Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians

Cordula Droege*

Cordula Droege is the Head of the Operational Law Unit, Legal Division, International Committee of the Red Cross (ICRC).

Abstract

Cyber warfare figures prominently on the agenda of policymakers and military leaders around the world. New units to ensure cyber security are created at various levels of government, including in the armed forces. But cyber operations in armed conflict situations could have potentially very serious consequences, in particular when their effect is not limited to the data of the targeted computer system or computer. Indeed, cyber operations are usually intended to have an effect in the 'real world'. For instance, by tampering with the supporting computer systems, one can manipulate an enemy's air traffic control systems, oil pipeline flow systems, or nuclear plants. The potential humanitarian impact of some cyber operations on the civilian population is enormous. It is therefore important to discuss the rules of international humanitarian law (IHL) that govern such operations because one of the main objectives of this body of law is to protect the civilian population from the effects of warfare. This article seeks to address some of the questions that arise when applying IHL – a body of law that was drafted with traditional kinetic warfare in mind – to cyber technology. The first question is: when is cyber war really war in the sense of

* I would like to thank my colleagues from the ICRC, Knut Dörmann, Bruno Demeyere, Raymond Smith, Tristan Ferraro, Jelena Pejic, and Gary Brown for their thoughtful comments on earlier drafts, as well as Nele Verlinden for her help with the references.
All the Internet references were accessed in October 2012, unless otherwise stated.
This article was written in a personal capacity and does not necessarily reflect the views of the ICRC.

doi:10.1017/S1816383113000246

'armed conflict'? After discussing this question, the article goes on to look at some of the most important rules of IHL governing the conduct of hostilities and the interpretation in the cyber realm of those rules, namely the principles of distinction, proportionality, and precaution. With respect to all of these rules, the cyber realm poses a number of questions that are still open. In particular, the interconnectedness of cyber space poses a challenge to the most fundamental premise of the rules on the conduct of hostilities, namely that civilian and military objects can and must be distinguished at all times. Thus, whether the traditional rules of IHL will provide sufficient protection to civilians from the effects of cyber warfare remains to be seen. Their interpretation will certainly need to take the specificities of cyber space into account. In the absence of better knowledge of the potential effects of cyber warfare, it cannot be excluded that more stringent rules might be necessary.

Keywords: cyber security, cyber warfare, cyber attack, international humanitarian law, cyber operations, cyber weapons, armed conflict in cyber space, conduct of hostilities, distinction, proportionality, indiscriminate attacks, precautions.

Introduction

Cyber security figures prominently on the agenda of policymakers and military leaders around the world. A recently published study by the United Nations Institute for Disarmament Research (UNIDIR) describes the measures taken by thirty-three states that have specifically included cyber warfare in their military planning and organisation, and gives an overview of the cyber security approach of thirty-six other states.[1] These range from states with very advanced statements of doctrine and military organisations employing hundreds or thousands of individuals to more basic arrangements that incorporate cyber attack and cyber warfare into existing capabilities for electronic warfare. A number of states are setting up specialized units in or outside of their armed forces to deal with cyber operations.[2] It has also been reported that twelve of the world's fifteen largest military forces are building cyber warfare programmes.[3]

Cyber security in general and cyber warfare in particular

Amid much discussion about cyber security generally, the public at large knows little, yet, of the military planning and policies of states for cyber warfare.

1 Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization*, UNIDIR Resources Paper, 2011, available at: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf; see also, Eneken Tikk, *Frameworks for International Cyber Security*, CCD COE Publications, Tallinn, 2011.

2 See, e.g., Ellen Nakashima, 'Pentagon to boost cybersecurity force', in *The Washington Post*, 27 January 2013; Gordon Corera, 'Anti-cyber threat centre launched', in *BBC News*, 27 March 2013.

3 Scott Shane, 'Cyberwarfare emerges from shadows of public discussion by US officials', in *The New York Times*, 26 September 2012, p. A10.

It appears that most government strategies consist of a mix of defensive and offensive strategies. On the one hand, states are increasingly seeking to protect their own critical infrastructure from cyber attacks. On the other hand, they appear also to be building technological capacities to be able to launch cyber operations against their adversaries in times of armed conflict.[4]

Policymakers and commentators are debating whether all or some of the new 'cyber weapons' should be banned altogether, whether attention should turn to confidence-building measures (similar to those on nuclear disarmament),[5] or whether 'rules of the road' should be established for behaviour in cyber space.[6] There has also been discussion for over a decade about the need for a new treaty on cyber security. The Russian Federation has advocated for such a treaty since the late 1990s, whereas the United States of America (US) and Western states have taken the position that none is needed.[7] In a letter to the Secretary-General of the United Nations (UN), China, the Russian Federation, Tajikistan, and Uzbekistan proposed an International Information Security Code of Conduct in September 2011, but this has a much broader scope than just for situations of armed conflict.[8] China, the Russian Federation, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan are also parties to an agreement adopted in the framework of the Shanghai Cooperation Organisation in 2009.[9] India, the Islamic Republic of Iran, Mongolia, and Pakistan participate as observers. An unofficial English translation of this agreement shows that it appears to enlarge the concepts of 'war' and 'weapon' beyond their traditional meaning in international humanitarian law (IHL).[10]

4 *Ibid.*

5 Ben Baseley-Walker, 'Transparency and confidence-building measures in cyberspace: towards norms of behaviour', in UNIDIR, *Disarmament Forum,* 'Confronting cyberconflict', Issue 4, 2011, pp. 31–40, available at: http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf; James Andrew Lewis, *Confidence-building and international agreement in cybersecurity*, available at: http://www.unidir.org/pdf/articles/pdf-art3168.pdf.

6 See William Hague, 'Security and freedom in the cyber age – seeking the rules of the road', Speech to the Munich Security Conference, 4 February 2011, available at: https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road, and 'Foreign Secretary opens the London Conference on Cyberspace', 1 November 2011, available at: https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace.

7 See draft resolution submitted by the Russian Federation to the General Assembly First Committee in 1998, letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Secretary-General, UN Doc. A/C.1/53/3, 30 September 1998; John Markoff and Andrew E. Kramer, 'US and Russia differ on a treaty for cyberspace', in *The New York Times*, 28 June 2009, p. A1; John Markoff and Andrew E. Kramer, 'In shift, US talks to Russia on internet security', in *The New York Times*, 13 December 2009, p. A1; see Adrian Croft, 'Russia says many states arming for cyber warfare', in *Reuters*, 25 April 2012, available at: http://www.reuters.com/article/2012/04/25/germany-cyber-idUSL6E8FP40M20120425; Keir Giles, 'Russia's public stance on cyberspace issues', paper given at the 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis and K. Ziolkowski (eds), NATO CCD COE Publications, Tallinn, 2012, available at: http://www.conflictstudies.org.uk/files/Giles-Russia_Public_Stance.pdf.

8 Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359 of 14 September 2011.

9 Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security.

10 Available at: http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf. Annex 1 defines 'information war' as a 'confrontation between two or more states in the information space aimed at damaging

This debate – in which all sides accuse the other of espionage and arms proliferation in an open or more or less veiled manner[11] – remains very general from the legal perspective. In particular, there is no differentiation between situations of armed conflict and other situations, although the applicability of IHL depends on such a differentiation. Much of the concern appears to concentrate on espionage, against the state as well as against economic interests, but there is also talk of cyber warfare and a need to avoid weapons proliferation in cyber space. There is generally no differentiation between situations of armed conflict and other situations in which cyber operations threaten the security of states, businesses, or private households. Most debates on cyber security do not even mention situations of armed conflict, and it is unclear whether such situations are implicitly included. Indeed, in many respects, especially in relation to the protection of computer infrastructure against infiltration, manipulation, or damage, it makes no difference whether a cyber attack is carried out in the context of an armed conflict or not. The technical means of protecting the infrastructure will mostly be the same. However, while it is probably fair to say that most of the threats in the cyber realm are not immediately related to situations of armed conflict but stem, rather, from economic or other espionage, or organized cyber crime, it is also clear that recourse to cyber weapons and cyber operations is playing a growing role in armed conflicts and that states are actively preparing for this new development.

In the meantime, there is confusion about the applicability of IHL to cyber warfare – which might in fact stem from different understandings of the concept of cyber warfare itself, which range from cyber operations carried out in the context of armed conflicts as understood in IHL to criminal cyber activities of all kinds. Some states, like the US,[12] the United Kingdom of Great Britain and

information systems, processes and resources, critical and other structures, undermining political, economic and social systems, mass psychologic brainwashing to destabilize society and state, as well as to force the state to taking decision in the interest of an opposing party'. Annex 2 describes the threat of 'development and use of information weapons, preparation for and waging information war' as emanating 'from creating and developing information weapons that pose an immediate danger to critical structures of States which might lead to a new arms race and represents a major threat in the field of international information security. Among its characteristics are the use of information weapons to prepare and wage information war, and impact transportation, communication and air control systems, missile defence and other types of defence facilities, as a result of which the state looses its defence capabilities in the face of the aggressor and fails to exercise its legitimate right to self-defence; breaching information infrastructure operation, which leads to the collapse of administrative and decision-making systems in the states; and destructive impact on critical structures'.

11 Kenneth Lieberthal and Peter W. Singer, 'Cybersecurity and US–China relations', in *China US Focus*, 23 February 2012, available at: http://www.chinausfocus.com/library/think-tank-resources/us-lib/peacesecurity-us-lib/brookings-cybersecurity-and-u-s-china-relations-february-23-2012/; Mandiant Intelligence Centre Report, *APT1: Exposing one of China's Cyber Espionage Units*, available at: http://intelreport.mandiant.com/?gclid=CKD6-7Oo3LUCFalxOgod8y8AJg; Ellen Nakashima, 'US said to be target of massive cyber-espionnage campaign', in *The Washington Post*, 11 February 2013; 'North Korea says US "behind hack attack"', in *BBC News*, 15 March 2013.

12 Harold Koh, 'International law in cyberspace', speech at the US Cyber Command Inter-Agency Legal Conference, 18 September 2012, available at: http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/; Report of the Secretary-General on Developments in the field of information and telecommunication in the context of international security (hereinafter 'Report of the Secretary-General'), 15 July 2011, UN Doc. A/66/152, p. 19; see also, US Department of Defense Strategy for Operating in Cyberspace: 'Long-standing international norms guiding state behaviour – in times of

Northern Ireland,[13] and Australia,[14] have stated that IHL applies to cyber warfare.[15] However, the public positions do not yet go into detail about questions such as the threshold for armed conflicts, the definition of 'attacks' in IHL, or the implications of cyber warfare with respect to so-called dual-use objects. It has been said that China does not accept the applicability of IHL to cyber warfare.[16] However, it is unclear whether this would really be China's official position in a situation of armed conflict within the meaning of IHL. Another view is that:

> China's stance is that the nations of the world should cherish the value of cyber space – the first social space created by humankind – and should firmly oppose the militarization of the Internet. . . . Its view is that the current UN Charter and the existing laws of armed conflict as well as the basic principles of International Humanitarian Law that relate to war and the use or threat of force all still apply to cyberspace – in particular the 'no use of force' and 'peaceful settlement of international disputes' imperatives as well as the principles of distinction and proportionality in regards to the means and methods of warfare.[17]

As far as can be seen, the Russian Federation has not taken an official stance on the applicability of IHL to cyber warfare.[18]

From a legal point of view, it is important to distinguish between cyber warfare in the sense of cyber operations conducted in the context of armed conflicts

peace and conflict – also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them', US Department of Defense Strategy for Operating in Cyberspace, July 2011, available at: http://www.defense.gov/news/d20110714cyber.pdf.

13 Report of the Secretary-General, 23 June 2004, UN Doc. A/59/116, p. 11; Report of the Secretary-General, 20 July 2010, UN Doc. A/65/154, p. 15.

14 Report of the Secretary-General, above note 12, p. 6.

15 See also, the proposal by the High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, JOIN (2013) 1 final.

16 See, e.g., Adam Segal, 'China, international law and cyber space', in *Council on Foreign Relations*, 2 October 2012, available at: http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/.

17 Li Zhang, 'A Chinese perspective on cyber war', in this edition. In his speech to the First Committee in September 2011, China's Ambassador stated that China proposed that countries 'commit themselves to non-use of information and cyber technology to engage in hostile activities to the detriment of international peace and security, and to non-proliferation of information and cyber weapons' and 'work to keep information and cyber space from becoming a new battlefield'; there is no mention of IHL. See the statement on information and cyberspace security made by H. E. Ambassador Wang Qun to the First Committee during the 66th Session of the General Assembly, 'Work to build a peaceful, secure and equitable information and cyber space', New York, 20 October 2011, available at: http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

18 The reported military doctrine of the Russian Federation does not mention IHL with respect to information warfare; see 'The Military Doctrine of the Russian Federation Approved by Russian Federation Presidential Edict on 5 February 2010', available at: http://www.sras.org/military_doctrine_russian_federation_2010; and neither does K. Giles, above note 7; Roland Heikerö, 'Emerging threats and Russian Views on information warfare and information operations', FOI Swedish Defence Research Agency, March 2010, p. 49, available at: http://www.highseclabs.com/Corporate/foir2970.pdf, reports that the Russian Federation has proposed the 'application of humanitarian laws banning attacks on non-combatants and a ban on deception in cyberspace'.

within the meaning of IHL and cyber operations outside such contexts. It is only in the context of armed conflicts that the rules of IHL apply, imposing specific restrictions on the parties to the conflict.[19] Thus, in this article the term 'cyber warfare' will refer to means and methods of warfare that consist of cyber operations amounting to or conducted in the context of an armed conflict within the meaning of IHL only. Such cyber operations – also frequently referred to as computer network attacks – are directed against or sent via a computer or a computer system through a data stream.[20] They can aim to do different things, for instance to infiltrate a computer system and collect, export, destroy, change, or encrypt data, or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated system. In other words, the following analysis deals with hostilities that consist of developing and sending computer code from one or more computers to the target computers.

The humanitarian concern

The International Committee of the Red Cross' (ICRC) humanitarian concern in respect of cyber warfare relates mainly to the potential impact on the civilian population, in particular because cyber operations could seriously affect civilian infrastructure[21] as a result of several features peculiar to the cyber realm.

