International Review of the Red Cross (2018), **100** (1-2-3), 165–183.
150 years of humanitarian reflection
doi:10.1017/S1816383119000055

INTERNATIONAL REVIEW of the Red Cross

Cyber operations and the Second Geneva Convention

Jeffrey Biller
Lieutenant-Colonel Jeffrey Biller, USAF, is the Associate Director for the Law of Air, Space, and Cyber Operations at the Stockton Center for the Study of International Law at the United States Naval War College.

Abstract

The recently released updated ICRC Commentary on the Second Geneva Convention (GC II) recognizes significant changes in both the conduct of naval conflicts and interpretations of the governing law. One such significant change is the addition of cyber operations to the conduct of naval operations. Modern vessels increasingly utilize computer networks to control critical ship systems, but discussions of how potential cyber operations should be viewed under GC II are understandably limited. This article aids in addressing that gap by analyzing how cyber operations could have implications for certain provisions of GC II.

Keywords: cyberspace, naval warfare, Geneva Conventions, prisoners of war, hospital ships.

Introduction[1]

As much as any other aspect of warfare, technological leaps periodically revolutionize the manner in which naval warfare is conducted. The digitalization and automation of modern warships have the potential to create another such leap as the result of offensive cyber operations against those systems. Real-world examples of how potential cyber operations target these systems are increasingly found in news reporting. In one example, the Electronic Chart Display (ECDIS)

system on an 80,000-ton ship was infected via a malware-containing USB stick.[2] ECDIS is a Windows-based computer system installed with navigation software that is utilized in vessels worldwide. These systems generally employ obsolete versions of Windows and rarely use anti-virus software. An unsophisticated cyber adversary could easily breach such a system, with potentially severe effects on navigation. Perhaps even more troubling, at least twenty ships near the Russian port of Novorossiysk reported that their ships' GPS systems had placed them at an inland position 25 nautical miles from their actual position.[3] This incident appears to be part of a trend in Russian waters of potential GPS disruption.[4]

Just as technology continues to evolve, so too does the law, requiring a constant re-evaluation of its tenets. In May 2017, the law of naval warfare took a significant step forward when the International Committee of the Red Cross (ICRC) released an updated Commentary on the Second Geneva Convention (GC II).[5] This convention constitutes a significant percentage of the rules applicable to naval warfare in international armed conflicts.[6] The focus of GC II is on the protection of wounded, sick and shipwrecked members of armed forces at sea, and the document builds upon provisions in the 1889 and 1907 Hague Conventions. The 2017 Commentary on GC II is the first produced by the ICRC since the original Commentary was released in 1960, and recognizes significant changes in both the conduct of naval conflicts and interpretations of the governing law. The latter half of the twentieth century featured major technological developments that contributed to both manner of changes. One such significant technological development is the advent of the cyber domain as a key component in military operations.

Naval forces are already planning for cyber operations to play a significant role in future naval conflicts.[7] This planning is a recognition of the tremendous possibilities and vulnerabilities that increasingly "wired" military forces present. Modern naval vessels utilize, and rely upon, programmable logic controllers to interface hardware components with the physical systems on board

1 This article builds upon a series of posts related to the subject that appeared in November 2017 on the website *Opinio Juris*.

2 Chris Baraniuk, "How Hackers Are Targeting the Shipping Industry", *BBC News*, 18 August 2017, available at: www.bbc.com/news/technology-40685821 (all internet references were accessed in March 2019).

3 David Hambling, "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon", *New Scientist*, 10 August 2017, available at: www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.

4 *Ibid.*

5 ICRC, *Commentary on the Second Geneva Convention: Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, 2nd ed., 2017 (2017 Commentary on GC II), available at: https://ihl-databases.icrc.org/ihl/full/GCII-commentary.

6 It should be noted that GCII does not apply to non-international armed conflicts (NIACs), despite the fact that non-State armed groups may possess significant naval and cyber capabilities. Although not the focus of this article, certain provisions of GC II may apply to NIACs through customary international law.

7 See, generally, United States Navy, *Fleet Cyber Command Strategic Plan 2015–2020*, available at: www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

a ship.[8] This creates valuable crew efficiencies, more accurate weapon systems, and pinpoint navigation. However, these networked control systems also create vulnerable attack vectors against power, hydraulic, steering, propulsion and other critical systems. While operations utilizing cyber methods may appear quite different from traditional kinetic operations in the maritime environment, they nevertheless have potential implications for protections under the Geneva Conventions.

The 2017 Commentary on GC II does recognize the potential impact of cyber operations on naval warfare. However, discussion of the impact of cyber operations on GC II protections is limited to a small number of topics. This is not to criticize the Commentary – consensus as to the applicability of international law to the cyber domain is in its infancy, and States have been reluctant to make anything more than rudimentary statements as to their interpretations. Given this lack of consensus, it is understandable that the authors of the updated Commentary would hesitate to include in-depth interpretations regarding the impact of cyber operations on GC II.

Helpfully, the 2017 Commentary does contain a lengthy discussion of cyber operations in the context of two important areas: GC II's scope of applicability provisions found in Article 2 common to the four Geneva Conventions,[9] and the prohibition on the use of secret code by hospital ships.[10] As common Article 2 is not concerned with naval warfare specifically, this article will not directly address the issue. The updated Commentary addresses the important question of cyber communications and Article 34, which prohibits hospital ships from "possess[ing] or us[ing] a secret code for their wireless or other means of communication",[11] but as the Commentary provides a lengthy discussion of this question, it is not covered in this article.

