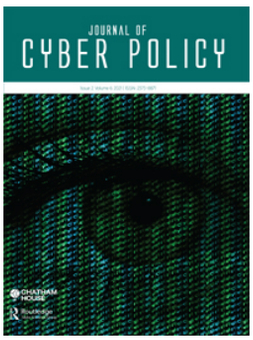

Routledge
Taylor & Francis Group

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Unblurring the lines: military cyber operations and international law

Kubo Mačák

To cite this article: Kubo Mačák (2021): Unblurring the lines: military cyber operations and international law, Journal of Cyber Policy, DOI: 10.1080/23738871.2021.2014919

To link to this article: https://doi.org/10.1080/23738871.2021.2014919

Published online: 14 Dec 2021.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2021.2014919

Routledge
Taylor & Francis Group

Unblurring the lines: military cyber operations and international law

Kubo Mačák *

Legal Division, International Committee of the Red Cross, Geneva, Switzerland

ABSTRACT

The bright lines between certain fundamental legal categories may appear to have dimmed in the cyber environment, especially in relation to military cyber operations. This article thus unblurs the lines between five such pairs of categories, proceeding from the general to the specific: Firstly, what separates international law from international norms as the two principal regulatory frameworks governing the conduct of military cyber operations? Secondly, what is the distinction between domain-specific and general rules of international law as they apply to military cyber operations? Thirdly, is it possible to distinguish between peacetime and armed conflict with respect to the regulation of such operations? Fourthly, once an armed conflict is underway, how do we distinguish combatants from non-combatants in cyberspace? And fifthly, what is the distinction between objects and non-objects in cyberspace, particularly with respect to computer data affected by military cyber operations during armed conflicts? Overall, the article's goal is to reduce the opacity surrounding the relationship between military cyber operations and international law. In doing so, it aims to contribute to the long-term goal of making cyberspace a more open, secure, stable, accessible and peaceful environment.

ARTICLE HISTORY
Received 14 June 2021
Revised 14 September 2021
Accepted 5 November 2021

KEYWORDS
Armed conflict; combatants; cyberattacks; data; international law; military operations

1. Introduction

States have long been acutely aware of the military utility of cyberspace. Several have openly acknowledged the use of military cyber capabilities during armed conflicts and many more are known to be developing such capabilities (ICRC 2021a, 8). Echoing these trends, UN member States warned in a high-level consensus report adopted in March 2021 'that the use of ICTs [information and communications technologies] in future conflicts between States is becoming more likely' and added that such uses may result in 'potentially devastating humanitarian consequences' (OEWG 2021, paras 16 and 18). In June 2021, in a historical first, another UN-based group of governmental experts expressly referred to international humanitarian law (IHL) in the cyber context,

CONTACT Kubo Mačák kmacak@icrc.org
*The opinions expressed herein are author's own and do not necessarily correspond to those held by the ICRC or its Legal Division.

noting that this branch of international law 'applies only in situations of armed conflict' (GGE 2021a, para. 71(f)).

These two new reports have brought a degree of much-needed clarity from States into the otherwise murky relationship between military cyber operations and international law. To some extent, the opacity is understandable: States tend to be tight-lipped about their military capabilities and shroud their cyber conduct in layers of secrecy (Clarke and Knake 2010, xi). At the same time, for many years, they had been reluctant to publicise their legal views on matters related to military cyber operations (Mačák 2017a, 881). However, the tide is now turning. Military cyber operations and their impact on civilians are becoming the focus of increased international attention (see, e.g. ICRC 2021a) and, one by one, States have started issuing national positions on international law and cyber operations, many of which include questions of military uses of cyberspace (see CCDCOE 2021a; Roguski 2020). As a new Open-Ended Working Group begins its work in late 2021, international regulation of military cyber operations is bound to remain a staple of future multilateral discussions.

Accordingly, it is the right time to look more closely at the less well-understood aspects of the application of international law to military cyber operations. For conceptual clarity, international law is understood here as the legal order meant to structure the interaction between actors participating in and shaping international relations, the predominant among which are States (Besson 2010, 163). With respect to military conduct, a key branch of international law is IHL, which consists of a body of rules that seek, for humanitarian reasons, to limit the effects of armed conflict (ICRC 2014). Military cyber operations are understood here as the use of cyber capabilities by military actors to achieve objectives in or through cyberspace. Such operations can fulfil a range of purposes but are perhaps most simply categorised into exploitation, defence and offence. These three categories are often interlinked: for example, exploitation often needs to be carried out before an offensive operation can be launched (see further, ICRC 2021a, 16–17).

In the particular nature of the cyber environment, the bright lines between a number of fundamental legal categories may appear to have dimmed, especially as these apply to military cyber operations. Each of the next five sections of this article thus unblurs the line between one such pair of key categories, going from the general to the specific. Firstly, what separates international law from international norms as the two principal normative frameworks governing the conduct of military cyber operations? Secondly, what is the distinction between domain-specific and general rules of international law as they apply to military cyber operations? Thirdly, is it possible to distinguish between peacetime and armed conflict with respect to the regulation of such operations? Fourthly, once an armed conflict is underway, how do we distinguish combatants from non-combatants in cyberspace? And fifthly, what is the distinction between objects and non-objects in cyberspace, particularly with respect to computer data that might be affected by military cyber operations during armed conflicts?

2. Regulatory frameworks for military cyber operations: international law and norms

The first line to be unblurred relates to the contours of international law regulation of military cyber operations. Certain areas of human conduct, such as the high seas or outer

space, benefit from dedicated treaties that codify key international legal rules governing these areas. No such international treaty has yet been agreed for State conduct in cyberspace, despite various proposals going back nearly three decades (Mačák 2017a). Accordingly, the exact scope and boundaries of the international legal framework governing cyber conduct are themselves subject to interpretation and disagreement.

To begin with, it is now universally agreed that international law is applicable to cyber operations. This means that cyberspace is not the 'Wild Wild West' that it had sometimes been described as (Perlroth and Sanger 2015). We do not have to start writing rules governing cyber conduct from scratch; conversely, existing rules of international law maintain, at least in principle, their relevance in cyberspace. This is the case even if those rules – such as those regulating State sovereignty or use of force – had emerged well before the advent of technologies that enable the existence of cyberspace as we know it today.

