was not prosecuted. In cases of espionage in the cyber domain, however, the US has issued indictments charging Russian intelligence officers, operating from Russian territory, for attempting, supporting and/or conducting computer intrusions targeting critical infrastructures,[99] as well as executing computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against or otherwise destabilize the United States as well as foreign countries other than the United States.[100]

96 US Court of Appeals, 9th Circuit, *Broidy Capital Management v. The State of Qatar*, No. 18-56256, 2020, p. 16, available at: https://tinyurl.com/yrpttpxw. In this case, the Court stated: "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."

97 The White House, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware", 18 March 2024, available at: www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/.

98 US District Court for the District of Massachusetts, *United States v. Zehe*, 601 F. Supp. 196 (D. Mass. 1985), 29 January 1985, available at: https://law.justia.com/cases/federal/district-courts/FSupp/601/196/1734505/.

99 US Department of Justice, "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide", press release, 24 March 2022, available at: www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

100 US Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace", press release, 19 October 2020, available at: www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

Peacetime cyber espionage: Interim conclusion

All in all, although at this stage it would appear premature to come to a definitive conclusion on the legality, *vel non*, of remote cyber espionage, it is safe to say that it should be limited to information-gathering. This means that cyber operations causing a loss of functionality (except for *de minimis* consequences) should be removed from the espionage definition. In addition, it is not insignificant to notice that some States, although reluctant to acknowledge openly the legality of espionage, seem open to accepting the possibility of cyber reconnaissance (i.e., the use of cyber capabilities to obtain information about activities, information resources or system capabilities) for security[101] or law enforcement reasons.[102] In the end, uncertainty surrounding espionage may – at most – allow us to consider as lawful (*rectius* not unlawful) cyber reconnaissance measures regardless of the consent of the territorial State concerned, but not cyber operations causing loss of functionality (except for *de minimis*

101 According to Germany, "[d]ue to the multifold and close interlinkage of cyber infrastructures 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 particularly thorough 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." Federal Government of Germany, *On the Application of International Law in Cyberspace*, Position Paper, March 2021, p. 14. As correctly observed by Michael Schmitt, "[b]y suggesting this precautionary step, Germany necessarily acknowledges that espionage as such is not a violation of international law". See Michael N. Schmitt, "Germany's Positions on International Law in Cyberspace Part I", *Just Security*, 9 March 2021, available at: www.justsecurity.org/75242/germanys-positions-on-international-law-in-cyberspace/.

102 In that respect, the Government of the Kingdom of the Netherlands has observed the following: "From the perspective of law enforcement (which is part of a state's internal sovereignty), the manner in which the principle of sovereignty should be applied has not fully crystallised at international level either. Shared investigative practices do seem to be developing in Europe and around the world, however. Data relevant to criminal investigations is increasingly stored beyond national borders, for example in the cloud, in mainly private data centres. And when it comes to criminal offences committed on, or by means of, the internet, the location of data – including malicious software or code – and physical infrastructure is often largely irrelevant. It is easy to hide one's identity and location on the internet, moreover, and more and more communications are now encrypted. Even in purely domestic criminal cases – including cybercrime – where the suspect and victim are both in the Netherlands, cyber investigations often encounter data stored beyond our borders, particularly when investigators require access to data held by online service providers or hosting services, or need to search networks or (covertly) gain remote entry to an automated system. The act of exercising investigative powers in a cross-border context is traditionally deemed a violation of a country's sovereignty unless the country in question has explicitly granted permission (by means of a treaty or other instrument). *Opinion is divided as to what qualifies as exercising investigative powers in a cross-border context and when it is permissible without a legal basis founded in a treaty. In cyberspace too, countries' practices differ in their practical approaches to the principle of sovereignty in relation to criminal investigations.* The Netherlands actively participates in international consultations on the scope for making investigations more effective, paying specific attention to ensuring the right safeguards are in place." Government of the Kingdom of the Netherlands, "Appendix: International Law in Cyberspace", 26 September 2019, pp. 2–3 (emphasis added), available at: www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

consequences). Notably, this proposed approach also seems consistent with the limited national case law available.[103]

Why is espionage so "attractive"?

At the end of this part of the article, it is opportune to try to comprehend why States seem particularly inclined to style/label cyber operations as intelligence operations, thereby relying on civilian intelligence agencies for their execution, including beyond mere intelligence-gathering. This question is not a mere pretext, since, generally speaking, civilian intelligence agencies' primary missions/tasks are intelligence-gathering, counter-espionage and analysis. Therefore, in cyberspace (*recte* in cyberspace only), States practice seems to support a broader remit for civilian intelligence agencies.

To understand States' preference in favour of civilian intelligence agencies, it is necessary to recall the concepts of covert action and clandestine operations. These two concepts can be summarized as follows: "clandestine operations are designed to be secret in the sense that the operators take action to avoid detection. In contrast, covert actions are unacknowledged in the sense that the deploying government refuses to admit that the actors are working on behalf of the State."[104] While clandestine operations are generally understood as usual and traditional response options available to military forces, covert actions are instead part of the legal framework applicable to civilian intelligence agencies only. The

103 In the *Tidal Music* case, the Supreme Court of Norway addressed the legality of a seizure of data stored on a cloud server located outside Norwegian territory vis-à-vis the sovereignty of the State where the server was located. The Court, which affirmed the legality of the seizure, noted that "[t]he legal issues brought to life by technological development and the use of coercion to obtain data stored in 'the cloud' have not been clarified, neither under Norwegian nor under international law". The Norwegian judge further argued that "it is clear that the data remains on the server abroad. Also, no changes are made to the stored information, for instance in the form of deletion [or] encryption. A possible seizure is carried out by copying the data onto storage media in Norway. At any rate, in a situation … like the one at hand, I cannot see that the search will affect another state to an extent that it constitutes a violation of the principle of sovereignty." Supreme Court of Norway, *Tidal Music AS v. The Public Prosecution Authority*, HR-2019-610-A, Case No. 19-010640STR-HRET, 28 March 2019, paras 70–71, available at: www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2019-610-a.pdf. With reference to Italy, a legal scholar has noted that "consolidated case law tends to bypass Mutual Legal Assistance (MLA) mechanisms when the technical assistance of another country is not necessary, as in the case of information held by service providers in the cloud or in the case of interceptions of communications, in particular when the target is outside Italy but access to his or her communications is possible through technical systems located in Italy (so called 'instradamento'). It should be noted that the recent case law also applies this reasoning to communication surveillance by means of 'State trojans' (malware). The Supreme Court of cassation has ruled that MLA is not necessary for intercepting face-to-face communication that took place in Canada, if the device used for the communication surveillance was 'infected' in Italy. Thus if the virus (the malware) was implanted in Italy, the law enforcement bodies are entitled to carry out interception of communication face-to-face all over the word." Gabriella Di Paolo, "Admissibility of E-Evidence, Transnational E-Evidence and Fair Trial Rights in Italy", in Lorena Bachmeier Winter and Farsam Salimi (eds), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Oxford University Press, Oxford, 2024, pp. 85–86. See also Italian Court of Cassation, Case No. 2936222, Judgment, July 2022.