Scope of applicability and encrypted communications may be among the most obvious ways in which cyber operations impact GC II rights and obligations, but many additional questions remain unanswered by the 2017 Commentary. This article will address four specific articles of GC II in light of potential offensive cyber operations. First, the article discusses Article 12 and the protections afforded to those shipwrecked at sea; specifically, the question of whether a crew may be "shipwrecked" through purely cyber means is analyzed. Second, the article considers Article 16 and the protections that must be afforded to naval crews who "fall into enemy hands". This section views the possibility of crews falling into enemy hands as the result of a cyber operation taking control of vital ship functions. Third is an analysis of Article 18's "end of engagements"

8 Office of Naval Research, United States Department of the Navy, "A New Defense for Navy Ships: Protection from Cyber Attacks", *Phys.org*, 17 September 2015, available at: https://phys.org/news/2015-09-defense-navy-ships-cyber.html.

9 2017 Commentary on GC II, above note 5, paras 275–278.

10 *Ibid.*, paras 2389–2403.

11 Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950), Art. 34.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

clause; although similar to the common Article 2 scope of applicability question, it contains elements unique to naval operations. Fourth and last, the obligation to "respect and protect" hospital ships and coastal rescue craft, found in Articles 22, 24, 25 and 27, raises many questions in the light of potential cyber operations. Here, the updated Commentary briefly addresses this requirement as related to cyber operations, and this section will build on that analysis.

Each section addresses two primary questions: one, how are obligations and rights under the relevant article impacted by potential cyber operations; and two, what steps should navies, particularly those increasingly reliant on networked systems, take in anticipation of cyber operations impacting naval engagements?

Cyber shipwrecks and Article 12

Major threats to modern navies through cyber operations include such attack vectors as the previously discussed ECDIS, as well as automatic identification systems, which are non-encrypted transponder systems that have shown vulnerability to spoofing attacks.[12] The next level of threat is the ability to manipulate, or even take over, the aforementioned programmable logic controllers by manipulating the supervisory control and data acquisition (SCADA) software that assists in controlling modern ships. This type of capability was demonstrated by researchers from the University of Texas's Cockrell School of Engineering in 2013, when they gained control over a modern 213-foot superyacht's navigational controls via a creative GPS-spoofing operation.[13] The research team was able to steer the yacht to a new course by altering positional inputs, while the ship's navigational systems showed the yacht maintaining its original course heading. This capability has the potential to put ships at risk from natural and human dangers alike and demonstrates but one potential cyber-related vulnerability of modern SCADA systems controlling vital ship functions. One of these potential dangers is that a crew could become shipwrecked through cyber means; in this situation, the crew would therefore receive protections under GC II.

Article 12 of GC II provides that "[m]embers of the armed forces … who are at sea and who are wounded, sick or shipwrecked, shall be respected and protected in all circumstances". Most importantly, Article 12 affords crews protection from further attack once they qualify as "shipwrecked". As indicated in the article, this entails two obligations: one restrictive and one protective. The restrictive obligation is against any violent actions directed at those enjoying the protection, and against indiscriminate violence that may affect them.[14] This obligation should be read broadly given the particularly vulnerable position of

12 Glenn Hayes, "Manipulating AIS", *Marine Electronics Journal*, 23 November 2015.
13 "Spoofing a Superyacht at Sea", *University of Texas News*, 30 July 2013, available at: https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea.
14 2017 Commentary on GC II, above note 5, para. 1400.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

those wounded, sick and/or shipwrecked.[15] The protective obligation is highly dependent upon the circumstances ruling at the time, including the level of potential harm to those protected and the resources available to those with the obligation. Of particular importance to the following discussions, the 2017 Commentary states that "once wounded, sick and shipwrecked persons are in the power of a Party to the conflict, the Party will have better options to protect them against the worsening of their medical condition and other dangers".[16]

Traditional notions of shipwreck conjure up images of ships ablaze and beginning to sink as the result of cannons, torpedoes or aerial bombs. However, Article 12 states that "the term 'shipwreck' includes shipwreck from any cause". Given the reliance of many modern warships on cyber-controlled critical systems, this begs the question: can the crew of a warship be shipwrecked, within the meaning of GC II, by purely cyber means, thereby affording protections from further attack? Although no State has yet officially addressed this specific question, a review of the 2017 Commentary's Article 12 analysis suggests an answer in the affirmative, but it is by no means clear.

Part of the difficulty in answering this question lies in ambiguities related to the determination of when a crew should be considered shipwrecked.[17] It may initially seem counterintuitive that the crew of a ship with no apparent physical damage and which has not been kinetically engaged by an opposing force can be thought of as shipwrecked. However, the 2017 Commentary is quite helpful here, stating that "to qualify as shipwrecked the person must be in a situation of peril at sea", and that "in all cases the person must refrain from any act of hostility".[18] Thus, we can break the analysis down into two separate elements: establishing whether the crew of a ship disabled by cyber means is in "peril at sea", and if so, how to determine whether that crew has refrained from engaging in hostilities. These elements will be examined individually below.

Peril at sea

Framing the analysis of whether a ship's crew disabled through cyber means can be considered in peril is the 2017 Commentary's guidance to read the term shipwreck "as being broad",[19] which reiterates the 1960 Commentary's exhortation for the term to be "taken in its broadest sense".[20] Despite a broad reading of the term "shipwrecked", it can initially be difficult to accept that a ship's crew should be considered in peril when aboard a ship with no outwardly apparent damage.

