International Law and Cyber Operations: Current Trends and Developments

Professor Aurel Sari

Associate Professor of Public International Law
University of Exeter, United Kingdom
A.Sari@exeter.ac.uk

24 March 2023, Strasbourg

Mr. Chair,
Members of the Committee of Legal Advisers on Public International Law,
Ladies and Gentlemen,

1. Thank you very much for inviting me today. It is a pleasure and a privilege to address the Committee and I am grateful for the opportunity to contribute to your discussions. In my remarks this morning, I would like to build on the excellent presentations delivered at the Committee's last meeting in Bucharest, in particular the remarks made by Professor Dapo Akande and Dr Cordula Droege.

2. Let me proceed in three steps. First, to set the scene, I would like to briefly revisit the applicability of international law in cyberspace. Second, I will discuss some of the cyber incidents and developments that have taken place in the context of Russia's war of aggression against Ukraine. This will allow us focus on certain specific questions of international humanitarian law (IHL) and to identify several trends that merit our attention. Third, I would like to turn to cyber operations taking place outside armed conflict to briefly touch on the question of sovereignty and certain related matters.

International Law in Cyberspace

3. Let me begin by recalling two questions that were addressed at the meeting in Bucharest, namely the applicability of international law in cyberspace and, more specifically, the applicability of IHL to cyber operations.

4. First, as regards the applicability of general international law, it is widely recognized today that cyberspace is not a legal vacuum, but that existing rules of international law extend to this domain. This position has been repeatedly affirmed by States, including in the context of the Group of Governmental Experts and in the Open-ended Working Group on Developments in the Field of Information and Telecommunications.[1] Indeed,

1 Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the

today it is difficult to find a State which does not share this position.

5. The fact that there is now a consensus on the applicability of international law should not come as a surprise. While cyberspace has some distinct features, other aspects of cyber are quite ordinary, even banal. Most definitions of cyberspace differentiate between the physical dimension of cyber, which includes information technology equipment and infrastructure, and the functional, logical or cognitive dimension of cyber, which includes software, data and even the exchange of data. There is absolutely no reason why existing rules of international law should not apply to the physical dimension of cyber, such as computers or other pieces of equipment. Nor is there any reason why rules that regulate intangible matters, such as freedom of speech or intellectual property, could not apply to the functional or cognitive dimension of cyberspace.

6. The real question, therefore, is not whether international law applies, but *how* it applies to cyberspace. Yet even this question needs to be broken down further. This is so because not all rules of international law are equally relevant. Take, for example, the Vienna Convention on Diplomatic Relations (VCDR) of 1961.[2] Article 22(1) of the Convention declares that 'The premises of the mission shall be inviolable. The agents of the receiving State may not enter them, except with the consent of the head of the mission.' Evidently, the inviolability conferred by this rule does not extend to the internet presence of a diplomatic mission, since the notion of 'premises' clearly refers to physical premises that can be entered. By contrast, other provisions of the Vienna Convention are framed as general principles that are not tied to a particular context. Article 27 provides that 'The receiving State shall permit and protect free communication on the part of the mission for all official purposes.' There is no reason why this rule should not apply to communication through cyber means, such as correspondence by email. A third group consists of rules that are potentially relevant to cyber, but it is not immediately obvious whether and how they might apply. Article 24 of the Convention provides that 'The archives and documents of the mission shall be inviolable at any time and wherever they may be'. Since the Vienna Convention codified rules developed in the pre-digital age, a narrow approach may suggest that Article 24 must be limited to non-digital 'archives' and 'documents'. By contrast, a more inclusive approach might point out that the purpose of the Vienna Convention is to 'ensure the efficient performance of the functions of diplomatic missions'[3] and that extending inviolability to electronic archives and documents is essential to this end.

7. The point of these examples is that we need to look at the specific content of individual rules to determine whether they are relevant to cyberspace at all and, if so, how they apply. While some cases are relatively straightforward because the rule in question

---

Context of International Security, 'Report', UN Doc. A/76/135 (14 July 2021), para. 69; 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 2010), para. 34.

2 Vienna Convention on Diplomatic Relations (18 April 1961) 500 UNTS 95.

3 Preamble, VCDR.

clearly does or does not apply, in many other cases the application of individual rules is open to reasonable disagreement. This is a source of considerable legal uncertainty. Since States make international law, it is ultimately for States to reduce this uncertainty by clarifying their understanding of the law.