104 Jens David Ohlin, "The Combatant's Privilege in Asymmetric and Covert Conflicts", *Yale Journal of International Law*, Vol. 40, 2015, p. 371, available at: https://ssrn.com/abstract=2473713.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

latter consideration, of course, is without prejudice to the possibility of also employing military assets for covert actions – should that be the case, however, military forces will not follow the usual war powers procedure, but rather the applicable law on intelligence. While the details differ from each national legal system to the next, from a practical point of view, relying on the law on intelligence, rather than war powers, allows governments broader freedom of action. Generally speaking, domestic law on intelligence has a more narrow scrutiny and a different timing for parliamentary oversight compared to war powers. In the case of military operations in accordance with war powers, these generally require *ex ante* (or nearly *ex ante*) approval by the parliamentary plenary assembly. In the case of covert actions authorized on the basis of domestic law on intelligence, however, the Executive is merely requested to notify – *ex post* and in a confidential manner – a selected committee of the parliament about the actions. A few examples in this regard seem opportune here.

As a derogation from the War Powers Resolution of 1973 – which aims to check the Executive Branch's power when committing US military forces to an armed conflict – a special provision for cyber operations has been adopted in the United States. US Code §394 (inserted within Title 10) establishes that

> [t]he Secretary of Defense shall develop, prepare, and coordinate; make ready all armed forces for purposes of; and, when appropriately authorised to do so, conduct, military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to a malicious cyber activity carried out against the United States or a United States person by a foreign power.

With regard to congressional oversight, US Code §394 establishes that "[t]he Secretary shall brief the congressional defense committees about any military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, occurring during the previous quarter".[105] In summary, as pointed out by some scholars, the US Congress "has given the green light for military cyberspace operations to 'go dark'",[106] enacting for the US Armed Forces a dedicated legislation for cyber operations, mirroring the already existing domestic legal framework applicable to the Central Intelligence Agency (CIA) (i.e., Title 50 of the US Code and specifically §3093 on covert actions).

In France, Article 2321-2 of the Code de la Défense, in order to respond to a cyber attack targeting information systems affecting the war or the economic potential, security or survival capacity of the nation, allows the agencies designated by the prime minister (i.e., intelligence agencies and the French Armed Forces as well)[107] to perform the technical operations necessary to classify

105 On US Code §394, see also Laura B. West, "The Rise of the 'Fifth Fight' in Cyberspace: A New Legal Framework and Implications for Great Power Competition", *Military Law Review*, Vol. 229, No. 3, 2021.
106 *Ibid.*, p. 316.
107 In accordance with the *Arrêté du 17 juillet 2015 déterminant les services de l'Etat mentionnés au second alinéa de l'article L. 2321-2 du code de la défense*, the designated agencies are (1) the National

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

the attack and to neutralize its effects by accessing the information system from which the attack originated. Measures adopted pursuant to Article 2321-2, however, fall outside the parliamentary prerogatives set out in Article 35 of the French Constitution.[108]

A similar law has been adopted in Italy as well: Decree-Law No. 115 of 9 August 2022 grants the Italian prime minister the authority to authorize the adoption of counter-intelligence measures in cyberspace (i.e., offensive cyber operations/"hack-back").[109] According to the Decree-Law, an implementing regulation issued by the prime minister, having sought the opinion of the Joint Parliamentary Committee for the Security of the Republic, defines the content of the counter-intelligence measures in cyberspace. Notably, such an implementing regulation is not required to be published, so it is not publicly available. From a procedural point of view, however, the text of the Decree-Law clarifies that counter-intelligence measures in cyberspace shall be executed by the intelligence agencies, eventually in cooperation with the Italian Armed Forces. The execution of counter-intelligence measures in cyberspace is decided by the prime minister on his own and is communicated to the Joint Parliamentary Committee for the Security of the Republic within thirty days of the date of conclusion of the operations. This means that counter-intelligence measures in cyberspace do not require *ex ante* parliamentary approval pursuant to Law No. 145 of 21 July 2016, as in the case of military deployment abroad.[110]

Finally, even British practice seems to confirm the impression that cyber operations are perceived as intelligence operations and, as such, the relevant domestic legal framework on intelligence is applied. In the UK, the National Cyber Force (NCF) has been established as a "partnership between defence and intelligence".[111] From a legal point of view, "[o]perations conducted by NCF are subject to rigorous governance and are consistent with all UK and international law, *including international humanitarian law when applicable*".[112] From a domestic point of view, NCF operations are conducted in line with the

Information Systems Security Agency (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI), (2) the French Cyber Command (Commandement de la Cyberdéfense, COMCYBER) and the Directorate General of Armaments (Direction Générale de L'armement, DGA), and (3) the Directorate-General for External Security (Direction Générale de la Sécurité Extérieure, DGSE) and the General Directorate for Internal Security (Direction Générale du Sécurité Intérieur, DGSI).

108 French Constitution, Art. 35: "A declaration of war shall be authorized by Parliament. The Government shall inform Parliament of its decision to have the armed forces intervene abroad, at the latest three days after the beginning of said intervention. It shall detail the objectives of the said intervention. This information may give rise to a debate, which shall not be followed by a vote. Where the said intervention shall exceed four months, the Government shall submit the extension to Parliament for authorization. It may ask the National Assembly to make the final decision. If Parliament is not sitting at the end of the four-month period, it shall express its decision at the opening of the following session."

109 Andrea Monti, "How the Italian Government's New Offensive Power in the Cyber Sector Works", 14 August 2022, available at: https://blog.andreamonti.eu/?p=2234.

110 On Law No. 145, see Andrea Crescenzi, "Legislation — Italian Participation in International Missions", *Yearbook of International Humanitarian Law*, Vol. 19, 2016, available at: www.asser.nl/media/3912/italy-yihl-19-2016v2.pdf.

111 Government of the United Kingdom, above note 8.

112 *Ibid.* (emphasis added).

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

intelligence legal framework, i.e. the Intelligence Services Act of 1994, the Regulation of Investigatory Powers Act of 2000 and the Investigatory Powers Act of 2016.[113]

Can a State employ civilians to take direct part in hostilities?

The previous section concluded that the notion of espionage might have limited application for justifying cyber operations, beyond information-gathering. The aim of this section is to corroborate the position that civilian intelligence agencies cannot be employed by States for combat cyber operations. This point, however, demands a premise aimed at defining the notion of combat operations. As stated above, intelligence-gathering, in the case of information useful for the conduct and/or execution of a tactical military operation, should be considered as DPH. As the discussed legal provision on wartime espionage does not preclude civilians from carrying out such activity, those civilians possibly involved in it can be attacked for such time as they are directly engaged in such activity. On the other hand, DPH is broader than intelligence-gathering for tactical purposes. Therefore, for the purposes of this article, the notion of combat operations, including in the cyber domain, should be construed as close to the concept of hostilities, meaning "acts of violence by a belligerent against an enemy in order to put an end to his resistance and impose obedience".[114] Those acts of violence, in the context of the cyber domain, should not, in the opinion of the present author, be limited to those implying physical consequences but should also comprise acts that may rest in the cyber domain causing loss of functionality. This position, although not fully settled as seen above, seems consistent with the need to consider espionage as limited to information-gathering only.

