Volume 94 Number 886 Summer 2012

INTERNATIONAL REVIEW of the Red Cross

Cyber conflict and international humanitarian law

Herbert Lin

Dr Herbert Lin is Chief Scientist at the Computer Science and Telecommunications Board of the National Research Council (NRC), where he has also been Study Director of major projects on public policy and information technology. He was co-editor of the NRC's 2009 report *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*,[1] and a 2010 NRC study on cyber deterrence, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.*

Abstract

Conflict in cyberspace refers to actions taken by parties to a conflict to gain advantage over their adversaries in cyberspace by using various technological tools and people-based techniques. In principle, advantages can be obtained by damaging, destroying, disabling, or usurping an adversary's computer systems ('cyber attack') or by obtaining information that the adversary would prefer to keep secret ('cyber espionage' or 'cyber exploitation'). A variety of actors have access to these tools and techniques, including nation-states, individuals, organized crime groups, and terrorist groups, and there is a wide variety of motivations for conducting cyber attacks and/or cyber espionage, including financial, military, political, and personal. Conflict in cyberspace is different from conflict in physical space in many dimensions, and attributing hostile cyber operations to a responsible party can be difficult. The problems of defending against and deterring hostile cyber operations remain intellectually unresolved. The UN Charter and the Geneva Conventions are relevant to cyber operations, but the specifics of such relevance are today unclear because cyberspace is new compared to these instruments.

doi:10.1017/S1816383112000811

Keywords: cyber conflict, cyberspace, cyber attack, national security, international humanitarian law.

In the twenty-first century, information is the key coin of the realm, and thus entities, from nation-states to individuals are increasingly dependent on information and information technology (IT), including both computer and communications technologies. Businesses rely on information technology to conduct operations (such as payroll and accounting, recording inventory and sales, and research and development (R&D)). Distribution networks for food, water, and energy rely on IT at every stage, as do transportation, health care, and financial services. Factories use computer-controlled machinery to manufacture products more rapidly and more efficiently than ever before.

Military forces are no exception. IT is used to manage military forces – for example, for command and control and for logistics. In addition, modern precision-guided munitions illustrate how the use of IT embedded in weapons systems increases their lethality and reduces the collateral damage associated with the use of such weapons. Movements and actions of military forces can be coordinated through networks that allow information and common pictures of the battlefield to be shared widely.

Terrorists and other non-state armed groups also use IT. Although the kinetic weapons of terrorists are generally low-tech, terrorist use of IT for recruitment, training, and communications is often highly sophisticated.

A common term for networked information technology is 'cyberspace'. The US Department of Defense defines cyberspace as a domain characterized by 'the use of electronics [that is, IT] and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures'.[2] Using this definition, civilian, military, and terrorist entities operate in cyberspace to conduct their business and operations.

As noted in the writer's biography, the writer of this article is a US scientist and a policy analyst rather than a lawyer, but it is important to be aware that a full understanding of the cyber domain requires insight into technology, policy, and the law. Further, the analysis presented in this article generally reflects US perspectives on the issues discussed.

This article begins with a short primer on the nature of conflict in cyberspace, describing the tools and techniques of such conflict, the hostile (offensive) operations in cyberspace made possible by such tools and techniques, the actors that might use these tools and techniques, and the reasons why they might

1 The intellectual content of this report is drawn primarily from National Research Council (NRC), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, William Owens, Kenneth Dam, Herbert Lin (eds.), National Academies Press, Washington, DC, 2009, available at: http://www.nap.edu/catalog.php?record_id=12651. All internet references were accessed in August 2012, unless otherwise stated.

2 Department of Defense, '2006 National Military Strategy for Cyberspace Operations', available at: http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

do so. The second section addresses three important issues about conflict in cyberspace: comparing conflict in cyberspace to conflict in physical space using traditional kinetic weapons, attributing hostile operations to a responsible party, and defending against and deterring hostile operations. The third section addresses a number of important international legal issues relating to the UN Charter and the Geneva Conventions; it also addresses some of the potential human rights implications of offensive operations in cyberspace. The fourth section comments on the role of the private sector as both a target, and a conductor of offensive operations in cyberspace. The final section addresses the largely unexplored topics of preventing conflict escalation and terminating conflicts in cyberspace.

Perhaps the most important point of this paper is that it seeks to identify important questions associated with conflict in cyberspace, especially with respect to the international legal regime that governs such conflict. Alas, it cannot provide many answers to these questions – indeed, the need to develop new knowledge and insight into technical and legal instruments to support informed policy-making in this area will provide full employment for many analysts for a long time to come.