8. This brings me to the application of IHL to cyber operations. Famously, in 2017, the Group of Governmental Experts was unable to reach a consensus on the applicability of IHL to cyberspace. At the time, the representative of Cuba suggested that recognizing the applicability of IHL would 'legitimize a scenario of war and military actions' in cyberspace.[4] This view overlooks the fact that the applicability of IHL does not legitimize or authorize any use of force inconsistent with the Charter of the United Nations.[5] Recognizing the applicability of IHL to cyber therefore does not legitimize war in cyberspace any more than it legitimizes war in other domains.

9. Again, the real question is not whether IHL as a regime of international law applies, but whether and how *individual rules* of IHL apply in cyberspace. Certain rules of IHL do not have any obvious cyber relevance at all. For example, detaining powers must provide prisoners of war with 'sufficient water and soap' for their personal hygiene: it is difficult to see any connection between this obligation and cyber.[6] By contrast, general principles and obligations of IHL, such as the duty to distinguish between protected persons and objects on the one side and military objectives on the other side, are clearly applicable. In still other cases, it is not immediately clear whether a particular rule is relevant or not. Consider the duty to enable prisoners of war to send 'capture cards' to their family to inform them of their captivity, their address and their state of health.[7] As originally drafted, the rule clearly envisages the sending of physical cards—but considering its purpose, should the rule not also entitle prisoners of war to inform their family through electronic means?

10. To develop these points, let me turn to the legal questions raised by cyber operations conducted in the context of Russia's war of aggression against Ukraine.

Cyber operations in and against Ukraine

11. Ukraine has been the target of hostile cyber operations linked to Russia well before

4 Declaration oy Miguel Rodríguez, Representative of Cuba, at the Final Session of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (23 June 2017) <http://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information>.

5 Preamble, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I) (8 June 1977) 1125 UNTS 3.

6 Convention Relative to the Treatment of Prisoners of War (Geneva Convention III) (12 August 1949) 75 UNTS 135, Article 29.

7 Geneva Convention III, Article 70.

Russia launched its full-scale invasion in 2022. For example, in March 2014, Ukrainian websites and services were hit by a major distributed denial-of-service (DDoS) attack. In 2015, the Ukrainian power grid was targeted, resulting in a loss of power for more than 230,000 consumers. In June 2017, Ukrainian institutions, businesses and services were hit by the *NotPetya* malware attack. The incident also affected numerous systems located outside Ukraine, causing an estimated loss of over USD 10 billion.

12. Ukraine continued to suffer cyber attacks following the launch of the full-scale Russian invasion in February 2022. One of the most damaging incidents, the Viasat attack, severely disrupted internet services across Ukraine, rendering thousands of satellite broadband modems inoperable, including modems used by the Ukrainian government and military. Since February 2022, both private and public networks have been targeted on an ongoing basis. The attacks have included operations against Ukraine's energy infrastructure, its postal and telecommunications services; false messages targeting the general public; phishing attacks directed against government officials and private persons; as well as various intelligence and surveillance activities carried out through cyber means. While many of these operations have been linked to pro-Russian groups and also to the Russian authorities, it should be noted that the Russian Government has denied its involvement.

13. Several features of these cyber operations merit attention. First, operations against Ukraine have pursued three broad aims: the disruption of Ukrainian networks, infrastructure and services; the dissemination of propaganda and conduct of psychological warfare; and the gathering of intelligence. Second, although Ukraine has been targeted by hundreds of cyber attacks, their impact on the course of the conflict has been limited. Cyber operations have brought neither decisive military nor decisive political advantages for Russia. Third, many cyber attacks were not launched in isolation, but to complement conventional military operations. For example, the Russian missile strike against a television tower in Kyiv on 1 March 2022 was followed by cyber attacks against a major broadcasting company on the same day. In May 2022, a Russian missile attack against the residential areas of Odesa was accompanied by a cyber operation targeting Odesa City Council. Finally, cyber operations have been carried out by a wide range of actors, including States and non-State actors. The latter include not only established groups and networks, but also thousands of cyber volunteers and 'hacktivists' who have engaged mostly in low-level cyber activities in support of the parties to the conflict.

14. Bearing these features in mind, the conduct of cyber operations in and against Ukraine poses a range of legal questions that are of wider interest and significance.

15. The first set of questions relates to the nexus between hostile cyber activities and the broader armed conflict. As I have indicated, Russian-linked cyber operations in and against Ukraine did not start in February 2022. In the weeks before the invasion, several waves of DDoS and data wiper attacks were launched against Ukrainian governmental and private networks and websites. Since Russia and Ukraine were engaged in an armed conflict already before Russia launched its full-scale invasion, were these cyber

attacks subject to IHL? The answer depends partly on whether the attacks were designed to hand a military advantage to Russia in the context of the ongoing hostilities. The answer is fact-dependent, but has significant legal implications: cyber operations against certain Ukrainian government sites and networks may have been permissible under IHL, assuming it did apply to them, but not under the rules of international law applicable outside the conduct of hostilities.

