INTERNATIONAL LAW STUDIES
Est. 1901
U.S. NAVAL WAR COLLEGE

Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations

Jann K. Kleffner and Heather A. Harrison Dinniss

89 INT'L L. STUD. 512 (2013)

Volume 89 2013

Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations

Jann K. Kleffner and Heather A. Harrison Dinniss[*]

I. INTRODUCTION

In recent years it has become an oft-cited truism that the majority of twenty-first century armed conflicts will contain a cyber element. The 2008 conflict between Russia and Georgia was the first publically available indicator of how cyber and conventional force might be used together in an inter-State conflict.[1] Beyond such a relatively clear-cut instance of full-blown international armed conflict, many ongoing situations of crisis, both below and above the level of armed conflict, have attracted a significant and persistent cyber component. Examples include the cyber intifada between Israeli and Palestinian hackers, which has continued since the increase in violence at the outset of the second intifada in 2000; the dispute

* Jann K. Kleffner, Head of the International Law Centre, Associate Professor of International Law, Swedish National Defence College; Heather A. Harrison Dinniss, Postdoctoral Research Fellow, International Law Centre, Swedish National Defence College. The authors gratefully acknowledge the research assistance of Lisen Bergqvist.

1. It should be noted that the attacks against Georgia were not attributed to the Russian Federation, but rather to so-called "patriotic hackers." Analysts did note, however, the high degree of coordination between the actions of the conventional armed forces and the targets of the cyber attacks. For a summary of the reports on the cyber incidents, see ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010).

between India and Pakistan over Kashmir, which has an ongoing and pernicious cyber element involving groups on both sides with varying degrees of alleged State sponsorship; and the Arab Spring, in which many of the States involved used a variety of Internet surveillance, monitoring, censorship and control techniques, and in some cases—notably Tunisia and more recently Syria—hacked the accounts and Internet content of individuals engaged in the revolution.[2]

At the same time, there is a discernible trend on the part of the UN Security Council to authorize various forms of peace operations tasked with an array of functions that are deployed into situations of armed conflicts and other crises. A combination of both trends—the increase of conflict and crisis situations with a cyber component and the deployment of complex peace operations—makes it only natural to assume that peacekeepers will increasingly find themselves on missions in which cyber incidents will occur during, following or even in the absence of, conventional hostilities. Indeed, recent reports have raised the concept of stand-alone cyber peacekeepers. The suggestion that the United Nations should employ specific personnel to deal with the increasing number of cyber incidents taking place between States is indicative of the relevance of cyber operations for the conduct of UN-mandated peace operations.[3] Although the feasibility of cyber-only peacekeeping occurring outside the context of a military operation has been largely dismissed by technical experts,[4] from a purely legal perspective it would certainly be within the purview of the Security Council to determine that cyber operations (whether in a specific situation or as a more general concept) amount to a threat to international peace and security under Article 39 of the UN Charter and to authorize those actions that it considers appropriate.[5]

---

2. BEN WAGNER, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE EUROPEAN UNION, AFTER THE ARAB SPRING: NEW PATHS FOR HUMAN RIGHTS AND THE INTERNET IN EUROPEAN FOREIGN POLICY 6–13 (2012); Ben Brumfield, *Computer Spyware is Newest Weapon in Syrian Conflict*, CNN (Feb. 17, 2012, 4:41 PM), http://www.cnn.com/2012/02/17/tech/web/computer-virus-syria.

3. Susan Watts, *Call for Cyberwar "Peacekeepers" Force*, BBC NEWS (Jan. 26, 2012, 17:40 GMT), http://news.bbc.co.uk/2/hi/programmes/newsnight/9687338.stm.

4. Ellyne Phneah, *Idea of Cyber Peacekeepers Premature, "Redundant,"* ZDNET NEWS (Feb. 6, 2012, 10:35 GMT), http://www.zdnet.com/idea-of-cyber-peacekeepers-premature-redundant-2062303742/.

5. *See generally* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 109–13 (2012).

What then are the legal parameters governing peace operations with regard to ongoing cyber threats? Do peacekeepers' responsibilities extend to monitoring cyber threats? When may a peace operation be mandated to conduct cyber operations? How may peacekeepers respond to a cyber attack against them? Are there any legal constraints on a troop-contributing State conducting cyber operations outside the mission area? These are some of the pertinent questions that arise. Answering them from an international law perspective will very much depend on the specifics of the cyber threat, the precise mandate of the peace operation and the operational cyber capabilities of troop-contributing States, among other considerations. We will, therefore, approach the issue in the following manner. First, we will briefly set the general context by defining and describing contemporary peace operations. We will then address the general law applicable to peace operations. Finally, we will discuss the potential types of cyber operations and the legal challenges they pose in more detail.

II. PEACE OPERATIONS DEFINED

For the purposes of this article, peace operations may be defined broadly to include not only traditional peacekeeping operations based on the three core principles of consent, impartiality and the use of force only in self-defense and defense of the mandate, but also peace enforcement operations authorized under Chapter VII of the UN Charter and peace building operations. Chapter VII enforcement differs fundamentally from other peace operations in that it does not require the consent of the target State or entity, and need not be impartial, reactive or restricted to defensive measures.[6] Of particular importance in the cyber context, enforcement measures may also be directed against non-State entities that are deemed to pose a threat to international peace and security. Whether authorized by the Security Council under Chapter VI or VII of the Charter (or under Chapter VIII in the case of regional peacekeeping operations), the legitimacy of the operation flows from the Council's primary responsibility for the maintenance of peace and security, which may be carried out by means of the mandate.[7]

---

6. Terry D. Gill, *Legal Characterisation and Basis for Enforcement Operations and Peace Enforcement Operations under the Charter*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS 85 (Terry D. Gill & Dieter Fleck eds., 2010).

7. *Id.* at 138.