113 It is interesting to note that UK war powers procedure is not formally defined by any piece of legislation. Nevertheless, "[i]n 2011, the Government acknowledged that a convention had developed in Parliament that before troops were committed the House of Commons should have an opportunity to debate the matter and said that it proposed to observe that convention except when there was an emergency and such action would not be appropriate" (Cabinet Office, *The Cabinet Manual: A Guide to Laws, Conventions and Rules on the Operation of Government*, HM Stationery Office, London, 2011, para. 5.38, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60641/cabinet-manual.pdf). However, as the exact scope of that constitutional convention seem to be disputed, the British government, on 13 April 2018, authorized a few air strikes against Syria's chemical weapons capability without any prior approval of the House of Commons (and without any authorization from the UN Security Council). Those air strikes were based on the government's position recalling international law theory on the use of force for humanitarian intervention (see Government of the United Kingdom, *Syria Action – UK Government Legal Position*, Policy Paper, 14 April 2018, available at: www.gov.uk/government/publications/syria-action-uk-government-legal-position/syria-action-uk-government-legal-position). That being said for the sake of completeness, the author of the present paper is of the opinion that reference to the Intelligence Services Act 1994, the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 is sufficient to conclude that the United Kingdom – from a domestic point of view – regulates cyber operations executed by the NCF as intelligence operations rather than as pure military operations.

114 Pietro Verri, "Dictionary of the International Law of Armed Conflict", ICRC, Geneva, 1992, p. 57, available at: www.icrc.org/en/doc/assets/files/publications/icrc-002-0453.pdf.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

Extensive literature has addressed the question of civilians' direct participation in hostilities. According to Baxter,[115]

> [c]landestine activities in warfare are not confined to the work of the spy, the armed guerrilla, and the *franc-tireur*. Sabotage, intelligence activities other than espionage, propaganda, and psychological warfare may also be carried [out] by civilians or disguised military personnel, and their importance, by comparison with hostilities in arms, has become so great that partisan warfare has been given the name of "sabotage with violence".[116]

For the purposes of the present article, however, the question to be discussed is slightly different. We are not discussing whether civilians can take part in hostilities, a question that is perhaps less clear than it may appear at first glance.[117] Instead, we are going to analyze whether a State can directly employ civilians taking part in hostilities. Therefore, the present article is not aimed at criticizing Baxter's view. It seems safe to say that Baxter considered it lawful for civilians to perform not only espionage but also other clandestine activities other than espionage, such as sabotage. This reasonable conclusion, however, should not necessarily be read as implying that Baxter was also supporting the possibility

115 Richard R. Baxter, "So-Called Unprivileged Belligerency: Spies, Guerrillas, and Saboteurs", *British Yearbook of International Law*, Vol. 28, 1951.

116 *Ibid.*

117 According to the ICRC Interpretive Guidance, above note 36, pp. 83–84, "civilian direct participation in hostilities is neither prohibited by IHL nor criminalized under the statutes of any prior or current international criminal tribunal or court". Surprisingly, however, the District Court of The Hague, sitting in the *MH17* criminal case concerning the shooting down of Flight MH17 by a pro-Russian armed group, took a different view. In order to motivate the rejection of combatant immunity claimed by the defendants, the Court concluded that "only members of the armed forces of one of the combatant parties in an international armed conflict may invoke immunity, under certain circumstances. The question is therefore whether the DPR [Donetsk People's Republic] and its members may be regarded as elements of the Russian armed forces. That would require the Russian Federation to accept the DPR as pertaining to it and taking responsibility for the conduct and actions of combatants under the command of the DPR. The court notes that this is not the case. To this day, the Russian Federation denies any control over or involvement with the DPR during that period. The accused have also publicly denied being part of the armed forces of the Russian Federation at that time. DPR combatants and therefore also the accused cannot be regarded as part of the armed forces of the Russian Federation. For that reason alone, they have no right to take part in the hostilities and likewise have no right to immunity from prosecution in connection with the crash of flight MH17." District Court of The Hague, *MH17 Case*, Judgment, 17 November 2022, available at: www.courtmh17.com/en/insights/news/2022/transcript-of-the-mh17-judgment-hearing/. Notably, the conclusion of the District Court of The Hague, while questionable, seems highly relevant if assessed in the overall context of the case. Firstly, in the *MH17* case the application of AP I, and so its broader definition of armed forces, was not an issue as all States concerned (Russia, Ukraine and the Netherlands) are signatories to AP I. Secondly, and most importantly, the defendants were indicted for ordinary crimes under Dutch law, rather than war crimes. Therefore, the denial of the combatant immunity claimed by the defendants was a key step for obtaining their conviction. That being said, one may legitimately question why the defendants had not been charged with war crimes, since the facts of the case may have allowed the Prosecution to do so. In that regard, as convincingly noted by some scholars, "substantively, charging the four accused in MH17 with war crimes would have put the Prosecutor in a much less favourable, potentially even losing, position than it is presently in". Lachezar Yanev, "Jurisdiction and Combatant's Privilege in the MH17 Trial: Treading the Line between Domestic and International Criminal Justice", *Netherlands International Law Review*, Vol. 68, 2021, p. 185.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

of States directly employing civilians to perform intelligence activities other than espionage, such as combat functions.

The CIA's "drone war" on terrorism

The Barron Memorandum

The first relevant document to discuss is the so-called Barron Memorandum on the applicability of federal criminal laws and the Constitution, which contemplated lethal operations against Shaykh Anwar al-Aulaqi,[118] issued by the Office of Legal Counsel of the US Department of Justice. The Barron Memorandum is particularly relevant since the previous Congress oversight[119] with respect to the CIA's "drone war" on terrorism had cast some doubts on its legality.[120] The Memorandum analyzed the legality of the use of drones. This assessment was not limited to international law, as it also – and mainly – addressed the question from a domestic legal point of view (i.e., federal criminal laws and the Constitution). In short, the Memorandum considered the use of drones lawful, in accordance with the "public authority justification, which can render lethal action carried out by a governmental official lawful in some circumstances".[121] Additionally, the Memorandum clarified that the public authority justification "would be available because the operation would constitute the 'lawful conduct of war'".[122]

Notably, the Barron Memorandum distinguished the position of the Department of Defense from the position of the CIA, although in both cases it reached the same conclusion. Unfortunately, the part of the Memorandum

118 David J. Barron, *Memorandum for the Attorney General Re: Applicability of Federal Criminal Laws and the Constitution to Contemplated Lethal Operations against Shaykh Anwar al-Aulaqi*, 16 July 2010 (Barron Memorandum), available at: www.justice.gov/sites/default/files/olc/pages/attachments/2015/04/02/2010-07-16_-_olc_aaga_barron_-_al-aulaqi.pdf. There is also a previous memo on the same topic, but it is still classified in so many of its parts that it cannot be usefully considered. See David J. Barron, *Memorandum for the Attorney General Re: Lethal Operation against Shaykh Anwar Aulaqi*, 19 February 2010, available at: www.justice.gov/sites/default/files/olc/pages/attachments/2015/04/02/2010-02-19_-_olc_aaga_barron_-_al-aulaqi.pdf.