Given the absence of a global cyber treaty, the applicable rules must be identified through a careful analysis of existing international legal obligations. These may be found in international treaties such as the 1945 Charter of the United Nations or the 1949 Geneva Conventions. They may also be of customary nature, which means that they reflect general practice accepted as law. For example, there is a general agreement that States must not conduct cyber operations that would directly or indirectly intervene in the internal affairs of another State, and thus violate the customary prohibition of intervention (GGE 2021b, para. 71(c)). The growing trend of publishing national positions on the application of international law to cyber operations – most recently, 15 States did so in an 'official compendium' that complemented the GGE report mentioned earlier (see GGE 2021b) – provides valuable material for the understanding of international law in the cyber context (see further, Mačák 2017a, 896–98). Ongoing projects that aspire to catalogue these emerging views – such as the Tallinn Manual 3.0 or the Cyber Law Toolkit – help reveal the points of convergence and divergence among States (see CCDCOE 2021b and 2021c).

However, not all internationally agreed standards of State conduct qualify as international law. In particular, in recent years, States have been actively discussing so-called norms of responsible State behaviour in cyberspace (also referred to as 'cyber norms'). In the cyber context, norms are understood as non-binding and voluntary in nature, and thus often portrayed as 'a pathway to easier consensus in a challenging realm' (Adamson 2020). A milestone in that regard was the 2015 report of an UN-mandated Group of Governmental Experts (GGE 2015), which recommended 11 such norms and recognised that additional ones could be developed over time. Although the next GGE failed to achieve consensus in 2017, contemporary reports of the 'death of the norms process' (e.g. Grigsby 2017) turned out to be rather exaggerated. This is now confirmed by the two 2021 consensus reports mentioned earlier – one by a renewed GGE and another one by a new Open-Ended Working Group (OEWG) – both of which have also reflected the increased attention paid to military cyber power by States (GGE 2021b, para. 7; OEWG 2021, para. 16).

Confusingly, these fora discuss cyber norms and international law side by side, with frequent overlaps. For instance, the 2015 GGE report referred to the need for States to respect human rights online both in the section dedicated to cyber norms (para. 13(e)) and in the section on international law (para. 28(b)). It has been suggested that these

repetitions highlight the fact that States have not been able to consistently distinguish between norms and law in their practice (Delerue, Douzet, and Géry 2020, 31–32). From a broader perspective, scholarly analyses have shown that many of the agreed norms actually reflect existing international law (e.g. Adamson 2020).

Indeed, the two types of standards do share a number of characteristics. They are both intended to set benchmarks for the evaluation of State behaviour, distinguishing between internationally acceptable and unacceptable forms of conduct. In this way, norms and law both provide the basis for calling out bad behaviour and overall aim to make State behaviour more predictable in volatile times such as during armed conflict (Broeders and van den Berg 2020, 4). In addition, norms and law are closely related concepts and, at least in theory, an inter-State agreement on norms may gradually influence the development of the law (Finnemore and Hollis 2016, 441–42).

However, norms and law also differ in fundamental aspects. The main among them is precisely the legally binding nature of international law, and that a violation of such a rule gives rise to international responsibility, which cannot be said of non-binding norms governing cyber conduct (Mačák 2017a, 882; Delerue, Douzet, and Géry 2020, 30). For States, this responsibility for a violation of international law triggers so-called secondary obligations under the law of State responsibility, which include in particular the obligations of cessation and reparation (ARSIWA 2001, Articles 30(a) and 31(1)). For example, if a State conducts a cyber operation that amounts to a prohibited intervention in the internal affairs of another State, it is legally obliged to cease its wrongful conduct (if it is continuing) and to provide full reparation to the injured State for the harm caused. Particularly grave forms of cyber conduct – for instance, military cyber operations directed against medical facilities during armed conflict – may additionally qualify as international crimes and result in individual criminal responsibility of the persons involved (Ambos 2015; Mačák, Gisel, and Rodenhäuser 2020).

International law thus sets down a minimum standard of responsible behaviour that is binding on States. Although the absence of a compulsory enforcement mechanism makes it more complicated to sanction violations of international law, States are nonetheless considerably more reluctant to breach international law, as opposed to non-binding norms (Schmitt and Vihul 2014). Importantly, commentators have warned that the norms discourse may sometimes serve to detract from, and thus undermine, international law (Delerue, Douzet, and Géry 2020, 35; Moynihan 2020, 14; Tikk 2020, 7; Akande, Coco, and de Souza Dias 2021), although others have argued that, conversely, norms and international law are mutually reinforcing (Adamson 2020, 19; Broeders 2021, 6). In addition, it has been noted that norms may be more effective for the purposes of peacetime use of cyber capabilities than for the regulation of military cyber operations (Ruhl et al. 2020, 13). These debates further underscore the need to clearly distinguish between the two standards.

As a matter of legal logic, non-binding norms can never override binding legal rules. The 2015 GGE report confirms that axiom when it notes that cyber norms do not seek to limit or prohibit action that is otherwise consistent with international law (para. 10). The reverse is also true: a non-binding norm cannot permit action that would otherwise be forbidden by international law. This has now been clarified in the new 2021 OEWG report, which has reaffirmed that norms do not replace or alter States' binding legal obligations or rights, but rather provide 'additional specific guidance' on what constitutes

responsible State behaviour in cyberspace (para. 25; for similar observations by individual States see, e.g. Australia 2021, 3; Germany 2021, 16; Japan 2021, 2). The 2021 GGE report added that in doing so, norms 'can help to prevent conflict in the ICT environment and contribute to its peaceful use' (para. 15).

Overall, international law provides binding legal boundaries on the permissible conduct in cyberspace by States, including their armed forces. Within this permitted space, States may engage in further 'normative construction' (Schmitt and Vihul 2014) and develop additional non-binding norms of responsible behaviour. In other words, these norms set a higher, more desirable standard of responsible behaviour, over and above the applicable minimum laid down by international law. Having demarcated the line between law and norms as it applies to military cyber operations, the remainder of the present article focusses on the legal regulation of such operations.

