ROYAL DANISH DEFENCE COLLEGE

Brief

APRIL 2018

LEGAL ISSUES IN CYBER TARGETING

By Jonas Alastair Juhlin, Institute for Military Operations, Royal Danish Defence College

Copenhagen April 2018

Royal Danish Defence College
Ryvangs Allé 1
DK-2100 Copenhagen
Denmark
Phone: +45 728 17000
E-mail: fak@fak.dk
Editor in Chief: Jens Ringsmose, Head of Institute for Military Operations
Internal peer review
Layout: Royal Danish Defence College
ISBN: 978-87-7147-236-3

TABLE OF CONTENT

Abstract
Imagine this scenario: Two states are in armed conflict with each other. In order to gain an advantage, one side launches a cyber-attack against the opponent's computer network. The malicious malware paralyze the military computer network, as intended, but the malware spreads into the civilian system with physical damage to follow.

This can happen and the natural question arises: What must be considered lawful targeting according to the international humanitarian law in cyber warfare? What steps must an attacker take to minimize the damage done to unlawful targets when conducting an offensive operation? How can the attacker separate military targets from civilian targets in cyber space?

This paper addresses these questions and argues that a network (civilian or military) consist of several software components and that it is the individual components that is the target. If the components are used in the civilian network as well as in a military network then the legal concept of dual-use becomes increasingly relevant.

Legal Considerations of Targeting in Cyber Network Operations (CNO)

Cyber space is the newest domain in warfare. It opens a new front for the military to conduct Cyber Network Operations (CNO) like the ship allowed operations in the "sea domain" and the airplane allowed operations in the "air domain". Land, sea and air have been extensively covered by regulations in the law of armed conflict (LoAC) (the older Hague conventions, Geneva conventions of 1949 and the additional protocol as well as customary law) but the limited experience in CNO makes it a challenge to regulate certain aspects of CNO in terms of LoAC.

According to the Tallin Manual and other works (such as the recent Royal Danish Defence College publication *Laws of Armed Cyber Conflict*[1] and the Danish *Military Manual*[2]) there appears to be a general consensus that the existing LoAC rules should apply to CNO, however there are certain aspects in CNO that differ considerably from the conventional kinetic military operations. The nature of cyber-weapons differs from conventional kinetic weapons, which require us to reconsider how we define targeting according to the laws of armed conflict.

One such aspect is the nature of cyber-weapons used in Cyber Network Attack (CNA) operations. Programs, malware, viruses and other software can be transported between networks and spread in an uncontrollable manner in cyber space by accident and create second- and third-order effects. This can lead to extensive damage which is beyond the attacker's control.

This paper will offer an alternative way of considering targeting in CNA operations. The paper will start by explaining some of the basic concepts and laws of targeting according to the LoAC. Next, the paper will present a fictional yet realistic scenario ("Operation Borodino"), which will illustrate the potential possibilities and dangers of a modern CNA operation. A legal analysis will follow with a focus on the aspect of targeting which differs from conventional targeting of the LoAC. The primary legal sources are The Hague and Geneva conventions.

The intended audience for this paper is NATO military planners in their national cyber command. The intention is to draw their attention to the aforementioned new aspects of targeting. This can have a significant impact of the design of cyber-weapons and planning of operations. The cyber command of the respective countries will have to consider the targeting issues presented in this paper.

Attack and Targeting in LoAC

Before proceeding to discuss the definitions and rules of attack and targeting, let's briefly outline the four core principles of the LoAC. All acts of violence must be committed according to these four principles. The principles are: distinction, military necessity, proportionality, and unnecessary suffering (sometimes mentioned as humanitarian conduct or just humanity)

1) See Yde, 2013.

2) *Militærmanual om folkeret for danske væbnede styrker i internationale militære operationer*, september 2016.

Distinction: Attacks must at all times distinguish between civilian targets and military targets. Military targets should be clearly distinguished from civilian targets and attacks should be limited to targets of a military nature.

Military Necessity: There must be a clear military advantage expected by attacking the target.

Proportionality: The damage done to civilian lives and property must be in proportion to the military advantage gained by the attack. The greater the military advantage, the greater damage to civilian lives and property is acceptable.