119 House Committee on Oversight and Government Reform, Subcommittee on National Security and Foreign Affairs, *The Rise of the Drones II: Examining the Legality of Unmanned Targeting*, 28 April 2010, available at: www.congress.gov/111/chrg/CHRG-111hhrg64922/CHRG-111hhrg64922.pdf.

120 In that respect, and limiting our analysis only to those doubts pertaining to IHL and the content of this article, a few points deserve to be particularly emphasized. According to the statement of Professor Mary Ellen O'Connell (University of Notre Dame Law School), "only a combatant, lawful combatant, may carry out the use of killing with combat drones. The CIA and civilian contractors have no right to do so. They do not wear uniforms, and they are not in the chain of command" (*ibid.*, p. 19). Not all the other experts heard by Congress, however, accepted such a stance. In particular, Professor Kenneth Anderson (Washington College of Law, American University) stated: "One [issue] is, what is the ability, if any, of the CIA lawfully to participate in something that is an armed conflict when they are civilians[?] It is more complicated, I think, than Professor O'Connell suggests, in the sense that their participation may or may not involve the combatant's privilege, but does not make it per se unlawful under international law necessarily" (*ibid.*, p. 49).

121 Barron Memorandum, above note 118, p. 2.

122 *Ibid.*, p. 20.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

concerning the CIA has not been fully disclosed, so it is difficult to understand and comment on the reasoning of the Memorandum in that respect. In any event, the disclosed footnote 44 may still be relevant for the present article. In particular, this footnote points out two arguments:[123] firstly, the mere fact that CIA personnel were involved in a drone strike is not *per se* a violation of the law of war, although CIA personnel could not enjoy immunity from prosecution under the domestic law of the countries where the strike occurred;[124] and secondly, any reference to the Supreme Court's decision in *Ex parte Quirin*, 317 U.S. 1 (1942) – "suggesting that passing through enemy lines in order to commit 'any hostile act' while not in uniform 'renders the offender liable to trial for violation of the laws of war'" – is not conclusive, as it was not clear whether the Court intended to refer only to conduct that would constitute perfidy or treachery. In any event, even though the Supreme Court's decision in *Ex parte Quirin* should be interpreted in the sense that any hostile acts performed by unprivileged belligerents are *per se* violations of the laws of war, such a conclusion lacks clear support and State practice.[125]

The *Targeted Killing in Pakistan* case

Discussions over the legal implications stemming from the CIA's "drone war" on terrorism were not confined to the United States, as the German Federal Public Prosecutor was forced to open a criminal case in response to press reports about a drone operation in which German citizens had allegedly been killed. After the investigation, the Prosecutor dismissed the case on the basis of a reasoned decision[126] which was not further validated/approved by an independent judge

123 In support of its conclusion, the Barron Memorandum also explains that "[i]f the killing by a member of the armed forces would comply with the law of war and otherwise be lawful, actions of CIA officials facilitating that killing should also not be unlawful". *Ibid.*, p. 33. In that respect, while such an explanation can be definitely relevant from a domestic criminal law perspective, it seems inconclusive from the viewpoint of international law.

124 "Nor would the fact that CIA personnel would be involved in the operation itself cause the operation to violate the laws of war. It is true that CIA personnel, by virtue of their not being part of the armed forces, would not enjoy the immunity from prosecution under the domestic law of the countries in which they act for their conduct in targeting and killing enemy forces in compliance with the laws of war – an immunity that the armed forces enjoy by virtue of their status. … Nevertheless, lethal activities conducted in accord with the laws of war, and undertaken in the course of lawfully authorized hostilities, do not violate the laws of war by virtue of the fact that they are carried out in part by government actors who are not entitled to the combatant's privilege. The contrary view 'arises … from a fundamental confusion between acts punishable under international law and acts with respect to which international law affords no protection.'" *Ibid.*, p. 33.

125 The relevant part of the Barron Memorandum reads as follows: "Statements in the Supreme Court's decision in *Ex parte Quirin*, 317 U.S. 1 (1942), are sometimes cited for the contrary view. … Because the Court in *Quirin* focused on conduct taken behind enemy lines, it is not clear whether the Court in these passages intended to refer only to conduct that would constitute perfidy or treachery. To the extent the Court meant to suggest more broadly that any hostile acts performed by unprivileged belligerents are for that reason violations of the laws of war, the authorities the Court cited (the Lieber Code and Colonel Winthrop's military law treatise) do not provide clear support." *Ibid.*, p. 33.

126 Bundesgerichtshof, *Aerial Drone Deployment on 4 October 2010 in Mir Ali/Pakistan (Targeted Killing in Pakistan Case)*, Case No. 3 BJs 7/12-4, Directions Issued by the Public Prosecutor General, 20 June 2013, p. 157.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

(such validation/approval is not required by German procedural law). For the purposes of this article, however, it is sufficient to mention just one of the conclusions of the Prosecutor's decision, which is that the latter argued that CIA operatives who were exercising operational responsibility for the aerial drone deployments should have qualified as armed forces for the purposes of the law of non-international armed conflict.[127]

States' reliance on civilians for combat operations

With respect to the possibility of relying on civilians to wage war, it should be noted that the only piece of legislation expressly precluding States from employing civilians in that respect is the Paris Declaration Respecting Maritime Law of 16 April 1856,[128] which prohibits privateering. The Paris Declaration, however, has been not ratified by many States (including the United States), and its capacity to reflect a customary international prohibition on privateering has been questioned by some scholars.[129]

To shed some light on the doubtful question of States' reliance on civilians for combat operations, it seems opportune to spend a few words on the definition of combatants and prisoners of war (PoWs). As pointed out by the Commentary on AP I, with regard to combatant and PoW status in guerrilla warfare,

> the law of The Hague coped rather well during 1939–1945, so as to survive virtually intact, even at the end of the Diplomatic Conference of 1949. Hundreds of thousands, if not millions of resistance fighters opposed the

127 According to the Prosecutor's decision, "CIA operatives participating in the counterinsurgency campaign in Pakistan must be regarded as forming part of the 'armed forces' of the United States within the meaning of Article 43 paragraph 1 of Additional Protocol I to the Geneva Conventions. Only this functional definition of the term 'armed forces' is aligned with the basic reasoning behind the principle of distinction between civilians and combatants. For civilian co-workers who have been assigned a 'continuous combat function' by a party to the conflict thereby become integrated de facto into that party's armed forces, and can no longer be considered 'civilians' for purposes of the principle of distinction between civilians and combatants. Also from a historical perspective, third parties taking direct part in hostilities under the authority, and at the behest, of a state actor have invariably been regarded as members of armed forces, and not civilians, from the standpoint of international humanitarian law. Even if one were to assume that the intelligence operatives commanding and executing the aerial drone deployments are in fact 'civilians' and not members of 'armed forces' within the meaning of Article 43 paragraph 1 of Additional Protocol I to the Geneva Conventions, this would not automatically mean that the combat operations of such persons were impermissible under international law. There is no general prohibition under international humanitarian law against the participation of civilians in hostilities. On the other hand, the consequences of such participation would be the (temporary) forfeiture of one's protected status as a civilian, as well as the inability to claim the immunity from domestic criminal prosecution that is generally accorded to members of national armed forces. A civilian's participation in hostilities will not constitute a breach of international humanitarian law, however, so long as he complies with the rules of war to which he is bound; this latter condition is met in the case at hand, given that the principle of distinction between combatants and civilians was being observed." *Ibid.*, pp. 757–760.