Peace operations have changed dramatically since they began in 1948. In addition to the introduction of enforcement operations in ongoing conflicts, even traditional peacekeeping operations have expanded into complex and multi-dimensional operations. Long established responsibilities of peacekeepers, such as monitoring ceasefires, are now supplemented by tasks which include, *inter alia*, the promotion of a stable environment, maintenance of public order, provision of humanitarian assistance, and protection of civilians from violations of humanitarian and human rights law to the extent possible under the terms of the mandate and the operational capabilities of the particular mission.[8] In future operations, all of these tasks may include a cyber component. The utility of cyber operations in more robust peace operations, including peace enforcement operations, is also apparent. For example, the ability to prepare the battlespace, neutralize networks and uncover and obtain documentary evidence will be useful tools in carrying out particular operations. The type of operation and its constituting mandate are important in determining what cyber operations can be undertaken by a mission.

III. LAW APPLICABLE TO PEACE OPERATIONS

The conceptual underpinning of, and the law applicable to, each type of operation depends on a complex interaction of general international law, human rights law, international humanitarian law and the domestic laws of both the host and troop-contributing States. However, the essential distinction in determining the applicable international legal framework is between those peace operations that fall below the threshold of armed conflict, for which the primary legal framework governing the operation (and any cyber operations which form part of it) is human rights law, and those which occur above that threshold. For operations occurring above the threshold, the law of armed conflict may apply.

A. The Mandate

The principal legal parameter determining the permissibility of actions taken by a peace operation is the mandate established by the Security Council.

8. UNITED NATIONS DEPARTMENT OF PEACEKEEPING OPERATIONS & UNITED NATIONS DEPARTMENT OF FIELD SUPPORT, UNITED NATIONS PEACEKEEPING OPERATIONS: PRINCIPLES AND GUIDELINES 24 (2008), *available at* http://pbpu.unlb.org/pbps/library/capstone_doctrine_eNg.pdf [hereinafter Capstone Doctrine].

It may range from a limited mandate to monitor a peace agreement or ceasefire to a more ambitious one that includes tasks such as protection of civilians, creating a safe and secure environment and training of both civilians and armed forces.[9]

Under Article 41 of the Charter, the Security Council may also mandate non-forceful measures be taken in situations it deems to be a threat to the peace, breach of the peace or act of aggression. Such enforcement measures may include, *inter alia*, partial or total disruption of telecommunications which may well contain a cyber element. Although authorized under Chapter VII and thus not requiring the consent of the host State, such operations fall somewhere between traditional peace operations and the more robust peace enforcement operations that have become common in recent years. Needless to say, not all cyber operations can be treated alike; those which would amount to a use of force would not fall within any mandate provided under Article 41. Whether a cyber operation amounts to a use of force or remains below that threshold raises issues identical to those discussed elsewhere in the present volume.[10]

B. Human Rights

For peace operations falling beneath the threshold of armed conflict, the primary legal paradigm is that of human rights. This includes both peacekeeping operations conducting the more traditional tasks for which the use of force is a last resort in personal and unit self-defense or defense of the mandate, and those authorized under Chapter VII for which the right to use "all necessary means" is authorized, but in which peacekeepers are not involved as combatants in an armed conflict.

Peace operations below the armed conflict threshold may, for instance, involve monitoring the implementation of, and compliance with, a peace agreement, or providing security in a post-conflict environment. In these cases, the international legal framework governing cyber operations is in-

9. For a good illustration of an ambitious mandate, see the United Nations Mission in the Democratic Republic of Congo (MONUC) mandate, containing by some counts no less than forty-nine different tasks for the operation. S.C. Res. 1565, U.N. Doc. S/RES/1565 (Oct. 1, 2004) and resolutions and documents referenced therein [hereinafter MONUC Mandate].

10. *See, e.g.,* William Banks, *The Role of Counterterrorism Law in Shaping* ad Bellum *Norms for Cyber Warfare*, 89 INTERNATIONAL LAW STUDIES 157 (2013); Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, *id.* at 406; Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, *id.* at 252.

ternational human rights law to the extent that the operation's functions are being exercised in a way that can be equated with the exercise of jurisdiction by a State.[11] States are bound by both international conventions and customary international human rights law. Several court decisions and quasi-judicial determinations have held that States' human rights law obligations do not automatically cease to apply in extraterritorial peace operations, provided that jurisdiction is exercised.[12]

Admittedly, there is no universal consensus on this question. The United States is one of the prominent opponents of the extraterritorial application of human rights law. However, both universal and regional human rights bodies, as well as a significant number of individual States have accepted—or have had to accept—that human rights law does not automatically cease to apply when operating beyond the State's borders. Although the question of when a State exercises extraterritorial jurisdiction has been addressed in numerous cases under the different human rights instruments, it will not be addressed in detail in this article beyond noting that the test may generally be seen as one of effective control over territory, or authority and control over persons.[13]

International organizations such as the United Nations are also bound by customary international law, including human rights law. As with States, if and when an international organization exercises effective control over territory or physical control over one or more persons, the international organization is bound to respect the human rights of those who find themselves within its jurisdiction. In the case of the United Nations, the binding force of international human rights law flows from its international legal personality, and is further strengthened by the UN Charter, the UN Safety Convention,[14] and their internal rules and practice.[15]

---

11. Jann K. Kleffner, *Human Rights and International Humanitarian Law: General Issues*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 67.

12. The International Court of Justice, UN Human Rights Committee, European Court of Human Rights and Inter-American Commission on Human Rights have each found that their instruments apply extraterritorially on the basis of jurisdiction.

13. *See generally* MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011); Ola Engdahl, *The Future of Human Rights Law in Peace Operations*, *in* LAW AT WAR: THE LAW AS IT WAS AND THE LAW AS IT SHOULD BE 105 (Ola Engdahl & Pål Wrange eds., 2008).

14. Convention on the Safety of United Nations and Associated Personnel, Dec. 9, 1994, 2051 U.N.T.S. 363 [hereinafter UN Safety Convention].

