BRIEF

The Law of Cyber Armed Conflicts:
Translating Existing Norms of International Humanitarian Law into Cyber Language

By Iben Yde, BA Law, LLM and Ph.D. Fellow, University of Aarhus
The Law of Cyber Armed Conflicts:  
Translating Existing Norms of International Humanitarian Law into Cyber Language

By Iben Yde, BA Law, LLM and Ph.D. Fellow, University of Aarhus

After earning her Master degree from Aarhus University and Rijksuniversiteit Groningen in 2010, Iben Yde has held the position as PhD fellow in public international law at the Law Department of Aarhus University. Iben’s research focuses on the relationship between the law of armed conflict and new developments in means and methods of warfare. Her thesis examines the legal implications of increasingly autonomous weapon systems. In addition to her PhD-research, Iben serves as military legal adviser of the Reserve to the Danish Admiral Fleet.
The Royal Danish Defence College is the Danish armed forces’ powerhouse for education, training and research-generated consultancy. Our research is conducted within a broad range of military-related topics. Our research priorities, such as topics and resource allocation are determined by the Commandant of the Royal Danish Defence College, who is aided by a research council.

Research at the Royal Danish Defence College should enlighten and challenge the reader, whether they are in the armed forces or in the surrounding environment. This is only achievable if the employees have the freedom to administer their own research projects and draw their own conclusions. This is a principle, which is honoured at the Royal Danish Defence College.

We hope you enjoy reading the Royal Danish Defence College’s publications!

© Royal Danish Defence College

All rights reserved. Mechanical, photographic or other reproduction or photocopying from this book or parts thereof is only allowed according to agreements between The Danish Defence and CopyDan.

Any other use without written consent from the Royal Danish Defence College is illegal according to Danish law on intellectual property right. Excepted are short extracts for reviews in newspapers or the like.
Introduction

Cyber space is turning into a new global domain that may be used for the conduct of hostilities, alone or alongside operations in other domains. Due to rapid technological change and high profile cyber operations, first and foremost the distributed denial of service attacks (DDoS) against Estonia in 2007\(^1\) and Georgia in 2008\(^2\) and the alleged Stuxnet attack against Iranian nuclear centrifuges in 2010\(^3\), the eyes of national security strategists and politicians have turned to cyber space, and cyber security has moved high on the agenda of many states. The UK’s 2010 National Security Strategy qualified cyberattacks as one of four Tier One threats against national security.\(^4\)

Likewise, the US has labelled cyber threats one of the most serious national security challenges\(^5\) and has released a strategy for operating in cyberspace, in which cyber space is designated as an operational domain.\(^6\) The concern is certainly not unwarranted. Hostile cyber operations have the potential to produce vast societal and economic disruptions\(^7\) as well as severe physical injury and damage caused by attacks against critical industrial installations. The increasing

---


(2) For more information about the distributed denial of service attacks conducted against Georgia during the armed conflict between Russia and Georgia in 2008 and the legal consequences thereof, see Leslie Swanson, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, in 32 Loyola of Los Angeles International and Comparative Law Review, 303, 2010.


dependence on information infrastructure for both civilian and military purposes has its disadvantages, as pointed out by the US DoD when stating that ‘the security and effective operation of U.S. critical infrastructure – including energy, banking and finance, transportation, communication, and the Defense Industrial Base – rely on cyberspace, industrial control systems, and information technology that may be vulnerable to disruption or exploitation.’\(^8\) While this dependence and interconnectivity certainly presents states with great cyber security challenges, it also provides a potential enemy with a wide range of high value targets that might not be prone to attacks by conventional kinetic means. With the right offensive cyber capabilities at hand, anything hooked up to a computer can be targeted.\(^9\) But the options are not unlimited. One potentially limiting factor for states seeking to exploit the opportunities of the cyber domain is international law. In 2008, a group of international experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, initiated a project aimed at clarifying the legal aspects of cyber warfare.\(^10\) The product of this effort, the Tallinn Manual on the International Law Governing Cyber Warfare (hereinafter the Tallinn Manual)\(^11\), has made an important contribution to the understanding of how norms of international law will apply to the new and very challenging area of cyber warfare.\(^12\) The manual will serve as central point of reference for this brief, the purpose of which is exactly to explore some of the legal issues attached to the military expansion into the cyber domain.