128 Paris Declaration Respecting Maritime Law, 16 April 1856, available at: https://ihl-databases.icrc.org/en/ihl-treaties/paris-decl-1856/declaration.

129 Brandon Schwartz, "U.S. Privateering Is Legal", *US Naval Institute Proceedings*, Vol. 146, April 2020, available at: www.usni.org/magazines/proceedings/2020/april/us-privateering-legal.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

> occupying armies in Europe and elsewhere, often with nothing more than makeshift equipment at their disposal, but the Hague Regulations were not, on the whole, seriously shaken thereby.[130]

During the negotiations on Article 43 of AP I, there was an attempt to enlarge the criteria for recognizing as lawful combatants even subjects/people who are not part of the regular armed forces.[131] This was done in order to deal with wars of national liberation and conflicts for self-determination, in which guerrilla fighters could not distinguish themselves from the civilian population during their military operations and still retain any chance of success. In that respect, the text finally

> restated the obligation of the guerrilla fighter to distinguish himself clearly from the civilian population, but limited that requirement to that part of the time in which he was conducting his military operations and accepted as an adequate minimum sign of distinction the carrying of arms openly.[132]

So, it should not be contentious that AP I was only aimed at regulating guerrilla fighters in cases of internal (non-international) armed conflict. The drafters of Article 43 of AP I had envisioned fighters autonomously organized in the context of wars of national liberation or occupation of their national territory by a foreign aggressor. Following a historical and teleological interpretation, nothing suggests that AP I was aimed at giving States the right to employ civilians for combat operations. In addition, the logical and coherent interpretation of IHL implies that States should not directly employ civilians for combat functions, including, of course, in the cyber domain. To that end, recalling the Commentary on AP I is helpful. The Commentary, speaking about guerrillas, clearly points out, firstly, that

> any concept of a part-time status, a semi-civilian, semi-military status, a soldier by night and peaceful citizen by day, also disappears. A civilian who is incorporated in an armed organization … becomes a member of the military and a combatant throughout the duration of the hostilities (or in any case, until he is permanently demobilized by the responsible command …), whether or not he is in combat, or for the time being armed.[133]

Secondly, the Commentary states that

> [a]ny interpretation which would allow combatants as meant in Article 43 to "demobilize" at will in order to return to their status as civilians and to take up their status as combatants once again, as the situation changes or as

130 ICRC Commentary on the APs, above note 54, para. 1370.

131 It is worth recalling that, according to the Hague Regulations of 1907, militia and volunteer corps which do not form part of the regular armed forces, could be considered as lawful combatants, provided that the following cumulative conditions are fulfilled: (1) they shall be commanded by a person responsible for his subordinates; (2) they shall have a fixed sign recognizable at a distance; (3) they shall carry arms openly; and (4) they shall conduct their operations in accordance with the laws and customs of war.

132 *Official Records of the Diplomatic Conference*, Vol. 15, Geneva, 1974–77, p. 453, para. 18, available at: https://tile.loc.gov/storage-services/service/ll/llmlp/RC-records_Vol-15/RC-records_Vol-15.pdf.

133 ICRC Commentary on the APs, above note 54, para. 1677.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

> military operations may require, would have the effect of cancelling any progress that this article has achieved.[134]

Thus, there is no plausible reason to allow States to directly employ civilians for combat cyber functions, since their employment, in practice, would have precisely the effect of allowing a situation that IHL seeks to prevent. It is true that the Additional Protocols – and their Commentary as well – do not explicitly preclude States from directly employing civilians for combat functions. To support the proposed view, it is pertinent to discuss Article 43(3) of AP I in conjunction with Article 43(7). On one hand, Article 43(3) recognizes that "there are situations in armed conflicts where, owing to the nature of the hostilities an armed combatant cannot so distinguish himself". As can be inferred from the *travaux preparatoires* and the provision's drafting history, "[t]hat exception recognized that situations could occur in occupied territory and in wars of national liberation in which a guerrilla fighter could not distinguish himself [from the civilian population] throughout his military operations and still retain any chance of success"[135]. Coherently with the exceptional nature of the Article 43(3), the subsequent paragraph 7 of the same article further clarifies that "[t]his Article is not intended to change the generally accepted practice of States with respect to the wearing of the uniform by combatants assigned to the regular, uniformed armed units of a Party to the conflict". Thus, precluding States from directly employing civilians for combat cyber functions is simply the only reasonable interpretation that does not deprive the mentioned paragraph 7 of all practical effect. This is of course without prejudice to the possibility of also applying Article 43(3) to "regular" armed forces, "though only under the same exceptional circumstances as for members of so-called guerrilla forces",[136] such as "advisers assigned to certain resistance units".[137] Article 43(3), which allows the incorporation of paramilitary or law enforcement agencies into the regular armed forces provided that a notification requirement to the other parties is fulfilled, also supports the view that States should not be allowed to directly employ civilians for combat cyber functions. While it may be true that "the notification does not seem to be a constitutive element of the status of the units concerned",[138] this cannot be interpreted as forfeiting the notification requirement as such. From a systematic point of view, should a government be free to employ civilian intelligence agencies for combat cyber operations, the said notification requirement for the incorporation of paramilitary or armed law enforcement agencies into the regular armed forces would not have any raison d'être. In other words – vis-à-vis States' relationships – failing to fulfil the notification requirements should be considered as a breach of IHL. Conversely, in case of application of the same provision by a

134 *Ibid.*, para. 1678.
135 *Official Records*, above note 132, p. 453, para. 19.
136 ICRC Commentary on the APs, above note 54, para. 1703.
137 *Official Records*, above note 132, p. 401, para. 84.
138 Frauke Lachenmann and Rudiger Wolfrum, *The Law of Armed Conflict and the Use of Force: The Max Planck Encyclopedia of Public International Law*, Oxford University Press, Oxford, 2017, p. 72.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

State vis-à-vis an individual, the lack of notification should not deprive an individual of the protection afforded by IHL.