Cyber operations carried out in the context of peace operations below the threshold of an armed conflict are thus governed by such human rights law provisions as the right to privacy, freedom of expression, freedom of association, etc., provided that the person whose rights are at issue finds himself or herself within the jurisdiction of the international organization or troop-contributing State. While the legal basis to conduct cyber operations may stem from the authorization in the Security Council resolution or from self-defence, the actual conduct of such operations is subject to the constraints of human rights law. The UN Human Rights Council has confirmed that "the same rights people have offline must also be protected online."[16] In other words, if jurisdiction is being exercised in a peace operation and it is considered necessary to gather intelligence or conduct operations in the cyber realm—for example, in order to prevent so called "spoilers" from reigniting an armed conflict or to prevent online postings that incite racial hatred—interference with cyber infrastructure or data must be carried out in compliance with the requirements of human rights law.

C. Law of Armed Conflict

When a peace operation involves the conduct of hostilities with a State or organized armed group that crosses the threshold of armed conflict, the law of armed conflict applies. The applicability of that body of law was confirmed in the UN Secretary-General's Bulletin, "[o]bservance by UN Forces of International Humanitarian Law," which sets out the fundamental principles and rules applicable to UN peacekeepers.[17] The bulletin's importance has been reemphasized in "United Nations Peacekeeping Operations: Principles and Guidelines," also referred to as the Capstone Doctrine.[18]

---

15. Kleffner, *supra* note 11, at 67. As examples, Article 1(3) of the UN Charter, which establishes promotion and encouragement of respect for human rights as one of the purposes of the organization, and Decision No. 2005/24 of the Secretary-General's Policy Committee on Human Rights in Integrated Missions, which directs that human rights be fully integrated into peace operations and that all human rights functions be coordinated by one component. Capstone Doctrine, *supra* note 8, at 14, 27.

16. U.N. Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, ¶ 1, U.N. Doc. A/HRC/20/L.13 (2012).

17. U.N. Secretary-General, *Secretary-General's Bulletin: Observance by United Nations Forces of International Humanitarian Law*, U.N. Doc. ST/SGB/1999/13 (Aug. 6, 1999).

18. Capstone Doctrine, *supra* note 8, at 15–16.

While there is little debate over the application of the law to the troops on the ground, a question does remain concerning which entity becomes the party to the armed conflict—the troop-contributing State, the responsible international organization (whether the United Nations, NATO, etc.) or both.[19] Likewise, the determination of whether and for what time the relevant legal actor is to be considered a party to an armed conflict involves complex issues of fact and law that must be determined on a case-by-case basis in light of the factual environment and the operationalization of the mandate for the specific operation within that environment. Some of the factors to be taken into account include, *inter alia*:

- relevant Security Council resolutions;
- specific operational mandates;
- roles and practices actually adopted by the operation during the conflict;
- rules of engagement and operational orders;
- nature of the arms and equipment used by the force;
- interaction between the operation's forces and the parties involved in the conflict, including any use of force between the operation's forces and the parties in an armed conflict, and the nature and frequency of such force; and
- the conduct of the alleged victim(s) and their fellow personnel.[20]

Similarly, whether individual members of a peace operation directly participate in hostilities requires a case-by-case assessment of whether the required threshold of harm, causation and belligerent nexus exists.[21]

Operations in which the hostilities amount to an armed conflict solely between a peace operation and an adversary, with no other parties involved, will be fairly exceptional. It is more likely that a peace operation will be deployed into an ongoing armed conflict or into a volatile situation that then deteriorates into an armed conflict. As it is not a party to the con-

19. For a more detailed examination of the question than is possible in this article, see Ola Engdahl, *Multinational Peace Operations Force Involved in Armed Conflict: Who Are the Parties?*, *in* SEARCHING FOR A "PRINCIPLE OF HUMANITY" IN INTERNATIONAL HUMANITARIAN LAW 233 (Kjetil M. Larsen et al. eds., 2012).

20. *Cf mutatis mutandis* Prosecutor v. Sesay, Kallon and Gbao, Case No. SCSL-04-15-T, Trial Chamber Judgment, ¶ 234 (Special Court for Sierra Leone Mar. 2, 2009).

21. *See generally* NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION UNDER INTERNATIONAL HUMANITARIAN LAW (2009).

flict, in these situations the peace operation cannot, without more, conduct military operations that would be subject to the law of armed conflict, nor can it be made the object of attack, whether through cyber means or otherwise. The right to conduct operations governed by the law of armed conflict requires that the peace operation be a party to the armed conflict. If it is not, its members enjoy the protection that international law provides to civilians, as well as the specific protections provided by the UN Safety Convention.

Finally, although controversial and the subject of much scholarly debate, the law of occupation may also apply to peace operations in certain circumstances, whether *de jure* or by analogy.[22] It is sufficient for the purposes of this article to note that territory is only considered occupied when it is *actually* placed under the authority of the occupying force and the law extends only to the territory where that authority has been established and can be exercised.[23] While cyber operations may be used in exercising an occupying power's authority, they would not be sufficient on their own to establish an occupation.[24] Thus, the use of cyber operations to project the execution of a peace operation's mandate into areas outside its effective physical control, for example, by monitoring communications, would not extend the application of the law of occupation to those areas.

We now turn to a more detailed analysis of the general legal framework applicable to different types of cyber operations and the different contexts in which such cyber operations may occur. These scenarios are: first, deployment of a peace operation into a situation of ongoing cyber operations between third parties; second, the use of force by a peace operation in response to cyber attacks; third, cyber operations conducted by a peace operation to protect civilians under imminent threat of physical violence; and, fourth, the conduct of offensive cyber operations by peace operations. Although these different scenarios may overlap to a certain extent, they raise distinct legal issues; hence, they will be treated separately.

---

22. *See, e.g.*, Tristan Ferraro, *The Applicability of the Law of Occupation to Peace Forces*, *in* INTERNATIONAL HUMANITARIAN LAW, HUMAN RIGHTS AND PEACE OPERATIONS 133 (Gian L. Beruto ed., 2008).

23. Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land art. 42, Oct. 18, 1907, 36 Stat. 2227 [hereinafter Hague Regulations].

24. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE ch. VI cmt. ¶ 3, at 196 (Michael N. Schmitt ed., 2013).