Unnecessary suffering: No weapon employed may cause superfluous injuries to the combatants. Note that this is only relevant to the combatants involved in the fighting. Civilians are protected in the other principles.

These four core principles are customary law and implemented in the Geneva conventions of 1949. As such they are the legal principles that must guide all military operations.

Definition of Attack and Targeting According to LoAC:

In the terms of LoAC, an attack is *an act which causes physical injury or death to persons and damage or destruction to objects.* This applies to all types of operations, both offensive and defensive. In rule 30 of the Tallin Manual, a cyber-attack is defined as:

"*A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects*"[3]

The same definition is used in the Danish *Military Manual*.[4] When not involved in an armed conflict, any attack is illegal according to the domestic law of the involved nations, and therefore should be subjected to a criminal investigation regardless of what type of damage is done by the attack.

An armed conflict is defined as protracted violence between two or more states (common article 2 conflict of an international character according to Geneva Convention III of 1949) or between a state and a non-state actor (common article 3 conflict of a non-international character according to Geneva convention III of 1949).

In this paper, we will deal with CNO as part of a joint military operation in an international armed conflict. The conflict will be one state against another state. According to *article 52.2 additional protocol I 1977*:

> Attacks shall be limited strictly to military objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial destruction, capture or neutralization offers a definite military advantage.[5]

This rule is supplemented by article 48: "The parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objectives and

3) p. 106, Tallin Manual.
4) *Militærmanual*, 2016
5) Article 52.2 of Additional protocol I of the Geneva Convention

military objectives" – this rule is to ensure the distinction between combatants and civilians, which is a core principle in the laws of armed conflict[6].

There are four criteria that make a military target lawful. Military targets are objects, which by their *nature*, *location*, *purpose* and *use* contribute significantly to the military effort[7].

Military objects by the nature: the intended target's nature refers to the type of object that it is. A defense- or weapons-related industrial complex is by its very nature a military object. The same goes for any weapons, any military vehicles, or any piece of infrastructure that is serving a military purpose. It is the intended utilization of the object for military actions and purposes that makes it a target by its nature. In terms of cyber warfare, this would include any electronic piece of infrastructure or any computer-network used by the military. A typical example could be a computer network used for communications and targeting by the armed forces. This could also be the computer network or program that is used in a weapons-related industrial plant[8].

Military objects by their location: location includes areas that are militarily important because they must be captured or denied to the enemy. This would include the tactically significant hill or the only place along a stretch of coastline where an amphibious force can land. This could also be an airport or harbor, even if these facilities are also being used by civilian traffic. In terms of cyber warfare, this could include a CNA against the computer networks of an airport that would result in its denial or capture[9].

Military objects by their purpose: purpose means its intended future use or possible use. It is a little vague when this rule will apply. The critical reader will ask if not all objects can be transformed, in one kind or another, into a possible future military use? It must be remembered that there must still be a clear military advantage by attacking the object. An example could be sinking of civilian cargo ships prior to these ships being commandeered for military use. In such a case, there must be a clear intent to commandeer the ships[10].

Military objects by their use: the use refers to the object's current use and not its intended or original use. Schools, hospitals, and religious buildings occupied by military forces and used as a fighting position make these otherwise-protected civilian objects into lawful military targets. In cyber warfare this could include computer networks normally used for civilian purposes, but in a time of conflict also used to support military operations. This network can then become a lawful target[11].

6) Rogers, "Law on the Battlefield" 104-108
7) Solis, "Law of Armed Conflict" p. 524-527
8) Solis, "Law of Armed Conflict" p. 524
9) Solis, "Law of Armed Conflict" p. 525
10) Solis, "Law of Armed Conflict" p. 525
11) Solis, "Law of Armed Conflict" p. 526

Dual-Use

Dual-use target does not appear in the Geneva Conventions or any of the additional protocols. It is a term that is used to describe the type of targets that have both a military use as well as a civilian function. A side will gain a clear military advantage by eliminating the target, but civilian property and lives will be damaged or lost. LoAC does not automatically protect dual-use targets but they do require some additional considerations before attacking. The core principals of *Proportionality* and *Military Necessity* will become increasingly difficult to assess but ever so important to judge.