First, because of its increasingly ubiquitous reliance on computer systems, civilian infrastructure is highly vulnerable to computer network attacks. In particular, a number of critical installations, such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control rely on so-called supervisory control and data acquisition (or SCADA) systems and distributed control systems (DCS). These systems, which constitute the link between the digital and the physical worlds, are extremely vulnerable to outside interference by almost any attacker.[22]

19 For the International Committee of the Red Cross (ICRC), it is important to draw attention to the specific situation of cyber operations amounting to or conducted in the context of armed conflicts – that is, cyber warfare in a narrow sense. This is because the ICRC has a specific mandate under the 1949 Geneva Conventions to assist and protect the victims of armed conflicts. It is also mandated by the international community to work for the understanding and dissemination of IHL. See, e.g., GC III, Art. 126(5), GC IV, Art. 143(5), and Statutes of the International Red Cross and Red Crescent Movement, Art. 5(2)(g).

20 US Department of Defense, *Dictionary of Military and Associated Terms*, 8 November 2010 (as amended on 31 January 2011), Washington, DC, 2010: 'Computer network attacks are actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.'

21 In the law on the conduct of hostilities, 'civilians', 'civilian population', and 'civilian objects' are different legal concepts to which different rules apply. However, when this article speaks about the impact of cyber warfare on the civilian population, it also refers to damage done to civilian infrastructure, which is the most likely way that cyber operations will affect the civilian population.

22 Stefano Mele analyses likely scenarios of interference with different types of military and civilian systems and states that the manipulation of electrical grid management systems is probably the greatest threat at present. See Stefano Mele, 'Cyber warfare and its damaging effects on citizens', September 2010, available at: http://www.stefanomele.it/public/documenti/185DOC-937.pdf.

Second, the interconnectivity of the Internet poses a threat to civilian infrastructure. Indeed, most military networks rely on civilian, mainly commercial, computer infrastructure, such as undersea fibre optic cables, satellites, routers, or nodes; conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems relying on global positioning system (GPS) satellites, which are also used by the military. Thus, it is to a large extent impossible to differentiate between purely civilian and purely military computer infrastructure. As will be seen below, this poses a serious challenge to one of the cardinal principles of IHL, namely the principle of distinction between military and civilian objects. Moreover, even if military and civilian computers or computer systems are not entirely one and the same, interconnectivity means that the effects of an attack on a military target may not be confined to this target. Indeed, a cyber attack may have repercussions on various other systems, including civilian systems and networks, for instance by spreading malware (malicious software) such as viruses or worms if these are uncontrollable. This means that an attack on a military computer system may well also damage civilian computer systems, which, in turn, may be vital for some civilian services such as water or electricity supply or the transfer of assets.

For the time being, we have no clear examples of cyber attacks during armed conflicts or examples in which the civilian population has been severely affected by computer network attacks during armed conflicts. However, technical experts seem to agree that it is technically feasible, even if difficult, to deliberately interfere with airport control systems, other transportation systems, dams, or power plants via cyber space. Potentially catastrophic scenarios, such as collisions between aircraft, the release of radiation from nuclear plants, the release of toxic chemicals from chemical plants, or the disruption of vital infrastructure and services such as electricity or water networks, cannot be discarded.

Such scenarios might not be the most likely ones; cyber operations are in all probability more likely to be used to manipulate civilian infrastructure leading it to malfunction or disrupting it without causing immediate death or injury. The effects of such 'bloodless' means and methods of warfare might not be as dramatic for civilians as shelling or bombing. They can nevertheless be severe – for instance, if the power or water supply is interrupted, or if communication networks or the banking system are down. These effects and how they must be taken into account under the rules of IHL must therefore be clarified.

Some commentators have argued that the threat of computer network attacks on the larger civilian infrastructure should not be overstated, in particular, because offensive cyber weapons would often need to be very specifically written to affect specific target computer systems (like the Stuxnet virus, for instance)[23] and

23 The so-called Stuxnet virus was launched against the Iranian uranium enrichment facility at Natanz, reportedly leading to the destruction of a thousand centrifuges. It is reported in the press that the United States and/or Israel were behind this virus, but this has not been officially acknowledged. David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant? Preliminary assessment', ISIS Report, 22 December 2010, available at: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/; David E. Sanger, 'Obama order sped up wave of cyberattacks against Iran', in *The New York Times*, 1 June 2012,

could therefore not easily be redirected at other targets.[24] Also, in an internationally interconnected Internet system and in a globalized economy, states might be reluctant to damage each other because the repercussions, for instance on financial systems, might damage them as much as their adversary.[25] That might or might not be the case. The fact that computer network attacks are potentially capable of targeting civilian objects, might in some instances be indiscriminate or be used in an indiscriminate manner, or could potentially have devastating incidental consequences for civilian infrastructure and the civilian population is reason enough to clarify the applicable rules on the conduct of hostilities that parties to conflicts must observe.

The role of international humanitarian law

Against this background, how does IHL address the potential consequences of cyber warfare on the civilian population?

IHL provisions do not specifically mention cyber operations. Because of this, and because the exploitation of cyber technology is relatively new and sometimes appears to introduce a complete qualitative change in the means and methods of warfare, it has occasionally been argued that IHL is ill adapted to the cyber realm and cannot be applied to cyber warfare.[26] However, the absence in IHL of specific references to cyber operations does not mean that such operations are not subject to the rules of IHL. New technologies of all kinds are being developed all the time and IHL is sufficiently broad to accommodate these developments. IHL prohibits or limits the use of certain weapons specifically (for instance, chemical or biological weapons, or anti-personnel mines). But it also regulates, through its general rules, all means and methods of warfare, including the use of all weapons. In particular, Article 36 of Protocol I additional to the Geneva Conventions provides that:

> [i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran. html?pagewanted=all&_moc.semityn.www.

24 Thomas Rid, 'Think again: cyberwar', in *Foreign Policy*, March/April 2012, pp. 5 *ff*., available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full; Thomas Rid and Peter McBurney, 'Cyber-weapons', in *The RUSI Journal,* February–March 2012, Vol. 157, No. 1, pp. 6–13; see also, Maggie Shiels, 'Cyber war threat exaggerated claims security expert', in *BBC News*, 16 February 2011, available at: http://www.bbc.co.uk/news/technology-12473809.

25 Stefano Mele (above note 22) argues that for this reason massive electronic attacks against financial systems of foreign countries are unlikely.

26 Charles J. Dunlap Jr., 'Perspectives for cyber strategists on law for cyberwar', in *Strategic Studies Quarterly*, Spring 2011, p. 81.

Beyond the specific obligation it imposes on states party to Additional Protocol I, this rule shows that IHL rules apply to new technology.

That said, cyber warfare challenges some of the most fundamental assumptions of IHL. First, IHL assumes that the parties to conflicts are known and identifiable. This cannot always be taken for granted even in traditional armed conflicts, in particular, non-international armed conflicts. However, in the cyber operations that occur on an everyday basis, anonymity is the rule rather than the exception. It appears to be impossible in some instances to trace their originator, and even when this is possible it is in most cases time-consuming. Since all law is based on the allocation of responsibility (in IHL, to a party to a conflict or to an individual), major difficulties arise. In particular, if the perpetrator of a given operation and thus the link of the operation to an armed conflict cannot be identified it is extremely difficult to determine whether IHL is even applicable to the operation. So, for instance, if a government's infrastructure is being attacked, but it is not clear who is behind the attack, it is difficult to define who the parties to the potential armed conflict are, and therefore to determine whether there is an armed conflict at all. Similarly, even if the parties to the conflict are known, it may be difficult to attribute the act to one particular party. Second, IHL is based on the assumption that the means and methods of warfare will have violent effects in the physical world. Many cyber operations are likely to have effects that are disruptive but not immediately perceivably physically destructive. Third, the entire structure of the rules on the conduct of hostilities – and in particular the principle of distinction – is founded on the assumption that civilian objects and military objects are, for the most part, distinguishable. In the cyber theatre of war this is likely to be the exception rather than the rule because most cyber infrastructure around the world (undersea cables, routers, servers, satellites) serves for both civilian and military communications.

The following analysis therefore seeks to explore how the rules of IHL can be interpreted to make sense in the cyber realm, and how cyber technology might touch upon their limits. As will be shown below, it is probably too early to give definite answers to many of the questions raised because examples are few and the facts not entirely clear and state practice with respect to the interpretation and implementation of applicable norms still has to evolve. To date, the Tallinn Manual on the International Law Applicable to Cyber Warfare (hereinafter 'Tallinn Manual') is the most comprehensive exercise seeking to interpret the rules of international law (*jus ad bellum* and *jus in bello*) to cyber warfare.[27] It was drafted by a group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, and provides a useful compilation of rules with commentary reflecting the different views on some of the thorny issues raised by this new technology. The ICRC took part in the deliberations of the group of experts as an observer, but does not endorse all the views expressed in the Manual.

27 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (forthcoming). The *Tallinn Manual* is available at: http://www.ccdcoe.org/249.html.

Applicability of international humanitarian law to cyber operations: what is an armed conflict in cyber space?

IHL is only applicable if cyber operations are conducted in the context of and related to an armed conflict. Thus, it should be fairly uncontroversial that when cyber operations are conducted in the context of an ongoing armed conflict they are governed by the same IHL rules as that conflict: for instance, if in parallel or in addition to a bomb or missile attack, a party to the conflict also launches a cyber attack on the computer systems of its adversary.

However, a number of operations referred to as cyber warfare may not be carried out in the context of armed conflicts at all. Terms like 'cyber attacks' or 'cyber terrorism' may evoke methods of warfare, but the operations they refer to are not necessarily conducted in an armed conflict. Cyber operations can be and are in fact used in crimes committed in everyday situations that have nothing to do with war.

Other situations that fall between situations of existing armed conflicts fought with traditional means and cyber operations and situations that are entirely outside the realm of armed conflict are harder to classify. This is the case, in particular, when computer network attacks are the only hostile operations carried out and even more so if they remain isolated acts. This scenario is not entirely futuristic. The Stuxnet virus, which appears to have targeted the uranium enrichment facility of the Islamic Republic of Iran at Natanz, has remained, for the time being, an isolated computer network attack (even if carried out over a period of time), possibly launched by one or more states against the Islamic Republic of Iran. While classification as an armed conflict has not arisen in the discourse of states, the reasoning of some commentators suggested that if carried out by a state, this attack would amount to an international armed conflict.[28] Another conceivable scenario would be large-scale and sustained cyber operations conducted by a non-state organised armed group against government infrastructure. Can such operations rise to the level of a non-international armed conflict?

Under existing IHL, there are two – and only two – types of armed conflict: international armed conflicts and non-international armed conflicts. Not all criteria for the existence of such conflicts will be discussed here. Instead, some aspects that seem to raise particularly difficult questions with respect to cyber operations will be addressed.

International armed conflicts

Under common Article 2 to the four Geneva Conventions of 1949, an international armed conflict is any 'declared war or any other armed conflict which may arise

28 Michael N. Schmitt, 'Classification of cyber conflict', in *Journal of Conflict and Security Law*, Vol. 17, Issue 2, Summer 2012, p. 252; see also, Gary Brown, 'Why Iran didn't admit Stuxnet was an attack', in *Joint Force Quarterly*, Issue 63, 4th Quarter 2011, p. 71, available at: http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html. G. Brown does not address the question of conflict classification, but considers that Stuxnet clearly amounted to an attack, possibly in violation of the prohibition against the use of force and the law of war.

INTERNATIONAL REVIEW of the Red Cross

between two or more States even if the state of war is not recognized by one of them'. There is no further treaty definition of international armed conflicts and it is by now accepted that, in the words of the International Criminal Tribunal for the former Yugoslavia (ICTY), an international armed conflict arises 'whenever there is a *resort to armed force* between States'.[29] The application of IHL depends on the factual situation and not on the recognition of a state of armed conflict by the parties thereto.

The specific question that arises in cyber warfare is whether an international armed conflict can be triggered by a computer network attack in the absence of any other (kinetic) use of force. The answer depends on whether a computer network attack is (1) attributable to the state and (2) amounts to a resort to armed force – a term that is not defined under IHL.

Attribution of conduct to the state

The question of attribution of an operation to a state could raise particularly difficult questions in cyber space where anonymity is the rule rather than the exception. Yet, as long as the parties cannot be identified as two or more states it is impossible to classify the situation as an international armed conflict. While this is a challenge in factual rather than in legal terms, a way of overcoming the uncertainty in fact would be through legal presumptions. For instance, if a computer network attack originated from the government infrastructure of a particular state, a presumption could be drawn that the operation is attributable to the state – especially in light of the rule of international law that states must not knowingly allow their territory to be used for acts contrary to the rights of other states.[30] There are, however, two objections to this approach.

First, the existing rules of international law do not support such a presumption. For instance, the Articles on Responsibility of States for Internationally Wrongful Acts of the International Law Commission do not contain rules on presumption of attribution of conduct to a state. Also, the International Court of Justice (ICJ) set a high threshold for attribution of conduct to a state in the context of the right to self-defence. In the *Oil Platforms* case, it effectively held that the burden of proof rests on the state invoking the right of self-defence:

> Court has simply to determine whether the United States has demonstrated that it was the victim of an 'armed attack' by Iran such as to justify it using armed force in self-defence; and the burden of proof of the facts showing the existence of such an attack rests on the United States.[31]

29 International Criminal Tribunal for the Former Yugoslavia (ICTY), *Prosecutor* v. *Tadic*, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70 (emphasis added). The situations foreseen in Article 1(4) AP I are also considered international armed conflicts for States Party to AP I.

30 International Court of Justice (ICJ), *Corfu Channel* case (*United Kingdom* v. *Albania*), Judgment of 9 April 1949, p. 22; see also, Rule 5 of the *Tallinn Manual*, above note 27.

31 ICJ, *Oil Platforms* case *(Islamic Republic of Iran* v. *United States of America)*, Judgment of 6 November 2003, para. 57.

While this statement was made in the context of the right to self-defence in *jus ad bellum*, it can be generalized to all factual questions of attribution of conduct to a state. Since it is a presumption about facts, it would be nonsensical to presume facts for one purpose and not for another.

Second, such a presumption would also be too far-reaching in the particular context of cyber warfare. Given the difficulty of shielding computer infrastructure from manipulation and the ease with which one can remotely control a computer and pose under a different identity in cyber space, it would be placing a very high burden on governments to hold them accountable for all operations originating from their computers without any further proof.[32]

Another more frequently discussed question is the attribution of cyber attacks launched by private parties, such as hacker groups, to the state. Apart from the factual questions raised by the anonymity of cyber operations, the legal rules for attribution of acts of private parties to a state are set out in the Articles on Responsibility of States for Internationally Wrongful Acts.[33] In particular, a state is responsible for the conduct of a person or group of persons 'if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'.[34] What exactly 'direction or control' means in international law will have to be clarified over time. The ICJ requires that for an act of a private party (be it an individual or a member of an organised group) to be imputable to the state the direction or effective control of the state over the operation in the course of which the alleged violations were committed has to be demonstrated, and not only generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.[35] In the absence of such control over the specific operation it cannot be imputed to the state, even when committed by a group with a high degree of dependency on the state authorities.[36] In the same vein, the commentary on the Articles on State Responsibility requires that the state direct or control the specific operation and that the conduct be an integral part of that operation.[37] The ICTY has gone further and argued that where a group, such as an armed opposition group, is organised it is enough that the state authorities exercise 'overall control' over such an organised and hierarchically

32 The *Tallinn Manual* takes a similar legal view in Rule 7: 'The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation'.