IV. SITUATIONS WHERE THERE ARE ONGOING CYBER OPERATIONS

When peacekeepers find themselves deployed in a situation in which there are ongoing cyber operations between third parties (State-based or otherwise), the mission's obligations and authority with regard to their response to those acts will be dependent on its mandate. However, some general observations may be made.

Clearly, when a peace operation is specifically tasked with acting in situations where there are ongoing cyber operations, it will be authorized to monitor and conduct cyber operations in response to cyber threats. Given the differing capabilities of troop-contributing States in terms of expertise and equipment, however, it seems likely that any specific requirement will contain caveats in terms of acting within the mission's capabilities and resources.[25]

A more likely—and perhaps more interesting—scenario may occur when a peace operation is tasked by the Security Council with deploying into an ongoing security situation that contains a cyber element, but where the mandate does not expressly refer to cyber operations.[26] For example, two of the traditional tasks of peacekeeping operations have been to promote a safe and secure environment and create the conditions for a lasting political solution to a conflict through the monitoring of a ceasefire and the parties' adherence to their commitments under the agreement. In such a case, the generic mandate may be interpreted broadly enough to include the monitoring of Internet traffic, as well as monitoring activities in physical space; however, the permissible methods used to perform those tasks will differ depending on the robustness of the mandate and the level of the

25. Similar wording is currently used with respect to protection of civilians in other peace operations. See, for example, MONUC, which is authorized "*within its capabilities* and in area where its armed units are deployed . . . to ensure the protection of civilians." S.C. Res. 1592, ¶ 5, U.N.Doc. S/RES/1592 (Mar. 30, 2005) (emphasis added). The initial instructions to the African Union mission in Darfur provided that it was to "[p]rotect civilians whom it encounters under imminent threat and in the immediate vicinity *within resources and capability*." Communiqué, Peace and Security Council (Oct. 20, 2004), *available at* http://www.africa-union.org/news_events/Communiqu%C3%A9s/Communiqu%C3%A9%20_Eng%2020%20oct%202004.pdf (emphasis added).

26. This article will restrict itself to the use of technology for monitoring cyber operations. For a discussion of some of the issues raised by intrusive intelligence gathering in peacekeeping operations, see Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICHIGAN JOURNAL OF INTERNATIONAL LAW 687 (2007); A. Walter Dorn, *The Cloak and the Blue Beret: Limitations on Intelligence in UN Peacekeeping*, 12 INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTERINTELLIGENCE 414 (1999).

threat. For example, although all data traffic coming into and out of the mission's networks can be monitored as a matter of good network security, the permissibility of using particular technologies, such as deep packet inspection (DPI),[27] outside of the mission's own networks depends on whether the applicable law permits those actions.

As noted above, both troop-contributing States and the United Nations must comply with human rights law in peace operations in areas subject to their jurisdiction. In the scenario of conducting DPI, the human rights of privacy and freedom of expression come to the fore. Neither of these rights are absolute. International human rights law permits certain interferences with them for reasons of national security and public order.[28] Such exceptions are subject to proportionality requirements. Thus, the parameters established for the use of DPI technology would need to be carefully thought through to avoid casting too wide a net.[29]

It should also be noted in considering multinational operations that in addition to differing approaches to the extraterritorial application of human rights law, judicial approaches to the use of DPI technologies also vary depending on the domestic jurisdiction. The United States and European Union member States, for example, have adopted different standards. Ongo-

---

27. Deep packet inspection involves looking at the content of the packets of information that make up a data stream, rather than merely the TCP/IP routing information contained in the header of the packet. While there are legitimate uses for deep packet inspection that could be valuable to a UN mission (for example, prioritizing particular kinds of data traffic, e.g., Skype), any use that makes the content of the packet available to someone other than the sender and receiver of the message may risk infringing the right to privacy by arbitrarily interfering with communications. Additionally, European Union (EU) member States may run afoul of the EU framework directive on privacy and electronic communications and the EU data protection directive. Directive 95/46/EC of the European Parliament and of the Council (Oct. 24, 1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

28. *Cf.* Article 19(3)(b) of the International Covenant on Civil and Political Rights (ICCPR). International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (Dec. 16, 1966), 999 U.N.T.S. 171. Although Article 17 on the right to privacy contains no explicit reference to exceptions on grounds of national security and public order, it allows for such exceptions, provided an interference with a person's privacy is neither arbitrary nor unlawful.

29. In the words of the Human Rights Committee, restrictions on the right of freedom of expression "must be 'provided by law' [and they] may only be imposed for one of the purposes set out in subparagraphs (a) and (b) of paragraph 3; and they must be justified as being 'necessary' for . . . one of those purposes." Human Rights Committee, General Comment No. 10: Freedom of Expression (Art. 19), U.N. Doc. HR1/GEN/1/rev.1 (June 29, 1983).

ing court cases are in the process of determining the contours of the right of government entities to engage in such behaviors. While the law remains far from settled at the time of this writing, rules of engagement for peace operations deployed in situations where there are ongoing cyber operations should be drafted in such a manner that the permissible limits on the use of DPI or other Internet surveillance technologies are clear. It makes no difference whether the peace operation is conducted with the consent of the host State or the Security Council has authorized the use of "all necessary means" as the rights' holder is the individual. While a Chapter VII mandate would allow States to claim legal authority for surveillance or interception, it is likely that most complaints regarding this technology would relate to the alleged arbitrariness of the surveillance or interception. Differences in interpretation may then be reflected in the national caveats of the troop-contributing States.

Once the applicable law for a peace operation has become the law of armed conflict, the problem is significantly alleviated. Although human rights law continues to apply during armed conflict,[30] the law of armed conflict permits the employment of those measures necessary for obtaining information about the enemy.[31] In fact, parties to an armed conflict are obliged to do so in order to meet the required precautions in attack. Such specific regulations in the law of armed conflict would prevail over the more generic conflicting rules of human rights law (*lex specialis derogat lege generali).*

V. USE OF FORCE IN RESPONSE TO CYBER ATTACKS

Despite the protections afforded to UN personnel,[32] peace operations have increasingly come under attack from those seeking to derail fragile peace processes or manipulate hostile environments for their own purposes. While there is no public record to date on the use of cyber attacks against UN peace operations specifically, other UN organs and the armed forces

30. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (July 8); Legal Consequences of the Construction of Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9).