In essence, the greater the military advantage that is gained by eliminating a certain objective, the more civilian deaths, injury to civilians and destruction of civilian property is accepted. There are no firm boundaries or limits to what is too much damage relative to its degree of military advantage. It will always be a concrete, case-by-case, assessment of each target whether a target is lawful or not[12].

Normally, it is not difficult to determine whether an object serves both a military and a civilian function. The most difficult part is to determine whether the military advantage outweighs the damage done to civilian life and objects[13].

An example is the 1999 NATO bombing of the Serbian state television and radio station in Belgrade. NATO stressed the dual-use of the station because the communication systems were also used to support military command and control because military traffic was routed through the civilian system. The targeting of the radio and television facility was legitimated because it used the facilities to relay and transmit communications for the Federal Republic of Yugoslavia's military and police forces in Belgrade[14]. The argument that the radio and television station was a military objective due to its propaganda broadcast was more controversial. This reason alone was not judged sufficient to warrant an attack.

Implications for Cyber Network Attack Operations

Cyber Attack Operations

There is still limited experience in cyber-network attack (CNA) operations. The few known examples are limited in scope and consequence (perhaps with the exception of Stuxnet). We have yet to see a cyber-network operation conducted as part of a major joint military operation with possible grave consequences for civilian lives and property[15].

12) Rogers, "Law on the Battlefield" p. 109-110

13) Solis, "Law of Armed Conflict" p. 534-536

14) Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia, June 12, 2000, paras. 72-4.

15) Because of this, we must imagine the scenarios. Unlike the real-world cases of WWII and later cases of Yugoslavia, where there is detailed information available from the trials for us to investigate, we must resort to imagination when dealing with hypothetical what-if scenarios in this virgin ground. It is often easier to relate to real world cases but for now, we are confined to the realms of imagination.

Stuxnet was probably the most ambitious and well-known cyber-weapon. The Stuxnet worm is a rootkit that exploits the target's Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are used in power, water and sewage plants, as well as in telecommunications, oil, and gas refining. Stuxnet contains code that can identify Siemens' SCADA software and then inject itself into the programmable logic controllers. Logic controllers automate the most critical parts of an industrial facility's processes, such as temperature, pressure, the flow of water, chemicals and gasses[16].

Stuxnet was used in a cyber-sabotage operation in 2009 directed against Natanz nuclear facilities in Iran. The malware sabotaged the Siemens manufactured centrifuge by targeting a specific software-component. This caused physical damage and limited Iran's capability to enrich uranium[17]. Officially, no one has claimed responsibility for the attack, but analysts from the Russian computer security company Kaspersky have said that due to the complexity of the malware, it would take 10 skilled people between 2-3 years to develop working full time. This fact together with the non-financial nature of the attack makes it most likely a government-sponsored action.

Operation Borodino: Cyber-Attack Operation during the Great Northern War of 2017

NATO military forces are ready for a counter offensive against an aggressive enemy force that has occupied a small independent country located in Europe.

The opponent has a modern military, using all the modern technology available, and the area of operation is a modern environment with all modern means of communication and computer networks available.

The enemy force has a particularly-advanced computer network that enables a very agile command and control with its military and paramilitary units in the occupied country. The military computer network in the occupied country shares many of the same software components as the civilian computer network in this country. It was the same private contractor who delivered essential components to both systems. Both systems are also connected with civilian railway traffic regulation because the military intended to synchronize civilian and military rail traffic in case of a general mobilization.

NATO is planning a major military operation. It will be a joint operation that will include Special Operations Forces as well as airborne and air-land infantry, with air operations including suppression of enemy air defense and air-ground bombing. Operational analysis shows that a critical point in the defense system is the hostile joint headquarters with the command and control network that runs everything including personnel, equipment, facilities, organization, procedures and chain of command. The system is extremely effective in detecting any incoming forces including drones, planes and missiles. The system will facilitate effective counter measures, and make any incursion into the enemy-held space a high-risk operation.

16) Lachow, "The Stuxnet Enigma", p. 126.
17) Lachow, "The Stuxnet Enigma", p. 120.

Because of these circumstances, the NATO joint force commander has decided to launch a cyber-attack to target the C2 network. It is the obvious choice since there is minimum risk to friendly troops and direct access to the target's critical vulnerability.