3. Identification of legal rules applicable to military cyber operations: domain-specific and non-domain-specific rules

The second line to be unblurred relates to the supposed distinction between domain-specific and other rules of international law. This question builds on the longstanding discussion about the type of legal rules that are appropriate for cyberspace governance and the way in which it is answered determines the extent to which cyber activities, including military cyber operations, are governed by international law. This section argues in favour of a broad approach, according to which there is no general requirement under international law to examine whether a given rule is specifically applicable in the 'cyber domain'.

The dichotomy underlying the discussion in this section can be traced back to the early stages of the internet's development, when it was argued that rules that had been designed for the 'offline world' should not reach into cyberspace (e.g. Johnson and Post 1996). Such proposals saw the 'online world' as a new form of space or a new domain, which would over time develop its own domain-specific system of rules and legal institutions. However, States soon began to understand the growing potential of cyberspace for the achievement of their vital interests, including national security, public safety and economic development (Mačák 2017a). Unfazed by the anarchic proposals of the mid-1990s, they gradually extended the reach of their domestic legal frameworks into cyberspace.

Although it took slightly longer for international law to catch up, in 2013, a consensus was finally reached in the international community that international law applies to cyberspace (GGE 2013, para. 19; UN Doc A/Res/68/243 2013). Read at face value, the statement would seem to imply that all international legal rules are relevant for human conduct in cyberspace, just as they are for conduct anywhere in the physical world. However, not all States are fully aligned with such interpretation.

For example, Russia and Nicaragua have both suggested that cyberspace is and will remain a 'de facto "legal vacuum"' until States agree on a global legal instrument providing for specific modalities of such applicability (Russia 2020a, 1; Nicaragua 2020, 2–3; see also Cuba 2020, 3). Without such binding guidelines, the argument went, the statement from the 2013 report is 'left hanging in the air and cannot be applied in practice' (Russia 2020b, 1).

More recently, Israel also argued against the automatic applicability of international legal rules in the cyber context. In a national position published in early 2021, it suggested that customary rules would only apply to cyberspace if the practice that they are based on was 'closely related to the activity envisaged in the cyber domain' and if the opinio juris which gave rise to the rule in question was not specific to some other domain (Israel 2021, 397).

However, such suggestions do not accurately reflect the nature and functioning of international law. First of all, there is no general requirement in international law to examine whether a given rule is applicable to a particular 'domain'. In fact, the notion of domains does not have an established international law definition. It may be useful in military and legal theory as an organisational concept that structures the thinking about particular forms of activities, interaction and resources (e.g. McCosker 2020). But there are no accepted criteria for clustering such activities, interaction or resources into specific 'domains'. This is well-illustrated by the unending controversy regarding whether cyberspace even qualifies as a standalone domain (in favour: e.g. Lynn 2010; Ryan et al. 2011, 1167–68; Wilson 2014, 8; against: e.g. Rid 2013, 166; Tallinn Manual 2017, 12; Delerue 2020, 11). This author shares the view that the answer to this controversy is in any case irrelevant for the purposes of applicability of international law to cyber operations (see, in the context of IHL, Gisel, Rodenhäuser, and Dörmann 2020, 298).

Secondly, even if we could agree on a categorisation of domains (and that cyberspace itself constitutes such a domain), it is not clear how the link between a rule and a domain would be established. Some rules are simply formulated in such general terms that searching for a narrow link of this kind would be meaningless. For example, IHL prohibits direct attacks against civilians and civilian objects, without distinction as to the weapons used or the location of the attacks (ICRC 2005, Rules 1 and 7). Applying similar logic, the International Court of Justice held that the fundamental principles and rules of humanitarian law apply to 'all forms of warfare and to all kinds of weapons' (*Nuclear* Weapons 1996, para. 86). Therefore, it does not matter what specific means (technological or otherwise) a party to a conflict uses, as long as doing so qualifies as an attack, it must not be directed at civilians or civilian objects.

Other rules might be restricted in their application to certain persons, times, locations or subject matter. In law, such limitations are considered to establish respectively the personal, temporal, geographical and material scope of application of those rules.[1] It may happen that these constraints, taken together, exclude the applicability of a given rule from the cyber context. For instance, Article 26(1) of the Third Geneva Convention prescribes that prisoners of war must be provided with sufficient basic daily food rations. The personal scope of application of this rule is limited to prisoners of war; its temporal scope, like the rest of the Convention, covers the period from the time they fall into the power of the enemy until their final release and repatriation; its geographical scope is limited to premises where the prisoners are interned, which are normally restricted to locations on land; and its material scope concerns the maintenance of the prisoners (see ICRC 2021b, 404, 721–22 and 766). Taken together, the rule leaves little meaningful scope to govern the conduct of cyber operations. However, the inapplicability of Article 26(1) to cyber operations follows from its scope of application, and not from any general proscription against applying 'land domain-specific' rules to other domains.

In fact, many rules that have emerged in non-cyber 'domains' such as land, sea or air, can still have implications for the regulation of cyber conduct. Consider, for instance, the legal regime governing the so-called innocent passage of foreign vessels through a coastal State's territorial sea (LOSC 1982, Articles 17–26). Clearly, the geographic scope of application of the relevant rules is limited to the maritime area up to 12 nautical miles from the baselines (i.e. the territorial sea), a part of the 'sea domain'. However, the range of activities governed by these rules may well include military cyber activities conducted from or through a vessel traversing the territorial sea. For example, passage of a foreign ship is not considered innocent if it engages in 'any act aimed at interfering with any systems of communication' of the coastal State (LOSC 1982, Article 19(2)(k)). This formulation is technology-neutral and it thus extends to interference by cyber means such as hacking the coastal State's systems through a transiting foreign ship (e.g. Swanson 2011, 730).

Overall, this analysis confirms that there is no general principle that would exclude the applicability of international law rules to the uses of new technologies, including those taking place 'in the cyber domain'. Accordingly, there is no requirement to look for a 'further proof of applicability to ICTs or other new technologies via specific state practice and opinio juris "in cyberspace"' (Akande, Coco, and de Souza Dias 2021). Rather, the starting point must be that existing international law is applicable, as a matter of principle, to all forms of human activity, whether they involve muskets or malware.