What is conflict in cyberspace?

Given the increasing importance of information and IT, it is not surprising that parties to a conflict might seek to gain advantage over their adversaries by using various tools and techniques for exploiting certain aspects of cyberspace – what this paper will call 'conflict in cyberspace' or 'cyber conflict'.[3]

Tools and techniques

The tools and techniques of conflict in cyberspace can be usefully separated into tools based on technology and techniques that focus on the human being. Offensive tools and techniques allow a hostile party to do something undesirable. Defensive tools and techniques seek to prevent a hostile party from doing so.

Technology-based tools

An offensive tool requires three components:

1. *Access* refers to how the hostile party gets at the IT of interest. Access may be remote (such as through the Internet, through a dial-up modem attached to it, or through penetration of the wireless network to which it is connected). Alternatively, access may require close physical proximity (for example, spies acting or serving as operators, service technicians, or vendors). Close access is also a possibility anywhere in the supply chain (for example, during chip

3 This definition implies that 'armed conflict' or 'military conflict' are subsets – and only subsets – of the broader term 'conflict', which may entail a conflict over economic, cultural, diplomatic, and other interests as well as conflict involving military matters or the use of arms.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

fabrication, assembly, loading of system software, shipping to the customer, or operation).
2. A *vulnerability* is an aspect of the IT that can be used to compromise it. Vulnerabilities may be accidentally introduced through a design or implementation flaw, or introduced intentionally (see close access, above). An unintentionally introduced defect (or 'bug') may open the door for opportunistic use of the vulnerability by an adversary.
3. *Payload* is the term used to describe the mechanism for affecting the IT after access has been used to take advantage of a vulnerability. For example, once a software agent (such as a virus) has entered a computer, its payload can be programmed to do many things – reproducing and retransmitting itself, or destroying or altering files on the system. Payloads can be designed to do more than one thing, or to act at different times. If a communications channel is available, payloads can be remotely updated.

Defensive tools address one or more of these elements. Some tools (such as firewalls) close off routes of access that might be inadvertently left open. Other tools identify programming errors (vulnerabilities) that can be fixed before a hostile party can use them. Still others serve to prevent a hostile party from causing damage with any given payload (for example, a confidential file may be encrypted so that even if a copy is stolen from the system, it is useless to the hostile party).

People-based techniques

People interact with IT, and it is often easier to trick, bribe, or blackmail an insider into doing the bidding of a hostile party than it is to gain access through purely technological means. For example, close access to a system may be obtained by bribing a janitor to insert a USB flash drive into a computer. A vulnerability may be installed by blackmailing a programmer into writing defective code. Note that in such cases, technical tools and people-based techniques can be combined.

Defensive people-based techniques essentially involve inducing people not to behave in ways that compromise security. Education teaches (some) people not to fall for scams that are intended to obtain log-in names and passwords. Audits of activity persuade (some) people not to use IT in ways that are suspicious. Rewards for reporting persuade (some) people to report questionable or suspicious activity to the proper authorities.

Possible offensive operations in cyberspace

Offensive activity in cyberspace can be described as cyber attack or cyber exploitation.

- Cyber attack refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting through these systems or networks. The activities may also affect entities connected to these systems

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

and networks. A cyber attack might be conducted to prevent authorized users from accessing a computer or information service (a denial of service attack), to destroy computer-controlled machinery (the alleged purpose of the Stuxnet cyber attack[4]), or to destroy or alter critical data (such as timetables for the deployment of military logistics). Note that the direct effects of a cyber attack (damage to a computer) may be less significant than the indirect effects (damage to a system connected to the computer).

- Cyber exploitation refers to deliberate activities designed to penetrate computer systems or networks used by an adversary, for the purposes of obtaining information resident on or transiting through these systems or networks. Cyber exploitations do not seek to disturb the normal functioning of a computer system or network from the user's point of view – indeed, the best cyber exploitation is one that such a user never notices. The information sought is generally information that the adversary wishes not to be disclosed. A nation might conduct cyber exploitations to gather valuable intelligence information, just as it might deploy human spies to do so. It might seek information on an adversary's R&D program for producing nuclear weapons, or on the adversary's order of battle, its military operational plans, and so on. Or it might seek information from a company's network in another country in order to benefit a domestic competitor of that company. Of particular interest is information that will allow the country to conduct further penetrations on other systems and networks in order to gather additional information.

Note that press accounts often refer to 'cyber attacks' when the activity conducted is in fact a cyber exploitation.