31. Hague Regulations, *supra* note 23, art. 24.

32. Protection of UN peacekeepers may stem from their status as civilians under the law of armed conflict or specific treaty protections provided by the UN Safety Convention, *supra* note 14, and its Optional Protocol. Optional Protocol to the Convention on the Safety of United Nations and Associated Personnel, G.A. Res. 60/42, U.N. Doc. A/RES/60/42 (Jan. 6, 2006).

of troop-contributing States have been the subject of cyber operations.[33] There is no reason to believe peace operations will remain untouched by this phenomenon. How then may a peace operation respond to such attacks?

In the first instance, peace operations may be specifically authorized by the mandate to use force to protect its personnel, facilities, installations and equipment.[34] Even absent such an explicit mandate, it is submitted that peace operations also have the authority to use force in response to cyber operations directed against them as an exercise of self-defense, either by an individual soldier, the unit or in extended self-defense (i.e., defense of the mandate.)

At their inception, UN peace operations operated under the principle of non-use of force except in self-defense. The notion of self-defense has subsequently come to include the authority to use force in response to armed attempts to prevent them from carrying out their mandate.[35] Defense of the mandate is now part of the approved UN guidelines and regulations for peacekeeping operations.[36] The right to use force against armed attempts to interfere with the execution of the mandate is not limited to operations authorized under Chapter VII of the UN Charter. It is equally available in more traditional peacekeeping operations, although these operations must also conform with the "bedrock principles of UN Peacekeep-

33. For example, Operation Shady RAT, which was a five-year espionage operation discovered in 2011. It was conducted by an unnamed State actor and directed against multiple entities (companies, governments and non-governmental organizations), including the United Nations. There have also been other low-level attacks specifically directed against UN agencies by non-State groups and individual actors. *See* Dmitri Alperovitch, *Revealed: Operation Shady RAT*, MCAFEE (2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf; *United Nations Agency "Hacking Attack" Investigated*, BBC NEWS (Nov. 29, 2011, 3:58 PM), http://www.bbc.com/news/technology-15951883.

34. See, e.g., the MONUC mandate, which authorizes MONUC to use all necessary means within its capability and in the areas where its armed units are deployed "to ensure the protection of United Nations personnel, facilities, installations and equipment." MONUC Mandate, *supra* note 9, ¶¶ 4(c), 6.

35. Capstone Doctrine, *supra* note 8, at 34.

36. Hans F.R. Boddens Hosang, *Force Protection, Unit Self-Defence, and Extended Self-Defence*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 418.

ing, namely impartiality and the necessity of consent and maintenance of consent of all parties to a conflict."[37]

What emerges from the foregoing as important in an examination of the legal parameters governing the use of force against cyber attacks is that the notion of self-defense in the context of peace operations can take on different meanings. It can mean personal self-defense by an individual soldier, unit self-defense or extended self-defense of the mandate. A distinction between those different forms of self-defense is legally relevant because the quintessential requirements for a lawful invocation of any of these, i.e., necessity and proportionality, will lead to different results as to the permissible degree of the use of force.[38]

When a cyber operation directed against a peace operation is severe enough to amount to armed force—that is, it causes death or injury to persons, or physical damage, including loss of functionality, to property and equipment—UN peacekeeping forces are authorized to use force in self-defense to the extent that such use of force complies with the requirements of necessity and proportionality. In other words, the use of force must be necessary to achieve the objective of defending the force and the amount of force must be proportional, that is, it must not greatly exceed the scale and intensity of the attack against which force is used in self-defense.[39] If a cyber operation interferes with the peace operation in such a manner that peacekeeping forces cannot perform their mission (e.g., the command and control systems of the operation have been compromised by a cyber attack) the UN forces would be entitled to use force in defense of the mandate under the same conditions. The use of force by the peacekeeping forces may be kinetic or cyber in nature.

A separate question is the right of a UN peace enforcement operation authorized under Chapter VII to use force against cyber threats that do not themselves amount to a use of force, but which nevertheless interfere with the ability of the enforcement operation to carry out its tasks. When peace enforcement operations are mandated under Chapter VII to use all neces-

37. TERRY D. GILL ET AL., GENERAL REPORT FOR THE 19TH CONGRESS OF THE INTERNATIONAL SOCIETY FOR MILITARY LAW AND THE LAW OF WAR 20 (2012), *available at* http://ismllw.org/congres/2012_05_01_Quebec_General%20Report_Congress-EN.pdf

38. With regard to personal self–defense, see Hans F.R. Boddens Hosang, *Personal Self-Defence and Its Relationship to Rules of Engagement*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 429. With regard to force protection and extended self–defense of the mandate, see Hosang, *supra* note 36.

39. GILL ET AL., *supra* note 37, at 10.

sary means, such operations are authorized to enforce the mandate at all times. Consequently, enforcement authority is not limited to defense against armed interference (reactive), but extends to enforcing any element in the resolution in order to restore or maintain international peace and security (proactive).[40]

Ironically, the usual difficulty in positively attributing the source of cyber threats and distinguishing between those that constitute attacks and those that are mere criminal acts may be less problematic in peace operations. When cyber operations are conducted against a peace operation that interferes with carrying out the mandate, the peace operation may respond in self-defense or defense of the mandate regardless of the origin of the attack. Likewise, if the Security Council mandates a peace operation to maintain law and order, contributing States should use all means reasonably available to them to implement the mandate.[41] Thus, the international force can deal with cyber threats that may destabilize the peace operation.