Narrowing down the scope
As reflected by the volume of the Tallinn Manual, the legal issues springing from cyber warfare are many and complicated, and they cannot all be dealt with in the present context. This brief will confine itself to the legal implications of cyber operations conducted during armed conflicts. The purpose is to shed light on how key concepts of *jus in bello* – the body of law that governs the way in which warfare is conducted - should be understood in a cyber context and to present some of the most important *in bello* restrictions on cyber operations during armed conflicts. In the remainder of this brief, the term ‘the law of armed conflict’ (LOAC) will be used instead of *jus in bello* because the term is more convenient and modern.\(^13\)

The legal implications of offensive cyber operations outside the context of an armed conflict will not be considered. Consequently, questions such as when offensive cyber operations constitute a breach of the prohibition on the use of force in Art.

---

\(^{8}\) See supra, note 6.


\(^{10}\) Tallinn Manual, the Introduction.

\(^{11}\) A draft of the Tallinn Manual is available at [http://www.ccdcoe.org/249.html](http://www.ccdcoe.org/249.html).

\(^{12}\) Please note that the Tallinn Manual is not a legally binding instrument.

\(^{13}\) The term ‘international humanitarian law’ is another commonly used name for the *jus in bello* and LOAC.
2 (4) of the UN Charter will not be dealt with, nor will questions of attribution and state responsibility for such hostile activities.

It is important to underline that this brief will not provide an account of the various types of malware and techniques used in hostile cyber operations. In relation to key LOAC principles brought forward in this brief, the effects of an attack determine the legal consequences, not the nature of the weapons, i.e. the type of malware used to conduct the attack. To this extent, the type of malware used is not relevant to the legal assessment of a cyberattack.\(^\text{14}\)

**Is cyberspace a law-free domain?**

There are presently no rules of public international law that specifically address cyber warfare.\(^\text{15}\) But this does not mean that the issue is left unregulated - quite to the contrary. The International Court of Justice, in its Nuclear Advisory Opinion, held the following:

‘Established principles and rules of humanitarian law applicable in armed conflicts... applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.'\(^\text{16}\)

The Court took an identical approach to the question of the application of the *jus ad bellum*.\(^\text{17}\) Thus, cyber space is, in the words of US State Department legal advisor Harold Koh, ‘not a law free zone where everyone can conduct hostile activities without rules or restraints.’\(^\text{18}\) The main problem when establishing the legal framework of cyber warfare is therefore not that there are no rules to apply, but how to apply existing rules in a new and very different environment. Because of the special character of cyberspace, it is inevitably necessary to clarify how key concepts of international law should be translated to fit the reality of cyber warfare. The more novel and unique the technology, the greater the legal translation challenges will be. But it does not affect the fact that existing law does apply; it only makes it more challenging to figure out how to apply it correctly.

---

\(^\text{14}\) However, as pointed out later, cyber weapons, i.e. malware must be subjected to legal reviews on par with conventional weapons. Clearly, the person assessing a specific type of malware will need to have detailed technical understanding of the malware in question in order to assess the legality of it *per se*.

\(^\text{15}\) In the context of this brief, the term cyber warfare simply denotes the conduct of cyber hostilities. The term is merely descriptive and has no legal implications in itself.

\(^\text{16}\) The ICJ Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ 1996.


Cyberattacks in the context of armed conflicts

Having established that existing international law regarding the use of force applies to use of force in the cyber domain, the assertion that cyber operations conducted in the context of an armed conflict are generally subject to LOAC is unproblematic. However, not all military cyber operations are covered by the fundamental rules of LOAC. In order to know and understand the legal restraints resting upon different states, it is necessary to draw some lines between operations that are subject to targeting law limitations and those that are not.

First of all, LOAC only applies to cyber operations executed in the context of an armed conflict. A cyber operation that appears in a situation that does not qualify as an armed conflict, whether international or non-international, is regulated by domestic law and human rights law, not LOAC. Consequently, because the situation never rose to the threshold of an armed conflict, the extensive and long-lasting denial of service (DDoS) attacks against Estonia in 2007 were not subject to LOAC regulation, whereas the similar kinds of cyber operations conducted as part of the international armed conflict between Russia and Georgia in 2008 were. In addition to the requirement of the existence of an armed conflict, there must be a nexus between the operation in question and the armed conflict, which is generally understood as requiring that the operation is carried out by a party to the armed conflict against the opponent. Consequently, activities of private individuals or entities that are not related to the armed conflict are not covered by LOAC either.