15 *Ibid.*, para. 1404.
16 *Ibid.*, para. 1411.
17 For additional discussion of the meaning of the term "shipwrecked", see Steven Haines, "Who is Shipwrecked?", in Andrew Clapham, Paola Gaeta and Marco Sassòli (eds), *The 1949 Geneva Conventions: A Commentary*, Oxford University Press, Oxford, 2015, pp. 767–780.
18 2017 Commentary on GC II, above note 5, para. 1379.
19 *Ibid.*, para. 1383.
20 Jean Pictet (ed.), *Commentary to the Geneva Conventions of 12 August 1949*, Vol. 2: *Geneva Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea*, ICRC, Geneva, 1960, pp. 84–92.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

However, the loss of propulsion, steering, life-support and other critical systems is enough to create a dangerous situation, even if not immediately life-threatening. To this point, the 2017 Commentary finds that "[p]ersons on a fully disabled ship … whose situation is dangerous but not necessarily imminently life-threatening, are also covered, as long as they refrain from any act of hostility".[21] Furthermore, the Commentary states: "Situations that are *potentially* life-threatening … also render persons on board 'in peril' at sea."[22]

While it appears clear that a ship disabled through cyber means can result in a legal determination of the crew being in "peril at sea", the primary practical difficulty is that the extent of the damage may be unknown, initially even to the crew itself. The damage to networked systems may require extensive repair, necessitating new equipment, or may require that information technology experts be brought on board for damage assessment. Conversely, it is possible that the damage might quickly be repaired and that the ship's weapon systems would thus again pose a deadly threat to opposing warships.

Furthermore, the factual attribution of who or what is responsible for the disabling of the ship's networks may initially be unclear. Indeed, it may be that the damage is entirely self-inflicted or unintentionally caused by malware previously and unknowingly introduced by a member of the ship's crew, as was the case with the malware-infected ECDIS updates mentioned above.[23] In these situations, the 2017 Commentary's inclusion of "shipwrecks caused by human error or a malfunction" in its definition of "any other cause" makes it clear that a ship's crew could be rendered shipwrecked through cyber means even if the damage to the ship's networks is self-inflicted or caused by means other than enemy action.[24] Accordingly, a determination of factual attribution as to the cause of the network malfunction is legally unnecessary in evaluating whether protections should be afforded. However, the potential confusion over the extent of damage caused through cyber means makes the requirement of "refraining from hostilities" even more important in assessing whether the crew must be afforded protections.

Refraining from hostilities

The 2017 Commentary indicates that a crew does not receive the protections of Article 12 unless, in addition to being in peril, they also refrain from any further act of hostility. Determining whether a warship's crew has complied with this requirement can be difficult even when the evidence is visually observable, such as when the crew can be seen abandoning the ship. A ship's weapon systems may remain functional even while other systems are severely damaged, and there may still be members of the crew operating those systems. Recall that the ship itself

21 2017 Commentary on GC II, above note 5, para. 1384.
22 *Ibid.*, para. 1385 (emphasis in original).
23 See above note 2 and accompanying text.
24 2017 Commentary on GC II, above note 5, para. 1386.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

remains a military object subject to attack throughout; it is only the crew that receives protections in a shipwreck situation. The 2017 Commentary recognizes this difficulty:

> However, it will likely be very difficult or even impossible for an enemy to know whether the crew is working to repair weapons with the aim of continuing hostilities without an outward sign indicating otherwise. Furthermore, as the sailors are on board a military objective, it is likely that a disabled or damaged warship would need to surrender (e.g. by striking its colours) in order for protection to be secured.[25]

A question specific to the cyber domain is what cyber measures a crew may take to repair or prevent further cyber damage to the ship, while still refraining from hostilities. Here, the distinction between active cyber defences and passive defences may hold the answer. Active defences, sometimes referred to as "hack-backs", consist of operations taken outside one's network against an opposing network, but with a defensive intent: for example, disabling a portion of the network through which the cyber operation against you is conducted in order to prevent further intrusion. Passive defences such as firewalls, anti-virus programs and intrusion detection programs, however, occur entirely within one's own system and do not affect the enemy network. Because active cyber defences may include operations against opposing actors in the conflict, they are likely to be viewed as a continuation of hostilities. However, passive defences pose no such threat and are akin to trying to save a damaged ship from sinking. Whereas refraining from further hostilities includes no requirement that a crew stop trying to save a damaged ship, there is an obligation to refrain from acts that pose a threat to opposing forces. Therefore, ship commanders should be aware that taking active cyber measures to defend their ship's networks may prevent the crew from receiving protected status.

Finally, determining whether a crew is refraining from hostilities in this context will likely require some communication to other forces taking part in the engagement. Unfortunately, the same cyber event that damaged other critical systems may also have damaged the disabled ship's communications equipment. Although the 2017 Commentary suggests the time-honoured method of signalling surrender by lowering one's battle ensign or national flag – "striking the colours" – as a means of signalling the cessation of hostilities, most naval engagements of the future are likely to be fought at standoff range and visual signals may be of limited value.

Future considerations

Whereas many practical difficulties inhibit the determination of whether the crew of a ship disabled by cyber means should be afforded Article 12 protections, the 2017 Commentary suggests that it is clearly possible. GC II makes no requirement as to

25 *Ibid.*, para. 1390.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

how a crew becomes shipwrecked, and the Commentary stresses that the protections are quite broad. This difficulty does raise several interesting questions for naval forces who operate warships largely dependent on networked systems. These naval powers may need to retain non-digital methods of communication such as analogue radios or high-range visual systems which can indicate that a ship's crew is in peril and refraining from hostilities. If possible, these methods should be made known to opposing forces at the beginning of the conflict.

Commanders of ships belonging to States employing cyber methods in an attempt to disable enemy warships should be particularly attuned to the fact that, despite the lack of visible damage, there may be crews that are nonetheless entitled to protections should they become shipwrecked. Concerted cyber campaigns against warships in armed conflicts raise not just the potential for shipwrecks, but also the potential to take physical control over opposing warships by cyber means. This raises a host of legal questions, but one question specific to protections under GC II is the status of the crew in such a scenario. The potential for such "cyber captives" is addressed in the following section.