Actors/participants and their motivations

What actors might conduct such operations? The nature of information technology is such that the range of actors who can conduct operations of national-level significance is potentially large. Certain nation-states, such as the United States, China, Russia, and Israel, are widely regarded as having potent offensive cyber capabilities, although less-developed nation-states can also conduct offensive operations in cyberspace.

To date, the known actors who have perpetrated acts of cyber exploitation and cyber attack are sub-national parties – mostly individuals, and mostly for profit. It is often alleged that Russia was behind the cyber attacks against Estonia in 2007 and Georgia in 2008,[5] that China is behind a number of high-profile cyber exploitations against entities in many nations,[6] and that the United States and/or Israel were responsible for the cyber attack on Iranian nuclear facilities (Stuxnet);

4 For a primer on Stuxnet, see 'Cyberattacks on Iran – Stuxnet and Flame', in *The New York Times*, 9 August 2012, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?scp=1-spot&sq=stuxnet&st=cse.

5 See NRC, above note 1, box 3.4.

6 As this article goes to press, the American security firm Mandiant released on 19 February 2012, a detailed report concluding that a special unit of the Chinese People's Liberation Army is responsible for a large

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

however, none of these nations have officially acknowledged undertaking any of these activities, and conclusive proof, if any exists, that the political leadership of any nation ordered or directed any of these activities has not been made public.

A variety of sub-national actors – including individuals, organized crime groups, and terrorist groups – might conduct cyber attacks and/or cyber exploitations. Indeed, some (but only some) such operations can be conducted with information and software found on the Internet and hardware available at any local computer store.

Motivations for conducting such operations – that is, for engaging in cyber conflict – also span a wide range. One of the most common motivations today is financial. Because a great deal of commerce is enabled through the Internet or through the use of IT, some parties are cyber criminals who seek illicit financial gain through their offensive actions. Cyber exploitations can yield valuable information, such as credit card numbers or bank log-in credentials; trade secrets; business development plans; or contract negotiation strategies. Cyber attacks can disrupt the production schedules of competitors, destroy valuable data belonging to a competitor, or be used as a tool to extort money from a victim. Perpetrators might conduct a cyber attack for hire (it is widely believed that the cyber attack on Estonia was conducted using a rented cyber weapon).[7]

Another possible reason for such operations is political – the perpetrator might conduct the operation to advance some political purpose. A cyber attack or exploitation may be conducted to send a political message to a nation, to gather intelligence for national purposes, to persuade or influence another party to behave in a certain manner, or to dissuade another party from taking certain actions.

Still another reason for conducting such operations is personal – the perpetrator might conduct the operation to obtain 'bragging rights', to demonstrate mastery of certain technical skills, or to satisfy personal curiosities.

Lastly, such operations may be conducted for military reasons, in the same way that traditional military operations involving kinetic weapons are used.

Some important issues

Cyber conflict raises many complex issues for national security. The issues described below are presented as a sample of the most salient, but this overview is not intended to be comprehensive.

How conflict in cyberspace compares to conflict in physical space

Much about cyber conflict upends our understanding of how conflict might unfold. Although most observers would acknowledge clear differences between the cyber

fraction of the cyber intrusions conducted against American corporations, organizations, and government agencies. See http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

7 William Jackson, 'Cyberattacks in the present tense, Estonian says', in *Government Computing News*, 28 November 2007, available at http://www.gcn.com/online/vol1_no1/45476-1.html.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

and physical domains, it is easy to underestimate just how far-reaching these differences are. Consider, for example, the impact of:

- Venue for conflict. In traditional kinetic conflict (TKC – that is, *conflict* conducted with kinetic weapons by organized, governmentally controlled forces), many military activities (specifically, those in the air and on or under the ocean) occur in a space that is largely separate from the space in which large numbers of civilians are found. In cyber conflict, the space in which many military activities occur is one in which civilians are ubiquitous.
- The offence-defence balance. In TKC, offensive technologies and defensive technologies are often in rough balance. In cyber conflict (at least prior to the outbreak of overt hostilities), the offence is inherently superior to the defence, in part because the offence needs to be successful only once, whereas the defence needs to succeed every time, and in part because there is no way to guarantee that harmful, incorrect, or flawed information inputs (either programs or data) will not be entered into an IT-based system.
- Attribution. TKC is conducted by military forces that are presumed to be under the control of national governments. No such presumptions govern the actors participating in cyber conflict, and definitive attribution of acts in cyberspace to national governments is very difficult or impossible (see discussion below).
- Capabilities of non-state actors. In TKC, the effects that are produced are generally a function of the number of military personnel that can engage in combat, and since such numbers tend to be smaller for non-state actors than those available to states, the effects that non-state actors can produce are relatively small compared to those that can be produced by comparably equipped state actors. In cyber conflict, non-state actors can leverage the capabilities of IT to produce some of the large-scale effects that can be achieved by large-scale actors.
- The importance of distance and national borders. In TKC, distance looms large, and violations of national borders are significant. In cyber conflict, distance is more or less irrelevant, and penetrations of national boundaries for both attack and exploitation occur routinely and without being noticed.