Cyber command attached to the NATO joint task force creates a plan to support the joint operation. Cyber command is looking to achieve what is known as Distributed Denial of Service (DDoS). The operation involves taking control of several computers by installing a very aggressive and destructive worm. Once the worm is inserted into one computer in a botnet, which is multiple computers linked together, the worm spreads and the computers in the network start to shut down the network, by flooding the servers with data request. This massive flow of data requests causes buffer overflow, and jams the servers thereby making them unusable. The computers in the network block the network. The worm and malware have a collective codename, Borodino. In support of this worm, malware is designed to destroy the cooler on the computer machines. This will lead to overheating of the machine and physical destruction in most cases.

Codename: Borodino

Borodino is set to go active on a command, and it is not self-destructive. It will continue to be effective until it is contained and eliminated. Borodino is designed to target a specific software component of the enemy computer network, but it is also compatible with other computer network systems if they share some of the same software components. The hostile joint headquarters computer network is a clear military target. However, the connection to the civilian rail traffic regulation is not clearly understood.

The Borodino malware is launched on the eve of D-day. Within a moment, Borodino has affected the targeted software components. The network is blocked and ineffective. At the same time the malware is effective in destroying the cooling mechanism on several machines thus destroying them physically.

A cyber response team responds by isolating the virus and extracts it from the computer network system.

Back in their laboratory, the technicians are working around the clock to analyze the data and to come up with a counter measure. The rail traffic regulation is also affected due to the shared software component, but this is not discovered before it is too late.

One of the technicians unintentionally inserts an infected USB-key into one of the research-computers that is linked to the internet. Before the technician discovers what he had done, the virus and malware are out on the internet and the open civilian network.

As the Borodino cannot distinguish between civilian and military use of the software, it immediately starts to attack the civilian computer infrastructure. The power supply is disabled. An entire region is left without power. This causes severe issues with sanitation and traffic; additionally, the ability for the emergency services to operate is greatly reduced. Trains full of civilian passengers collide due to the rail traffic regulation failures. The loss of civilian life is severe, with more than 200 reported dead, and almost 400 wounded.

The Legal Implications

The scenario you have just read belongs to the future, but technology, techniques, and tactics are developing at a rapid rate. This scenario can very quickly become reality. The closest scenario known to the public is the case of Stuxnet.

Because of the nature of cyber weapons, as illustrated by this scenario, they differ from conventional kinetic weapons in some distinguishable way. This will have implications for how we understand and apply the targeting rules according to the laws of armed conflict.

In our scenario the attack is initially directed against a purely military object which is a legal object according to The Hague convention of 1923 and according to article 52 (1) of the additional protocol I of the Geneva convention that prohibits any attack directed against all objects which are not military objects.

The cyber-attack weapon is not purposefully or intentionally designed to cause superfluous damage, as this would be prohibited.

Civilian cyber infrastructure is also exposed to the effects of the cyber-weapon due to the design of the weapon. This can be seen as either an attack on a dual-use target or an indiscriminate attack. Indiscriminate attacks are prohibited because they violate the proportion and distinction principles and it is prohibited by article 51.4 of additional protocol I of the Geneva Convention and by The Hague convention of 1923, article 24(3).

According to article 51.4 of additional protocol I indiscriminate attacks are:

> (a) Those which are not directed at a specific military objective
> (b) Those which employ a method or means or means of combat the effects of which cannot be directed at a specific military objective or
> (c) Those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each case, are of a nature to strike military objectives and civilians or civilian objects without distinction.[18]

Parts a and b refers to the core principle of distinction, that attacks must be directed against military objects only. Part c refers to the core principle of proportionality.

In historical scenarios, using conventional weapons, indiscriminate attacks are typical massive bombardments aimed at an area and hitting civilians *en masse* with only a limited effect on military targets like some of the areal bombings of WWII.

If we apply this rule to our scenario we might consider the virus and malware to be indiscriminate because it can attack a major civilian computer network and cause extensive damage to civilian lives and property.

However, the CNA was specifically aimed at the military computer network. The intention was never to target civilian cyber networks, and it was never delivered by the attacker to the civilian network. *There was a clear military use of the specific targeted software-components in the military network*.