Cyber captives and Article 16

Those familiar with naval history, or even Patrick O'Brian's Aubry–Maturin series of novels, will know that the boarding and seizure of ships was a common feature of naval warfare in the Age of Sail.[26] However, modern naval conflicts more typically involve the sinking or disabling of ships as opposed to their capture. Although the standoff range of most modern weapons weighs against an imminent change of this situation, cyber warfare raises the question of capture once again. The previous section examined the question of whether a crew can be "shipwrecked" within the meaning of GC II for the purposes of Article 12 protections. This section takes that scenario one step further and examines the status of a crew on a ship commandeered by the enemy through cyber means.

Although probably more difficult from a technical standpoint, it stands to reason that if a ship could be completely disabled through an offensive cyber operation, those same networked systems could also be controlled by an outside entity. As previously mentioned, this possibility was demonstrated by the University of Texas researchers. Given the increasing reliance on network control of vital ship functions, a ship could theoretically be transformed into a remotely operated vessel, similar to other drone-type vehicles.[27] The first question to ask is whether the analysis differs from a ship disabled by cyber means. This could simply be a situation where the crew is "in peril" and, if they refrain from

26 See, generally, Brian Lavery, *Jack Aubrey Commands: An Historical Companion to the Naval World of Patrick O'Brian*, Naval Institute Press, Annapolis, MD, 2003.

27 Rolls-Royce, "Rolls-Royce Demonstrates World's First Remotely Operated Commercial Vessel", press release, 20 June 2017, available at: www.rolls-royce.com/media/press-releases/yr-2017/20-06-2017-rr-demonstrates-worlds-first-remotely-operated-commercial-vessel.aspx.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

hostilities, must be afforded Article 12 protections. However, if someone is in control of the ship and it is otherwise operating as normal, are they really "in peril"?

This question would be void if the crew decided either to abandon the ship or to disable it through mechanical means in order to prevent enemy forces from gaining control. However, assuming the crew chooses to stay on board the ship and not disable it through mechanical means, what is the status of the crew that remains on board but without control over the ship? Does the enemy's control over the ship result in a requirement to afford prisoner of war (PoW) protections to the crew? Article 16 states that "the wounded, sick and shipwrecked of a belligerent who fall into enemy hands shall be prisoners of war, and the provisions of international law concerning prisoners of war shall apply to them". Breaking that article down into its parts, we must first examine the phrase "wounded, sick and shipwrecked of a belligerent". It may be tempting to suggest that, at this point, the crew is not wounded, sick or shipwrecked, so Article 16 would not apply. However, the 2017 Commentary states that:

> Although in setting down who is a prisoner of war Article 16 uses the looser formulation 'the wounded, sick and shipwrecked of a belligerent' rather than the more technical terms used in Article 13, the definition of prisoners of war in the Second Convention is not meant to diverge from that in the Third Convention.[28]

Article 4 of the Third Geneva Convention (GC III) clearly states that "[p]risoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy";[29] this is interpreted to cover those "soldiers who became prisoners without fighting".[30] Essentially, this means that in whatever manner a sailor comes into the power of the enemy, regardless of being wounded, sick, or shipwrecked, they are then considered a PoW. Prior to the advent of cyber operations, falling into the "power of the enemy" was a fairly straightforward proposition and was difficult to imagine taking place without the physical presence of enemy forces. Whether, and how, a crew could come under the power of the enemy through purely cyber means, however, requires further analysis. Perhaps the determinative factor in the analysis is that of proximity and whether the physical presence of the enemy is required.

Capture and proximity of enemy forces

The primary difficulty here is understanding the phrase "who fall into enemy hands" and whether this is possible when the enemy is not physically present. The 2017 Commentary on GC II states that "the phrase 'fall into enemy hands'

28 2017 Commentary on GC II, above note 5, para. 1575.
29 Geneva Convention (III) relative to the Treatment of Prisoners of War of 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950), Art. 4.
30 Jean Pictet (ed.), *Commentary to the Geneva Conventions of 12 August 1949*, Vol. 3: *Geneva Convention (III) relative to the Treatment of Prisoners of War*, ICRC, Geneva, 1960, Art. 4.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

is sufficiently broad to cover capture or surrender".[31] Here, let us assume that although the ship in question has been commandeered by cyber means, the crew has neither chosen to leave the ship nor made an affirmative action of surrender. Although the 2017 Commentary suggests that "[n]o active 'capture' is necessary",[32] the enemy certainly seems to have captured the ship, so if the crew is unwilling or unable to abandon the captured ship, are they also captured? The updated Commentary makes no further definition, which is understandable. Capture without the physical presence of the enemy is a novel concept with few, if any, analogies.