Recent events in which significant unrest has been created by cyber activities illustrate the relevance of this point. For example, in August 2012, a mass exodus of twenty to thirty thousand migrant workers from Bengaluru to their home States in northeastern India was prompted by the combination of SMS, social media and morphed photos appearing to depict violence against Muslims.[42] While the majority of messages appear to have been sent by bulk SMS text and MMS messages, social media and websites have borne the brunt of the government's response to the crisis. In addition to issuing public statements and imposing a ban on bulk text messages, the Indian government blocked 245 webpages for "hosting provocative and harmful content" and has said it will share evidence with the government of Pakistan to back claims that the messages came from that country.[43] If a peace operation mandated with the maintenance of law and order

40. Capstone Doctrine, *supra* note 8, at 34–35; Hosang, *supra* note 36, at 419.

41. Timothy McCormack & Bruce M. Oswald, *The Maintenance of Law and Order in Military Operations*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 460.

42. In an indication of the dangerous inaccuracy of such media, early figures placed the number of workers fleeing at three hundred thousand.

43. *India to Share Exodus Messages Proof with Pakistan*, BBC NEWS (Aug. 21, 2012, 00:15 AM), http://www.bbc.co.uk/news/world-asia-india-19328364; *India Blames Pakistan for Exodus of Migrant Workers*, BBC NEWS (Aug. 18, 2012, 6:22 PM), http://www.bbc.co.uk/news/world-asia-india-19309982; *State Govts Providing Enough Security to NE People: Centre*, HINDUSTAN TIMES (Aug. 18, 2012), http://www.hindustantimes.com/India-

were confronted with a similar situation, it stands to reason that it could take similar measures, provided that such measures were necessary and proportional under the circumstances.

VI. CYBER OPERATIONS TO PROTECT CIVILIANS

Following a series of tragic incidents, the Security Council has increasingly granted peace operations the authority to use force to "protect civilians under imminent threat of physical violence."[44] The mandate to protect civilians is typically limited to the extent that such protection is possible and within mission capabilities. Conceptually, the right to use force to protect civilians can be viewed, in part, as an extension of the domestic law concept of the right of individual self-defense, which generally allows for defense of a third party, and, in part, as having a distinct basis in the express provisions of the operation's mandate and its attendant rules of engagement.[45] When endowed with such a mandate, a peace operation is entitled to use force when the lives or safety of civilians come under imminent threat of physical danger from a cyber operation, for example, the opening of floodgates on a dam by cyber means. A more difficult question, however, is the ability of the peace operation to use force against a cyber operation that is not so directly linked to physical danger, because the mandate to protect civilians is regularly limited to circumstances where the threats of physical violence are "imminent."

Unfortunately, what the Security Council means by imminence is not clear. Political leaders, UN departments, the UN force commander and national contingent commanders all have an impact on how this term—and the mandate more generally—is interpreted and operationalized in the field.[46] As the Bangalore panic illustrates, cyber operations are certainly capable of making civilian populations believe they are in imminent physical

---

news/NewDelhi/Exodus-continues-30000-NE-people-left-Bangalore-in-3-days/Article1-915431.aspx.

44. S.C. Res. 1590, ¶ 16(1), U.N. Doc. S/RES/1590 (Mar. 24, 2005). The language used by the Security Council in expressly providing for the protection of civilians has been notably consistent over time. *See generally* VICTORIA HOLT & GLYN TAYLOR, PROTECTING CIVILIANS IN THE CONTEXT OF UN PEACEKEEPING OPERATIONS: SUCCESSES, SETBACKS AND REMAINING CHALLENGES 44–47 (2009).

45. GILL ET AL., *supra* note 37, at 22.

46. VICTORIA K. HOLT & TOBIAS C. BERKMAN, THE IMPOSSIBLE MANDATE? MILITARY PREPAREDNESS, THE RESPONSIBILITY TO PROTECT AND MODERN PEACE OPERATIONS 91 (2006).

danger, and, in certain circumstances, cyber operations are linked with very real physical threats. For example, repressive regimes use cyber operations to locate, track and surveil opposition networks and potential dissidents.[47] Whether the correlation between tracking the civilian subjects of that surveillance and their ultimate death or disappearance is direct enough to argue that the imminence requirement is satisfied will depend very much on the context. When the condition is met, the legal justification required for the destruction of the functionality of the surveillance system or the relevant part of it, whether by kinetic or cyber means, may flow from the explicit mandate to protect civilians, or if an explicit mandate to protect civilians is absent, such a legal justification could arguably flow from an extended concept of the right of self-defense.

Irrespective of the legal justification, the use of force to protect civilians under imminent threat of physical violence is constrained by the principles of necessity and proportionality. Both principles would, as a general rule, militate against the necessity of the use of lethal force in response to cyber operations that are the source of an imminent threat. This is because it will generally be possible to counter a cyber threat by technological measures, such as diverting a distributed denial of service (DDoS) attack stream or blocking a port, rather than using lethal force against the person conducting the attack. Given the non-linear progression of technological development, however, the use of force cannot be ruled out. Moreover, as noted previously, the mandate to protect civilians is typically expressed in terms of "to the extent possible" and "within mission capabilities." To date, peace operations, particularly those conducted under the command and control of the United Nations, have had limited technological capacity for intelligence and information analysis[48] and thus may not possess the technical resources or abilities to prevent cyber operations from affecting the civilian population.

The use of force in self-defense—including in defense of the mandate or defense of civilians—does not necessarily mean the forces are involved

47. For an example from Syria, see WAGNER, *supra* note 2; Peter Apps, *Disinformation Flies in Syria's Growing Cyber War*, REUTERS (Aug. 7, 2012, 2:11 PM), http://www.reuters.com/article/2012/08/07/us-syria-crisis-hacking-idUSBRE8760GI20120807.

48. A. Walter Dorn, *United Nations Peacekeeping Intelligence*, *in* THE OXFORD HANDBOOK OF NATIONAL SECURITY INTELLIGENCE 275, 290–92 (Loch K. Johnson ed., 2010).

in an armed conflict such that the laws of armed conflict apply.[49] It is only when a peace operation becomes so actively engaged with a State or organized armed group that hostilities reach the level of armed conflict that the law of armed conflict will apply.[50] In such a case, the right to respond to cyber operations is not constrained by the limits of self-defense; members of the armed forces and military objectives of the adversary may be lawfully attacked. Likewise, of course, the military personnel and military equipment of the peace operation, including military cyber infrastructure and information systems, become lawful targets.