4. Situational context of military cyber operations: peacetime and armed conflict

The third line to be unblurred relates to the distinction between situations of peace and war as legal categories. It is sometimes suggested that this 'binary' distinction is no longer adequate in today's complex, multipolar and interconnected world (e.g. Brooks 2018). Compounding the problem, States and other actors engage in so-called 'grey-zone operations', which are described by experts as referring to competition that appears to fall between the standard categories of peace and war (ICRC 2021a, 15). And it was recently argued in this Journal that States use cyberspace 'first and foremost to wage wars', although – somewhat paradoxically – the authors added that 'the attacks conducted until today have remained below the threshold of war according to international law' (Douzet and Géry 2021, 2). So, is it possible to distinguish between peace and war with respect to the regulation of military cyber operations?

To begin with, it should be noted that the boundary between these two categories of international law has not remained static over time. Traditionally, international law had been a composite of two disparate, mutually exclusive bodies of rules: one set for peacetime (the law of peace) and another for the time of war (the law of war) (e.g. Phillimore 1879, 794). However, that is no longer true today. Rules that used to be clumped together as peacetime law—such as those concerning State responsibility, treaty interpretation, identification of custom or human rights—continue to apply after the outbreak of hostilities (Mačák 2017b, 137; Fleck 2021, 78).

However, the same is not the case in reverse. In other words, the body of law designed for the application in times of armed conflict – IHL – has retained its conceptual separation from the rest of international law. Crucially, with very few exceptions, the material scope

of application of IHL rules is limited to armed conflicts;[2] this was very recently expressly confirmed in the cyber context by the GGE (GGE 2021a, para. 71(f)). Generally speaking, IHL rules have been formulated in such a way as to take into account the special circumstances of warfare (Gasser 1993). Therefore, absent a situation of armed conflict, it would not necessarily be protective (or humanitarian) to apply the rules of IHL.

In that regard, it is sometimes suggested – particularly in the Western context – that States should apply IHL to the conduct of military cyber operations, whether these take place within or outside of armed conflicts (see, e.g. Ney 2020). On the one hand, such statements of policy should be welcomed insofar as they amount to States' voluntary adoption of constraints going above and beyond their existing obligations applicable in peacetime. For example, it is now well-understood that peacetime international law does not unequivocally rule out hostile cyber operations against medical facilities (see Mačák, Gisel, and Rodenhäuser 2020). Conversely, the protections under IHL can be described as comprehensive, given that the applicable rules require that medical facilities must be respected and protected at all times (ibid; see also First Oxford Statement 2020, para. 5). Accordingly, a policy the application of which effectively rules out any military cyber operations against hospitals whether in peacetime or in war should certainly be considered a step forward. This is irrespective of whether such policy would be grounded in ethical considerations, in extending IHL principles to non-armed conflict situations, or in a combination of both of these approaches.

On the other hand, no unilaterally adopted policy may extricate a State from its existing obligations under international law. Specifically, the legal framework applicable in peacetime contains no equivalent to the IHL notions of military objectives (which may be attacked during armed conflicts provided all relevant rules are respected) or of incidental civilian harm (which IHL tolerates unless it is excessive in relation to the expected military advantage, and provided that precautions have been taken to avoid it). Accordingly, outside of armed conflicts, States cannot refer to the rules of IHL – which remain technically inapplicable – to justify cyber conduct that would amount to a violation of the rules applicable in peacetime. Instead, in such situations, the conduct of military cyber operations by States is regulated by other branches of international law, including the law on the use of force and human rights law, as applicable (Gisel, Rodenhäuser, and Dörmann 2020, 306).

What remains to be determined, then, is whether a given situation qualifies as an armed conflict, or not. This question poses little difficulty where cyber operations complement ongoing kinetic hostilities such as, for instance, in the conflict between the US-led coalition and the Islamic State group or in the conflict between Israel and Hamas. It is also generally accepted among scholars that the resort to cyber operations with similar effects to classic kinetic operations between two States would amount to an international armed conflict (Tallinn Manual 2017, 384). However, the law remains unsettled with respect to the qualification of cyber operations that merely disrupt the operation of military or civilian infrastructure, without physically damaging it (ICRC 2021b, 106). It should thus be welcomed that States have started to express their views on the matter (e.g. France 2019, 12; Germany 2021, 7). Others should follow in their footsteps in order to allow for a gradual consolidation of the law on this crucial point.

To sum up, in order to determine the applicable legal framework for specific forms of cyber conduct, one must first establish whether these occur in the context of an armed

conflict, or not. In the absence of an armed conflict, IHL does not apply and the conduct in question remains governed by other branches of international law. Conversely, when an armed conflict is underway, IHL is applicable; in the cyber context, this may raise new interpretive challenges such as those that are the subject of the next two sections.

5. Individuals engaged in military cyber operations during armed conflicts: combatants and non-combatants

The fourth line to be unblurred relates to the distinction between combatants and civilians in the context of military cyber operations. For IHL of international armed conflicts,[3] this is a critical dichotomy: combatants are authorised to participate directly in hostilities (and therefore enjoy combatant immunity from prosecution), whereas civilians are not (Additional Protocol I 1977, Article 43(2)). By the same token, combatants may be made the object of attack unless they surrender or are otherwise *hors de combat*, whereas civilians are granted a general protection from the dangers arising from military operations (Additional Protocol I 1977, Articles 41(1)–(2) and 51(1)).

While the distinction between civilians and combatants is a 'cardinal principle' of IHL (*Nuclear* Weapons 1996, para. 78), its transposition to the cyber context is not without interpretive difficulties. For instance, Russia has noted that it is 'very difficult (if not impossible) to draw a distinction in virtual space between … combatants and non-combatants' (Russia 2020b, 2). Similarly, the former Ambassador of Switzerland to the US, Martin Dahinden wrote that in cyberspace, 'the fundamental distinction in international humanitarian law between civilians and combatants is particularly unclear' (Dahinden 2021, 8). And Japan recently underscored the question of how the existing law on 'the scope of combatants applies to cyberspace' as one of the key unsettled issues in IHL (Japan 2021, 7).

However, IHL does contain specific rules for the determination of status during armed conflict. To begin with, it lays down the fundamental rule that within an international armed conflict, every person is either a combatant or a civilian (Additional Protocol I 1977, Article 50(1)). It thus follows that if a given person does not fall under one of the categories of combatants, that person must be considered a civilian. Also, in case of doubt as to a person's status in the context of the conduct of hostilities, IHL requires that the person be considered a civilian (Additional Protocol I 1977, Article 50(1)).