One potential analogy is the case of aerial combat systems, such as helicopters or drones, when unaccompanied by ground forces. If the operator of an attack drone witnesses a group of enemy combatants with weapons dropped and waving a white flag, should those soldiers be considered *hors de combat* and no longer subject to attack?[33] This question was considered by the Harvard Program on Humanitarian Policy and Conflict Research (HPCR) Group of Experts in the *Manual on International Law Applicable to Air and Missile Warfare* (HPCR Manual), but was left unresolved as some members believed such a rule "could easily lead to misuse".[34] Although not expounded upon further in the HPCR Manual, the basic rule on surrender indicates that there would need to be some reason to suspect the surrender was not clearly expressed or was other than genuine.[35] This reading would be consistent with the ICRC Commentary to Additional Protocol I to the Geneva Conventions, which finds that an air force "can certainly have enemy troops in its power without being able, or wishing, to take them into custody or accept a surrender (for example, in the case of an attack by helicopters)".[36]

There seems to be little qualitative difference over the potential case of a helicopter having power over forces on the ground and the degree of control exercised over those aboard a remotely controlled ship at sea. It may be the case that the cyber operator with control over a ship at sea holds even greater power over the enemy than that of an aircraft over a defenceless group of soldiers on the ground. The crew of a ship they no longer control is subject to the whims of the ship's controllers while they remain on board the ship. The crew could potentially be driven into a perilous situation, or perhaps the gunnery controls could be manipulated to internally detonate the ship's munitions if the weapon

31 2017 Commentary on GC II, above note 5, para. 1568.
32 *Ibid.*, para. 1571.
33 For a definition of persons *hors de combat*, see Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005, Rule 47.
34 HPCR, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, 2010, comment accompanying Rule 15(b), para. 8.
35 Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I).
36 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987, para. 1612.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

systems control networks have been accessed. However, the case of cyber control over a ship remains distinct in that there is no physical presence. Thus, further analysis into the question of power and control is necessary.

Full and effective control

Given the difficulty of defining what is required for capture without the presence of enemy soldiers, it may be instructive to turn to a separate, but related, body of law: international human rights law (IHRL). Although this article does not delve into the controversial question of IHRL applicability in armed conflicts, IHRL can offer a useful example in analyzing what level of control is required for certain protective obligations to attach under international law. For example, the European Court of Human Rights (ECtHR) held in *Al-Skeini and Others v. The United Kingdom* that the European Convention on Human Rights applies extraterritorially either through the exercise of effective control over an area or through the exercise of control over a person by a State agent.[37] In an earlier case, *Medvedyev and Others v. France*, the Court had also held that human rights obligations attach to civilians on board a ship when military forces place the crew under guard and gain control of the ship's navigation, thereby exercising "full and effective" control.[38] In *Al-Skeini*, the ECtHR ruled that the "exercise of physical power and control over the person in question" was critical in establishing jurisdiction.[39]

Although "full and effective control" is a human rights concept and ECtHR case law is only applicable for States party to its governing convention, it illustrates that physical power and operational control of a ship's navigational functions are potential factors in determining what level of power is required by enemy forces before corresponding obligations are placed upon them. If that level of control can be obtained by the use of cyber means, then the crew should be considered as PoWs with the corresponding GC II Article 16 protections, requiring that "the provisions of international law concerning prisoners of war shall apply to them".

Potential obligations to cyber PoWs

Although the legal provisions regarding PoWs are primarily contained in GC III and are therefore not the focus of this article, the 2017 Commentary on GC II does comment on certain provisions. Of note, it states that "the time a person is held on board is limited to the absolutely necessary", referring to the GC III Article 22 requirement that prisoners be interned on land.[40] However, this does not necessarily mean a direct return to port. Rather, the determination is made based

37 ECtHR, *Al-Skeini and Others v. United Kingdom*, Appl. No. 55721/07, 2011, paras 133–140, available at: http://hudoc.echr.coe.int/eng?i=001-105606.
38 ECtHR, *Medvedyev and Others v. France*, Appl. No. 3394/03, 2010, paras 66–67, available at: http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-97979.
39 ECtHR, *Al-Skeini*, above note 37, para. 136.
40 2017 Commentary on GC II, above note 5, para. 1579.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

upon "what is 'expedient' in the 'circumstances'".[41] These circumstances include "operational reasons that do not permit a ship to change its course immediately".[42] There is nothing in this analysis that wholly precludes the possibility of combat operations while the crew remains aboard, although other areas of the law of naval warfare will play a role in this determination.[43]

Future considerations

If the potential exists for PoWs to be taken under such circumstances, what should navies do to prepare? First, navies looking to employ cyber operations to gain control over ships should formulate a plan of what to do with the crew if they remain on board. The Geneva Conventions place certain obligations on how they are to be treated, and States must understand how they will transfer the crew to a more appropriate facility fulfilling the requirements established in GC III.[44] Second, navies that employ networked systems would be wise to ensure there is a mechanism to immediately revert to mechanical control or formulate clear plans as to their operating procedures in the event of a successful cyber-attack in order to avoid situations where the status of the crew may come into doubt. An additional aspect of naval warfare that may see an increase in ambiguity with the advent of cyber operations is the determination of when a naval engagement has ended. This is a determining factor in judging when certain GC II obligations begin, and this subject is therefore taken up in the following section.

Article 18's end of engagements clause

On 27 May 1941, the British battleships *King George V* and *Rodney* engaged the German battleship *Bismarck*, which had been previously disabled by a torpedo attack from aircraft belonging to the British carrier *Ark Royal*. After almost two hours of fighting, the *Bismarck* and her 2,200-man crew were sunk, clearly marking the end of that particular naval engagement between the British and German navies. As the *Bismarck*'s escort ship, the *Prinz Eugen*, had previously detached, the shipwrecked crew was entirely dependent on the Royal Navy for rescue. The British ships *Dorsetshire* and *Maori*, acting in accordance with Article 16 of the 1907 Hague Convention (X) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention, began rescue of the German crew.[45]

41 *Ibid*., para. 1579.
42 *Ibid*., para. 1579.
43 For example, the prohibition on flying a false flag once the enemy is engaged, as presumably the crew aboard will not be changing the ensign. Louise Doswald-Beck (ed.), *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, Cambridge University Press, Cambridge, 1995, Rule 110.
44 GC III, Art. 12.
45 This article required, in part, that "[a]fter every engagement, the two belligerents, so far as military interests permit, shall take steps to look for the shipwrecked, sick, and wounded, and to protect them, as well as the dead, against pillage and ill-treatment".