33 International Law Commission, Draft Articles on the Responsibility of States for Internationally Wrongful Acts, *Yearbook of the International Law Commission*, 2001, Vol. II (Part Two). Text reproduced as it appears in the annex to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol. I)/Corr.4 (hereinafter 'Articles on State Responsibility').

34 Article 8 of the Articles on State Responsibility.

35 ICJ, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua* v. *United States of America*), Judgment of 27 June 1986, paras 115–116 (hereinafter '*Nicaragua* case'); ICJ, *Case concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina* v. *Serbia and Montenegro*), Judgment, 26 February 2007, paras 400–406.

36 *Nicaragua* case, above note 35, para. 115.

37 Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, Commentary on Article 8 of the Draft Articles on State Responsibility, para 3.

structured group without a need for specific control or direction over individual conduct.[38] However, the ICTY has also acknowledged that where the controlling state is not the territorial state, 'more extensive and compelling evidence is required to show that the State is genuinely in control of the units and groups' – meaning that the state's involvement in the planning of military operations or its coordination role might be more difficult to demonstrate.[39] The International Law Commission's commentary states: 'it will be a matter of appreciation in each case whether particular conduct was or was not carried out under the control of a State, to such an extent that the conduct controlled should be attributed to it'.[40] This discussion, however, is not specific to the cyber domain. Once the facts are established, the same legal criteria apply as with any other attribution of the conduct of private parties to a state. The difficulty, here again, will most likely lie in the factual assessment.

Resort to armed force

The second criterion to be fulfilled is that of 'resort to armed force' between states.

Before turning to the questions raised by cyber warfare in this respect, it is worth clarifying very briefly that the classification of a conflict as an international armed conflict under IHL (*jus in bello*) is separate from the question of *jus ad bellum*. The two are often amalgamated, including in cyber warfare.

Under *jus ad bellum*, the question is whether and when cyber operations amount to a use of force within the meaning of Article 2(4) of the UN Charter and/or to an armed attack within the meaning of Article 51 of the UN Charter, and under what circumstances they trigger a right to self-defence.[41] Whatever the views in this *jus ad bellum* discussion, it should be recalled that the objects of regulation of *jus ad bellum* and *jus in bello* are entirely distinct: while *jus ad bellum* specifically regulates inter-state relations and the requirements for the lawful resort to force between states, *jus in bello* regulates the behaviour of parties to the conflict and its object and purpose is to protect the military and civilian victims of war. Thus, an act could constitute a resort to armed force for the purpose of qualifying an international armed conflict, without prejudice to the question whether it also constitutes a use of force within the meaning of Article 2(4) of the UN Charter

38 ICTY, *Prosecutor* v. *Dusko Tadic*, IT-94-1, Appeals Chamber Judgment of 15 July 1999, para. 120. It is sometimes said that the question before the Tribunal was one of qualification of the conflict as non-international or international; however, the argument that the two questions are entirely separate is not convincing as it would lead to the conclusion that a state could be a party to a conflict by virtue of its control over an organized armed group but not be responsible for the acts committed during that conflict.

39 *Ibid.*, paras 138–140.

40 Commentary on Article 8 of the Draft Articles on State Responsibility, above note 37, para. 5.

41 See Marco Roscini, 'World wide warfare – *jus ad bellum* and the use of cyber force', in *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010, p. 85; Michael N. Schmitt, 'Computer network attack and the use of force in international law: thoughts on a normative framework', in *Columbia Journal of Transnational Law*, Vol. 37, 1998–1999, p. 885; Herbert S. Lin, 'Offensive cyber operations and the use of force', in *Journal of National Security Law and Policy*, Vol. 4, 2010, p. 63; David P. Fidler, 'Recent developments and revelations concerning cybersecurity and cyberspace: implications for international law', in *ASIL Insights*, 20 June 2012, Vol. 16, no. 22; *Tallinn Manual*, above note 27, Rules 10–17.

(though it is likely), let alone an armed attack under Article 51. This differentiation equally applies to cyber operations.

Turning to *jus in bello*, there is no treaty definition of the meaning of armed force in IHL because it is a jurisprudential criterion. Traditionally, the objective of war is to prevail over the enemy, and in traditional warfare, conflict entails the deployment of military means, leading to military confrontation. Thus, when traditional means or methods of warfare are used – such as bombing, shelling, or the deployment of troops – it is uncontroversial that these amount to armed force. But computer network attacks do not entail the use of such arms.

In the absence of traditional weapons and kinetic force – what can be considered to amount to armed force in the cyber realm?

The first step is to compare the analogous effects of computer network attacks to those of kinetic force. Most commentators are of the view that if a computer network attack is attributable to a state and has the same effects as kinetic resort to force it would trigger an international armed conflict.[42] Indeed, if a computer network attack causes airplanes or trains to collide, resulting in death or injury, or widespread flooding with large-scale consequences, there would be little reason to treat the situation differently from equivalent attacks conducted through kinetic means or methods of warfare.

This parallel is therefore useful for situations in which computer network attacks lead to death or injury, or physical damage or destruction of infrastructure. However, it might be insufficient to capture the whole range of possible effects of cyber operations and the damage that they can cause, which will not necessarily resemble the physical effects of traditional weapons. Cyber operations will frequently be resorted to in order not to physically destroy or damage military or civilian infrastructure, but rather to affect its functioning, for instance by manipulating it, and even to do so without the manipulation being detected. For instance, an electrical grid might be left untouched physically but nonetheless be put out of commission by a computer network attack. Similarly, a country's banking system might be manipulated without any of the infrastructure being damaged physically and without the manipulation of the underlying system even being noticeable for some time. At first sight, even in the absence of traditional military means or of immediate physical destruction, the potential effects of such disruptions – which might be far more extensive or severe than, say, the destruction of a particular building or group of buildings – on the population would speak in favour of considering them a resort to armed force. However, states – even victim states – might seek to avoid an escalation of international confrontations or have

42 M. N. Schmitt, 'Classification of cyber conflict', above note 28, p. 251; Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', ICRC, 2004, p. 3, available at: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 131; Nils Melzer, *Cyberwarfare and International Law*, UNIDIR Resources Paper, 2011, p. 24, available at: http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf. Nils Melzer argues that since the existence of an international armed conflict depends mainly on the occurrence of armed hostilities between states, cyber operations would trigger an armed conflict not only by death, injury, or destruction, but also by directly adversely affecting the military operations or military capacity of the state.

other reasons to avoid treating such types of attacks as triggering an armed conflict. It is difficult at this point to infer any legal positions, since states appear to remain mostly silent in the face of cyber attacks.[43] In the absence of clear state practice there are several possible approaches to this question.

One approach is to consider any hostile cyber operation that affects the functioning of objects as a resort to armed force. The object and purpose of IHL in general, and in particular the absence of a threshold of violence for the existence of an international armed conflict – which is to avoid a gap in protection, particularly the protection of the civilian population from the effects of war – would speak in favour of including such cyber operations in the definition of armed force for the purpose of triggering an armed conflict. Also, considering the importance that states attach to the protection of critical infrastructure in their cyber strategies, it might well be the case that they will consider computer network attacks by another state aimed at incapacitating such infrastructure as the beginning of an armed conflict.[44] Moreover, in the absence of an armed conflict the protective scope of IHL would not govern the situation. Other bodies of law such as *jus ad bellum*, cyber crime law, space law, or telecommunications law might, of course, apply and provide their own protection. The analysis of their effect is beyond the scope of this article, but all of the other bodies of law would pose their own set of questions. For instance, international human rights law might apply, but would a computer network attack, conducted from the other side of the globe against civilian infrastructure, fulfil the requirement of effective control for the purpose of applicability of human rights law? Also, to what extent would human rights law provide sufficient protection against the disruption of infrastructure the effects of which on the lives of civilians is not necessarily immediately identifiable?

Another approach would be to not focus exclusively on the analogous effects of the cyber operation but to consider a combination of factors that would indicate armed force. These factors would include a certain severity of the consequences of the cyber operation, the means employed, the involvement of the military or other parts of the government in the hostile operation, the nature of the target (military or not), and the duration of the operation. Taking an example outside of the cyber realm, if the chief of staff of a state's armed forces was killed in an air attack by another state this would certainly be considered as amounting to an international armed conflict. However, if he or she was killed by the sending of a

43 See also, G. Brown, above note 28.

44 N. Melzer, above note 42, p. 14. Melzer argues that reference might be made to the concept of critical infrastructure to consider the 'scale and effects' of a computer network attack for the purposes of identifying an armed attack within the meaning of Article 51 of the UN Charter. For French policy, see Agence Nationale de la Sécurité des Systèmes d'Information, *Défense et sécurité des systèmes d'informations,* available at: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf; for German policy, see Bundesamt für Sicherheit in der Informationstechnik, *Schutz Kritischer Infrastrukturen*, available at: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/Kritis/Kritis_node.html; for Canadian policy, see *National Strategy for Critical Infrastructure*, available at: http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx; for the policy of the United Kingdom, see *The UK Cyber Security Strategy*, available at: http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy; for Australian policy, see CERT Australia, *Australia's National Computer Emergency Response Team*, available at: https://www.cert.gov.au/.

poisoned letter would this also be considered in and of itself as amounting to an international armed conflict?[45] What if the target was a civilian? Are the means of destroying infrastructure relevant? For instance, if parts of a nuclear installation were sabotaged by infiltrated foreign agents, would this also amount to a resort to armed force? Does it make a difference whether the target is military or civilian?

In the cyber realm, it is possible, for instance, that states might treat computer network attacks on their military infrastructure differently from those affecting civilian systems. This might not be entirely technically logical because use of force is use of force, whether against a civilian or a military object. But the threshold of harm that states are willing to tolerate might be lower when it comes to operations that are targeted at and degrade their military capability.

Following such an approach, if the computer network attack is only punctual and of short duration, it may be that it will only be considered as armed force if its consequences are of a particular severity. The example of the Stuxnet attack as reported in the press seems to indicate that computer network attacks might – at least for some time – remain isolated hostile acts of one state towards another, without other kinetic operations, particularly if the attacker wishes to remain anonymous, wishes for the attack to remain undetected for some time, or wishes (for political or other reasons) to avoid an escalation of force and further hostilities and armed conflict. If one relied solely on whether a kinetic attack with the same effects amounts to armed force, one might have to come to the conclusion that such an attack constitutes armed force because the Stuxnet virus is reported to have caused the physical destruction of about one thousand IR-1 centrifuges which had to be replaced at the uranium enrichment facility at Natanz.[46] Indeed, if the centrifuges of a nuclear installation were destroyed by bombardment by another state's air force, such an attack would be considered a resort to armed force and trigger an international armed conflict. But because the means of the attack were not kinetic, no other attacks in connection to it were reported and it caused no known damage beyond the centrifuges, it arguably falls short of armed force triggering an international armed conflict.

To sum up, it remains to be seen if and under what conditions states will treat computer network attacks as armed force. The mere manipulation of a banking system or other manipulation of critical infrastructure, even if it leads to serious economic loss, would probably stretch the concept of armed force beyond its object and purpose – the effects are not equivalent to the destruction caused by physical means. But the disruption of such vital infrastructure as electricity or water supply systems, which would inevitably lead to severe hardship for the population if it lasted over a certain period, even if not to death or injury, might well have to be

45 In *How Does Law Protect in War?*, Vol. I, 3rd edn, ICRC, Geneva, 2011, p. 122, Marco Sassòli, Antoine Bouvier, and Anne Quintin differentiate between force by the military or other agents of the state: '[w]hen the armed forces of two States are involved, suffice for one shot to be fired or one person captured (in conformity with government instructions) for IHL to apply, while in other cases (e.g. a summary execution by a secret agent sent by his government abroad), a higher level of violence is necessary'.

46 This is the opinion of M. N. Schmitt, above note 28, p. 252; on the damage caused see D. Albright, P. Brannan and C. Walrond, above note 23; D. E. Sanger, above note 23.

considered as armed force. Although the effects are not equivalent to physical effects, they are precisely the kind of severe consequences from which IHL seeks to protect the civilian population.

It is true that states cannot circumvent their obligations under IHL by their own designation of the act. The application of the law of international armed conflict was divorced from the need for official pronouncements many decades ago in order to avoid cases in which states could deny the protection of this body of rules. This is made clear by common Article 2, as the ICRC Commentary thereto suggests:

> [a] State can always pretend, when it commits a hostile act against another State, that it is not making war, but merely engaging in a police action, or acting in legitimate self-defence. The expression 'armed conflict' makes such arguments less easy.[47]

Nonetheless, while it is true that in a specific incident, the classification of the conflict does not depend on the position of the states concerned, state practice and *opinio juris* determine the interpretation of the international law definition of 'international armed conflicts'.The classification of cyber conflicts will probably be determined in a definite manner only through future state practice.

Non-international armed conflicts

When it comes to non-international armed conflicts in the cyber realm, the main question is how to differentiate between criminal behaviour and armed conflict. It is not rare to hear or read about the actions of hacker or other groups, including groups such as Anonymous or Wikileaks, being referred to as 'war'.[48] Of course, such statements do not necessarily allude to armed conflict, or more precisely non-international armed conflict, in a legal sense. Nevertheless, it is worth clarifying the parameters for qualifying a situation as a non-international armed conflict.

In the absence of a treaty definition, state practice and doctrine has led to a definition of non-international armed conflicts that the ICTY has summed up as follows: a non-international armed conflict exists 'whenever there is … protracted armed violence between governmental authorities and organised armed groups or between such groups within a State'.[49] The 'protracted' requirement has with time

47 Jean Pictet (ed.), *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, ICRC, Geneva, 1952, p. 32. This is a different question from that of *animus belligerendi*: isolated acts are sometimes not considered to amount to armed conflict, not because they do not reach a certain level of intensity, but rather because they lack *animus belligerendi*, for instance accidental border incursions; see *UK Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004, para. 3.3.1, available at: http://www.mod.uk/NR/rdonlyres/82702E75-9A14-4EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf.