Secondly, only cyber operations that amount to attacks as defined in Art. 49 of AP 1 are covered by the LOAC rules regulating the conduct of hostilities. AP 1 defines ‘attack’ as ‘acts of violence against the adversary, whether in offense or
Importantly, acts of violence are not limited to the use of kinetic force. Thus, cyberattacks are cyber operations, whether offensive or defensive, which are reasonably expected to cause injury or death to persons or damage to and destruction of objects, whether it be on the targeted system or other entities. The crucial factor is the real-world consequence of the attack. Therefore, if the cyber operation is expected to produce the injury or death to persons or destruction of or damage to objects, it is an attack in the sense of AP 1, regardless of the mechanisms causing these consequences and regardless of whether it is carried out successfully or prevented by the victim state. In this respect, cyberattacks do not differ from traditional operations using kinetic means.

There are many possible scenarios of cyber operations that may cause death, injury or damage of significant scale to human beings and physical installations and thereby qualify as an attack under LOAC. Just imagine an attack directed against a SCADA controlling an installation such as a dam.

**SCADA**

An industrial control network (ICN) is a system of interconnected equipment used to monitor and control physical equipment and processes in industrial environments. SCADA (supervisory control and data acquisition) is an advanced type of ICN used to monitor and remotely control large-scale industrial and geographically widely distributed processes. SCADA networks are the underlying control systems of most critical national infrastructures including power, energy, water, transportation and telecommunication and are widely involved in the make-up of vital enterprises such as pipelines, manufacturing plants and building climate control.

The direct effect of the attack, i.e. the incapacitation, destruction or damage done to the SCADA system, may have severe indirect effects in the form of damage to the dam and the surroundings. If the attack is intended to result in the release of large quantities of water.
amounts of water that cause downstream flooding and thereby injury or death to persons or damage to materiel, it is undoubtedly an IHL attack.29

Cyber operations that do not reach the threshold of a LOAC armed attack are most likely not subject to LOAC targeting limitations and are therefore generally considered legal.30 Thus, activities such as the blocking of e-mail communication or the conduct of psychological warfare such as the dissemination of propaganda is not illegal, even if it causes significant inconvenience for the civilian population.

Throughout the rest of this brief, the term attack will exclusively be used to denote LOAC attacks as defined above and the term ‘cyberattacks’ to denote cyber-to-cyber attacks only.31

LOAC restraints on cyberattacks

Generally speaking, states involved in armed conflicts are allowed to attack each other in pursuance of the defeat of the enemy. However, it is a recognized and well-established principle of international law that the parties to an armed conflict are subject to limitations in their choice of means and methods of warfare.32 If a state is in possession of cyber weapons, it may only use them to the extent that LOAC allows for. In order to ensure that weapons introduced to the battlefield can actually be used in accordance with LOAC, states developing, acquiring or using new cyber weapons are required to subject the weapon in question to a legal review.33 The primary focus of the review is to establish whether the cyber weapon per se is legal in the light of existing weapons law.34


(30) Ibid. This is also the contention of the majority of experts behind the Tallinn Manual. However, the rules are expressed in careful terms, taking into consideration that the law may change in this area, cf. Tallinn Manual, Rule 30, commentary 12.

(31) See the ‘scope’ of the Tallinn Manual for more information about cyber-to-cyber operations.

(32) AP 1, Art. 35.

(33) For states that are parties to AP 1, this requirement has resulted in an affirmative duty to conduct formal reviews of any weapon studied, developed or acquired, cf. AP 1 Art. 36. States that are not parties have a customary but less formalized duty to ensure that they only develop, acquire and use weapons in accordance with LOAC. For more information about the conduct of weapons reviews, see ICRC’s Guide to the Mapons, mnee to the Ithat causesLegal Review of Mapons, mnee to the Ithat causesNewMapons, mnee to the Ithat causes Weapons, MMMapons, mnee to the Ithat causes and Methods of Warfare, publication reference 0902, available at http://www.icrc.org/eng/resources/documents/publication/p0902.htm.

(34) The term ‘weapons law’ denotes the LOAC rules that pertain to legality of weapons as such and includes general weapons law principles as well as regulation of specific types of weapons, such as chemical weapons or cluster munitions.
Cyber weapons

According to Rule 41 of the Tallinn Manual, cyber means of warfare include any cyber device, material, instrument, mechanism, equipment and software used, designed or intended to be used to conduct cyberattacks, while cyber methods are the cyber tactics, techniques and procedures by which hostilities are conducted.