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

However, after 110 sailors were rescued, a U-boat alarm was sounded, forcing the Royal Navy to break off the rescue. All but five of the remaining German crew were lost at sea.[46]

The legal obligation guiding the British rescue of the crew of the *Bismarck* was expanded upon in Article 18 of GC II. However, the extent of the obligation placed upon warship commanders to search for and collect the shipwrecked, sick and wounded following an engagement continues to be criticized as ambiguous and in need of clarification.[47] This section examines how the advent of cyber operations introduces an additional element of ambiguity.

Article 18 requires that "[a]fter each engagement, Parties to the conflict shall, without delay, take all possible measures to search for and collect the shipwrecked, wounded and sick, to protect them against pillage and ill-treatment, to ensure their adequate care, and to search for the dead and prevent their being despoiled". The 2017 Commentary rightly recognizes that "Article 18(1) is among the most important provisions in the Second Convention", and that it sets out the obligations flowing from the protections accorded in Article 12.[48] Although a detailed understanding of this article is key to a proper understanding of the entire convention, here we will look solely at the first element in the light of cyber operations.

Land versus naval obligations

Article 18 makes plain that, unlike land operations, the requirement to tend to the sick and wounded at sea does not arise until after the engagement.[49] This is understandable in the naval context given the increased risk of harm that a commander would face by breaking off an ongoing engagement to collect the shipwrecked, wounded and sick. As the 2017 Commentary notes, this obligation applies "without discriminating between their own and enemy personnel".[50] Furthermore, at the time of GC II's drafting, naval engagements tended to be very violent but short-lived affairs. In the case of the *Bismarck*, the engagement was clearly ended when the ship, though her ensign was never struck, went under the sea after two hours of fighting. However, for modern navies equipped with advanced long-range weapon systems, including cyber capabilities, the end of the engagement may be more difficult to discern.

The 2017 Commentary discusses Article 18's post-engagement limitation, finding that whereas this element may limit the obligation temporally, it may also

46 For an in-depth treatment of this particular engagement, see C.S. Forester, *Hunting The Bismarck*, Academy Chicago Publishers, Chicago, IL, 1983.

47 Peter Barker, "The Sea is Still Cruel – A Mariner's Perspective on Some Aspects of the Updated ICRC Commentary on the Second Geneva Convention", *Opinio Juris*, 16 November 2017, available at: http://opiniojuris.org/2017/11/16/the-sea-is-still-cruel-a-mariners-perspective-on-some-aspects-of-the-updated-icrc-commentary-on-the-second-geneva-convention/.

48 2017 Commentary on GC II, above note 5, para. 1617.

49 Article 15 of the First Geneva Convention requires that "[a]t all times, and particularly after an engagement, Parties to the conflict shall, without delay, take all possible measures …".

50 2017 Commentary on GC II, above note 5, para. 1618.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

expand the obligation's material scope.[51] It reasons that "since the particular engagement will have ceased, this may limit the extent to which a Party to the conflict may invoke security or military considerations as a justification for not undertaking search and rescue activities".[52] Thus, determining the exact scope of the temporal requirement takes on increased importance.

Temporal scope of engagements

Fortunately, the 2017 Commentary provides guidance on interpreting the temporal scope clause of Article 18. It provides that "the term 'engagement' is 'a battle between armed forces', i.e. involving the use of methods and means of warfare between military units of the Parties to the conflict".[53] Pre-empting the question of whether these methods and means are limited to the naval forces, the Commentary suggests that the term "engagement" "covers any kind of engagement, including from the air or from land but inflicting casualties at sea".[54] Cyber operations are not explicitly mentioned here, although "any kind of engagement" suggests that cyber operations are covered as well. However, it should be noted that States have been reticent to apply international law obligations to cyber operations in all contexts. Therefore, it is worth discussing whether the cessation of cyber operations, in addition to the conclusion of more traditional kinetic operations, is required to "end the engagement" and initiate potential Article 18 obligations.

First, the Commentary's suggestion that "inflicting casualties at sea" is required for an engagement is most likely poorly worded. It may be more correct to state that the operation has the *aim* of inflicting casualties at sea. It is easy to imagine that ships may be engaged prior to actually inflicting casualties. Prior to her own sinking, the *Bismarck* sunk the *HMS Hood* in large part by achieving the "weather gauge", manoeuvring to gain an advantageous position in relation to the enemy prior to opening fire. Therefore, simply because a cyber operation does not inflict casualties, this should not signal that a cyber operation related to a kinetic strike is not part of the overall engagement. However, whether cyber operations, absent the kinetic portion, can constitute an engagement or the continuance of an engagement is a slightly different matter.

Although the Commentary to Article 18 does not refer specifically to cyber operations, they are discussed in relation to the scope of application provisions of common Article 2, specifically whether cyber operations alone can constitute "armed force", making the Geneva Conventions applicable. The Commentary states that "[i]t is generally accepted that cyber operations having similar effects to classic kinetic operations" would suffice.[55] However, it also recognizes the current reality that cyber operations falling beneath this threshold are legally

51 *Ibid.*, para. 1648.
52 *Ibid.*, para. 1648.
53 *Ibid.*, para. 1655.
54 *Ibid.*, para. 1655.
55 *Ibid.*, para. 277.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

unsettled.[56] It is safe to say that cyber operations achieving a kinetic effect would therefore continue the engagement. But what of those cyber operations that affect network systems without achieving kinetic effects? This may again be determined by whether the cyber operation is a precursor, or enabler, of follow-on kinetic operations that intend to "inflict casualties".[57]

Until such time as the *jus in bello* develops more fully in this area, it may be necessary to leave the legal reasoning as to whether the engagement has ended to a good-faith assessment by the ship's commander. Although this seems initially unsatisfying, it is consistent with the Commentary's understanding of Article 18, which states that "[w]hat constitutes an engagement in any given case will remain context-specific" and that "those acting on behalf of the Party to the conflict, each at his or her own level of decision-making, will need to make a good-faith assessment as to the moment it becomes possible to take one or more of the measures referred to in Article 18".[58] Such "good-faith assessments" are a common and necessary part of international humanitarian law (IHL), even if open to occasional abuse.