48 See, e.g., Mark Townsend *et al.*, 'WikiLeaks backlash: The first global cyber war has begun, claim hackers', in *The Observer*, 11 September 2010, available at: http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war; Timothy Karr, 'Anonymous declares cyberwar against "the system"', in *The Huffington Post*, 3 June 2011, available at: http://www.huffingtonpost.com/timothy-karr/anonymous-declares-cyberw_b_870757.html.

49 ICTY, *Prosecutor* v. *Tadic*, above note 29, para. 70.

been subsumed under a requirement that the violence must reach a certain intensity. Thus, two criteria determine the existence of a non-international armed conflict: the armed confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum of organisation.[50]

Organised armed groups

For a group to qualify as an organised armed group that can be a party to a conflict within the meaning of IHL, it needs to have a level of organisation that allows it to carry out sustained acts of warfare and comply with IHL. Indicative elements include the existence of an organisational chart indicating a command structure, the authority to launch operations bringing together different units, the ability to recruit and train new combatants, and the existence of internal rules.[51] While the group does not need to have the level of organisation of state armed forces, it must possess a certain level of hierarchy and discipline and the ability to implement the basic obligations of IHL.[52]

With respect to hacker or other similar groups, the question that arises is whether groups that are organised entirely online can constitute armed groups within the meaning of IHL. As Michael Schmitt puts it:

> The members of virtual organisations may never meet nor even know each other's actual identity. Nevertheless, such groups can act in a coordinated manner against the government (or an organized armed group), take orders from a virtual leadership, and be highly organized. For example, one element of the group might be tasked to identify vulnerabilities in target systems, a second might develop malware to exploit those vulnerabilities, a third might conduct the operations and a fourth might maintain cyber defences against counter-attacks.[53]

However, the requirement that organised armed groups must have some form of responsible command and the capacity to implement IHL would seem to preclude virtually organised groups from qualifying as organised armed groups; it would be difficult, for instance, to establish an effective system of discipline within such a group in order to ensure respect for IHL.[54] In other words, it is unlikely that groups of hackers or groups that are merely linked by virtual communication would have

50 There are two types of non-international armed conflicts. All non-international armed conflicts are covered by common Article 3 to the Geneva Conventions; in addition, the provisions of Additional Protocol II apply to non-international armed conflicts 'which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol' (AP II, Art. 1(1)).

51 For a review of the indicative factors taken into account by the ICTY in its case law, see ICTY, *Prosecutor* v. *Boskoski*, IT-04-82-T, Trial Chamber Judgement of 10 July 2008, paras 199–203. See also, ICTY, *Prosecutor* v. *Limaj*, IT-03-66-T, Trial Chamber Judgement of 30 November 2005, paras 94–134; ICTY, *Prosecutor* v. *Haradinaj*, IT-04-84-T, Trial Chamber Judgement of 3 April 2008, para. 60.

52 ICTY, *Prosecutor* v. *Boskoski*, *ibid.*, para. 202.

53 M. N. Schmitt, above note 28, p. 256.

54 *Ibid.*, p. 257.

the organisation or command (and disciplinary) structure required to constitute a party to the conflict.[55]

Intensity

Cyber operations conducted in the context of and in relation to an existing non-international armed conflict are governed by IHL. The question that arises, although it may seem futuristic at this point, is whether the required level of intensity for a non-international armed conflict could be reached if cyber means alone are being used (assuming that there are two or more parties to the conflict).

Contrary to the classification of international armed conflicts, there is agreement that a non-international armed conflict only exists if the hostilities reach a certain level of intensity. The ICTY has pointed to a number of indicative factors to be taken into account to assess the intensity of the conflict, such as the collective character of hostilities, the resort to military force, not simply police force, the seriousness of attacks and whether there has been an increase in armed clashes, the spread of clashes over territory and over a period of time, the distribution of weapons among both parties to the conflict, the number of civilians forced to flee from the combat zones, the types of weapons used, in particular the use of heavy weapons, and other military equipment, such as tanks and other heavy vehicles, the extent of destruction and the number of casualties caused by shelling or fighting.[56] Would the necessary intensity threshold be reached by cyber operations alone?

The starting point, again, is to compare the intensity of the consequences to that of kinetic operations. There is no reason why cyber operations cannot have the same violent consequences as kinetic operations, for instance if they were used to open the floodgates of dams, or to cause aircraft or trains to collide. In such circumstances, and if such violence is not merely sporadic, it may meet the threshold for a non-international armed conflict.

However, cyber operations in themselves would not have many of the effects mentioned above as indicators of the intensity of the violence (armed clashes, the deployment of military force, heavy weapons, etc.). It would likely be the consequences of the cyber operations alone that are severe enough to reach the intensity required, such as extensive destruction or disastrous effects on large parts of the population through repeated attacks.

Summary

It is likely to be uncontroversial that IHL will apply to cyber operations that are conducted within the framework of an ongoing international or non-international armed conflict alongside kinetic operations. In the absence of kinetic operations,

55 See the discussion in the *Tallinn Manual* about the different types of groups that could be considered, above note 27, Commentary on Rule 23, paras 13–15.

56 See, *e.g.*, ICTY, *Prosecutor* v. *Limaj*, above note 51, paras 135–170; ICTY, *Prosecutor* v. *Haradinaj*, above note 51, para. 49; ICTY, *Prosecutor* v. *Boskoski*, above note 51, paras 177–178.

'pure' cyber warfare is not excluded in theory, but it remains to be seen whether there will be many examples in practice in the near future.

In particular, it remains unclear in what direction state practice will tend. Given the reluctance of states to admit situations of armed conflict, in particular non-international armed conflict, the tendency could be to avoid a discourse of armed conflict. This is not only due to the likely anonymity of many computer network attacks and the practical problems of attribution, but also to the fact that most of the situations might not amount to extreme cases of physical destruction caused by computer network attacks but rather to low-level, bloodless manipulation of infrastructure. States might choose to deal with such situations as matters of law enforcement and criminal law, and not see them as being governed by the legal framework applicable to armed conflicts.

Application of the rules on the conduct of hostilities

If cyber operations are conducted in the context of an armed conflict they are subject to the rules of IHL, in particular the rules on the conduct of hostilities. The fact that cyber weapons rely on new technologies does not by itself call into question the applicability of IHL to them.

However, cyber warfare poses serious challenges to the very premises on which IHL is predicated, in particular the distinction – and actual possibility to distinguish – between military and civilian objects. Thus, the question is not so much whether the rules on the conduct of hostilities apply to cyber warfare, but rather how they apply – how they must be interpreted to make sense in this new realm.

Which acts are subject to the IHL rules on the conduct of hostilities?

Before turning to the rules on the conduct of hostilities – in particular the principles of distinction, proportionality, and precaution – it is important to address a question that has been a subject of debate for some time, namely what type of conduct, in particular what type of cyber operation, triggers the rules on the conduct of hostilities.

The question is critical. Only if a certain cyber operation is subject to the principle of distinction is it prohibited to target it directly at civilian infrastructure; and if it is directed at a military objective, the incidental effects on the civilian infrastructure must be taken into account if the operation is subject to the principle of proportionality.

The reason why this debate arises is that cyber space is different from traditional theatres of war in that the means and methods of attack do not entail traditional kinetic force, or what is commonly understood as violence. Thus, a number of cyber operations can have a severe effect on the targeted object by disrupting its functioning, but without causing the physical damage to the object that would occur in traditional warfare.

It is therefore critical for the civilian population that this question be clarified. Depending on how narrowly or broadly one views the types of cyber

operations that are subject to the rules on the conduct of hostilities, the following could be prohibited or lawful in the context of an armed conflict:

- disrupting the civilian electrical grid or water treatment system (without physical damage thereto);
- directing a denial of service attack on an Internet banking system with significant impact on the ability of a few million bank customers to access banking services;[57]
- disrupting the website of an adversary state's stock exchange without affecting its trading functions;[58]
- directing a denial of service attack on a private airline's online booking system in order to cause inconvenience to the civilian population;
- blocking the websites of Al Jazeera or the BBC because they contain information that contributes to the enemy's operational picture;
- blocking access to Facebook for the entire population because it contains pro-insurgency propaganda;
- shutting down the Internet and cell phone networks in a specific region of a country to curb propaganda by the adversary.[59]

This leads to two questions: first, do the core rules of IHL on the conduct of hostilities – that is, the principles of distinction, proportionality, and precaution – only apply to operations that constitute attacks within the meaning of IHL, or do they apply to military operations more generally? Second, which cyber operations constitute attacks within the meaning of IHL?

What triggers the rules on the conduct of hostilities: 'attacks', 'military operations', 'hostilities'?

As to the first question, the difference in views arises from the general rule on the conduct of hostilities, as formulated in Articles 48 *et seq.* of Additional Protocol I and largely recognized as customary law. Article 48 of Additional Protocol I requires that:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and

57 This occurred in Estonia in May 2007; see Larry Greenemeier, 'Estonian attacks raise concern over cyber "nuclear winter"', in *Information Week*, 24 May 2007, available at: http://www.informationweek.com/estonian-attacks-raise-concern-over-cybe/199701774.

58 See, for example, Yolande Knell, 'New cyber attack hits Israeli stock exchange and airline', in *BBC News*, 16 January 2012, available at: http://www.bbc.co.uk/news/world-16577184.

59 In Egypt, the government shut down the Internet and cell phone network for five days to curb protests: 'Internet blackouts: reaching for the kill switch', in *The Economist*, 10 February 2011, available at: http://www.economist.com/node/18112043. Similar measures were taken by the Chinese government in reaction to unrest in Xinjiang and Tibet: Tania Branigan, 'China cracks down on text messaging in Xinjiang', in *The Guardian*, 29 February 2010, available at: http://www.guardian.co.uk/world/2010/jan/29/xinjiang-china, and Tania Branigan, 'China cut off internet in area of Tibetan unrest', in *The Guardian*, 3 February 2012, available at: http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.

> military objectives and accordingly shall *direct their operations* only against military objectives. (emphasis added)

The subsequent rules on the conduct of hostilities are then mainly formulated as restrictions on attacks more specifically. For instance, Article 51 of Additional Protocol I, after stating, in its first paragraph, that '[t]he civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations', goes on to state that '[t]he civilian population as such, as well as individual civilians, shall not be the object of attack' and that 'indiscriminate attacks are prohibited'. An attack in violation of the principle of proportionality is defined in Article 51(5)(b) of Additional Protocol I as 'an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'. Article 51(6) prohibits 'attacks against the civilian population or civilians by way of reprisals'. Article 52 states that 'attacks shall be limited strictly to military objectives'. The principle of precaution in Article 57 requires that 'with respect to attacks', a number of precautions should be taken. There are many more Articles that use the term 'attack' when restricting the rights of belligerents.[60]

Thus, the first argument revolves around the question whether the rules on the conduct of hostilities are limited to those acts of hostilities that constitute attacks (as defined in Article 49 of Additional Protocol I) or whether they apply to a broader range of military operations. Broadly speaking, three views have been put forward.

Most commentators are of the opinion that the structure and wording of Additional Protocol I show that, while Article 48 provides a general principle of protection of the civilian population, this general principle is 'operationalized' in the subsequent articles. Only those cyber operations that constitute attacks are subject to the principles of distinction, proportionality, and precaution.[61] An argument made by Michael Schmitt in this regard is that some military operations can be intentionally directed against civilians, for instance psychological operations – which in his view shows that not all military operations are subject to the principle of distinction.[62]

Nils Melzer considers that the debate on the concept of attack does not provide a satisfactory answer to the question because the rules on the conduct of hostilities do not only apply to attacks strictly speaking, but to other operations, too. In his view:

> accurately understood, the applicability of the restraints imposed by IHL on the conduct of hostilities to cyber operations depends not on whether the operations in question qualify as 'attacks' (that is, the predominant form of

60 See, *e.g.*, AP I, Arts 12, 54–56.

61 M. N. Schmitt, 'Cyber operations and the *jus in bello*: key issues', in *Naval War College International Law Studies*, Vol. 87, 2011, p. 91; Robin Geiss and Henning Lahmann, 'Cyber warfare: applying the principle of distinction in an interconnected space', in *Israeli Law Review*, Vol. 45, No. 3, November 2012, p. 2.

62 M. N. Schmitt, *ibid*., p. 91.

> conducting hostilities), but on whether they constitute part of 'hostilities' within the meaning of IHL.[63]

His view is that cyber operations that are designed to harm the adversary, either by directly causing death, injury, or destruction or by directly adversely affecting military operations or military capacity, must be regarded as hostilities.[64] For instance, cyber operations aiming to disrupt or incapacitate an enemy's computer-controlled radar or weapons systems, logistic supply, or communication networks would qualify as hostilities even if they do not cause physical damage. However, cyber operations conducted for the general purpose of intelligence gathering would not fall under hostilities. As far as the non-destructive incapacitation of civilian objects is concerned, Melzer does not come to a definite conclusion but points to the dilemma between adopting a too restrictive or a too permissive interpretation of the law.[65]

Melzer's argument is attractive in that it gives effect to the very object and purpose of the rules on the conduct of hostilities, which is that 'innocent civilians must be kept outside hostilities as far as possible and enjoy general protection against danger arising from hostilities'.[66] However, it leaves open the most critical question, namely whether operations that disrupt civilian infrastructure without destroying it fall under the concept of hostilities.

Heather Harrison Dinniss argues that the prohibition of targeting civilians and civilian objects is not limited to attacks.[67] Rather, she points to the wording of Article 48 of Additional Protocol I and the first sentences of Articles 51 and 57 to argue that the civilian population must be protected not only against attacks, but also more generally against the effects of military operations. Thus, she submits that the principles of distinction, proportionality, and precaution also apply to computer network attacks that fall within the definition of a military operation. To fall within the definition, 'the computer network attack must be associated with the use of physical force, but it does not have to result in violent consequences itself'.[68]

Despite these arguments in favour of expanding the types of operations to which the rules on the conduct of hostilities must apply, it is clear that states did differentiate in Additional Protocol I between the general principles in the respective chapeaux of the rules of distinction and precaution and the specific rules relating to attacks, and that they found it necessary to define attacks specifically in Article 49 of the Protocol. It is difficult to depart from this dichotomy between military operations and attacks.