So who qualifies as a combatant? Article 43(2) of Additional Protocol I states that members of the armed forces of a party to an international armed conflict (other than medical personnel and chaplains) are combatants. This treaty definition today reflects customary international law binding upon all States, including those that have not yet ratified the Protocol (ICRC 2005, Rule 3). Thus, members of military cyber units such as the US Cyber Command, China's People's Liberation Army's Strategic Support Force Network Systems Department, or Israel's Unit 8200 would qualify as combatants during an international armed conflict.

Although the remote nature of their operations makes this unlikely, if such persons fall into enemy hands, they become prisoners of war protected by the 1949 Third Geneva Convention and they may not be punished for the mere fact of having participated in hostilities during an international armed conflict. By contrast, they may and must be prosecuted for any war crimes they may have committed, such as intentionally directing

attacks against civilian objects (ICC Statute 1998, Article 8(2)(b)(ii)) – while noting that what is an attack and what is an object with regard to the application to cyber operations of the IHL rules on the conduct of hostilities remains in some aspects unsettled (with regard to attacks, see Mačák and Gisel 2022; with regard to objects, see next section).

Under customary law, members of the armed forces who fail to distinguish themselves while engaged in an attack or in a military operation preparatory to an attack (e.g. by not wearing a uniform), forfeit the right to prisoner-of-war status and, consequently, the combatant privilege (see ICRC 2021b, 363). There is some debate on the extent to which this rule is relevant to cyber operations (Tallinn Manual 2017, 405–06). In particular, it has been argued that the requirement to distinguish oneself only applies in circumstances in which the failure to do so 'might reasonably cause an attacker to be unable to distinguish between civilians and combatants', which would thus increase the risk of mistaken attack against civilians (ibid. 405). The alternative view, to which this author subscribes, is that the rule on distinction should be complied with even if the remoteness of the combatants from the targets of their cyber operations reduces the 'practical significance' of wearing a uniform (see United States 1999, 8). Requiring that cyber combatants distinguish themselves at the requisite times will also avoid any allegations that they were acting under the false pretence of being a civilian, which could amount to the war crime of perfidy (Horowitz 2021). More broadly, this interpretation also safeguards the fundamental principle of distinction against erosion caused by the introduction of additional criteria that may lead to arbitrary application (such as reasonableness with respect to the attacker's ability to distinguish or to the expected risk of mistaken attack). Overall, the customary rule should thus be seen as fully applicable also with respect to the military personnel engaged in cyber operations.

In some States, non-military personnel, such as intelligence agency staff or other government employees, may also be involved in the conduct of military cyber operations (ICRC 2021a, 9). If such agencies or other State organs are incorporated into the armed forces (on which, see ICRC 2005, 16–17 and Tallinn Manual 2017, 406), their personnel become combatants. That means that they have the right to participate directly in hostilities, which includes conducting military cyber operations against the enemy during an international armed conflict, and if they are captured, they are entitled to prisoner-of-war status (Geneva Convention III 1949, Article 4A).

Conversely, if entities are not incorporated into the armed forces and their personnel are not otherwise members of armed forces, they are not combatants, and accordingly must be considered as civilians. While IHL does not strictly prohibit civilians from participating in hostilities (see ICRC 2009, 83; United States 2016, paras 4.15.2.2 and 16.5.5), it certainly does not encourage it, either. Specifically, civilian government employees who take a direct part in hostilities are liable to attack for such time as they are directly participating in hostilities. If they fall into enemy hands, they do not benefit from prisoner-of-war status. And because civilians are not entitled to the combatant privilege, such persons would also not enjoy immunity from domestic prosecution of the detaining State for having directly participated in hostilities even if they had respected IHL in doing so.

More broadly, involvement of civilians in military operations is in direct tension with the IHL principle of distinction. As noted by the ICRC, civilians 'were never meant to directly participate in hostilities on behalf of a party to a conflict' (ICRC 2009, 38–39). The principle of distinction requires that parties to armed conflicts distinguish between

combatants and civilians at all times. The principle is most effective in practice if participation in hostilities is limited to those endowed with the combatant privilege. As such, the practice of involvement of civilians in combat functions is eroding the principle of distinction (Bartolini 2010; Sassòli 2019) and, in the opinion of some writers, it violates the States' obligation to uphold that principle (Cameron and Chetail 2013, 104). Overall, States should thus ensure that military cyber operations that amount to taking direct part in hostilities are conducted only by members of the armed forces (see United States 1999, 8).

6. Electronic data affected by military cyber operations during armed conflicts: objects and non-objects

The final blurry line relates to the distinction between objects and non-objects in IHL. Whether something is an object is critical for its protection in times of armed conflict, given that the protection that IHL offers against civilian harm is expressed through a prohibition against attacking civilian persons (Additional Protocol I 1977, Article 51(2)) and civilian *objects* (Additional Protocol I 1977, Article 52(1)). More broadly, the legal category of 'objects' is central to the entirety of the law of targeting, given that it constitutes a key element of, among others, the prohibition of indiscriminate attacks, the definition of military objectives, or the rules on active and passive precautions (Additional Protocol I 1977, Articles 51(4), 52(2), and 57–58). In the pre-digital period, determining whether something was an object posed little difficulty: while concrete things like civilian buildings or paper files were protected objects, abstract notions like civilian morale or loyalty were not. However, since computers came on the scene, a new category has appeared, which was harder to qualify: digital or electronic data.

To illustrate, imagine that Ambrosia and Ruritania are two independent States engaged in an international armed conflict against one another. Ambrosian armed forces launch a cyber operation against the Ruritanian central registry office, which maintains digital records on Ruritanian citizens, with regard to various non-military purposes such as census taking, the provision of social benefits, voting and taxation. The operation results in the destruction of all data held by the registry office—but it does not directly or indirectly cause any physical destruction, and it also does not affect the cyber infrastructure which supports the system used by the office. In other words, the data is gone, but all the computers continue to function as they did before. Did Ambrosia violate IHL by destroying the datasets held by the Ruritanian authorities?