Future considerations

Given the potential for abuse, what are nations employing cyber operations as part of naval conflicts to do? Parties to a conflict still have a vested interest in ensuring that the shipwrecked, sick and wounded are recovered and cared for as quickly as possible. The Commentary once again provides a potential solution, suggesting that opposing commanders reach a "special agreement" on the rescue of those shipwrecked in the sense of Article 6,[59] allowing parties to fulfil Article 18 obligations without fear of attack, adding that "such an agreement may be concluded orally, between commanders on the spot".[60] Alert commanders will be sure to add prohibitions on offensive cyber operations as part of any such agreement. Another area of naval warfare that benefits from increased coordination between the parties is the use of hospital ships and rescue craft. Although the vital function served by these vessels is widely recognized, their use has nonetheless been marred by repeated tragedies.

Cyber operations and obligations to "respect and protect"

The use of hospital ships and rescue craft in wartime has always been a contentious issue. These ships serve a humanitarian need recognized by most parties, and have

56 *Ibid.*, para. 278.
57 For a general discussion of cyber operations and the scope of IHL applicability, see Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0), Rule 80.
58 2017 Commentary on GC II, above note 5, para. 1655.
59 Specifically, Article 6 states that "the High Contracting Parties may conclude other special agreements for all matters concerning which they may deem it suitable to make separate provision".
60 2017 Commentary on GC II, above note 5, para. 1651.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

therefore been afforded protections similar to those given to the shipwrecked and wounded.[61] However, profound suspicion of their misuse has led to many attacks against these protected vessels, particularly during the First and Second World Wars. Although some attacks resulted from misidentification, many were quite intentionally targeted.[62] Unrestricted maritime warfare campaigns often included deliberate attacks on hospital ships. One such example was the Soviet hospital ship, the *Armenia*.[63] On 7 November 1941, a German torpedo bomber attacked the *Armenia*, sinking her without warning. All but eight of the 7,000 on board died in the attack.

Although this was a tragedy by any measure, there were several questions as to the *Armenia*'s status as a hospital ship. It was clearly marked with large red cross symbols and, at the time, was certainly being used to transport the sick and wounded. However, it also had light anti-aircraft weapons on board, was under armed escort, and had previously been used in the conflict to transport military supplies. This tragic incident, and many others like it, demonstrated the need to clarify and progress the rules related to the protection of hospital ships in GC II. This section analyzes the obligation to "respect and protect" hospital ships and coastal rescue craft found in Articles 22, 24 and 27 of GC II, in the light of cyber operations. Hospital ships are those "ships built or equipped by the Powers specially and solely with a view to assisting the wounded, sick and shipwrecked, to treating them and to transporting them",[64] whereas coastal rescue craft are "small craft employed by the State or by the officially recognized lifeboat institutions for coastal rescue operations".[65] However, the protections afforded to both are substantially the same and will be discussed below.

Attack and capture

First, it should be stated that Article 22's obligation to respect and protect includes the more specific language that protected vessels should "in no circumstances be attacked or captured". Although the obligation to respect and protect is broader than these specific terms, it is helpful nonetheless because "attack" is an IHL term of art that has been frequently analyzed in the cyber context. The 2017 Commentary explicitly states that the prohibition on attack includes "the use of means and methods that, by whatever mechanisms or effects, severely interfere with the functioning of the equipment necessary for the operation of a military hospital ship, such as so-called 'cyber-attacks'".[66] Given that the Commentary

61 Article 22 of GC II, for example, provides that hospital ships "may in no circumstances be attacked or captured, but shall at all times be respected and protected".

62 See, e.g., a statement by the German government in the First World War that it would "no longer suffer any hospital ship in the English Channel or parts of the North Sea": Lassa Oppenheim and Ronald Francis Roxburgh, *International Law: A Treatise*, Vol. 2: *War and Neutrality*, 3rd ed., Longmans, London, 1921, p. 287.

63 Rupert Colley, *World War Two: History in an Hour*, London, Harper Collins, 2013.

64 GC II, Art. 22.

65 GC II, Art. 27.

66 2017 Commentary on GC II, above note 5, para. 1985.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

references the *Tallinn Manual on the International Law Applicable to Cyber Warfare*'s (Tallinn Manual) Rule 70 here (incorporated into the Tallinn Manual 2.0 as Rule 131),[67] it is helpful to follow the reference for further analysis.[68]

The black-letter rule in the Tallinn Manual 2.0, Rule 131, states that medical personnel and transports, including those vessels identified in GC II, "may not be made the object of a cyber attack". Here we should recall that "cyber attack" is the exact phrase used in the Commentary, though it does not define the phrase. The Tallinn Manual 2.0's Rule 92 defines a cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction of objects". It is well understood that the Tallinn Manual 2.0 is only the opinion of a group of experts and is therefore not a binding source of primary law. However, Rule 92's definition tracks with the Additional Protocol I definition of attack, requiring "acts of violence against the adversary".[69] Thus, the 2017 Commentary and the Tallinn Manual 2.0 appear to agree that cyber operations resulting in injury or death, and (at least) physical damage and destruction, to a protected crew or vessel are prohibited. The logical follow-on question is whether "damage" to a network system includes the pure loss or degradation of functionality. The law here is unsettled, and thus the loss of functionality, on its own, cannot be read definitively to qualify as an attack.[70]

Respect and protect

The 2017 Commentary and the Tallinn Manual 2.0 agree that the requirement to respect and protect goes beyond the prohibition against attack. The Commentary summarizes the extended obligation to respect and protect in para. 1996 as the obligation "to refrain from all actions that interfere with or prevent such ships from performing their humanitarian tasks". Therefore, cyber operations are prohibited that result in loss or degradation of network functionality necessary to a protected vessel's performance of its humanitarian function.