Nonetheless, Dinniss's argument makes sense of the fact that Articles 48, 51, and 57 contain general clauses that impose limitations for military operations

63 N. Melzer, above note 42.
64 *Ibid.*, p. 28.
65 *Ibid.*
66 Y. Sandoz, C. Swinarski and B. Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC/Martinus Nijhoff Publishers, Dordrecht, 1987, para. 1923 (hereinafter *Commentary on the Additional Protocols*).
67 H. H. Dinniss, above note 42, pp. 196–202.
68 *Ibid.*, p. 201.

and not only attacks and the content of which would otherwise be difficult to explain. A systematic interpretation of these clauses means that the chapeaux have a meaningful content and are not superfluous. Also, the argument made by Michael Schmitt that some operations, such as psychological operations, can be directed at civilians, implying that some *military* operations could be directed at civilians, rests on a misunderstanding of the concept of military operations. Indeed, while it is true that some cyber operations, such as psychological operations, can be directed at the civilian population, this is because they do not fall under military operations or hostilities within the meaning intended by the Protocol's drafters. According to the ICRC Commentary, the term 'operations' in Article 48 means military operations and refers to 'all movements and acts related to hostilities that are undertaken by armed forces'.[69] The term 'military operations' in Article 51 is described as 'all the movements and activities carried out by armed forces related to hostilities'.[70] And in Article 57 it 'should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat'.[71] In other words, operations such as propaganda, espionage, or psychological operations will not fall under the concepts of hostilities or military operations and are therefore not governed by the principles of distinction, proportionality, and precaution, even if they are carried out by the armed forces.

Thus, while some of the more specific content of Articles 51 and 57 of Additional Protocol I might address the specificities of attacks, there is a good argument that other military operations cannot be entirely exempt from the obligations of distinction, proportionality, and precaution, since Article 48 and the chapeaux of Articles 51 and 57 would otherwise be superfluous. However, since there is disagreement about this question it is prudent to nonetheless have a closer look at the definition of 'attack' and what types of cyber operation fall under it. Indeed, most of the cyber operations in the examples mentioned above fall under the concept of attack and would be prohibited if targeted at civilian infrastructure. Thus, it will be shown that in most of the examples given above the operations amount to attacks, and hence the question whether only 'attacks' or also 'hostilities' or 'military operations' are subject to the rules on the conduct of hostilities is moot.

What is an attack?

As said above, operations in cyber space differ from traditional warfare in that the means and methods of attack do not entail traditional kinetic force, or what is commonly understood as violence. Yet, attacks are defined in Article 49(1) of Additional Protocol I (which reflects customary IHL) as 'acts of violence against the

69 *Commentary on the Additional Protocols*, above note 68, para. 1875.
70 *Ibid.*, para. 1936.
71 *Ibid.*, para. 2191.

adversary, whether in offence or in defence'. In the mind of the drafters, this connoted physical violence.

First, it should be recalled that, based on the fact that an attack must be an act of violence, there is broad agreement nowadays that violence does not refer to the means of the attack – which would only encompass kinetic means.[72] Military operations that result in violent consequences constitute attacks. For instance, it is uncontroversial that the use of biological, chemical, or radiological agents would constitute an attack, even though the attack does not involve physical force.[73] Therefore, it has been accepted for a long time that what defines an attack is not the violence of the means, but the violence of the consequences.[74] Thus, even a data stream passed through cables or satellite could fall under the concept of attack.

The controversy lies on the side of the effects of cyber operations. It turns on those operations that do not cause death or injury to persons or physical destruction or damage to objects as kinetic operations would, but rather disrupt the functioning of objects without causing them physical damage – such as in the examples given above. As these examples show, the consequences of cyber operations do not necessarily have violent effects in that they do not cause physical damage or destruction. In the examples given above the consequences in the physical realm would be at the most indirect: for instance, if the electrical grid is shut down, this may lead to power outages for vital services such as hospitals. In some cases the consequences are limited to the ability to communicate or engage in commercial activities, such as when a banking system is disrupted. Can such operations be considered attacks within the meaning of Article 49 of Additional Protocol I?

Two positions have been put forward with respect to this question. According to Michael Schmitt's earlier writings:

> [a] cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects.[75]

Damage, in this view, only refers to physical damage. Computer network attacks that cause mere inconvenience, or merely temporarily interrupt the functioning of objects, do not constitute attacks unless they cause human suffering. Critically, the mere disruption of the functionality of an object, short of leading to such human

72 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2004, p. 84; M. N. Schmitt, above note 61, p. 5.

73 ICTY, *Prosecutor* v. *Dusko Tadić*, Decision on the Defence Motion for Interlocutory Appeal, 2 October 1995, paras. 120 and 124 (regarding chemical weapons); *Tallinn Manual*, above note 27, Commentary on Rule 30, para. 3; Emily Haslam, 'Information warfare: technological changes and international law', in *Journal of Conflict and Security Law*, Vol. 5, No. 2, 2000, p. 170.

74 Michael N. Schmitt, 'Wired warfare: computer network attack and *jus in bello*', in *International Review of the Red Cross*, Vol. 84, No. 846, June 2002, p. 377; *Tallinn Manual*, above note 27, Commentary on Rule 30, para. 3.

75 M. N. Schmitt, above note 61, p. 6.

suffering or short of resulting in physical damage or the complete and permanent loss of functionality of the targeted object, does not amount to an attack.[76]

According to Knut Dörmann, cyber operations can also constitute attacks even if they do not lead to the destruction of the object. This view is predicated on the definition of a military objective in Article 52(2) of Additional Protocol I, which states that a military objective is one '... whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'. From the term 'neutralization' it can be seen that '[i]t is irrelevant whether an object is disabled through destruction or in any other way'.[77] Critics answer that the definition of military objectives is not entirely on point because it presupposes an attack in the first place and does not define the attack in itself.[78] This criticism fails to acknowledge that 'neutralization' was meant to encompass 'an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it'.[79] This shows that the drafters had in mind not only attacks that are aimed at destroying or damaging objects, but also attacks for the purpose of denying the use of an object to the enemy without necessarily destroying it. So, for instance, an enemy's air defence system could be neutralized through a cyber operation for a certain duration by interfering with its computer system but without necessarily destroying or damaging its physical infrastructure.[80]

More recently, the Tallinn Manual 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 to objects'.[81] However, as the commentary shows, experts disagreed as to what exactly was to be understood as 'damage' to objects, and whether or what type of impairment of the functioning of an object would fall within its definition.[82]

The weakness of the first opinion is that it is under-inclusive. First, it would not make sense to consider that if a civilian object is rendered useless, regardless of the way in which this was done, it is not damaged. Whether an electrical grid is put out of order by physical damage or interference with the computer system by which it is run cannot be a relevant criterion. A contrary opinion would lead to the conclusion that the destruction of one house by bombing would be an attack, but the

76 Michael Schmitt now takes a somewhat different position and argues that '[d]estruction includes operations that, while not causing physical damage, nevertheless "break" an object, rendering it inoperable, as in the case of a cyber operation that causes a computer-reliant system to no longer function unless repaired'; '"Attack" as a term of art in international law: the cyber operations context', in *2012 4th International Conference on Cyber Conflict*, C. Czosseck, R. Ottis and K. Ziolkowski (eds), 2012, NATO CCD COE Publications, Tallinn, p. 291; see also M. N. Schmitt, above note 28, p. 252.

77 K. Dörmann, above note 42, p. 4.

78 M. N. Schmitt, above note 61, p. 8.

79 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff Publishers, Dordrecht, 1982, p. 325.

80 This was reportedly done in the September 2007 Israeli air attack on a Syrian structure believed to be housing a nuclear-weapons development programme. Israel had hacked into the Syrian air defences and controlled them during the attack; see 'Arab & Israeli cyber-war', in *Day Press News*, 22 September 2009, available at: http://www.dp-news.com/en/detail.aspx?articleid=55075.

81 *Tallinn Manual*, above note 27, Rule 30.

82 *Ibid.*, Commentary on Rule 30, paras 10–12.

disruption of an electrical grid supplying thousands or millions of people would not. Second, reference to the principle of proportionality gives an indication of the incidental effects against which the rules on the conduct of hostilities mean to protect civilians, namely excessive 'incidental loss of civilian life, injury to civilians, damage to civilian objects'. 'Damage' is different from 'destruction'. It means 'harm . . . impairing the value or usefulness of something . . .'.[83] Thus, disrupting the functioning of certain systems by interfering with their underlying computer systems can amount to damage insofar as it impairs their usefulness. Third, the view that there must be complete and permanent loss of functionality without physical damage does not make sense in information technology. Since data can always be restored or changed there is no permanent and complete loss of functionality of an object short of physical damage. Thus, an attack must also be understood to encompass such operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary.

Yet, an overly broad interpretation of the term 'attack' would mean that all interferences with civilian computer systems would amount to attacks: the interruption of email or social network communications, of online booking or shopping systems, etc. To equate such disruptions of what are essentially communication systems with attacks would probably go beyond the scope of what was envisaged by the rules on the conduct of hostilities. These rules have traditionally sought to prevent damage to civilian infrastructure that manifests itself in the physical world, not interference with propaganda, communication, or economic life. In today's world, the reliance of civilian life on communication systems blurs these lines, and it is not easy to distinguish between what is 'mere' communication and what goes beyond.

Existing IHL norms and their object and purpose provide a number of indications for distinguishing between operations that amount to attacks and those that do not. First, as said above, the concept of 'attacks' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare.[84] Cyber operations that are equivalent to espionage, to the dissemination of propaganda, to embargoes, or other non-physical means of psychological or economic warfare will not fall under the definition of 'attacks'.

Second, IHL does not prohibit blockades or economic sanctions that deliberately target not only the military but also the civilian population and economy. Thus, the term 'attack' cannot comprise cyber operations that would be tantamount to economic sanctions. This is not to say that such operations would not have limits under IHL (such as the prohibition of destroying, removing, or rendering useless objects indispensable to the survival of the civilian population or obligations with respect to the passage of humanitarian relief), but, since they do not constitute attacks, there is no prohibition under IHL against directing them at civilians.

83 *Concise Oxford Dictionary.*
84 M. Bothe *et al.*, above note 79, p. 289.

Third, the rules on the conduct of hostilities do not intend to prohibit all operations that interfere with civilian communication systems. For instance, not all denial of service operations,[85] such as blocking a television broadcast or a university website, would amount to an attack. Mere interference with propaganda, for instance, will probably also not constitute an attack. The parallel of such operations in the physical world is probably the jamming of radio communications or television broadcasts – which is not considered an attack in the sense of IHL.

To differentiate between those operations that amount to attacks and those that do not, the criterion of inconvenience is sometimes put forward.[86] The argument is inconvenience, such as rationing of food, need not be taken into account for 'incidental civilian damage'. Therefore, something that causes mere inconvenience cannot amount to and attack. While the criterion of inconvenience is not without its merits, there might be disagreement on what represents inconvenience in terms of interferences with cyber technology and communication. For instance, while it might be possible to agree that the interruption of an online booking system causes mere inconvenience, consensus might be more difficult to achieve around issues such as interference with banking services. It remains to be seen how these interferences will be considered in the future, in particular in state practice.

Summary

In sum, a cyber operation can constitute an attack within the meaning of IHL when it causes death or injury or physical destruction or damage, but also if it interferes with the functioning of an object by disrupting the underlying computer system. Thus, if an air defence system is put out of order by a cyber operation, if a cyber operation disrupts the functioning of an electrical grid, or if the banking system is disabled, this amounts to an attack. However, not all cyber operations directed at disrupting the functioning of infrastructure amount to attacks. Where the operation is not directed at the physical infrastructure relying on the computer system, but essentially at blocking communication, it is more akin to jamming radio signals or television broadcasts – unless it is, of course, part of an attack, such as blocking an air defence system. The difference lies in the fact that in some cases it is the communication function of cyber space alone that is being targeted; in other cases, it is the functioning of the object beyond cyber space in the physical world. While interference with cyber systems that leads to disruption in the physical world constitutes attacks, the question of

85 That is, cyber operations that make the targeted computer's service unavailable to the usual users or customers.

86 M. N. Schmitt, above note 74, p. 377; Program on Humanitarian Policy and Conflict Research at Harvard University, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare,* 2010, Commentary on Article 1(d), para. 7, available at: http://www.ihlresearch.org/amw/aboutmanual.php (hereinafter *Commentary on HPCR Manual on Air and Missile Warfare*); Michael N. Schmitt, 'Cyber operations in international law: the use of force, collective security, self-defense and armed conflict', in National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks*, Washington, DC, The National Academies Press, 2010, p. 155.

interference with communication systems such as email systems or the media is not entirely solved.

The principle of distinction

The principle of distinction requires that parties to a conflict distinguish at all times between civilians and combatants and between civilian objects and military objectives.[87] It is, in the words of the ICJ, a cardinal principle of IHL.[88] Attacks may only be directed against combatants or military objectives. This means that, in planning and carrying out cyber operations, the only targets permissible under IHL are military objectives, such as computers or computer systems that make an effective contribution to concrete military operations. Attacks via cyber space may not be directed against computer systems used in purely civilian installations.

Some of the discussion around military objectives in cyber space is a cause for concern from the point of view of the protection of the civilian population. Indeed, it appears that cyber operations might be particularly well suited to target certain civilian objects, because they enable the belligerents to reach some targets that might have been less reachable previously, such as financial networks or medical data networks.[89] Some have argued that cyber warfare might lead to a sort of 'expanded target list'[90] compared to traditional warfare. Also, because cyber operations can disable an object's functioning without causing physical damage, some commentators have argued that the use of cyber operations expands the range of legitimate targets because it enables attacks with reversible effects against objects that it would otherwise be prohibited to attack.[91] It has also been argued that:

> [t]he potentially non-lethal nature of cyber weapons may cloud the assessment of an attack's legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare.[92]

Against this background, it is important to recall the rules of IHL governing attacks on objects and to address a number of specific legal problems that might arise through the use of computer network attacks.

87 AP I, Arts 48, 51 and 52; Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Vol. I, Rules*, (hereinafter 'Study on customary international humanitarian law'), ICRC and Cambridge University Press, 2005, Rules 1–10.

88 ICJ, *Legality of the Threat of Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, para. 78.

89 Michael N. Schmitt, 'Ethics and military force: the *jus in bello*', Carnegie Council for Ethics in International Affairs, 7 January 2002, available at: http://www.carnegiecouncil.org/studio/multimedia/20020107/index.html.

90 This is the expression used by Eric Talbot Jensen, 'Unexpected consequences from knock-on effects: a different standard for computer network operations?', in *American University International Law Review*, Vol. 18, 2002–2003, p. 1149.

91 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, 1999, pp. 963 *ff*.

92 Jeffrey T. G. Kelsey, 'Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare', in *Michigan Law Review*, Vol. 106, 2007–2008, p. 1439.