Attribution

As noted above, a key technical attribute of cyber operations is the difficulty of attributing any given cyber operation to its perpetrator. In this context, the definition of 'perpetrator' can have many meanings:

- The attacking machine that is directly connected to the target. Of course, this machine – the one most proximate to the target – may well belong to an innocent third party who has no knowledge of the operation being conducted.
- The machine that launched or initiated the operation.
- The geographical location of the machine that launched or initiated the operation.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

- The individual sitting at the keyboard of the initiating machine.
- The nation under whose jurisdiction the named individual falls (for example, by virtue of his physical location when he typed the initiating commands). Thus, a machine located in Russia could be controlled by an individual in France acting at the behest of the Iranian government.
- The entity under whose auspices the individual acted, if any.

In practice, a judgement of attribution is based on all available sources of information, which could include technical signatures and forensics collected regarding the act in question, intelligence information (such as intercepted phone calls monitoring the conversations of senior leaders), prior history (similarity to previous cyber operations, for example), and knowledge of those with incentives to conduct such operations.

It is commonly said that attribution of hostile cyber operations is impossible. This statement does have an essential kernel of truth: if the perpetrator makes no mistakes, uses techniques that have never been seen before, leaves behind no clues that point to himself, does not discuss the operation in any public or monitored forum, and does not conduct his actions during a period in which his incentives to conduct such operations are known publicly, then identification of the perpetrator may well be impossible.

Indeed, sometimes all of these conditions are met, and policy-makers rightly despair of their ability to act appropriately under such circumstances. But in other cases the problem of attribution is not so dire, because one or more of these conditions are not met, and it may be possible to make some useful (if incomplete) judgements about attribution. For example, even if one does not know the location of the machine that launched a given attack, signals or human intelligence might provide the identity of the entity under whose auspices the attack was launched. The latter might be all that is necessary to take further action against the perpetrator.

Deterrence and defence in cyberspace

A great deal of policy attention today is given to protecting information and IT that is important to the nation. There are two ways (not mutually exclusive) of providing such protection: defending one's assets against offensive actions, and dissuading a hostile party from taking such actions.

Defence involves measures that decrease the likelihood that an offensive action will succeed. These include measures that prevent a perpetrator from gaining access, that eliminate vulnerabilities, or that enable the victim of an operation to recover quickly from a successful offensive action.

Dissuasion involves persuading an adversary not to launch the offensive action in the first place. Deterrence is an approach to dissuasion that involves the certain imposition of high costs on any adversary that is unwise enough to initiate an offensive action. Such costs may be imposed on an identified adversary in the cyber domain in response to some hostile action in cyberspace. There is no

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

logical need to restrict a response to this domain, however, and decision-makers have a wide choice of response options that include changes in defensive postures, law enforcement actions, economic actions, diplomacy, and military operations involving traditional forces, as well as cyber operations.

The United States' national security posture has traditionally been based on a robust mix of defence and deterrence, but cyberspace turns this mix on its head. The inherent superiority of offensive cyber operations over defensive operations has led many to consider a strategy of deterrence to dissuade adversaries from conducting such operations against the United States. But senior policy-makers have concluded that because deterrence in cyberspace is such a difficult strategy to implement, we must do a more effective job of defence.[8] If the reader finds this intellectual state of affairs unsatisfactory, he is not alone.

The laws of war as they apply to cyber conflict

The differences between TKC and cyber conflict have pervasive effects on how we should conceptualize conflict. The Law of Armed Conflict (LOAC) and the laws regulating the use of force in international relations found in the UN Charter were developed to cope with TKC, but although the fundamental principles underlying these laws remain valid, how they apply to cyber conflict in any specific instance is at best uncertain today. The intuitions of commanders (and their legal advisers) have been honed in environments of TKC. And apart from a few specialists, an understanding of cyber conflict does not exist broadly within the personnel of today's armed forces.