The Commentary does include a qualifier to that protection, referencing the Article 31 allowance for parties to the conflict to "control and search the vessels mentioned in Articles 22, 24, 25 and 27".[71] This includes the right to "control the use of their wireless and other means of communication" and "put on board their ships neutral observers who shall verify the strict observation of the provisions contained in the present Convention". These "control and search" provisions are in place "to verify whether their employment conforms to the provisions of Articles 30 and 34 and to the other provisions of the Convention", as the 2017 Commentary puts it.[72] Recognizing that a physical presence is no

67 Tallinn Manual 2.0, above note 57, Rule 131.
68 See also Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", *International Review of the Red Cross*, Vol. 94, No. 886, 2012, pp. 556–560.
69 AP I, Art. 49.
70 Tallinn Manual 2.0, above note 57, comment accompanying Rule 92, para. 10.
71 2017 Commentary on GC II, above note 5, para. 1996.
72 *Ibid.*, para. 2276.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

longer required to verify compliance, it also suggests that "innocent employment of these vessels can often be ascertained by other means, at least to some extent, in particular by satellites and other means of reconnaissance".[73] This could indicate that cyber intelligence operations are appropriate if, while not affecting the functionality of the vessel, they are used to verify its compliance with GC II. Indeed, this was the conclusion drawn by the Tallinn Manual's Group of Experts in the commentary to Rule 132, governing the requirement to respect and protect computer systems related to medical units and transports.

Future considerations

This analysis leaves open questions regarding several potential categories of cyber operations – for example, cyber intelligence operations not for the purpose of compliance verification, but rather for the collection of intelligence regarding associated forces. Another potential category is the use of protected naval vessels as a pass-through to levy cyber effects against non-protected enemy systems. These and other examples may not explicitly violate the terms of protection in GC II, but they nevertheless open the possibility of protected vessels becoming a cyber battleground. This could divert protected vessels from focus on their missions and raise the likelihood of unintentional damage to network systems vital to the performance of their humanitarian mission. Given the ambiguity present in this aspect of the law, and the importance of protecting humanitarian missions, perhaps the obligation to respect and protect is an area where nations can work together to develop ever-elusive cyber norms.

Conclusion

Modern naval powers are awakening to the fact that, despite being a somewhat "closed system", warships are not immune to malicious cyber operations. The advantages to be gained in efficiency and performance through network control of ship systems are clear. Electrical, propulsion, steering and life-support systems all benefit from SCADA and other network controls. The result is that ships require smaller crews while levying increased combat power. However, these same systems introduce critical vulnerabilities. Future conflicts between naval powers will undoubtedly include cyber operations, and such operations will target these critical network control systems.

Given that the ability to target these critical systems has already been demonstrated, States must begin thinking though the legal ramifications of offensive cyber operations on the law of naval warfare. Much of this law is contained within GC II. With the recent release of the updated 2017 Commentary and its recognition of military cyber operations, the present is the perfect time for States to begin this analysis. This article has identified four areas

73 *Ibid.*, para. 2277.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press

of rights and obligations contained in GC II where cyber operations may have a significant impact, and has discussed some considerations for States in preparing for such a scenario.

First, the article considered the question of shipwrecks and whether a crew could be considered shipwrecked as the result of a cyber operation against their ship. This article reached the conclusion that this was a very real possibility under the law, that States should work through scenarios to indicate a cessation of hostilities in such a situation, and that opposing ships should be prepared to recognize that these shipwrecked crews must be afforded the corresponding protections. Second, the article presented the possibility that a ship's crew could fall into the power of the enemy as the result of an adversary gaining remote control over the ship. Again, technological advancements have demonstrated the potential to take control of vital ship functions, making the legal question quite relevant. Should the level of control over the ship result in the crew falling into the power of the enemy, the party gaining control over the ship must be prepared to deal with the crew as PoWs. Thirdly, the article analyzed the "end of engagements" clause in Article 18 of GC II. This vitally important clause signals when the obligation to search for, collect and protect the shipwrecked, wounded and sick attaches. Ongoing cyber operations could potentially extend an engagement past the cessation on kinetic operations, with a deleterious effect on those shipwrecked, wounded and sick. States would be wise to take this consideration into account when determining whether to continue cyber operations against an adversary. The final section contemplated the impact of cyber operations on the use of hospital ships and rescue craft. The somewhat anomalous legal position of these ships has resulted in severe consequences in past conflicts. The ways in which cyber operations further complicate their status must be reviewed by States in order to prevent future disasters. As the purpose of these ships remains entirely humanitarian, perhaps this is an area where coordination and understandings between navies may occur.

Although it is certain that cyber operations will be part of future conflicts, the extent to which these operations will succeed is unknown. However, as States will certainly attempt such operations, they must also prepare for the protections and obligations that the law of naval warfare will impose upon them should they succeed. With the 2017 Commentary providing a step forward in our understanding of GC II, this is a perfect time to start making such preparations.

https://doi.org/10.1017/S1816383119000055 Published online by Cambridge University Press