The answer to that question hinges on whether data is considered to be more like a paper file, or like loyalty. In other words, is data an object? If it is, then cyber operations against data (such as deleting a dataset held by a registry office) are governed by the IHL rules on the conduct of hostilities and the protection these rules afford to civilian objects. If it is not, then these rules and protections would not apply, meaning that many types of civilian data would be considered 'fair game' as long as the effects of the cyber operation against them remain confined to cyberspace (Mačák 2015, 78). It should be noted, however, that specific protection that IHL affords to some categories of objects covers data belonging to those objects even if data itself is not considered as an object.[4]

On the question whether data qualifies as an object for the purposes of the IHL rules on the conduct of hostilities, experts hold different views. On the one hand, the majority of experts involved in the Tallinn Manual process considered that the ordinary meaning of

the term 'object' cannot be interpreted as including data because objects are by definition visible and tangible (Tallinn Manual 2017, 437). Some States also subscribe to this view (see, e.g. Denmark 2016, 292; Chile 2020, para. 36; Israel 2021, 401). The key ramification of this view is that military cyber operations against civilian data (including, for instance, the registry datasets mentioned in the scenario above) would be outside the scope of all IHL rules that only protect civilian 'objects', resulting in a significant gap in legal protection.

On the other hand, others have argued that either all or some types of data should be considered as objects under IHL. One view, taken by several States, is that the protection of civilian objects extends to civilian data (see, e.g. Finland 2020, 7; Germany 2021, 8; Romania 2021, 78; Norway 2013, para. 9.58). This implies that all data constitute objects for the purposes of IHL. This interpretation is supported by the modern meaning of the notion of objects in today's society as well as by the object and purpose of the relevant IHL rules (Mačák 2015, 80). It is also consistent with the traditional understanding of the notion of 'objects' under IHL, which is broader than the ordinary meaning of the word and encompasses also locations and animals (Gisel, Rodenhäuser, and Dörmann 2020, 319). Another approach, thus far endorsed by one State, is to consider content data as protected under the principle of distinction (presumably this would include civilian registry datasets mentioned in the scenario above), leaving to the side whether other types of data (such as code) formally qualify as objects or not (France 2019, 14).

Overall, this wide spectrum of views shows that the question of whether and to what extent data constitute objects for the purposes of their protection under IHL remains unresolved at the present time. It may be that new approaches will need to be developed to adequately protect the various functions of data in modern societies (for such proposals, see, e.g. Schmitt 2019; Geiss and Lahmann 2021). Until then, it should be underscored that whatever approach is taken, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them (ICRC 2019, 28). It might be that this final line cannot yet be fully unblurred, but to view cyber operations against essential civilian data (such as the Ruritanian registry datasets mentioned earlier) as permitted by IHL would result in a serious protection gap during armed conflicts.

7. Conclusion

The point of departure of this article was that the seemingly blurred lines concerning the regulation of military cyber operations reduce the legal certainty in cyberspace. However, once we look more closely at the existing normative framework applicable to cyber operations, much of the mist begins to lift. As we have seen, in the first place, it is essential to clearly distinguish between international law and norms of responsible behaviour as the regulatory frameworks applicable to military cyber operations. International law lays down the applicable binding minimum, while norms provide additional specific guidance on what constitutes responsible State behaviour in cyberspace (see section 2).

Secondly, in the identification of specific legal rules applicable to military cyber operations, the starting point is that existing international law is applicable, as a matter of principle, to all forms of human activity. There is accordingly no general requirement to examine whether or not a rule is 'domain-specific', though the scope of a given rule

might exclude its applicability from the cyber context (see section 3). By contrast, to determine the applicable legal framework for specific forms of cyber conduct, it is essential to establish whether these occur in the context of an ongoing armed conflict, or not. If they do, IHL is applicable; if they do not, they are regulated by other branches of international law (see section 4).

Thirdly, during armed conflicts, it is possible to distinguish between combatants and civilians also insofar as the conduct of military cyber operations is concerned, by reference to the existing rules of IHL. Generally speaking, States should ensure that military cyber operations that amount to taking direct part in hostilities are conducted only by members of the armed forces (see section 5). Finally, the distinction between objects and non-objects, as applied to electronic data during armed conflicts, remains unsettled under IHL. However, whichever legal approach prevails over time, essential civilian data should not be excluded from protection afforded by IHL so as not to create a serious protection gap (see section 6).

To summarise, the interpretations proposed here aim to reduce the opacity surrounding the relationship between military cyber operations and international law. Unblurring the lines separating the legal categories discussed in this article is essential to the generally shared goal of making cyberspace a more open, secure, stable, accessible and peaceful environment. It is hoped that this article will contribute towards this goal, including through informing the future development of national positions on international law in cyberspace and the multilateral discussions surrounding these issues.

Notes

1. Sometimes, the combined effect of those limitations – especially the geographic and material ones – is used to refer to certain sets of rules as being domain-specific. For example, IHL rules regulating naval and air warfare are sometimes referred to as governing only the sea and the air domain, respectively. However, as the discussion below demonstrates, such delineation may be imprecise given that there are certain aspects of those rules that apply across the supposed domains.
2. These exceptions relate primarily to measures that must be taken in peacetime in order to ensure the respect for IHL in the event an armed conflict occurs, such as the duties to disseminate and train IHL, to adopt certain implementing domestic legislation, to carry out legal reviews of new weapons, means and methods of warfare, or to take measures to protect civilians against the effects of attacks.
3. In non-international armed conflicts, the notion of combatant status and the associated concept of combatant privilege do not exist under IHL. Whether persons are allowed to take part in hostilities in a non-international armed conflict is governed by domestic law. Regardless of the legality of their participation in hostilities under domestic law, members of the State armed forces, fighters for non-state armed groups and civilians taking a direct part in hostilities must respect IHL, including when carrying out military cyber operations.
4. In particular, the obligations to respect and protect medical facilities and humanitarian relief operations extend to medical data belonging to those facilities and data of humanitarian organizations that are essential for their operations. Similarly, deleting or otherwise tampering with data in a manner that renders useless objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation systems, is prohibited under IHL (see further, Mačák and Gisel 2022, section 4.2.).