VII. PEACE OPERATIONS CONDUCTING OFFENSIVE CYBER OPERATIONS

To date there is no public record of cyber operations being used by a UN peace operation. The United States has stated that it used cyber operations successfully in Afghanistan.[51] However, given the dual nature of the U.S. presence in the country and the double-hatted command of the troops involved, it is not possible to determine whether the cyber operations were conducted under the auspices of the UN-mandated, NATO-led International Security Assistance Force or the independent U.S. Operation Enduring Freedom. Cyber attacks to disrupt or disable the Libyan air defense networks prior to strikes by coalition aircraft were also contemplated by the United States in that UN-mandated operation, but the idea was discarded in the early stages of operational planning and conventional strikes were ultimately used to achieve the same results.[52] For a peace operation constrained in its use of armed force and likely to be involved in a subsequent transition to reconstruction and development efforts, the ability to

---

49. Ola Engdahl, *The Status of Peace Operation Personnel under International Humanitarian Law*, 11 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 109, 116 (2008); Christopher Greenwood, *International Humanitarian Law and United Nations Military Operations*, 1 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 3 (1998).

50. See *supra* pp. 518-520 for a discussion of the debate on where the threshold lies.

51. Raphael Satter, *US General Says His Forces Carried Out Cyberattacks on Opponents in Afghanistan*, ASSOCIATED PRESS, Aug. 24, 2012, http://seattletimes.com/html/nationworld/2018983462_apusafghancyberattacks.html ("I was able to get inside his nets, infect his command–and–control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."). A Pentagon spokesman declined to elaborate on the comments, stating merely that the operations were properly authorized and within the bounds of international law. *Id.*

52. Eric Schmitt & Thom Shanker, *U.S. Weighed Use of Cyberattacks to Weaken Libya*, NEW YORK TIMES, Oct. 18, 2011, at A1.

merely turn off a network rather than destroying it means that cyber operations will prove a useful tool in the toolbox of peace operations.

Cyber operations may also allow the mission to project their mandate into regions beyond its area of deployment, which it could not otherwise reach with current capabilities. In addition to their utility for intelligence and monitoring activities, cyber operations provide the ability to remotely shut down the networks of opposing actors, allowing for a significant advantage to a mission seeking to disrupt the activities of those threatening a peace process.

Furthermore, in many circumstances cyber operations provide a mission with a non-forceful method to influence the actors involved in the process, consistent with the principle that a UN peace operation should only use force as a measure of last resort after other methods of persuasion have been exhausted.[53] This includes enabling the mission to take action against outside interference that may be inflaming an already tense situation. For example, the 2007 cyber incidents that accompanied rioting in Estonia were largely conducted from outside the country.[54] Attack scripts were passed in Russian language forums and posted on Russian-hosted websites. Similarly, websites hosting generic attack scripts for use in the cyber elements associated with Operation Cast Lead in the Gaza Strip in 2008 and 2009 were hosted in multiple jurisdictions by both sides. A site called "Help Israel Win" that sought volunteers for a botnet dubbed "Patriot" was moved multiple times in response to attacks from the opposing side. Opposing hacker teams were located in multiple jurisdictions, and included hackers of Saudi Arabian, Egyptian, Turkish, Algerian and Moroccan origin.[55] Comparable situations of outside interference could easily confront a peace operation.

While the specific legal issues raised depend, among other things, on the nature of the cyber action, the type of mandate, applicable law and the facts on the ground, a number of progressively offensive oriented cyber activity examples may prove illustrative of some of the issues involved.

---

53. Capstone Doctrine, *supra* note 8, at 35.

54. *See* TIKK, KASKA & VIHUL , *supra* note 1, at 23 & nn.76–88.

55. GREYLOGIC, PROJECT GREY GOOSE, PHASE II REPORT: THE EVOLVING STATE OF CYBER WARFARE ch. 2 (2009), *available at* http://fserror.com/pdf/GreyGoose2.pdf.

A. Removal or Blocking of Online Content

Online content—whether extremist websites, highly offensive video footage or social media sites—have the potential to inflame, exacerbate and ignite tensions on the ground in areas where the peace operations are working. In some cases, online content may even be a direct incitement to physical violence. Removal of the content could, therefore, contribute to the promotion of a safe and secure environment in accordance with a peace operation's mandate. If webhosts and Internet Service Providers (ISPs) are unable or unwilling to remove the content, can peace operations proactively remove or block access to such materials? One of the factors will be where the content is posted. Peace operation mandates are generally geographically constrained to a specific territory or area of deployment. Thus, the authorization to act provided by the mandate—whether or not it involves the use of force—will be limited to that territory.[56] The same is true of cross-border cyber operations conducted in an effort to remove potentially inflammatory content from sites outside the mission area.

Blocking the availability of particular online content within the geographical confines of the mission area is a far easier way to accomplish the same effect. The most extreme example of governmental intervention in communications technology for security purposes is perhaps the Egyptian government's actions in completely shutting off access to the Internet for four days during the Arab Spring. Other States have taken a more nuanced approach by blocking specific sites or particular content. While States, such as China, with its "great firewall," and regimes in the Middle East and North Africa that engage in heavy web filtering and censorship have technology in place to make such a task easy, other States also have the capacity to engage in such behaviors.[57] For example, India blocked access to approximately 250 websites in an effort to stop the spread of videos and images that caused the Bangalore panic. The Afghan government pushed Internet providers in that country to bar access to websites hosting an anti-Islamic video in order to head off potentially violent demonstrations.[58]

---

56. The exception will be in situations when a peace operation is acting in unit or personal self-defense, which is an inherent right and not linked to the mandate. *See generally* Hosang, *supra* note 36, at 418–27.

57. *See generally*, WAGNER, *supra* note 2.