Armed conflict between nations (or 'international armed conflict') is today governed by two bodies of international law: *jus ad bellum*, the body of law that governs the question when a nation may have recourse to armed force (any such recourse between states amounting to an 'armed conflict'), and *jus in bello*, the body of law that regulates how a party engaged in an armed conflict must behave. The sources of both bodies of law are listed in Article 38 of the Statute of the International Court of Justice (ICJ), and are to be found primarily in treaties (written agreements among nations) and customary international law (that is, rules that come from 'a general practice accepted as law' and that exist independent of treaty law).[9]

This section provides a short overview of the legal dimensions of cyber conflicts. Other articles in this publication address this topic in more detail.[10]

8 William Lynn, 'Defending a new domain: the Pentagon's cyberstrategy', in *Foreign Affairs*, Vol. 89, No. 5, September–October 2010, available at: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

9 Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Volume I: Rules*, ICRC/Cambridge University Press, Cambridge, 2005, available at: http://www.icrc.org/eng/war-and-law/treaties-customary-law/customary-law/index.jsp.

10 See Cordula Droege, 'Get off my cloud – Cyber warfare, international humanitarian law and the protection of civilians' in this edition of the *Review*.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

Jus ad bellum

Today, the primary treaty source of *jus ad bellum* is the United Nations Charter, which explicitly forbids all signatories from using force (Article 2(4)) except in two instances – when authorized by the Security Council (pursuant to a resolution issued under Chapter VII of the UN Charter), and when a signatory is exercising its inherent right of self-defence when it has been the target of an armed attack (pursuant to Article 51). Complications and uncertainty regarding how the UN Charter should be interpreted when cyber attacks occur result from three fundamental facts.

First, the UN Charter was written in 1945, long before the notion of cyber attacks was even imagined. The underlying experiential base for the formulation of the Charter involved TKC among nations, and thus the framers of the Charter could not have imagined how it might apply to cyber conflict.

Second, the UN Charter itself contains no definitions for certain key terms, such as 'use of force', 'threat of force', or 'armed attack'. Thus, what these terms mean cannot be understood by direct reference to the Charter. Definitions and meanings can only be inferred from historical precedent and practice – how individual nations, the United Nations itself, and international judicial bodies have defined these terms in particular instances. Given a lack of clarity for what these terms might mean in the context of TKC, it is not surprising that there is even less clarity for what they might mean in the context of cyber conflict. One might therefore hope for future case law to clarify those terms, as it did for TKC. How and even whether case law will hear about cases involving cyber attack is entirely unclear at this point, however.

Third, the Charter is in some ways internally inconsistent. Article 2(4) bans uses of force that could damage persons or property other than in self-defence or authorized by the UN Security Council. However, Article 41 allows other acts (specifically, economic sanctions) that could damage persons or property. The use of operations not contemplated by the framers of the UN Charter – that is, cyber operations – may well magnify such inconsistencies. An example will help to illustrate some of the complications that may arise. An offensive operation involving a number of cyber attacks conducted over time against a variety of different financial targets in an adversary nation could cause extensive economic loss and panic in the streets, and shake public confidence in the incumbent regime, but without directly causing physical damage or any loss of life. Assuming the perpetrator of this operation could be identified, on what basis, if any, would such an operation be construed under the UN Charter as a use of force or an armed attack, rather than as an economic or 'political' sanction?

One possible answer to this question – put simply, what would constitute an armed attack in cyberspace? – is that if a cyber attack causes the same effects as a kinetic attack that rises to the threshold of an armed attack, the cyber attack would itself be considered an armed attack.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

The answers to such questions under various circumstances involving cyber attack matter both to the attacked party and the attacking party.

- The answers matter to the attacked party because they may influence when and under what governmental agency the response may occur (for example, in the United States, the answers influence whether the attack is considered a law enforcement or military matter), and what rights the victim might have in responding.
- The answers matter to the attacking party because they set a threshold for a legal recourse to force that policy-makers may not wish to cross in taking assertive/aggressive actions to further the party's interests.

Jus in bello

Jus in bello is based in large part on the provisions of the Geneva Conventions and their customary counterparts. Some of the fundamental principles underlying *jus in bello* are the principle of military necessity (military operations must be intended to assist in the military defeat of the enemy and must serve a concrete military purpose) the principle of distinction (military operations may be conducted only against 'military objectives' and not against civilian targets), and the principle of proportionality (the expected incidental loss of civilian life, injury to civilians or damage to civilian objects must not be disproportionate to the anticipated military advantage).