Under IHL, civilian objects are all objects that are not military objectives.[93] Military objectives are defined in Article 52(2) of Additional Protocol I as:

> those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

According to Article 52(3) of Additional Protocol I, objects that are normally dedicated to civilian purposes shall be presumed not to be used to make an effective contribution to military action. So, for instance, if some particularly sensitive civilian infrastructure, such as most chemical plants, relies on a closed computer network, this network must be presumed to be civilian.

As the wording of Article 52(2) makes clear, there must be a close nexus between the potential target and military action. The term 'military action' denotes the enemy's war-fighting capabilities. This nexus is established through the four criteria of nature, location, purpose, and use. Nature refers to the intrinsic character of an object, such as a weapon. Objects that are not military in nature may also make an effective contribution to military action by virtue of their particular location, their purpose, or their present use.

In this respect, four issues in particular should be highlighted that can have potentially serious implications for civilian infrastructure: most importantly, the fact that most international cyber infrastructure is in practice so-called dual-use infrastructure; the question whether factories producing hardware and software used by the military become military objectives; the targeting of objects with so-called war-sustaining capability; and the legal consequences of the social media networks being used for military purposes, such as information on targets.

Dual-use objects in cyberspace

So-called dual-use objects – a term not found as such in IHL provisions – are those that are used for both civilian and military purposes. Due to their use for military purposes, they become military objectives under Article 52(2) of Additional Protocol I and legitimate targets of attack. Examples frequently given are parts of the civilian infrastructure that supply the military for their operations, such as power plants or electrical grids.

According to today's prevailing view, an object cannot be a civilian and a military object at the same time. The moment it is used for military action it becomes a military objective in its entirety (except if separable parts remain civilian – for instance, different buildings of a hospital).[94] As opposed to the ICRC's 1956 proposal, which, outside purely military material and installations, mentioned

93 AP I, Art. 52(1), reflective of customary international law; *Study on customary international humanitarian law,* above note 87, Rule 9.

94 *The Commander's Handbook on the Law of Naval Operations*, Department of the Navy/Department of Homeland Security, USA, July 2007, para. 8.3; *Tallinn Manual*, above note 27, Commentary on Rule 39, para 1.

civilian communication, transport, or industry 'of fundamental military importance' or 'fundamental importance for the conduct of the war',[95] it is generally considered today that the object becomes a military objective even if its military use is only marginal compared to its civilian use. For instance, if a plant provides a small percentage of fuel used in military operations, even if this is not its main purpose, it becomes a military objective.

The dangers in cyber space are evident: virtually the entire international cyber infrastructure – that is, computers, routers, cables, and satellites – is used for both civilian and military communications.[96] An undersea cable that transports military communications becomes a military objective – with the consequence that (subject to other rules of IHL, namely proportionality) it can not only be the subject of a cyber operation to interrupt the military communication, it could also be destroyed. Similarly, a server containing 5 per cent military data would become a legitimate target. This is particularly important to bear in mind in an era of increased cloud computing, where the users of cloud computing are typically not aware on what servers their data are being stored and what other data are stored on that server. It is reported that approximately 98 per cent of US government communications use civilian-owned and -operated networks.[97]

The danger that any part of the cyber infrastructure could be targeted is very real. Indeed, while in certain circumstances states might seek to disable very specific functions of the adversary's military infrastructure, the fact that all of cyber space is used for military operations means that in any armed conflict it will be of important strategic interest to degrade the adversary's communication networks and access to cyber space. This will mean denying the adversary access to critical routes in cyber space, degrading its main routers or access to major communication nodes, not just targeting specific computer systems of the military infrastructure.[98] Unlike in the naturally occurring theatres of war, such as land or airspace, the man-made theatre of cyber space means that the

95 In the ICRC's Draft Rules for the Limitation of Danger incurred by the Civilian Population in Time of War, the list drawn up by the organization with the help of military experts and presented as a model, subject to modification, was as follows: 'I. The objectives belonging to the following categories are those considered to be of generally recognized military importance: . . . (6) *Those* of the lines and means of communication (railway lines, roads, bridges, tunnels and canals) which are of *fundamental military importance*; (7) The installations of broadcasting and television stations; telephone and telegraph exchanges of *fundamental military importance*; (8) Industries of fundamental importance for the conduct of the war: (a) industries for the manufacture of armaments . . .; (b) industries for the manufacture of supplies and material of a military character . . .; (c) factories or plant constituting *other* production and manufacturing centres of fundamental importance for the conduct of war, such as the metallurgical, engineering and chemical industries, *whose nature or purpose is essentially military*; (d) storage and transport installations whose basic function it is to serve the industries referred to in (a)–(c); (e) installations providing energy *mainly for national defence*, e.g., coal, other fuels, or atomic energy, and plants producing gas or electricity mainly for military consumption.' (emphasis added). See *Draft Rules for the Limitation of the Dangers incurred by the Civilian Population in Time of War*, ICRC, 1956, available at: http://www.icrc.org/ihl/INTRO/420?OpenDocument.

96 See also R. Geiss and H. Lahmann, above note 61, p. 3.

97 Eric Talbot Jensen, 'Cyber warfare and precautions against the effects of attacks', in *Texas Law Review*, Vol. 88, 2010, p. 1534.

98 US Department of Defense, *Quadrennial Defence Review Report*, February 2010, pp. 37–38, available at: http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

belligerents will not only focus on the travelling weapon but on the routes themselves.[99] For instance, in airspace, only the aircraft qualifies as a military objective; in cyber warfare, however, the physical infrastructures through which the cyber weapons (malicious codes) travel qualify as military objectives.

The humanitarian consequences of this situation are of utmost concern for the protection of the civilian population. In a world in which a large part of civilian infrastructure, civilian communication, finance, economy, and trade rely on international cyber infrastructure it becomes all too easy for parties to conflicts to destroy this infrastructure. There is no need to argue that a banking network is used for military action, or that an electrical grid is dual use. Disabling the major cables, nodes, routers, or satellites that these systems rely on will almost always be justifiable by the fact that these routes are used to transmit military information and therefore qualify as military objectives.

The Tallinn Manual states:

> the circumstances under which the Internet in its entirety could be attacked [are] so highly unlikely as to render the possibility purely theoretical at the present time. Instead, the International Group of Experts agreed that, as a legal and practical matter, virtually any attack against the Internet would have to be limited to certain discrete segments thereof.[100]

It also mentions the principles of precaution and proportionality, which would have to be respected if the Internet or large portions thereof were targeted. However, while this might seem reassuring at first sight, it leaves the problem that whether or not the Internet in its entirety can be targeted, any of its segments can be targeted if used for military communication and its destruction or neutralization offers a definite military advantage (again subject to proportionality and precautions).

Furthermore, cyber space is resilient in the sense that if information cannot flow through one channel there are multiple routes and alternatives and the information can usually be transmitted through another path. As the Tallinn Manual states:

> Cyber operations pose unique challenges in this regard. Consider a network that is being used for both military and civilian purposes. It may be impossible to know over which part of the network military transmissions, as distinct from civilian ones, will pass. In such cases, the entire network (or at least those aspects in which transmission is reasonably likely) qualifies as a military objective.[101]

The consequence of this would be that in some circumstances virtually all parts of the Internet might qualify as a military objective because they are all possible routes for the transmission of military information.

99 R. Geiss and H. Lahmann, above note 61, p. 9.
100 *Tallinn Manual*, above note 27, Commentary on Rule 39, para 5.
101 *Ibid.*, Commentary on Rule 39, para 3.

The prevailing wide interpretation of dual-use objects as military objectives is already not without its problems in the physical world.[102] In cyber space the consequences could be exacerbated to an extreme point where nothing civilian remains and the basic rule that the civilian population shall enjoy general protection against dangers arising from military operations becomes virtually empty of content, subject only to the principles of proportionality and precaution.

Lastly, if most of the cyber infrastructure around the world is of a dual-use nature and could be considered a military objective, this raises the fundamental question of the geographical limits of the armed conflict. There are truly no borders in cyber space, and computer systems from anywhere can be (remotely) attacked, manipulated, or transformed into means of warfare and military objectives. It must be borne in mind that the consequence would not only be that such computers could be counter-hacked by the targeted computer systems. In theory, as military objectives they could be destroyed through kinetic means. For instance, a botnet could be used to launch an attack destroying an adversary's cyber infrastructure. To conduct such an operation, the party to the conflict launching the attack would remotely control thousands or millions of computers around the world, which would transmit the malware to the target computers. If such a botnet were to lead to all of the millions of computers that it uses throughout the world being defined as military objectives liable to attack, the result would be a sort of total cyber war. The logical consequence, that all these computers around the world become military targets, would be contrary to the foundations of the law of neutrality in international armed conflicts (and mainly with its underlying rationale, which is to spare the third country and its inhabitants from the effects of hostilities) or with the geographical limitations of the battlefield in non-international armed conflicts.[103] In an international armed conflict the law of neutrality would put certain limits on the right of the attacked state to defend itself by attacking infrastructure in neutral territory.[104] First, the attacked state must notify the neutral state and give it a reasonable time to terminate the violation; second, the attacked state is allowed to take measures to terminate the violation of neutrality only if that violation

102 See also Marco Sassòli, 'Legitimate targets of attacks under international humanitarian law', Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge, 27–29 January 2003, HPCR, 2003, pp. 3–6, available at: http://www.hpcrresearch.org/sites/default/files/publications/Session1.pdf; William M. Arkin, 'Cyber warfare and the environment', in *Vermont Law Review*, Vol. 25, 2001, p. 780, describing the effects in 1991 of the air attacks on Iraqi electrical power on not only the civilian electricity supply, but also water distribution, purification, sewage, and the health infrastructure; R. Geiss and H. Lahmann, above note 61, p. 16.

103 The boundaries of the battlefield of non-international armed conflict are a matter of dispute and would go far beyond the scope of this article – but the difficulties raised by cyber warfare seem almost unanswerable in this respect. For the ICRC's view, see ICRC, *Report on International Humanitarian Law and the challenges of contemporary armed conflicts*, 31st International Conference of the Red Cross and Red Crescent, Geneva, 28 November–1 December 2011, Report prepared by the ICRC, October 2011, pp. 21–22; for a discussion of the geographical implications in cyber warfare, see the *Tallinn Manual*, above note 27, Commentary on Rule 21.

104 These are derived from Article 22 of the San Remo Manual on International Law Applicable to Armed Conflicts at Sea, of 12 June 1994, available at: http://www.icrc.org/IHL.nsf/52d68d14de6160e0c12563da005fdb1b/7694fe2016f347e1c125641f002d49ce!OpenDocument.

constitutes a serious and immediate threat to its security and only if no other feasible and timely alternative exists to respond to the threat. These restrictions are relatively broad, and in order to be truly protective for the civilian population of the neutral state they would presumably have to be narrowly interpreted. In non-international armed conflicts the law of neutrality is not applicable. However, it would completely break open the geographical limits of the battlefield of non-international armed conflicts to consider that the armed conflict takes place anywhere where a computer, cable, or node is used for military action (and would therefore normally constitute a military objective).

In sum, it becomes clear that, in cyber space, the principle of distinction appears to hold little promise for the protection of civilian cyber infrastructure and all the civilian infrastructure that relies on it. In such situations the main legal protection for civilian infrastructure will be the principle of proportionality – which will be addressed below.[105]

The problem that, in cyber space, most infrastructure is dual use is certainly the most important concern and other legal issues appear less pressing. Some of them will nonetheless be addressed in the following paragraphs.

Corporations that produce information technology used for military action

Since hardware and software are used for much military machinery, information technology (IT) corporations that produce them could be seen as 'war-supporting military objectives'[106] – in parallel with munitions factories. This would likely mean that a number of IT corporations around the world would constitute legitimate targets as many of them probably provide some IT infrastructure for the military.[107] Eric Talbot Jensen, for instance, asks whether the Microsoft Corporation would constitute a legitimate target 'based on the support it provides to the U.S. war effort by facilitating U.S. military operations'. In his view, '[t]he fact that the corporation and its headquarters provide a product that the military finds essential to function, as well as customer service to support that product, may provide sufficient facts to conclude that it is a dual use target', but he doubts whether a definite military advantage would accrue from such an attack.[108]

The example shows that the parallel with munitions factories should not be overstretched. The relevant criterion of Article 52(2) of Additional Protocol I is that the object must by its use make an effective contribution to military action.

105 *Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 22(d), para. 7; *Tallinn Manual*, above note 27, Commentary on Rule 39, para. 2; E. T. Jensen, above note 90, p. 1157.

106 M. N. Schmitt, above note 61, pp. 8 *ff*.

107 It is reported that the US Department of Defense will host contractors who want to propose new technologies for cyber warfare: S. Shane, above note 3.

108 E. T. Jensen, above note 90, pp. 1160 and 1168; see also E. T. Jensen, above note 97, p. 1544: 'If a civilian computer company produces, maintains, or supports government cyber systems, it seems clear that an enemy could determine that company meets the test of Article 52 and is targetable'.

First, corporations as such are not physical objects, but legal entities, and so the question would instead be whether any of their locations (that is, buildings) have become military objectives. Second, there is a difference between weapons and IT tools. Weapons are by their nature military objectives, which generic IT systems are not. Thus, one might have to differentiate between factories that actually develop what might be called cyber weapons, that is specific codes/protocols that will be used for a specific computer network attack (so, for instance, the location where a specific virus like Stuxnet is being developed), and those that just provide the military with generic IT supplies, which are not so different from, say, food supplies.[109]

War-fighting capability or war-sustaining capability?

In cyber warfare, where the temptation to target civilian infrastructure is possibly higher than in traditional warfare, it is important to keep in mind that for a civilian object to become a military objective its contribution to military action must be directed towards the actual war-fighting capabilities of a party to the conflict. If an object merely contributes to the war-sustaining capability of a party to the conflict (its general war effort), it does not qualify as a military objective.

In the US *Commander's Handbook on the Law of Naval Operations*, the expression 'makes an effective contribution to military action' from Article 52(2) of Additional Protocol I has been widened and replaced by 'effectively contribute to the enemy's war-fighting or war-sustaining capability'.[110] This position is mainly geared towards economic targets, which may indirectly support or sustain the enemy's military capability.[111] A 1999 assessment of the law by the US Department of Defense's Legal Counsel in respect of cyber operations states:

> purely civilian infrastructures must not be attacked unless the attacking force can demonstrate that a definite military advantage is expected from the attack. . . . In a long and protracted armed conflict, damage to the enemy's economy and research and development capabilities may well undermine its war effort, but in a short and limited conflict it may be hard to articulate any expected military advantage from attacking economic targets.[112]

109 The *Tallinn Manual* also fails to come to a definite conclusion on this question: 'The difficult case involves a factory that produces items that are not specifically intended for the military, but which nevertheless are frequently put to military use. Although all of the Experts agreed that the issue of whether such a factory qualifies as a military objective by use depends on the scale, scope, and importance of the military acquisitions, the Group was unable to arrive at any definitive conclusion as to the precise thresholds.'