16. Stepping away from the specific circumstances of the conflict in Ukraine, the fact that Russia's full-scale invasion was preceded by cyber operations aimed at shaping the battlespace highlights that cyber attacks may straddle the line between war and peace. Cyber shaping operations that predate the outbreak of hostilities are not governed by the law of armed conflict, yet the rules applicable in times of peace may not adequately reflect the fact that such operations may actually be a prelude to war.

17. Second, as noted earlier, cyber operations have been deployed in support of kinetic attacks. This too has significant legal implications. The bulk of IHL is concerned with kinetic matters. The majority of the rules governing the conduct of hostilities apply in the case of 'attacks', which are defined as 'acts of violence against the adversary, whether in offence or in defence'.[8] Cyber operations that do not entail acts of violence are not 'attacks' within the meaning of IHL and therefore are not subject to some of its key rules and principles, such as the rule of proportionality. Even those rules that are concerned with non-physical effects may require a kinetic component. For example, 'Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited'.[9] The rule only covers cyber operations that cause terror among the civilian population through an act or threat of violence, but not cyber operations that cause fear and panic by disrupting vital infrastructure and services through non-kinetic means. However, where cyber operations are carried out to complement kinetic acts of violence, it would not be unreasonable to treat the cyber action and the kinetic action as part of a single 'attack' within the meaning of IHL, provided the cyber action is integral to the kinetic action. This means that basic rules, such as the principle of distinction or the prohibition of indiscriminate attacks, would be applicable to cyber actions that do not cause material destruction or injury.

18. Third, the widespread participation of 'hacktivists' in hostile cyber operations raises questions about their status under IHL. While civilians are normally immune from attack, they lose that immunity for such time that they directly participate in hostilities (DPH). The International Committee of the Red Cross has identified three constituent parts of DPH.[10] First, harm: the act by the civilian must inflict injury, death or destruction or, alternatively, be likely to adversely affect the military operations or military capacity of a party to the conflict. Second, causation: there must be a direct causal link between the act performed by the civilian and the harm likely to result from the act or the military

8 Additional Protocol I, Article 49(1).

9 Additional Protocol I, Article 51(2).

10 International Committee of the Red Cross, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (2008).

action of which the act forms an integral part. Third, belligerent nexus: the act must be designed to directly cause harm in support of one party to the conflict against another. The notion of harm is critical for DPH: since harm does not have to involve kinetic effects, participation in cyber operations that are likely to inflict non-kinetic harm on an adversary (such as intelligence gathering, degrading their communications or adversely affecting command and control through ruses) may count towards DPH. Participation in hostile cyber operations may, therefore, amount to DPH and hacktivists and cyber volunteers who engage in such acts thus lose their immunity from attack. It is worth noting that this loss of immunity does not depend on their geographical location, meaning that they are targetable as a matter of IHL even when they are located outside active combat zones.

19. Related to DPH is the question whether hacktivists and other cyber volunteers may lose their civilian status on a permanent basis? States may seek to enhance the effectiveness of cyber volunteers by coordinating and supporting their activities. Depending on the level and nature of State involvement, groups of cyber volunteers may qualify as irregular 'militias' or 'volunteer corps' belonging to the State party, meaning that their members would lose their civilian status and gain combatant status.

20. Fourth, State reliance on cyber volunteers raises questions whether this practice is compatible with the duty to take precautions. Belligerents are bound to take the 'necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations'.[11] Encouraging and facilitating the participation of civilians in hostilities through cyber means, especially if this rises to the level of DPH, does not seem to be compatible with this duty. For example, Ukraine has developed an app for mobile phones (the ePPO app) that enables Ukrainian civilians to report the location of incoming Russian missiles or other airborne threats. The information is then relayed to Ukrainian air defence units. Since usage of this app may amount to DPH and render civilians liable to attack, its distribution by the Ukrainian authorities is difficult to reconcile with the precautionary duty to protect civilians from the dangers resulting from military operations. The question is not settled, however, partly because the precautionary duty is not absolute and partly because other relevant rules, such as the right of self-defence, may also have a bearing on the matter.