As with the UN Charter, the Geneva Conventions are silent on cyber attack as a modality of conflict, and the question of how to apply the principles mentioned above in any instance involving cyber conflict may be problematic. The following hypothetical cases are offered to raise some key issues:

- Under the provisions of the Geneva Conventions and Additional Protocols related to distinction, parties to a conflict must distinguish between civilians and combatants and between civilian objects and military targets.[11] In the context of cyber warfare, an attack on an adversary's IT system or network would have to be intended to result in a definite military advantage (and not merely a political or economic advantage).[12] Today, military forces are likely to route a large fraction of their communications over communications facilities that are primarily used for civilian purposes. Similarly, military bases often depend on the host nation's power grid. Do these facts suggest that communications facilities and power grids would be valid military targets?[13]

11 Additional Protocol I of 1977 (hereafter AP I), Art. 48; and see J.-M. Henckaerts and L. Doswald-Beck (eds), above note 9, rule 7.

12 AP I, Art. 52(2).

13 Communications facilities and power grids could be considered examples of dual-use entities. The legality of deliberately targeting dual-use entities is not explicitly addressed in the text of the Geneva Conventions or the Additional Protocols thereto. However, the ICRC Commentary of the Additional Protocols of 1977 (commentary of Art. 52(2)), para. 2023, suggests that attacks on such entities are permissible, although the proportionality test for an attack must be satisfied as well. Attacks on such entities conducted with

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

- The provisions related to precautions against the effects of attacks also require the party targeted in an attack to protect civilians and civilian objects under its control against the effects of attacks – for example, by not locating military targets within or near densely populated areas and by removing civilian persons and objects from the vicinity of military targets.[14]
- Under the provisions related to proportionality,[15] some degree of collateral damage is allowable, but not if the 'expected' collateral damage is disproportionate compared to the 'anticipated military advantage'.[16] If, for example, a power plant is the target of a cyber attack, an assessment must be made as to whether the harm to the civilian population caused by disruption of electrical service is not disproportionate to the military advantage that might ensue from attacking the plant. Before such an assessment could be made, the commander would have to have adequate intelligence about the plant (and what was dependent on the plant) on which to base the judgement.
- The provisions related to non-perfidy state that military forces cannot pretend to be legally protected entities, such as hospitals. The rule is a consequence of maintaining the distinction between civilian and military entities. What if nation A uses the information systems of a hospital as a launching point for its cyber attacks against nation B? Can a cyber counterattack legally be launched against the information systems involved?
- Another crucial issue relates to the status of the operator. In the case of international armed conflict, a civilian operator would benefit from immunity from attack unless he or she took a 'direct part in hostilities',[17] at which time he or she would become a legitimate military target. Given that civilians will likely be key participants in conducting certain kinds of cyber attacks, how and to what extent, if any, does the criterion of direct participation relate to the planning, preparation, and/or execution of a cyber attack? Consider, for example, the following spectrum of civilian involvement:
  - A civilian posts a vulnerability notice for the open-source Linux operating system that a cyber attack exploits.
  - A civilian contractor for the DOD identifies the presence of this vulnerability on an adversary's system.
  - A civilian contractor exploits the vulnerability by introducing a hostile agent into the adversary's system that does not damage it but that can be directed to cause damage at a subsequent time.
  - A civilian contractor dictates to a military officer the precise set of commands needed to activate the hostile agent.

the intention of injuring civilians or damaging civilian property would not be legitimate, but making that determination is difficult.

14 AP I, Art. 58. See also J.-M. Henckaerts and L. Doswald-Beck (eds), above note 9, rules 22–24.

15 As codified in AP I, Art. 51(5)(b) and Art. 57(2)(a)(iii); see also J.-M. Henckaerts and L. Doswald-Beck (eds), above note 9, rule 14.

16 AP I, Art. 51(5)(b).

17 AP I, Art. 51(3).

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

Such examples suggest that there may be considerable uncertainty about how a serious LOAC analysis of any given operational scenario might proceed if cyber attacks were involved.

Potential human rights implications

Human rights restrain governmental action with respect to individuals under the government's jurisdiction. Such rights can originate nationally (such as the rights granted to Americans under the United States Constitution), in international treaties (such as the Convention on the Elimination of All Forms of Discrimination Against Women), or in customary international law.

Two of the rights enumerated in the International Covenant on Civil and Political Rights (ratified by the United States in September 1992) may be relevant to the cyber domain. Article 17 (protecting privacy and reputation) might be relevant to cyber operations intended to harm the reputation of an individual – for example, by falsifying computer-based records about transactions in which he or she had engaged – or to uncover private information about an individual (potentially constituting a provocation prior to conflict if the individual is prominent or politically influential). Article 19 (protecting rights to seek information) might be relevant to cyber attacks intended to prevent individuals from obtaining service from the Internet or other media. A number of other rights, such as the rights to life, to health, and to food, may be implicated as well depending on the nature and targets of the cyber attack. Respect for these other rights could suggest, for example, that a cyber attack intended to enforce economic sanctions would still have to allow transactions related to the acquisition of food and medicine.