Of course, not allowing States to directly employ civilians for combat functions does not mean that States – including governments in exile or States partially occupied by an aggressor State – should also be precluded from providing weapons or political, financial and logistic support to guerrilla and resistance movements, including in the cyber domain, as in the case of the Ukrainian IT Army. From a law of State responsibility perspective, as long as support to a non-State actor is below the (high) threshold of effective control,[139] the supporting State cannot be held responsible for the actions of a non-State actor.[140] We are aware that the settled ICJ case law on the law of State responsibility – particularly the effective control test – might appear contradictory with IHL, particularly with Article 91 of AP I (according to which a belligerent party shall be responsible for all acts committed by persons forming part of its armed forces) in conjunction with Article 43(1) of AP I (according to which guerrilla and resistance movements shall fall within the notion of armed forces belonging to a belligerent party). Indeed, this is precisely the situation here. Nevertheless, as rightly argued by Milanovic, Article 91 is not necessarily to be interpreted as meaning that the conduct of guerrilla and resistance movements should be attributable to the State, as "it could just as easily mean that the State is responsible for failing to properly supervise the group and ensure respect for IHL, that is, for failing to discharge a positive obligation of due diligence".[141]

Precluding States from employing civilian intelligence agencies (and even more so, of course, private contractors) for combat cyber operations is also consistent with Article 58 of AP I on precautions against the effects of attacks.[142] With this provision, as explained by the Commentary,

139 In order to reach the threshold of effective control, there should exist a relationship of "complete dependence" on the supporting State, and the State's instructions to guerrilla and resistance movements should be given "in respect of each operation" and "not generally in respect of the overall actions". ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, 2007 ICJ 108, 26 February 2007, para. 400.

140 Marko Milanović, "Special Rules of Attribution of Conduct in International Law", *International Law Studies*, Vol. 96, 2020, p. 295, available at: https://ssrn.com/abstract=3623309. According to Milanović, "to the extent that irregular armed forces are neither de jure nor de facto organs of a State, because they either do not possess such status under the State's domestic law or are not factually completely dependent on and controlled by the State, their conduct cannot be attributed to the State, unless some other attribution rule in the ILC's ASR [Articles on State Responsibility] could apply" (p. 329).

141 *Ibid.*, p. 328.

142 In accordance with the Article 58 of AP I, "[t]he Parties to the conflict shall, to the maximum extent feasible: (a) without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives; (b) avoid locating military objectives within or near densely populated areas; (c) take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations". According to the ICRC Customary Law Study, "State practice establishes this rule as a norm of customary international law applicable in both international and non-international armed conflicts" Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rule 22, available at: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule22.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

> States have subscribed here to a triple duty to act, which must imperatively be translated into instructions to be given, and first of all into measures to be taken already in peacetime, even though, strictly speaking, the article is only addressed to Parties to a conflict. Some of these measures have a preventive or precautionary character since they are concerned with preventing the construction of certain buildings in particular places, or removing objectives from an area where such buildings are located, or otherwise separating the population and their homes from dangerous places.[143]

Therefore, the practical location of military cyber forces and civilian intelligence agencies within the same premises – which is a concrete precondition usually needed to employ civilians for combat cyber operations – seems hard to reconcile with the provision on precautions against the effects of attacks.[144] In addition, practical – and permanent – location of military cyber forces and civilian intelligence agencies within the same premises would also render almost inapplicable the provision on civilian DPH limiting the "targetability" of civilians only to such time as they take direct part in hostilities.

If we look to the law of naval warfare, the conclusion that States should not rely on civilian intelligence agencies for combat cyber operation is further corroborated. Under the law of naval warfare, legitimate combatants are warships only. A warship, in accordance with Article 29 of the UN Convention on the Law of the Sea, is defined as

> *a ship belonging to the Armed Forces of a State* bearing the external marks distinguishing such ships of its nationality, under the command of an officer duly commissioned by the government of the State and whose name appears in the appropriate service list or its equivalent, and *manned by a crew which is under regular Armed Forces discipline.*[145]

The prohibition against relying on civilian vessels for combat operations is also corroborated by the strict limits, including the notification requirement, applicable to the possibility of converting merchant ships into warships in accordance with the Convention relating to the Conversion of Merchant Ships into War Ships.[146]

In the end, precluding States from directly employing civilian intelligence agencies for combat functions is an implicit obligation, on the basis of a systematic and structural interpretation of IHL. Such an implicit obligation, it

143 ICRC Commentary on the APs, above note 54, para. 2244.

144 According to the UK government's official website, "[t]he permanent site of the NCF will be established in Samlesbury, cementing the North-West region's position as the cyber centre of the UK. … The NCF draws together personnel from intelligence, cyber and security agency GCHQ, the MoD, the Secret Intelligence Service (MI6) and the Defence Science and Technology Laboratory (DSTL), under one unified command for the first time." Government of the United Kingdom, "Permanent Location of National Cyber Force Campus Announced", 4 October 2021, available at: www.gov.uk/government/news/permanent-location-of-national-cyber-force-campus-announced.

145 UN Convention on the Law of the Sea, 10 December 1982, Art. 29 (emphasis added).

146 Convention (VII) relating to the Conversion of Merchant Ships into War Ships, 18 October 1907, available at: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-vii-1907?activeTab=default.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

should be emphasized, does not infringe on States' warfighting capability. Every State remains free to employ anyone for combat functions; the State is just requested to formally enrol him or her into its armed forces or to duly notify the other parties in accordance with Article 43(3) of AP I.

Prosecution of war crimes committed by belligerents without privileges

According to the Barron Memorandum mentioned above, CIA drones strikes were lawful because, *inter alia*, the US Supreme Court's decision in *Ex parte Quirin* was not conclusive or, in any event, its conclusion lacked clear support and practice. It should be noted that the Barron Memorandum disregarded US practice, for example, under the *Manual for Military Commissions*, Part IV, §5(13), which criminalizes unprivileged belligerent acts. So, if one were to embrace the Barron view, the conclusion should be that US practice would not be consistent with international law. This seems not to be the case, as the Barron Memorandum justification, rather than the mentioned US practice, seems not to be consistent with international law.[147]

The US Supreme Court's decision in *Ex parte Quirin* should instead be considered in line with relevant State practice on the prosecution of unlawful combatants (*recte* belligerents without privileges, such as saboteurs not wearing uniform and not carrying arms openly), which appears to be legally sound from an international law perspective. In this respect, reference should be made to (1) the Federal Court of Singapore's decision in *Krofan and Andea v. Public Prosecutor*,[148] (2) the Privy Council's decision in *Bin Haji Mohamed Ali and Another v. Public Prosecutor*,[149] and (3) the Israeli Military Court sitting in

147 According to the ICRC Interpretive Guidance, above note 36, pp. 83–84, civilian DPH is not criminalized *per se* by international law (but it may be prosecuted by domestic law). In any event, the absence of any international criminal law provision criminalizing civilian DPH should be considered only in the context of war crimes prosecutions of individuals and should not be interpreted as creating rights in favour of States.