Acknowledgements

The author would like to thank Ana Beduschi, Laurent Gisel, Jonathan Horowitz, and Tilman Rodenhäuser, as well as the anonymous peer reviewers and the editors of the Journal for their valuable comments on earlier drafts of this article.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Kubo Mačák is a Legal Adviser in the Legal Division of the International Committee of the Red Cross (ICRC), assigned jointly to the Arms and Conduct of Hostilities Unit and the Commentaries Unit. Prior to joining the ICRC in 2019, he worked as an Associate Professor at the University of Exeter in the UK. Kubo is the author of the book *Internationalized Armed Conflicts in International Law* (Oxford University Press 2018) and of multiple articles in peer-reviewed journals including the *International Review of the Red Cross*, the *Journal of Conflict and Security Law*, and the *Cambridge International Law Journal*. Kubo is also the General Editor of the *Cyber Law Toolkit*, an interactive online resource on the international law of cyber operations.

ORCID

Kubo Mačák http://orcid.org/0000-0001-5062-2041

References

Adamson, L. 2020. "International Law and International Cyber Norms A Continuum?" In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by D. Broeders, and B. van den Berg, 19–44. London: Rowman & Littlefield.

Additional Protocol I. 1977. *Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts*. Adopted at Geneva on 8 June 1977, entered into force on 7 December 1978.

Akande, D., A. Coco, and T. de Souza Dias. 2021. "Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond." *EJIL:Talk!* 5 January 2021. https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

Ambos, K. 2015. "International Criminal Responsibility in Cyberspace." In *Research Handbook on International Law and Cyberspace*, edited by N. Tsagourias, and R. Buchan, 118–143. Cheltenham: Edward Elgar.

ARSIWA. 2001. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. International Law Commission. UN Doc A/56/10.

Australia. 2021. "National Contribution on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States." In *GGE* 2021b, 3–17.

Bartolini, G. 2010. "The Participation of Civilians in Hostilities." In *Rules and Institutions of International Humanitarian Law Put to the Test of Recent Armed Conflicts*, edited by M. Matheson, and D. Momtaz, 321–409. Leiden: Martinus Nijhoff Publishers.

Besson, S. 2010. "Theorizing the Sources of International Law." In *The Philosophy of International Law*, edited by S. Besson, and J. Tasioulas, 163–185. Oxford: Oxford University Press.

Broeders, D. 2021. "The (Im)Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: A Mid-Process Assessment." *Journal of Cyber Policy*. doi:10.1080/23738871.2021.1916976

Broeders, D., and B. van den Berg, eds. 2020. *Governing Cyberspace: Behavior, Power, and Diplomacy*. London: Rowman & Littlefield.
Brooks, R. 2018. "Rule of law in the gray zone." Modern War Institute. 2 July 2018. https://mwi.usma.edu/rule-law-gray-zone/.
Cameron, L., and V. Chetail. 2013. *Privatizing War*. Cambridge: Cambridge University Press.
CCDCOE. 2021a. "Strategy and Governance: Statements on International Law." https://ccdcoe.org/library/strategy-and-governance/.
CCDCOE. 2021b. "CCDCOE to Host the Tallinn Manual 3.0 Process." https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.
CCDCOE. 2021c. "Cyber Law Toolkit Presents Annual Update Including an Overview of National Positions, Invites New Submissions." https://ccdcoe.org/news/2021/cyber-law-toolkit-presents-annual-update-including-an-overview-of-national-positions-invites-new-submissions/.
Chile. 2020. Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire (14 January 2020), cited in OAS. "Improving Transparency: International Law and State Cyber Operations: Fifth Report." OAS Doc. CJI/doc. 615/20 rev.1, 7 August 2020.
Clarke, R. A., and R. K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: Ecco.
Cuba. 2020. "Considerations on the Initial Pre-draft of the Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security." 15 April 2020. https://front.un-arm.org/wp-content/uploads/2020/04/considerations-on-the-initial-pre-draft-of-the-oewg-cybersecurity-cuba-15-april.pdf.
Dahinden, M. 2021. *Swiss Neutrality in the Age of Cyber Warfare*. Geneva: ICT4Peace Foundation.
Delerue, F. 2020. *Cyber Operations and International Law*. Cambridge: Cambridge University Press.
Delerue, F., F. Douzet, and A. Géry. 2020. *The Geopolitical Representations of International Law in the International Negotiations on the Security and Stability of Cyberspace*, Report No. 75, IRSEM/EU Cyber Direct, November 2020.
Denmark. 2016. *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*. Danish Ministry of Defence. Defence Command Denmark. September 2016.
Douzet, F., and A. Géry. 2021. "Cyberspace is Used, First and Foremost, to Wage Wars: Proliferation, Security and Stability in Cyberspace." *Journal of Cyber Policy* 6 (1): 96–113.
Finland. 2020. "International Law and Cyberspace: Finland's National Positions." October 2020. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.
Finnemore, M., and D. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425–479.
First Oxford Statement. 2020. *Oxford Statement on the International Law Protections in Relation to Cyber Operations Targeting the Health Care Sector*. Oxford: Oxford Institute for Ethics, Law and Armed Conflict. May 2020. https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea#/.
Fleck. 2021. "Scope of Application of International Humanitarian Law." In *The Handbook of International Humanitarian Law. 4th Edition*, edited by D. Fleck, 50–80. Oxford: Oxford University Press.
France. 2019. "International Law Applied to Operations in Cyberspace." Ministère des Armées.
Gasser, H. 1993. *International Humanitarian Law: An Introduction*. Geneva: Henry Dunant Institute.
Geiss, R., and H. Lahmann. 2021. "Protection of Data in Armed Conflict." *International Law Studies* 97: 556–572.
Geneva Convention III. 1949. *Convention (III) relative to the Treatment of Prisoners of War*. Adopted at Geneva on 12 August 1949, entered into force on 21 October 1950.
Germany. 2021. "On the Application of International Law in Cyberspace: Position Paper." March 2021. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.
GGE. 2013. "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.