A number of nations have declared that access to the Internet is a fundamental right of their societies (as of August 2011, these nations include Estonia,[18] France,[19] Spain,[20] and Finland[21]). Thus, if access to the Internet is a human right, then actions curtailing or preventing Internet access violate that right.

In addition, an important and contested point in human rights law is the extent of its applicability during acknowledged armed conflict or hostilities. The position of the United States government is that the imperatives of minimizing unnecessary human suffering are met by the requirements of the LOAC, and thus that human rights law should not place additional constraints on the actions of its armed forces. By contrast, a number of international bodies, such as

18 Colin Woodard, 'Estonia, where being wired is a human right', in *The Christian Science Monitor*, 1 July 2003, available at: http://www.csmonitor.com/2003/0701/p07s01-woeu.html.

19 'Top French court declares internet access "basic human right"', in *FoxNews.com*, 12 June 2009, available at: http://www.foxnews.com/story/0,2933,525993,00.html.

20 'Spain govt to guarantee legal right to broadband', in *Reuters*, 17 November 2009, available at: http://www.reuters.com/article/2009/11/17/spain-telecoms-idUSLH61554320091117.

21 '1Mb Broadband access becomes legal right', in *Yle Uutiset*, 14 October 2009, available at: http://yle.fi/uutiset/1mb_broadband_access_becomes_legal_right/1080940.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

the ICJ[22] and the Human Rights Committee,[23] argue that human rights law can and should apply as well as LOAC during hostilities.

The role of the private sector as target and conductor of offensive cyber operations

The private sector is deeply involved in matters related to cyber conflict in many ways – and much more so than it is involved in traditional kinetic conflict. The most obvious connection is that private-sector entities are quite often the targets of hostile cyber operations. The perpetrators of most such operations against private-sector entities are generally believed to be criminals (such as those seeking credit card numbers), but nation-states may conduct cyber operations against them for a variety of purposes as well (as discussed in the section 'Deterrence and defence in cyberspace', above).

In addition and especially in the United States, military and civilian actors share infrastructure to a very large degree. A very large fraction of US military communications pass over networks owned by the private sector and operated largely for the benefit of civilian users. The same is true for electric power – US military bases depend on the civilian power grid for day-to-day operations. Under many interpretations of the LOAC, military dependence on civilian infrastructure makes that civilian infrastructure a legitimate target (a 'dual-use object') for an adversary's military operations.

Another important connection is that the artefacts of cyberspace are largely developed, built, operated, and owned by private-sector entities or companies that provide IT-related goods and services. In some cases, the cooperation of these entities may be needed to provide adequate defensive measures. For example, some policy-makers argue that an adequate defensive posture in cyberspace will require the private sector to authenticate users in such a way that anonymous behaviour is no longer possible. In other cases, private-sector cooperation may be needed to enable offensive cyber operations against adversaries. For example, the cooperation of a friendly internet service provider may be needed to launch a cyber attack over the Internet.

Many questions arise regarding the private sector's connection to cyber conflict. For example:

- What actions beyond changes in defence posture and informing law enforcement authorities should the private sector be allowed to take in response

22 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, *ICJ Reports 1996*, para. 25; ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, *ICJ Reports 2004*, paras. 106–113; ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgement, 19 December 2005, *ICJ Reports 2005*, para. 216.

23 UN Human Rights Committee, General Comment No. 31, CCPR/C/21/Rev.1/Add.13, 26 May 2004, para. 11.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

to hostile cyber operations? Specifically, how aggressive should the responses of private-sector entities be?
- How and to what extent, if any, should the United States government conduct offensive operations to respond to cyber attacks on private-sector entities (or authorize an aggressive private-sector response)? Under what circumstances, if any, should it do so?
- How might private-sector actions interfere with US government cyber operations?
- What is the United States government's responsibility for private-sector actions that rise to the threshold of 'use of force' (in the UN Charter sense of the term)?

Preventing escalation and terminating conflicts in cyberspace

Small conflicts can sometimes grow into larger ones. Of particular concern to decision-makers is the possibility that the violence could increase to a level not initially contemplated or desired by any party to the conflict.