148 Federal Court of Singapore, *Krofan and Andea v. Public Prosecutor*, 5 October 1966, available at: www.asser.nl/upload/documents/DomCLIC/Docs/NLP/Singapore/Kofran_Judgment_5-10-1966.pdf. Of note is the following extract of the judgment: "[T]he position of members of the armed forces caught out of uniform while acting as saboteurs in enemy territory is not dealt with by the Hague Regulations. In the Saboteur's Case (*Ex parte Quirin & Ors.*)(1) the Supreme Court of the U.S.A. in 1942 treated disguised saboteurs as being in the same position as spies. This view is also held by the authors of the Manual of Military Law Part III an official publication in 1958 of the United Kingdom War Office at paragraph 96 page 34 where it is stated 'Members of the armed forces caught in civilian clothing while acting as saboteurs in enemy territory are in a position analogous to that of spies.' *We are of the opinion that this view does not offend against the rules of the law of nations respecting warfare and indeed states the position under customary international law.* It seems to us to be consistent with reason and the necessities of war to treat a regular combatant in disguise who acts as a saboteur as being in the same position as a regular combatant in disguise who acts as a spy" (p. 4, emphasis added).

149 Judicial Committee of the Privy Council, *Bin Haji Mohamed Ali and Another v. Public Prosecutor*, Appeal No. 20 of 1967 by Special Leave from a Judgment (5 October 1966) of the Federal Court of Malaysia, 29 July 1968, available at: www.internationalcrimesdatabase.org/Case/915/Bin-Haji-Mohamed-Ali-and-Another-v-Public-Prosecutor/. Of note is the following extract of the judgment: "[T]heir lordships are of the opinion that *under international law it is clear that the appellants, if they were members of the Indonesian armed forces, were not entitled to be treated on capture as prisoners of war under the Geneva Convention when they had landed to commit sabotage and had been dressed in civilian clothes*

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

Ramallah's decision in *Military Prosecutor v. Omar Mahmud Kassem and Others*.[150]

It is true that the judgment in the case of *Skorzeny and Others*, issued by the General Military Government Court of the US Zone of Germany,[151] may support a different conclusion, as the defendants were acquitted on all charges, including those related to engagement in a reconnaissance mission while wearing the uniform of the adversary. However, the acquittal was based on the lack of sufficient evidence, and based on questions of fact. In any event, the *Skorzeny* case still offers some interesting points to be considered on the use of enemy uniforms. Particularly, the judgment pointed out that

> [i]t is a generally recognised rule that the belligerents are allowed to employ ruses of war or stratagems during battles. … When contemplating whether the wearing of enemy uniforms is or is not a legal ruse of war, one must distinguish between the use of enemy uniforms in actual fighting and such use during operations other than actual fighting.[152]

Moreover, while the use of enemy uniforms during actual fighting is undisputedly unlawful,

> [o]n the use of enemy uniforms other than in actual fighting, the law is uncertain. Some writers hold the view that until the actual fighting starts the combatants may use enemy uniforms as a legitimate ruse of war, others think that the use of enemy uniforms is illegal even before the actual attack.[153]

That said, the further development of IHL cannot be disregarded, as State practice subsequent[154] to *Skorzeny* supports a restrictive approach on the use of enemy uniforms as a legitimate ruse of war. As the notion of attack includes not only situations where combatants are actually engaged in an attack but also operations preparatory to an attack, some leading scholars have concluded that "[u]ndoubtedly, therefore, camouflage in plain clothes or the enemy's uniform by members of special units of armed forces is a violation of the applicable norms of international law, for which legally permissible sanctions may be imposed".[155] In

both when they had placed the explosives and lit them and when they were arrested. In their opinion Chua J. and the Federal Court were right in rejecting the appellants' plea on this ground" (p. 8, emphasis added).

150 Israeli Military Court Sitting in Ramallah, *Military Prosecutor v. Omar Mahmud Kassem and Others*, 13 April 1969, available at: https://casebook.icrc.org/case-study/israel-military-prosecutor-v-kassem-and-others. Of note is the following extract of the judgement: "*International Law is not designed to protect and grant rights to saboteurs and criminals*. The defendants have no right except to stand trial in court and to be tried in accordance with the law and with the facts established by the evidence, in proceedings consonant with the requirements of ethics and International Law" (emphasis added).

151 General Military Government Court of the US Zone of Germany, *Trial of Otto Skorzeny and Others*, 18 August–9 September 1947, in *Law Reports of Trials of War Criminals*, Vol. 8, 1949, pp. 90–93, available at: https://tile.loc.gov/storage-services/service/ll/llmlp/Law-Reports_Vol-9/Law-Reports_Vol-9.pdf

152 *Ibid.*, p. 92.

153 *Ibid.*, p. 92.

154 Among others, Germany and Italy made a reservation to AP I stating that "[t]he term 'military deployment' is interpreted to mean any movements towards the place from which an attack is to be launched".

155 Dieter Fleck (ed.), *The Handbook of International Humanitarian Law*, 4th ed., Oxford University Press, Oxford, 2021, p. 122. The *Handbook* further notes that "Article 44, para. 3, 2nd sentence lit. b, AP I

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

conclusion, wearing a uniform, in the case of armed forces, or otherwise complying with the requirement of distinction, in the case of guerrilla fighters, is definitely a requirement for – lawfully – directly participating in hostilities. We should not forget, however, that Article 44(3) of AP I could change this conclusion. On the one hand, the "relaxed" level of distinction provided for in that article, as convincingly argued by some scholars, should be applied "only in 'enemy-controlled battlespace'".[156] This implies that Article 44(3) should be relevant only in the exceptional case of cyber operations executed from a location where control by the adversary "rise[s] to the level of physical control by the military or other security forces over a relatively well-defined area".[157] Secondly, and, more importantly, Article 44(3) confirms for combatants the obligation to distinguish themselves from the civilian population in the moment of the execution of the attack. Failing to do so can entail the prosecution of such unprivileged belligerent acts.

Should the foregoing conclusion be accepted, there is no reason not to apply it also to cyber warfare. The fact that cyber warfare is characterized by remote and over-the-horizon engagements may support the idea that the requirement of wearing a uniform is no longer indispensable, but the relevance of such a requirement cannot be denied as a matter of *lex lata*. Failing to do so would otherwise support the conclusion that civilian intelligence agencies may also shoot cruise missiles or employ other long-range weapons. If this were true, the principle of distinction as a whole would be irretrievably jeopardized. Indeed, as pointed out by some scholars, "the post-Westphalian construction expanding the license to kill by making persons lawful military targets who according to a traditional legal understanding would just be civilian criminals has not been accepted as law by the international community at large".[158] In addition, it goes

describes the special situation wherein arms are required to be carried openly during 'a military deployment preceding the launching of an attack' and thus clearly equates this phase with an act of military operations. As many states have formally declared upon ratification, such acts include any movement towards a place from which an attack is to be launched. This legal position clearly falls within the scope of interpretation of the applicable provision of the Protocol. Consequently a military deployment preceding an attack or an advance of commando forces as a whole is deemed to be an act of military operations within the meaning of Article 39, para. 2, AP I, and thus invariably the wearing of the enemy's uniform will be deemed to be for the prohibited purpose of shielding, favouring or protecting that military operation. If members of the armed forces involved in special units are caught wearing the uniform of the adverse party to the conflict 'while engaging in attacks', then the violation of the prohibition contained in Article 39, para. 2, AP I is evident" (pp. 121–122).