21. Fifth, the support provided by third States to Ukraine in cyberspace or through cyber means raises questions about neutrality and co-belligerency. It is common knowledge that third States have provided extensive assistance to Ukraine to bolster its cyber capabilities, including technical assistance and support, financial aid and intelligence on cyber threats. To the extent that these forms of support assist Ukraine in the conduct of its military operations against Russia, they are incompatible with traditional conceptions of neutrality. Other forms of support provided to Ukraine through cyber means, for example the sharing of military intelligence, may also be incompatible with the traditional requirements of neutrality. However, some nations adhere to the concept of 'qualified neutrality', whereby third States are entitled to support a belligerent that has been the

11 Additional Protocol I, Article 58(c).

victim of a flagrant act of aggression without loss of their neutral status. The matter is not settled though. In addition, the assistance provided by third States to Ukraine in the form of cyber means or to support its cyber operations may be of such kind as to render the third States providing this assistance co-belligerents. Whether or not this is the case depends on whether the assistance makes a direct and integral contribution to the conduct of hostilities by Ukraine. In principle, this could be the case where cyber assistance directly and integrally contributes to conduct of specific kinetic attacks.

Cyber operations below the threshold

22. Let me now turn briefly to cyber operations below the threshold of armed conflict. Depending on the nature of these operations, they may engage a wide range of specialized regimes of international law, such as international human rights law. In addition, they may also engage general rules of international law, including the rule of territorial sovereignty.

23. There has been some debate in recent years about the exact nature and scope of the sovereignty rule. There is broad agreement that sovereignty prohibits certain types of cyber activities. Thus, the unauthorised conduct of cyber activities by the agents of one State present in the territory of another State is a violation of sovereignty, as are remote cyber operations that cause physical damage in the territory of another State, operations that involve the exercise of governmental functions by the agents of one State in the territory of another or operations which interfere with the exercise of inherently governmental functions by the territorial State. All of these scenarios are relatively straightforward, as they merely extend to cyberspace prohibitions that are well-established in the non-digital world. However, some States take the position that sovereignty also prohibits cyber operations that cause cyber systems in another State to loose functionality or become inoperable, even where no material damage occurs. A handful of States, such as France and Iran,[12] go even further to claim that the mere penetration of national cyber systems, in particular those critical for national security, is a violation of sovereignty. This reflects the fear that the penetration of national cyber systems may be part of shaping operations, rendering the targeted State more vulnerable in the future.

24. These expansive interpretations of sovereignty reflect the fact that hostile cyber operations may cause significant harm, or pose significant threats, to vital national interests even without causing physical damage or injury. This does not always sit well with the pre-digital mindset of the applicable rules of international law, many of which are framed in kinetic and geographical terms. For example, Israel has noted that there is a tension between the legitimate interests of a State to protect its cyber assets located outside national territory, for example data stored in cloud systems, and the territorial

12 Ministère des Armées, 'Droit international appliqué aux operations dans le cyberespace' (2019), p. 6; Declaration of the General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace (2020), Article II(3).

focus of the rule of sovereignty.

25. This creates an incentive for an expansive interpretation not only of sovereignty, but also other relevant rules of international law, including the prohibition of intervention and the prohibition of the use force. The United Kingdom, for example, has taken the view that coercive acts prohibited by the principle of non-intervention include not only acts compelling a State to act differently than it would otherwise have done, but also acts that constrain its freedom of control over matters within its domestic jurisdiction.[13] In other words, on this view, the principle prohibits acts that impair another State's *capacity* to carry out its functions. In essence, this could transform the prohibition of coercive interference into a prohibition of harmful interference. Similarly, some States have taken the position that cyber operations which severely disrupt the functioning of the State, including its economy, could amount to a use of force even where these operations do not cause physical damage.

26. Given that cyber operations may cause significant non-kinetic harm and pose critical threats and vulnerabilities, it is likely that a growing number of States will support expansive interpretations of the pre-digital rules. Such a development raises two questions that deserve our attention: what effect will such expansive interpretations have on the ability of States to conduct counter-cyber operations and what effect will they have on the interpretation and application of these rules outside cyberspace?

Concluding thoughts

27. In conclusion, let me leave you with five take-aways. First, cyber operations in armed conflict are both a driver and a symptom of the diffusion of warfare: cyber helps to extend warfare across different domains, actors, time and geographical spaces. Second, while cyber operations pose a multitude of legal challenges, we should be careful not to overestimate their novelty and distinctness. Similar or identical legal difficulties exist in other domains too. Third, the application of the existing rules of international law to cyberspace is not a one-way street: how States interpret and apply the law in cyberspace may have a significant effect on the application and interpretation of the rules in other domains. Fourth, we must acknowledge the limits of the law. Agreeing on clear legal standards and fostering legal certainty is vitally important, but this alone does not guarantee compliance. Where compliance is not forthcoming, and in the absence of effective enforcement mechanisms, States will continue to turn to measures of self-help. Finally, for this reason, we cannot escape difficult choices and the fact that the legal dimension of cyberspace is not just about rules, but about order and strategic competition.

28. Thank you for your attention.

13 Attorney General, 'International Law in Future Frontiers' (2022).