110 *The Commander's Handbook on the Law of Naval Operations*, above note 94, para. 8.2.

111 M. N. Schmitt, 'Fault lines in the law of attack', in S. Breau and A. Jachec-Neale (eds), *Testing the Boundaries of International Humanitarian Law*, British Institute of International and Comparative Law, London, 2006, pp. 277–307. For the underlying rationale of such an approach, see, for instance, Charles J. Dunlap, 'The end of innocence, rethinking noncombatancy in the post-Kosovo era', in *Strategic Review*, Vol. 28, Summer 2000, p. 9; Jeanne M. Meyer, 'Tearing down the façade: a critical look at current law on targeting the will of the enemy and Air Force doctrine', in *Air Force Law Review*, Vol. 51, 2001, p. 143; see J. T. G. Kelsey, above note 92, p. 1447, who advocates a new definition of military objectives in order to include certain civilian infrastructure and services.

112 Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, p. 7, available at: http://www.au.af.mil/au/awc/awcgate/dod-io-legal/

These approaches overlook the legal restrictions imposed by IHL. Damage to the enemy's civilian economy, research, and development capabilities in themselves is never allowed under IHL, regardless of the perceived military advantage, and regardless of the duration of the conflict. Otherwise, there would be no limits to warfare as virtually the entire economy of a country can be considered to be war-sustaining.[113] It is particularly important to recall this in the context of cyber warfare and to point to the potentially devastating consequences of a broad definition of military objectives for the civilian population.

The media and social networks

The Tallinn Manual addresses the thorny question of social networks being used for military purposes:[114]

> Recent conflicts have highlighted the use of social networks for military purposes. For example, Facebook has been used for the organization of armed resistance operations and Twitter for the transmission of information of military value. Three cautionary notes are necessary. First, it must be remembered that this Rule [that an object used for both civilian and military purposes is a military objective] is without prejudice to the rule of proportionality and the requirement to take precautions in attack … Second, the issue of the legality of cyber operations against social networks depends on whether such operations rise to the level of an attack. If the operations do not, the issue of qualification as a military objective is moot … Third, this does not mean that Facebook or Twitter as such may be targeted; only those components thereof used for military purposes may be attacked [so long as the attack complies with other requirements of the law of armed conflict].[115]

The qualification of social networks such as Facebook or Twitter as military objectives would pose a number of problems. Indeed such networks contain such vast amounts of data – most of which is entirely unrelated to the specific information that would need to be targeted – that it would appear to be difficult to

dod-io-legal.pdf. The position of the United States in the latest Report of the Secretary-General is ambiguous at best when it states that the principles of *jus in bello* 'prohibit attacks on purely civilian infrastructure, the disruption or destruction of which would produce no meaningful military advantage'. If this is meant to imply that attacks on purely civilian infrastructure would not be allowed if the destruction or disruption would produce a meaningful military advantage, it would be incompatible with IHL, which never allows attacks on purely civilian objects (Report of the Secretary-General, 15 July 2011, UN Doc. A/66/152, p. 19).

113 M. Sassòli, above note 102; Stephan Oeter, 'Means and methods of combat', in Dieter Fleck (ed.), *The Handbook of Humanitarian Law in Armed Conflicts*, Oxford University Press, Oxford, 1995, para. 442.5.

114 It has been reported, for instance, that NATO acknowledged that social media such as Twitter, Facebook, and YouTube contributed to their targeting process in Libya, after being checked against other sources: Graeme Smith, 'How social media users are helping NATO fight Gadhafi in Libya', in *The Globe and Mail*, 14 June 2011; Tim Bradshaw and James Blitz, 'NATO draws on Twitter for Libya strikes', in *The Washington Post*, 16 June 2011.

115 *Tallinn Manual*, above note 27, p. 114.

qualify any such network as one military objective. A further question would be whether it is technically possible to only attack those components that are used for military purposes among the unstructured data of such networks.

An equally difficult question arises with respect to the media. The Tallinn Manual states:

> An interesting case involves media reports. If such reports effectively contribute to the enemy's operational picture, depriving the enemy of them might offer a definite military advantage. Some members of the International Group of Experts took the position that cyber infrastructure supporting their transmission qualifies as a military objective, although they cautioned that the infrastructure could only be attacked subject to the Rules regarding attack, especially those on proportionality … and precautions in attack … In particular, they noted that the latter requirement would usually result in a requirement to only mount cyber operations designed to block the broadcasts in question. Other Experts argued that the nexus between the cyber infrastructure's contribution to military action was too remote to qualify the infrastructure as a military objective. All members of the International Group of Experts agreed that such assessments are necessarily very contextual.[116]

Even if a particular report would make an effective contribution to military action, this should not lead to the conclusion that either the media corporation responsible or the cyber infrastructure transmitting it can be the subject of attack. As far as media corporations are concerned, the potential consequences of accepting their targetability would be momentous. Take an international broadcaster like the BBC. First, the expression 'contributing to the enemy's operational picture' is far too broad, is broader than making a direct contribution to the enemy's military action, as required by Article 52(2) of Additional Protocol I. Second, even if the media report contained tactical information, for instance on specific targets, the proposition that the media company could be targeted is highly problematic. Beyond the corporation itself, if all of the cyber infrastructure through which the reports are transmitted were to be considered a military objective, this would mean a large part of the globe's cyber infrastructure – again, as with dual-use objects, bearing in mind that the consequence of considering an object a military objective is that it can also be targeted by kinetic means, implying that the physical location from where and through which the reports are being transmitted – could be damaged or destroyed. Last, as said above, the example of media corporations brings into sharp contrast the problem of the geographical limits of the battlefield. Also, the law of neutrality would impose a number of limits in an international armed conflict on a state's ability to target infrastructure in a neutral state.[117]

116 *Ibid.*, p. 113.
117 See above section '*Dual-use objects in cyberspace*'.

The prohibition of indiscriminate attacks and of indiscriminate means and methods of warfare

Indiscriminate attacks are prohibited.[118] Indiscriminate attacks are those:

- which are not directed at a specific military objective,
- which employ a method or means of combat which cannot be directed at a specific military objective, or
- which employ a method or means of combat the effects of which cannot be limited as required by IHL,

and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction. Parties to a conflict 'must consequently never use weapons that are incapable of distinguishing between civilian and military targets'.[119]

As said above, the fact that most of cyber space can probably be considered dual use is likely to make it difficult to separate military from civilian infrastructure. However, even where military and civilian infrastructure can still be separated and distinguished, another risk is that attacks will be indiscriminate because of the interconnectedness of cyber space.[120] Cyber space consists of innumerable interwoven computer systems across the world. Even if military computer systems are separate from civilian ones they are often interconnected with commercial, civilian systems and rely on them in whole or in part. Thus, it might well be impossible to launch a cyber attack on military infrastructure and limit the attack or its effects to just that military objective. Viruses and worms are examples of methods of computer network attack that could fall into this category if their effects are not limited by their creators. The use of a worm that replicates itself and cannot be controlled, and might therefore cause considerable damage to civilian infrastructure, would be a violation of IHL.[121]

This concern has been dismissed by some commentators as exaggerated, particularly based on the fact that, because most cyber operations would only be efficient if they targeted very specific, highly specialized systems, their effects on other computers would not be damaging. The example given is that of the Stuxnet virus, which was very precisely written to be used against the nuclear installations in the Islamic Republic of Iran.[122]

Indeed, if a virus is introduced into a closed military system or written to prevent its spreading into other systems, there might be no risk for outside civilian infrastructure. But it is quite imaginable that a party to a conflict takes no such precautions or develops cyber weapons that have effects on networks that it might

118 *Study on customary international humanitarian law*, Rule 12; AP I, Art. 51(4).
119 ICJ, above note 88, para. 78.
120 K. Dörmann, above note 42, p. 5.
121 The worm could either not be able to be directed at a specific military objective (cf. *Study on customary international humanitarian law*, Rule 12 (b), AP I, Art. 51(4)(b)) or have effects that cannot be limited as required by IHL (see *Study on customary international humanitarian law*, Rule 12(c), AP I, Art. 51(4)(c)).
122 T. Rid, above note 24.

not have foreseen. The fact that it is possible to design cyber weapons that are not indiscriminate does not mean that there is not a high potential for indiscriminate attacks. Even the Stuxnet virus – as reported in the media – shows how difficult it is to control the effects of viruses; it is reported that this virus was not intended to infect computers outside the targeted systems of the nuclear installations, yet somehow it replicated itself outside Iran.[123] While the spread of the virus far beyond the intentions of its creators might not have caused any damage, it shows how difficult it is to control that spread.

There is therefore a twofold burden on the belligerent parties. First, they may not employ cyber weapons that are indiscriminate by nature, such as viruses or worms that replicate without any possibility of controlling them (in parallel to bacteriological weapons, for instance). The use of such weapons should be outlawed during the review of the weapon when it is being developed or acquired – if it can never be employed without striking military and civilian objectives alike, it is incompatible with IHL requirements.[124] Second, at each attack, the belligerent party has to verify whether, in the particular circumstances of the case, the cyber weapon employed can be and is directed at a military target and whether its effects can be controlled within the meaning of IHL.

The principle of proportionality

Considering the dual-use nature of most cyber infrastructure, on the one hand, and the risk of repercussions on civilian infrastructure when exclusively military computers or computer systems are targeted due to the interconnectedness of cyber space, on the other, there is serious concern that civilian infrastructure will be severely affected by cyber operations in armed conflicts. Thus, the principle of proportionality becomes a crucial rule for the protection of the civilian population.

The principle of proportionality is formulated in Article 51(5)(b) of Additional Protocol I, which reflects customary international law.[125] An attack is prohibited if it 'may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.

As said above, damage to objects means 'harm . . . impairing the value or usefulness of something . . .'.[126] Thus, it is clear that the damage to be taken into account comprises not only physical damage, but also the loss of functionality of civilian infrastructure even in the absence of physical damage. It has been argued that 'cyber attacks may change the weight given to temporary consequences' in the

123 D. E. Sanger, above note 23.
124 This follows not only from AP I, Art. 36 for states party to the Protocol, but also from the general obligation of belligerent parties not to employ indiscriminate weapons.
125 *Study on customary international humanitarian law*, above note 87, Rule 14.
126 *Concise Oxford Dictionary*.

proportionality assessment,[127] but there is no legal basis for this in IHL. As Geiss and Lahmann put it, any other reading would have the consequence that:

> whereas the destruction of a single civilian car would amount to legally relevant, albeit rather insignificant, 'collateral damage', the disconnection of thousands or millions of households, companies and public services from the internet or other communication services, or the severance of online financial transactions for a country's entire economy and the corresponding economic and societal effects as such would not count as relevant elements to be factored into the proportionality calculus.[128]

It should be recognized, however, that if and when computer network attacks do cause damage to civilian infrastructure, including by temporarily disrupting it, the principle of proportionality suffers from a number of limitations (as it also does in traditional warfare).

First, as in all applications of the principle of proportionality, there remains a measure of uncertainty about what can be considered as excessive incidental damage to civilian objects as compared to the concrete and direct military advantage. Findings that incidental damage to civilian infrastructure is excessive as compared to the military advantage appear to be few and far between.[129] This is not to say that proportionality poses no limits at all to attacks. But it remains to be seen how it will be interpreted with respect to cyber attacks.

On the one hand, it may be argued that since cyber operations are still in their infancy, little is known about their impact and commanders cannot be expected to anticipate their effects, and it is difficult to know what is 'expected' incidental civilian loss or damage in cyber warfare. On the other hand, this uncertainty is quantitative rather than qualitative; precisely because of the interwoven networks, the consequences for civilian infrastructure are obvious. In other words, incidental damage must be expected in most cases, even if its exact extent is difficult to assess.

Second, while it is by now largely undisputed that reverberating effects – that is, indirect second- or third-tier effects from an attack – must be taken into account, there remains some discussion as to how far this obligation

127 Oona Hathaway *et al.*, 'The law of cyber-attack', in *California Law Review*, Vol. 100, No. 4, 2012, p. 817.
128 R. Geiss and H. Lahmann, above note 61, p. 17.
129 See Louise Doswald-Beck, 'Some thoughts on computer network attack and the international law of armed conflict', in Michael N. Schmitt and Brian T. O'Donnell (eds), *Computer Network Attack and International Law,* International Law Studies, Vol. 76, 2002, p. 169 : '… examples … have usually been when either the possible target was something that was military in nature but in the circumstances unusable or where the object's value as a military objective could not be verified.' See also, ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia* (hereinafter *Final Report to the Prosecutor*), 13 June 2000, para. 19. In response to the bombardment of the Pancevo industrial complex and of a petroleum refinery in Novi Sad by NATO forces during the war in Kosovo in 1999, which lead to the release of some 80,000 tonnes of crude oil into the soil and of many tonnes of other toxic substances, the Committee stated that '[i]t is difficult to assess the relative values to be assigned to the military advantage gained and harm to the natural environment, and the application of the principle of proportionality is more easily stated than applied in practice'.

goes.[130] Considering the wording of Article 51(5)(b) of Additional Protocol I ('may be expected'), it is reasonable to argue that foreseeable damages, even if they are long-term, second- and third-tier damages, must be taken into account.[131] In cyberspace, because of the interconnectedness of networks, it may be more difficult to foresee the effects than with a classic kinetic weapon, but at the same time it is all the more critical to do everything feasible to assess those effects. In practical terms this leads mainly to the question of precautions to be taken in attacks. Given the interconnectedness of information networks and the systems that rely on them, what can be expected of a commander in terms of verification in order to assess what the reverberating effects of the computer network attack will be?[132]

The principle of precaution

The principle of precaution in IHL has two aspects: precautions in attack and precautions against the effects of attacks.[133]

Precautions in attack

In the conduct of military operations constant care must be taken to spare the civilian population or civilian objects.[134] Particular precautions required by IHL include doing everything feasible to verify that targets are military objectives,[135] and taking all feasible precautions in the choice of means and methods of warfare with a view to avoiding and in any event minimizing incidental civilian casualties and damages to civilian objects.[136] It also requires that parties to the conflict cancel or suspend an attack if it becomes apparent that it will cause excessive 'collateral damage'.[137]

Thus, precautions may entail such obligations as taking measures to gather all available information to verify the target and the potential incidental effects of an attack.[138] In cyber warfare, precautions may include mapping the network of

130 See, *e.g., Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 14, para. 4; Michael N. Schmitt, 'Computer network attack: the normative software', in *Yearbook of International Humanitarian Law*, The Hague, TMC Asser Press, 2001, p. 82.