156 Kubo Mačák and Michael N. Schmitt, "'Enemy-Controlled Battlespace': The Contemporary Meaning and Purpose of Additional Protocol I's Article 44(3) Exception", *Vanderbilt Journal of Transnational Law*, Vol. 53, No. 4, 2018, p. 1374, available at: https://cdn.vanderbilt.edu/vu-wp0/wp-content/uploads/sites/78/2019/01/04190344/7.-Macak-Schmitt-READY-FOR-PRINT.pdf.

157 *Ibid.*, p. 1374. Notably, several States made interpretive declarations supporting this view. As noticed by some scholars, "[t]en States (Australia, Belgium, Canada, France, Germany, Ireland, the Netherlands, New Zealand, the Republic of Korea and the United Kingdom) consider that the provision is only applicable in cases of occupation and in conflicts of self-determination covered by Article 1(4). Spain and Italy limit the 'situations' to cases of occupation alone." Julie Gaudreau, "The Reservations to the Protocols Additional to the Geneva Conventions for the Protection of War Victims", *International Review of the Red Cross*, Vol. 85, No. 849, 2003, available at: www.icrc.org/en/doc/assets/files/other/irrc_849_gaudreau-eng.pdf.

158 Michael Bothe, "Will Current International Crises Result in Structural Shifts in International Law?", *Recueils de la Societe Internationale de Droit Penal Militaire et de Droit de la Guerre*, Vol. 20, 2015, p. 243.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

without saying that wearing a uniform is not just "dressing in some clothes" for the sole purposes of visual identification, but rather marks the individual's membership in the armed forces – or in an equivalent entity entitled to be a legitimate combatant – with all the rights and obligations stemming from such status. As argued by some scholars, the underlying rationale for wearing a uniform is "that soldiers identify themselves as belonging to a particular political entity on whose behalf they fight".[159] As a consequence, the practice of relying on civilian intelligence agencies for combat cyber operations – through the styling/labelling of such operations as espionage rather than as military operations – should be further objected to as it undermines the "conceptual and political link between the soldier and a collective force"[160] that is required by IHL. In the end, as pointed out by Sean Watts,

> [e]xisting treaty-based definitions of the combatant class thus could be interpreted to restrain individual conduct *as well as states' composition of their fighting forces*. Such a view interprets the combatant-civilian status regime as not merely a means of classifying individuals for purposes of treatment upon capture, *but also as a self-imposed limit on how states organize for combat. States that employ civilians to take direct part in hostilities would be in breach of such limits.*[161]

Of course, as seen above, given that providing tactical intelligence could be qualified as DPH, we are not ready to rule out the possibility of States relying on civilians in the cyber domain. States should, however, be precluded from employing such civilians (or otherwise relying on them) for cyber operations that go beyond intelligence-gathering, including those causing loss of functionality.

Conclusion

Competition and confrontation between the United States and its allies versus China and Russia is a fact that no one can reasonably contest, particularly in cyberspace.[162] This competition is resulting in ongoing low-intensity cyber warfare, and so it calls on us to revitalize the debate over the possibility of overcoming the dichotomy between peace and war. The need to consider also a *status mixtus* – or state of intermediacy – was already acknowledged in the course of the Cold War.[163] The

159 J. D. Ohlin, above note 104, p. 381.
160 *Ibid.*
161 Sean Watts, "Combatant Status and Computer Network Attack", *Virginia Journal of International Law*, Vol. 50, No. 2, 2010, p. 423 (emphasis added), available at: www.law.berkeley.edu/files/watts--combatant_status_and_computer_network_attack.pdf.
162 See above notes 14–19.
163 Notably, already in the 1958, it had been pointed out that "[s]ome recognition that the classical twofold categorization of the process of coercion has but minimal correspondence to contemporary realities in the interactions of states is apparent in the work of a number of modem scholars". Myres S. McDougal and Florentino P. Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War", *Yale Law Journal*, Vol. 67, No. 5, 1958, p. 776.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

relevance of such a *status mixtus* is today even more pressing than in the past. Particularly, differently from the Cold War, nowadays cyber competition is waged through means and capabilities that are indistinguishable from those that would characterize wartime. Therefore, in the present author's opinion, the IHL principle of distinction should be considered and applied, even before the eruption of a full-scale war, whenever wartime means and capabilities – including cyber ones – are employed by States.

This state of intermediacy is fostered by some opacities surrounding how international law applies to cyberspace. Apart from the vagueness of the notion of DPH, as is common in the other domains, this paper has identified five opacities that are cyber-specific: the use of force threshold, the notion of object in IHL, the definition of espionage under international law, the threshold of control for a State's attribution in case of non-State actors, and questions of evidence and proof for State attribution. To minimize the ongoing low-intensity warfare currently being waged, tackling the identified opacities would be beneficial. With a view to possible (and desirable) de-escalation, this paper has investigated some possible mitigation measures to address the identified opacities. The conclusion in that respect, as international law now stands, is that the only viable solution is a return to a narrow interpretation of the notion of espionage. A genuine notion of espionage, indeed, cannot legitimize civilian intelligence agencies' involvement in combat operations, including in the cyber domain. Despite some legal documents on the CIA's "drone war" on terrorism suggesting otherwise, the viable mitigation measure, as shown in this article, is consistent with the principle of distinction. That principle, indeed, should be interpreted as precluding States from directly employing civilians – including, but not limited to, those who are part of civilian intelligence agencies – for cyber operations that go beyond intelligence-gathering, including those causing loss of functionality.

State practice, however, shows that military and intelligence capabilities are increasingly merged out of the "desire for perceived operational and fiscal efficiency".[164] This practice has blurred the division of responsibilities between armed forces and civilian intelligence agencies. From a practical point of view, there are other ways to involve civilian experts in cyber warfare without necessarily relying on civilian intelligence agencies and undermining the principle of distinction between civilians and combatants. To that end, it is important to recall the Cyber Defence Unit of the Estonian Defence League, which is a national defence organization, voluntary and militarily organized, operating under the authority of the Ministry of Defence.[165]

At the end of the day, the discussion on civilian involvement in cyber operations goes beyond a "turf war" between civilian intelligence agencies and armed forces, because it impinges on the core values of IHL. Consequently, as a question of principle rather than a question of organizational design between

164 E. Lawson, above note 9, p. 75.

165 Estonian Defence League Act, 1 July 2024, available at: www.riigiteataja.ee/en/eli/ee/523122016002/consolide/current.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press

different branches of the Executive, the possibility of employing civilian intelligence agencies for cyber operations other than intelligence-gathering should be carefully limited. Failing to do so may not only undermine the achievements reached so far by IHL in terms of the protection of civilians, but may also weaken the overall credibility of any démarche against States that may be engaged in sponsoring malicious cyber activities performed by civilians entities, such as criminal gangs.

https://doi.org/10.1017/S1816383124000390 Published online by Cambridge University Press