But the obligation to respect LOAC does not end here. If the result of the legal review is positive, the weapon can be deployed to the armed forces and used in the conduct of hostilities during an armed conflict. But each time a state launches a cyberattack against the adversary using the approved cyber weapon, it must design the operation in accordance with existing targeting law, i.e. the rules regulating the conduct of hostilities, first and foremost the principles of distinction, proportionality and precautions in attack.

Below, a brief account of the rules and restrictions of special interest to cyber-attacks is provided. Any state that seeks to exploit its offensive cyber capabilities as means of conducting attacks against the adversary needs to be able to understand the legal concerns that the special features of the cyber domain give rise to.

Weapons Law restrictions

Since there are no specific treaties or treaty provisions directed at cyber weapons, the rules against which their legality must be tested are the two main customary principles of weapons law, namely the prohibition of indiscriminate weapons and weapons causing indiscriminate effects, and the prohibition of weapons causing superfluous injury or unnecessary suffering.

---

(35) AP 1, Art. 51(4)(b) and (c), and the ICRC’s customary law study, Rule 71.
(36) AP 1, Art. 35(2) and the ICRC’s customary law study, Rule 70.
The two main customary weapons law restrictions

The prohibition of indiscriminate weapons and weapons causing indiscriminate effects requires that weapons used must be capable of being directed against a specific military objective and the effects of the weapons must be capable of being limited to striking legitimate military objectives discriminately and within the boundaries of the principle of proportionality.

The prohibition of weapons causing superfluous injury or unnecessary suffering requires that weapons used must not cause injury or suffering that exceeds the generic military advantage which the use of the weapon offers.

It is highly unlikely that the latter rule will be relevant to cyber weapons, since it is a rule normally directed at the part of the weapon or the weapon system directly causing the physical injury, such as a projectile. But, as an integral part of weapons law, it will have to be part of the review. The prohibition of indiscriminate weapons, on the other hand, may prove more relevant. If a cyber weapon is of a kind that makes it entirely impossible to predict whether it will strike legitimate military cyber assets or protected civilian computers or networks, it would be inherently indiscriminate and prohibited by this rule. However, there are reasons to believe that cyber weapons generally will be discriminate, because they are often designed to target very specific systems, e.g. specific SCADA systems controlling important industrial processes and facilities. The risk that the cyber weapon in question may be used to conduct attacks causing disproportionate collateral damage does not render it inherently indiscriminate. In fact, most types of weapons are capable of indiscriminate use, but only those that in circumstances of intended use are incapable of direction against specific military objectives are rendered illegal by this rule.39

Targeting Law Restrictions - Distinction and Proportionality Issues

Any cyberattack must comply with the fundamental, customary LOAC principles of distinction and proportionality, which serve to provide the highest possible degree of protection to the civilian population during armed conflicts and apply equally to international and non-international armed conflicts.

Pursuant to the principle of distinction, a state may only direct a cyberattack against enemy combatants or objects that are being used for or are intended to being used for military purposes. The application of the principle in practice is difficult, and unfortunately it is not likely to become any easier in the cyber domain. The main reason is that, in practice, it is very difficult if not impossible to distinguish civilian cyber objects from military cyber objectives. Computers and computer networks, unlike combatants, do not carry a distinguishing emblem, which makes it harder for states to verify the status of cyber targets. But, in any event, states conducting attacks must make sure that both the system, which is the initial object of the attack, and potential subsidiary objects of attacks are, in fact, military objectives. The intermingling of military and civilian cyber infrastructure further complicates cyber targeting. For example, 95% of the US military communication goes through civilian infrastructure, and many computers and computer networks are used for multiple purposes. When shared by military and civilian users, computers, networks and communication or transmission notes are dual-use objects. In the eyes of the law, such dual-use objects are, by definition, military objectives liable to attacks, but the civilian use of the system may render an attack illegal if it is expected to cause disproportionate damage to the civilian population or civilian objects.

(40) Also, civilians taking direct part in hostilities may be lawfully attacked for such time as they participate, cf. AP 1, Art. 51(3). This rule has been the source of some controversy in the cyber context. For more information about what amounts to direct participation in cyber hostilities, see the Tallinn Manual.
(41) AP 1, Art. 48 and 51(2)
(42) AP 1, Art. 52.
(47) A written expression of the principle of proportionality can be found in AP 1, Art. 51(5)(b).
The targeting law restriction of the principle of proportionality

The principle of proportionality requires that the expected incidental loss of civilian life, injury to civilians or damage to civilian objects may not be excessive in relation to the concrete and direct military advantage anticipated from the attack.