In considering TKC, analysts have often thought about escalation dynamics and terminating conflict. In a cyber context, escalation dynamics refers to the possibility that initial conflict in cyberspace may grow. Much of the thinking regarding cyber conflict is focused on the first (initial) stages of conflict – it asks, for example, 'What do we do if X conducts a serious cyber attack on the United States?', with the implicit assumption that such a serious attack would be the first cyber attack.

But what if it is not? How would escalation unfold? How could it be prevented (or deterred)? There are theories of escalation dynamics, especially in the nuclear domain, but because of the profound differences between the nuclear and cyber domains, there is every reason to expect that a theory of escalation dynamics in cyberspace would be very different from a theory of escalation dynamics in the nuclear domain. Some of the significant differences include the fact that attribution is much slower and/or more uncertain, the fact that the ability of non-state actors to interfere in the management of a conflict is increased in cyber conflict, and the existence of a multitude of states that have meaningful capabilities to conduct cyber operations.

Escalation can occur through a number of mechanisms (which may or may not simultaneously be operative in any instance).[24] One party to a conflict may deliberately escalate the conflict with a specific purpose in mind. It might inadvertently escalate the conflict by taking an action that it does not believe is escalatory but that its opponent perceives as escalatory. It might accidentally escalate a conflict if its forces take some unintended action (such as striking the wrong target). Lastly, catalytic escalation occurs when some third party

24 RAND, *Dangerous Thresholds: Managing Escalation in the 21st Century*, 2008, available at: http://www.rand.org/pubs/monographs/2008/RAND_MG614.pdf.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

succeeds in provoking two parties to engage in conflict ('let's you and him fight'). Catalytic provocation is facilitated by the possibility of anonymous or unattributable action.

Conflict termination in cyberspace poses many difficulties as well. Conflict termination is the task faced by decision-makers on both sides when they have agreed to cease hostilities. A key issue in implementing such agreements is knowing that the other side is abiding by the negotiated terms. How would one side know that the other side is honouring a cease-fire in cyberspace, given the risk that one or both sides are likely to be targets of hostile cyber operations from third parties independently from the cyber conflict between the two principal actors? In other words, there is a constant background of hostile cyber operations going on all the time. And would one side be obliged to inform the other of all of the battlefield preparations it had undertaken prior to the conflict? Such an act, analogous to de-mining operations, would require each side to keep careful track of its various preparations.

Conclusion

Conflict can and does occur in cyberspace. How and to what extent does recent history about conflict in cyberspace presage the future?

Two things are clear today. First, only a small fraction of the possibilities for cyber conflict has been experienced to date, and actual experience with cyber conflict has been limited. Indeed, nearly all of the adversarial actions known to have been taken in cyberspace against the United States or any other nation, including both cyber attack and cyber exploitation, have fallen short of any plausible threshold for defining them as 'armed conflict', 'use of force', or even 'armed attack'. This fact has two consequences: there are many possibilities for serious cyber conflict that have not yet been seen,[25] and the question of how to respond to hostile actions in cyberspace that do not rise to these thresholds is the most pressing concern of policy-makers today, as nearly all hostile cyber operations conducted to date do not rise to these thresholds.[26]

Second, many of our assumptions and understandings about conflict – developed in the context of TKC – either are not valid in cyberspace or are applicable only with difficulty. Thus, decision-makers are proceeding into largely unknown territory – a fact that decreases the predictability of the outcome of any actions they might take.

25 Gregory Rattray and Jason Healey, 'Categorizing and understanding offensive cyber capabilities and their use', in NRC, *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, National Academies Press, Washington, D.C., 2010, pp. 77–98, available at: http://www.nap.edu/catalog/12997.html.

26 Herbert Lin, 'Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion', in *Georgetown Journal of International Affairs*, Special Issue, *International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity*, 2011, pp. 127–135.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press

The 2009 NRC report on which this article is based[27] recommended *inter alia* that the United States government conduct a broad, unclassified national debate about cyber attack policy, and that it should work to find common ground with other nations regarding cyber attack, where common ground included better mutual understanding regarding various national views of cyber attack, how the laws of war and the UN Charter might or might not apply to cyber attack, the significance of non-state parties that might launch cyber attacks, and how nations should respond to such attacks. Both of these recommendations[28] are still valid today, and indeed they constitute good advice not only for the United States government but also for the governments of all nations that are party to the UN Charter and the Geneva Conventions.

27 See NRC, above note 1.
28 See *Idem*., recommendations 2 and 3.

https://doi.org/10.1017/S1816383112000811 Published online by Cambridge University Press