58. Alissa J. Rubin, *Afghanistan Tries to Block Video and Head Off Rioting*, NEW YORK TIMES (Sept 13, 2012), http://www.nytimes.com/2012/09/14/world/asia/afghanistan-tries-to-block-video-and-head-off-rioting.html?_r=0.

While it appears reasonable to assume that peace operations can block the availability of particular online content within the geographical confines of the mission area on similar legal grounds as provided for by a mandate to protect civilians or one to provide a safe and secure environment, the human rights implications of doing so, particularly for a peace operation under UN command and control, are significant. In a "Joint Declaration on Freedom of Expression and the Internet," rapporteurs on freedom of expression from the United Nations, Organization of American States and the African Commission on Human and Peoples' Rights and the Organization for Security and Cooperation in Europe's representative on freedom from the media stated, "[c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can *never* be justified, *including on public order or national security grounds*."[59] Although not legally binding, given the breadth of the organizations represented in the declaration, this statement will carry significant weight when applied to a UN peace operation. The right to freedom of expression is not absolute, however, and while blocking entire sections of the Internet may not be justified, restriction of certain content may be appropriate if authorized by the mandate, proportionate under international standards and necessary to protect a recognized interest. Clearly, when the content amounts to incitement to commit crimes, such as genocide or certain other forms of hate speech, blocking of content would be permissible for the peace operation.

B. Neutralization of Command and Control and Air Defense Networks

The ability of cyber operations to neutralize networks without destroying them may prove to be a valuable tool for peace operations. For example, multiphase operations that involve policing no-fly zones or aerial monitoring of disarmament programs may initially benefit from suppression or neutralization of the air defense networks. However, such networks will be needed once peace is restored and the operation moves on to supporting redevelopment.

---

59. Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression & the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and the Internet*, ¶ 6(b) (2011) (emphases added).

Whether neutralizing, but not destroying, such a network is legally permissible depends on the categorization of the acts and the mandate of the particular operation. There has been a great deal of debate whether mere neutralization of a network by cyber means would amount to an attack under the laws of armed conflict.[60] Agreement appears to have been reached that destruction of the functionality of objects, to include network components, such that a physical component has to be replaced would amount to an attack.[61] The same analysis may be used in evaluating whether actions by a peace operation constitute a use of force. Therefore, merely turning a network off as a proactive measure would not overstep an authorization limiting the use of force to that necessary in self-defense.[62] Other potential restrictions on taking such an action would be dependent on the mandate for the particular operation and the associated rules of engagement.

Neutralization of computers engaging in cyber operations from outside the area of operations, such as against international "spoilers" that take part in DDoS attacks similar to those directed against Estonia, face the same geographical constraints outlined in the previous section with regard to removal of content. At the same time, peace operation mandates in Security Council resolutions almost always call on member States to provide assistance to peace operations. In some cases they require States to ensure that their nationals, individuals and firms within their territory or subject to their jurisdiction refrain from particular behaviors.[63] As a result, peace operations are able to call on the member State in which the perpetrators are located or of which they are nationals to assist in preventing "spoiler" activities and punishing those who engage in such activities. Simultaneously, the peace operation could block and/or redirect the DDoS traffic emanating from particular Internet Protocol addresses using ISPs or webhosts located in the geographical area of the peace operation.

---

60. *See, e.g.*, HARRISON DINNISS, *supra* note 5, at 196–202.

61. TALLINN MANUAL, *supra* note 24, at 105–110.

62. Clearly, however, if the network had actually been used against aircraft involved in the peace operation or indicated hostile intent, e.g., by acquiring a radar lock on an operation aircraft, any use of force against the system would be authorized as self-defense.

63. *See*, *e.g.*, S.C. Res. 1973, ¶¶ 9, 19, 21, U.N. Doc S/RES/1973 (Mar. 17, 2011), concerning general assistance by UN member States to the UN-authorized Libya operation and the specific tasks States were to take in support of the freeze on Libyan assets.

C. Destruction of Surveillance or Command and Control Capabilities

When more destructive offensive cyber measures are envisaged, such as those causing physical damage to equipment of the opposing party in non-self-defense circumstances, authorization must derive from the mandate. As noted above, physical destruction by cyber means is a use of armed force and must, therefore, be authorized by the Security Council. Since traditional peacekeeping missions are authorized only to use force in self-defense as defined above, offensive cyber operations are not permitted. Peace enforcement operations endowed with a Chapter VII authorization to use "all necessary means," may, on the other hand, use force to enforce the mandate. Thus, offensive cyber operations causing damage, destruction or personal injury are authorized in any situation that kinetic force would be permissible, provided they are necessary to fulfill mission objectives. Likewise, when members of the peace operation find themselves actively engaged in hostilities under the laws of armed conflict, destructive offensive cyber operations may be used against military objectives in accordance with that body of law.[64]

VIII. CONCLUSION

The foregoing analysis confirms that a detailed answer of the legal parameters governing peace operations that confront or conduct cyber operations cannot be provided in the abstract. The mandates and capabilities of peace operations and the contexts in which they are deployed are too varied and complex. Nonetheless, one can draw some general conclusions.

First, it seems certain that cyber operations directed against or conducted by peace operations can be expected to increase. Second, it would appear equally reasonable to assume that the majority of instances in which peace operations are involved in cyber operations—either as actors engaging in such activity or as the object of cyber operations of other actors—will take place when the peace operation is not a party to an armed conflict; hence, it will not be operating under the law of armed conflict. To the extent this is true, international human rights law will remain at the fore as the main international legal framework governing cyber operations.

Whether operating under a law of armed conflict regime or a human rights regime, peace operations will always be able to conduct cyber opera-

64. *See, e.g.*, Banks, *supra* note 10; Blank, *supra* note 10; Lubell, *supra* note 10.

tions of some type. Indeed, the importance of cyber capabilities is likely to increase in light of their operational utility and efficiency. Exactly what type of cyber operation will be legally permissible, and how intrusive, disruptive and offensive it may be, will however, ultimately depend on the specific mandate.