The principle of proportionality thus becomes a crucial factor in cyber targeting, but it is by no means easy to apply. Not only may a cyberattack have potentially grave effects on civilians, either because many civilian activities depend on cyber infrastructure or because the secondary effects of attacks directed against SCADA systems may have devastating consequences; it may also be extremely difficult to map the expected consequences of an attack due to the interconnectivity of computer networks and control systems. However, since both direct and indirect effects of cyberattacks, which may comprise delayed and/or displaced second-, third-, and higher order effects, are covered by the rule, mapping may, in some situations, be essential to creating an overview of potential consequences and thereby qualify as a meaningful proportionality assessment. When conducting the proportionality assessment, it must be remembered that not all effects on the civilian population qualify as collateral damage - only those involving incidental loss of civilian life, injury to civilians or damage to civilian objects. Thus, immaterial effects such as inconvenience, stress and fear are not taken into consideration when assessing the proportionality of a given attack.

The targeting law restriction regarding the obligation to take precautions in attack

The obligation to take precautions in attack requires that constant care is taken to spare the civilian population, civilians and civilian objects, and it places those who plan or decide upon a cyberattack under an obligation to take all feasible precautions in the choice of means and methods of warfare in furtherance of this objective.

(48) See supra, note 30.
(49) Tallinn Manual, Rule 50.
(50) AP 1, Art. 57.
It should finally be noted that the obligation to take precautions in attack might likewise have important implications for targeting in the cyber domain.\textsuperscript{51} The principle of precaution operationalizes the principles of distinction and proportionality\textsuperscript{52} by setting out the standards of care, which must be exercised by those carrying out attacks whether in cyber or other domains. Most importantly, the duty to take precautions is of a continuous nature and therefore must be observed throughout the planning and execution phase of any attack. The available information on which the operation is based must thus be reviewed continuously, and new information must be taken into consideration in order to adjust the means and methods chosen for the operation should it become apparent that the situation on the ground has changed or that the pursued military advantage can be achieved by other and less harmful means or tactics available. Ultimately, those who plan or decide upon an attack must be prepared to cancel or suspend an attack or change tactics, including weapons, even if that would mean abandoning the use of the cyber weapon originally envisaged in favour of more traditional kinetic means.\textsuperscript{53}

**Conclusion**

The analysis above shows that the legal challenges facing states that seek to exploit the tactical advantages offered by cyber warfare are complicated and plentiful. But, with the knowledge that international law does apply to the use of force in cyber space, we have been given a legal framework and the certainty that cyber space is not lawless territory, which is not such a bad point of departure. We know which rules to resort to, and we can begin the difficult task of translating well-established legal concepts and applying existing rules to the new and challenging cyber domain. In this regard, the Tallinn Manual has made an important contribution. It provides us with a comprehensive analysis of all relevant issues surrounding cyber operations and attempts to translate the requirements of existing international legal norms into a set of rules that specifically addresses the use of force in cyber space. However, no matter how convincing the arguments of various scholars may be, in the end, the precise scope and application of international law to cyber operations is decided by state practice. Presently, there is little evidence as to how exactly states apply or intend to apply the relevant rules of LOAC to cyberattacks, and therefore no definitive conclusions can be made. But, once the difficult task of classifying different kinds of cyber conduct under international law has been accomplished, it becomes possible to get an overview of the rules regulating the conduct in question. If the conduct qualifies as an attack under LOAC, the principles of distinction and proportionality and the requirements derived thereof will inevitably stand out as the key legal components that states must be in accordance with when modelling their cyber

\textsuperscript{51} However, the scope of Art. 57 is limited to cyberattacks that have effects on land, cf. Tallinn Manual, Section 7.
\textsuperscript{52} AP 1, Art. 57.
\textsuperscript{53} Another important aspect of the precautionary principle is the duty for those who plan or decide upon an attack to cancel or suspend an attack if it becomes clear that the target is not a military objective or the attack would have disproportionate effects.
operations. Although compliance with these principles in the cyber domain will be challenging and will require access to experts with detailed knowledge about the cyber weapons used, the target and the possible effects of the attack, they must be respected. Thus, knowledge about the legal obligations resting upon a state in a particular situation is crucial. Only if states are aware of the rules regulating cyberattacks will they be equipped to make informed decisions about whether or not to extend their war fighting activities to the cyber domain and design operations in accordance with LOAC.