131 *Tallinn Manual*, above note 27, Commentary on Rule 51, para. 6; R. Geiss and H. Lahmann, above note 61, p. 16.

132 This must be differentiated from an indiscriminate attack in which the effects cannot be controlled.

133 See AP I, Arts 57 and 58; *Study on customary international humanitarian law*, above note 87, Rules 15–24.

134 AP I, Art. 57(1); *Study on customary international humanitarian law*, above note 87, Rule 15.

135 AP I, Art. 57(2)(a)(i); *Study on customary international humanitarian law*, above note 87, Rule 16.

136 AP I, Art. 57(2)(a)(ii); *Study on customary international humanitarian law*, above note 87, Rule 17.

137 AP I, Art. 57(2)(b); *Study on customary international humanitarian law*, above note 87, Rule 19.

138 ICTY, *Final Report to the Prosecutor*, para. 29: In its Final Report, the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia described the obligation thus: 'A military commander must set up an effective intelligence gathering system to collect and evaluate information concerning potential targets. The commander must also direct his forces to use available technical means to properly identify targets during operations. Both the commander and the aircrew actually engaged in operations must have some range of discretion to determine which available resources shall be used and how they shall be used.'

the adversary,[139] which will often be part of the development of computer network attacks in any case if they are specifically designed for a particular target computer system. If the information available is incomplete – as might be the case in cyber space due to its interconnectedness – the scope of the attack might have to be limited to only those targets on which there is sufficient information.[140]

The principle of precaution might require special technical expertise. The *Tallinn Manual* states that '[g]iven the complexity of cyber operations, the high probability of affecting civilian systems, and the sometimes limited understanding of their nature and effects on the part of those charged with approving cyber operations, mission planners should, where feasible, have technical experts available to assist them in determining whether appropriate precautionary measures have been taken'.[141] If expertise, and therefore the capacity to evaluate the nature of the target or the incidental civilian loss or damage, is not available, the attacker might have to refrain from the attack.

It is likely, however, that many cyber attacks in defence will be automatic, pre-programmed cyber operations against intrusions from the outside.[142] Such 'hack-backs' are automatic and simply target the computers from which the intrusion originates; as they are tackling a technical problem, they are not concerned with the civilian or military nature of the computers. In such contexts, and given that such cyber attacks will come from thousands or even millions of computers, states will have to carefully evaluate the lawfulness of such automatic hack-backs in light of the principle of precaution.

From another angle, the principle of precaution could, in some instances, entail an obligation to resort to cyber technology when it is available. Indeed, cyber operations might also cause less incidental damage to civilians or civilian infrastructure than kinetic operations. For instance, it might be less damaging to disrupt certain services used for military and civilian purposes than to destroy infrastructure completely. However, the extent of an obligation to resort to more sophisticated technology – in this case cyber technology – is not entirely settled. Indeed, there is as yet no international consensus that belligerent parties must at all times employ the most precise or the most technologically advanced weapon (the discussion on this issue mainly takes place with respect to precision-guided munitions).[143] Nonetheless, the principle of precaution contains an obligation not only to abide by the principles of distinction and proportionality, but also to do everything feasible to 'avoid and in any event minimize' incidental civilian loss or damage. In such cases, the principle of precaution arguably implies that

139 E. T. Jensen, above note 90, p. 1185.
140 *Tallinn Manual*, above note 27, Rule 53, para. 6.
141 *Ibid.*, Rule 52, para. 6.
142 According to AP I, Art. 49, such defensive operations are also attacks' that have to abide by the principles of distinction, proportionality, and precaution.
143 See Jean-François Quéguiner, 'Precautions under the law governing the conduct of hostilities', in *International Review of the Red Cross*, Vol. 88, No. 864, December 2006, p. 801; *Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 8, para. 2.

commanders should choose the less harmful means available at the time of the attack to achieve their military aim.[144]

Precautions against the effects of attacks

The principle of precautions against the effects of attacks requires that the parties to conflicts, among others, 'to the maximum extent feasible . . . endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives' and 'take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers arising from military operations'.[145] This means that states have an obligation to either keep military objects apart from civilians and civilian objects, or (and particularly if this is not feasible) to take other measures to protect civilians and civilian infrastructure from the dangers resulting from military operations.

As the Tallinn Manual states, this may include 'segregating military from civilian cyber infrastructure; segregating computer systems on which critical civilian infrastructure depends from the Internet; backing up important civilian data elsewhere; making advance arrangements to ensure the timely repair of important computer systems against foreseeable kinds of cyber attack; digitally recording important cultural or spiritual objects to facilitate reconstruction in the event of their destruction during armed conflict; and using antivirus measures to protect civilian systems that might suffer damage or destruction during an attack on military cyber infrastructure'.[146]

It is indeed frequently advocated that military and civilian networks should be segregated.[147] As the legal assessment of the US Department of Defense recommends, 'where there is a choice, military systems should be kept separate from infrastructures used for essential civilian purposes'.[148] However, this is hardly realistic. In the early days of the Internet, construction probably proceeded without consideration for these matters. There exist, of course, closed military networks, and certain highly sensitive civilian infrastructure is also segregated from outside networks. But considering the inherent weakness of the rule on segregating civilian from military objects (Article 58(a) of Additional Protocol I), which only obliges states to endeavour to separate military and civilian objects and only to the maximum extent feasible, it is highly unlikely that it will be interpreted in state practice as entailing an obligation to segregate civilian and military networks. While it might theoretically be feasible to do this, it would be so impractical and costly as to

144 K. Dörmann, above note 42; Michael N. Schmitt, 'The principle of discrimination in 21st century warfare', in *Yale Human Rights and Development Law Journal*, Vol. 2, 1999, p. 170; *Commentary on HPCR Manual on Air and Missile Warfare*, above note 86, Commentary on Rule 32(b), para. 3, on weapons with greater precision or lesser explosive force.

145 AP I, Art. 58; *Study on customary international humanitarian law*, above note 89, Rules 22 and 24.

146 *Tallinn Manual*, above note 27, Commentary on Rule 59, para. 3.

147 E. T. Jensen, above note 97, pp. 1533–1569; Adam Segal, 'Cyber space governance: the next step', Council on Foreign Relations, *Policy Innovation Memorandum No. 2*, 14 November 2011, p. 3, available at: http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

148 Department of Defense Office of General Counsel, above note 112, p. 7.

be seen as unfeasible in the sense of Article 58 of Additional Protocol I. Governments would have to create their own computer hardware and software for military use and establish their own military lines of communication, including cables, routers, and satellites, throughout the world.[149]

In addition, the separation of military from civilian cyber infrastructure rests on the assumption that they are distinct and should be kept distinct. Strictly speaking, Article 58 does not prohibit dual use: it rests on the assumption that there is a differentiation between civilian and military objects, even if some civilian objects are used as military objectives. Already in the physical world, large parts of critical infrastructure are dual use, for example, electrical grids, but also, in many instances, oil pipelines, power plants, and road networks. In cyber space the principle becomes relatively meaningless where the problem is not the co-location of civilian and military infrastructures but the fact that it is one and the same.[150]

The question, then, is whether Article 58(c) of Additional Protocol I would require that at least some civilian infrastructure (for instance, nuclear power stations, chemical factories, hospitals) is protected against damage in the case of a cyber attack, requiring that states take action to maintain its functionality. For instance, Eric Talbot Jensen recommends that, in order to comply with its obligation under Article 58, the US take a number of measures such as mapping the civilian systems, networks, and industries that will become military objectives, ensure that the private sector is sufficiently protected, establish or maintain hack-back solutions, or create a strategic reserve of Internet capability.[151] The tendency of numerous countries to protect their critical infrastructure certainly goes in this direction – though it is unlikely that governments conceive of this protection in terms of passive precautions within the meaning of Article 58(c).

Conclusion

As noted in the introduction, cyber operations will entail new means and methods of combat, the effects of which are still untested or poorly understood. It appears, however, that military use of information technology poses serious challenges to the application of IHL, in particular with respect to the very premise that civilian and military objects can and must be distinguished in armed conflict. In order to obtain clear statements about how states intend to respect the principles of distinction, proportionality, and precaution, this should be discussed more openly and candidly than has been the case until now.

In light of the dangers that cyber warfare poses to civilian infrastructure a number of solutions are being proposed *de lege lata* and *de lege ferenda*. One proposal is for states to make declaratory statements about digital safe havens, that is, civilian targets that they will consider off-limits in the conduct of cyber

149 E. T. Jensen, above note 97, pp. 1551–1552.
150 See also R. Geiss and H. Lahmann, above note 61, p. 14.
151 E. T. Jensen, above note 97, pp. 1563 ff.

operations.[152] If agreed among the parties, this would be akin to the demilitarized zones foreseen in Article 60 of Additional Protocol I. It would require the process of dialogue and confidence-building measures currently advocated, which go beyond the subject of this article. Adam Segal stipulates that 'there is likely to be relatively easy consensus around some areas – hospitals and medical data – and much less agreement around others such as financial systems, power grids, and Internet infrastructure'.[153] While this is an interesting path to explore – and might ultimately be explored as part of an international dialogue on confidence-building measures – it is probably not being overly pessimistic to be sceptical about the short-term feasibility of this avenue. Given the concealed nature of much of what appears to be the current manipulation and infiltration of cyber space, it is not clear how much trust will be put in agreements or statements on cyber areas that would be off-limits for military use.

Another proposal made by Geiss and Lahmann is to expand the list of 'works and installations containing dangerous forces' in Article 56 of Additional Protocol I by analogy.[154] This could apply to specific cyber infrastructure components, such as major Internet exchange nodes or central servers on which millions of important civilian functions rely. Just like dams, dykes, and nuclear electrical generating stations, they could not be made the object of attack even if they constituted military objectives because the dangers for the civilian population would always be considered to outweigh the military advantage of attacking them. However, Geiss and Lahmann also acknowledge that it is unlikely that such a proposal would find favour among states. In particular, although the reverberating effects of neutralizing or destroying cyber infrastructure could be momentous, it would be difficult to argue that they would be comparable to the release of emissions such as radioactive material or the waters of a dam. If, however, they had such comparable disastrous effects, the underlying rationale of Article 56 of Additional Protocol I could equally provide a persuasive argument to protect cyber infrastructure.

Going further, the challenges posed by the cyber realm have also raised the question whether (some) means and methods of cyber warfare should be banned altogether or regulated by international treaty. As mentioned in the introduction, some states have advocated for a new treaty in this respect, although the contours of what should and should not be allowed are not always entirely clear. A parallel debate is also being held among cyber security experts and academics. Some have proposed new treaties on cyber warfare,[155] while others argue that there should be a type of disarmament treaty with a ban on all or at least some cyber weapons.[156]

152 A. Segal, above note 147.
153 *Ibid.*
154 R. Geiss and H. Lahmann, above note 61, p. 11.
155 Mark R. Shulman, 'Discrimination in the law of information warfare', in *Columbia Journal of Transnational Law*, Vol. 37, 1999, p. 964; Davis Brown, 'A proposal for an international convention to regulate the use of information systems in armed conflict', in *Harvard International Law Journal*, Vol. 47, No. 1, Winter 2006, p. 179; Duncan B. Hollis, 'Why states need an international law for information operations', in *Lewis and Clark Law Review*, Vol. 11, 2007, p. 1023.
156 Mary Ellen O'Connell, 'Cyber mania', in *Cyber Security and International Law*, Meeting Summary, Chatham House, 29 May 2012, available at: http://www.chathamhouse.org/sites/default/files/public/

Still others counter that a treaty would not be enforceable because of the difficulties of attribution, that it would be technically impossible to distinguish between instruments of cyber warfare and cyber espionage, that the banned weapons could be less damaging than traditional weapons, and that verification would be impossible.[157]

Some commentators propose other solutions, such as 'informal multilateralism',[158] or an international cyber security organisation, along the lines of the International Atomic Energy Agency, as an independent platform for international cooperation, with the aim of developing treaties to control cyber weapons.[159]

It is difficult to know, at this point, where these discussions will lead, and especially whether states are willing to discuss the real dangers of cyber warfare openly and to take measures to prevent the worst-case scenarios. In the meantime, if parties to conflicts choose cyber weapons during armed conflicts they must be aware of the existing legal framework as a minimum set of rules to respect, despite their limitations. They must instruct and train their forces accordingly. It is important to promote the discussion of these issues, to raise awareness of the need to assess the humanitarian impact of developing technologies, and to ensure that they are not prematurely employed under conditions in which respect for the law cannot be guaranteed.

In conclusion, there is no question that IHL applies to cyber warfare. However, whether it will provide sufficient protection to the civilian population, in particular by shielding civilian infrastructure from harm, will depend on how IHL – whose drafters did not envisage such operations – is interpreted with respect to them. Only if interpreted in good faith and with the utmost care will it be possible to protect civilian infrastructure from being directly targeted or from suffering damage that could potentially be disastrous for the civilian population. Even then, considering the potential weaknesses of the principles of distinction, proportionality, and precaution – and in the absence of more profound knowledge of offensive capabilities and effects – it cannot be excluded that more stringent rules might be necessary.

Research/International%20Law/290512summary.pdf; Misha Glenny, 'We will rue Stuxnet's cavalier deployment', in *The Financial Times*, 6 June 2012, citing Russian antivirus expert Eugen Kaspersky; Scott Kemp, 'Cyberweapons: bold steps in a digital darkness?', in *Bulletin of the Atomic Scientists*, 7 June 2012, available at: http://thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness; Bruce Schneier, 'An international cyberwar treaty is the only way to stem the threat', in *US News*, 8 June 2012, available at: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat; Duncan Holis, 'An e-SOS for cyberspace', in *Harvard International Law Journal,* Vol. 52, No. 2, Summer 2011, who argues for a system of e-sos.

157 Herb Lin and Thomas Rid, 'Think again: cyberwar', in *Foreign Policy,* March/April 2012, p. 7, available at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full; Jack Goldsmith, 'Cybersecurity treaties: a skeptical view', in Peter Berkowitz (ed.), *Future Challenges in National Security and Law* (forthcoming), available at: http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

158 A. Segal, above note 108.

159 Eugene Kaspersky, 'Der Cyber-Krieg kann jeden treffen', in *Süddeutsche*, 13 September 2012, available at: http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.1466845.