GGE. 2015. "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/70/174, 22 July 2015.
GGE. 2021a. "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.
GGE. 2021b. "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.
Gisel, L., T. Rodenhäuser, and K. Dörmann. 2020. "Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts." *International Review of the Red Cross* 102 (913): 287–334.
Grigsby, A. 2017. "The End of Cyber Norms." *Survival* 59 (6): 109–122.
Horowitz, J. 2021. "The International Legal Consequences of Enrolling Private Companies and Civilians in National Defense Cyber Operations During Armed Conflict." [working title] Forthcoming.
ICC Statute. 1998. *Rome Statute of the International Criminal Court*. Adopted at Rome on 17 July 1998, entered into force on 1 July 2002.
ICRC. 2005. *Customary International Humanitarian Law, Volume I:Rules*, edited by J.-M. Henckaerts, and L. Doswald-Beck. Geneva: ICRC.
ICRC. 2009. *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, edited by N. Melzer. Geneva: ICRC.
ICRC. 2014. "What is International Humanitarian Law?" https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf.
ICRC. 2019. "International Humanitarian Law and Cyber Operations During Armed Conflicts: ICRC Position Paper." November 2019. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.
ICRC. 2021a. *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict*, edited by E. Lawson, and K. Mačák. Geneva: ICRC. https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations.
ICRC. 2021b. *Commentary on the Third Geneva Convention*. Cambridge: Cambridge University Press.
Israel. 2021. "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations." *International Law Studies* 97: 395–406.
Japan. 2021. "Basic Position of the Government of Japan on International Law Applicable to Cyber Operations." 28 May 2021. https://www.mofa.go.jp/files/100200935.pdf.
Johnson, D. R., and D. Post. 1996. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48 (5): 1367–1402.
LOSC. 1982. *United Nations Convention on the Law of the Sea*. Adopted at Montego Bay, Jamaica, on 10 December 1982, entered into force on 16 November 1994.
Lynn, W. J. 2010. "Defending a New Domain:The Pentagon's Cyberstrategy." *Foreign Affairs*. September/October. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.
Mačák, K. 2015. "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law." *Israel Law Review* 48 (1): 55–80.
Mačák, K. 2017a. "From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers." *Leiden Journal of International Law* 30 (4): 877–899.
Mačák, K. 2017b. "From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law." In *Defending the Core*, edited by H. Rõigas, R. Jakschis, L. Lindström, and T. Minárik, 135–148. Tallinn: NATO CCD COE.
Mačák, K., and L. Gisel. 2022. "Rules in a Cyber Conflict." In *Cyber Defence in the European Union*, edited by P. Pawlak, and F. Delerue. Chaillot Paper. Paris: EUISS, forthcoming.

Mačák, K., L. Gisel, and T. Rodenhäuser. 2020. "Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?" *Just Security*. 27 March 2020. https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

McCosker, S. 2020. "Domains of Warfare." In *Oxford Guide to International Humanitarian Law*, edited by B. Saul, and D. Akande, 77–98. Oxford: Oxford University Press.

Moynihan, H. 2020. "The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace." *Journal of Cyber Policy*. doi:10.1080/23738871.2020.1832550

Ney, P. 2020. "Department of Defense General Counsel Remarks at US Cyber Command Legal Conference." 2 March 2020. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

Nicaragua. 2020. "Nicaragua's Considerations on the Initial Document of the Open-Ended Working Group on Progress in the Field of Information and Telecommunications in the Context of International Security." 3 April 2020. https://front.un-arm.org/wp-content/uploads/2020/04/minic-mis-143-04-2020-permanent-mission-of-switzerland.pdf.

Norway. 2013. *Manual i Krigens Folkerett*. Helsinki: Merkur-Trykk.

Nuclear Weapons. 1996. "International Court of Justice." *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, 226.

OEWG. 2021. "Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security." UN Doc. A/75/816, 18 March 2021.

Perlroth, N., and D. E. Sanger. 2015. "Obama Calls for New Cooperation to Wrangle the 'Wild West' Internet." New York Times, 13 February 2015. https://www.nytimes.com/2015/02/14/business/obama-urges-tech-companies-to-cooperate-on-internet-security.html.

Phillimore, R. J. 1879. *International Law, Volume III*. London: Butterworths.

Rid, T. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Roguski, P. 2020. *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague Program for Cyber Norms Policy Brief. March 2020. https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

Romania. 2021. "National Contribution on the Subject of how International Law Applies to the Use of Information and Communications Technologies by States." In *GGE* 2021b, 75–79.

Ruhl, C., D. Hollis, W. Hoffman, and T. Maurer. 2020. *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Carnegie Endowment for International Peace Working Paper. February 2020. https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf.

Russia. 2020a. "Commentary of the Russian Federation on the Initial 'Pre-draft' of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security." April 2020. https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

Russia. 2020b. "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.

Ryan, D. J., M. Dion, E. Tikk, and J. J. Ryan. 2011. "International Cyberlaw: Normative Approach." *Georgetown Journal of International Law* 42 (4): 1161–1198.

Sassòli, M. 2019. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*. Cheltenham: Edward Elgar.

Schmitt, M. 2019. "Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations." *International Review of the Red Cross* 101 (1): 333–355.

Schmitt, M., and L. Vihul. 2014. "The Nature of International Law Cyber Norms." *Tallinn Paper No. 5*. Special Expanded Issue. NATO Cooperative Cyber Defence Centre of Excellence.

Swanson, S. R. 2011. "Google Set Sail: Ocean-Based Server Farms and International Law." *Connecticut Law Review* 43: 709–751.

Tallinn Manual. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition*, edited by M. Schmitt, and L. Vihul. Cambridge: Cambridge University Press.

Tikk, E. 2020. "International Law in Cyberspace: Mind the gap." Cyber Policy Institute. March 2020. https://eucyberdirect.eu/content_research/international-law-in-cyberspace-mind-the-gap/.

UN Doc A/Res/68/243. 2013. *Developments in the Field of Information and Telecommunications in the Context of International Security*. 27 December 2013.

United States. 1999. "An Assessment of International Legal Issues in Information Operations." Department of Defense, Office of General Counsel. May 1999.

United States. 2016. *Department of Defense Law of War Manual*. Department of Defense, Office of General Counsel. June 2015 (updated December 2016).

Wilson, J. R. 2014. "Cyber Warfare Ushers in 5th Dimension of Human Conflict." *Military & Aerospace Electronics* 25 (12): 8–15.