18) Solis, "The Law of Armed Combat" p. 536

According to 51 (5, b) of additional protocol I if there is a known and feasible way of effecting only the military system, then any method that also targets the civilian systems would be illegal. However, that is not the case in our scenario.

The virus and malware was designed to take out a specific system. In this case, it was the military command and control system. However, this system shared some critical components with a civilian infrastructure. The virus does not target the specific military network, but instead it attacks a specific software-component within the military network. If this specific component is also a feature of a civilian network, then the target (the software components and not the military network) has both a military and civilian use and qualifies for dual-use target status.

Dual-Use Targets Including Dual-Use Software Components

As previously mentioned, Dual-use targets have both a military and civilian use. In our case, the intended target of the cyber-attack, the military command and control network, is a purely military target according to all relevant rules of armed conflict. However, due to the nature of the cyber-weapon, a reevaluation of targeting is necessary.

Unlike conventional kinetic weapons, the cyber-weapon is not necessarily expended or depleted once it has hit the intended target. The cyber weapon is active and aggressive in nature, and it will continue to be destructive against the targeted software components.

This level of complexity is an added feature in cyber warfare and it will require careful research on both the military and civilian use of the targeted software components. The Tallinn manual states that an unintentional spread of a cyber-weapon, for example by a storage device, is not considered foreseeable by the attacker and thus will not be considered by the attacker[19]. However, in terms of targeting, the attacker must consider the immediate collateral effects of the attack and he must consider the delayed and/or displaced second, third, or higher-order consequences of action, created through intermediate events or mechanisms[20].

The Tallinn manual concludes that the collateral damage factored into the proportionality calculation includes any indirect effects that should be expected by those individuals planning, approving, or executing a cyber-attack[21].

With our current technology and network connectivity, it is very easy for the cyber-weapon to be spread unintentionally (transfer by USB storage devices is an obvious method). This happened in the Stuxnet case and unless this is taken into consideration, it could happen again. It is a very simple process and does not require many links or what-ifs, indeed only one commonplace act is necessary: a human putting an infected storage device into a connected machine.

The issue of distinction in cyber warfare is clearly framed here by Gervais:

> Distinction is a problem for cyber attackers, whose targets are very frequently dual-use. However, if the intent of a cyber attack is to achieve a military advantage by targeting computer systems used for military

19) Tallinn Manual p. 161
20) Joint Chiefs of Staff, Joint Publication 3-60, Joint Targeting I-10 (2007)
21) Tallinn Manual p. 160

> objectives, and if the attackers conduct such attacks with reasonable precaution for likely collateral effects, cyber weapons are a more precise and adaptable means for attack than traditional weapons[22]

Instead of seeing the military computer-network as a single entity, as would be the custom in conventional targeting, it would be more accurate to consider the target as a computer-network consisting of several software and hardware components. The target of an attack is specific software components within the system.

The cyber-weapon is designed to achieve an end-result by attacking various components within the network. The weapon will be directed against the components and disable these components in order to disable the network. The actual target is not the network but the specific components (be it software, codes or maybe programmable logic controllers like the Stuxnet).

When there is a chance that a cyber-weapon can spread to, or in any way effect, a new system, the attack is against the targeted software-component of the cyber-network, wherever it may be present. If the software-component is also in use in civilian networks, then the attack should be considered an attack on a target that has both a military use and a civilian use.

In the scenario, the attackers do not attack *a military network* but instead they are attacking *a specific software-component with a dual military and civilian use.* This line of reasoning should help focus the proportionality calculations and help assert the possible collateral effects of an attack.

The legal analysis must follow the standard four core principles including distinction and proportionality of the military advantage gained as opposed to damage done to civilian lives and property.

It is not prohibited to attack dual use targets but generally there is a higher requirement to prove the military advantage gained in order to sanction an attack.

To sum up, the necessary legal analysis before a cyber-attack are as follows:

1. Determine the target according to the legal criteria for a military target.
2. Determine the specific software components that are the target. Answer the following questions in relation to each targeting software:
   - 2a. Are the targeted software-components in use in civilian cyber-networks?
   - 2b. What is the potential damage if the cyber-weapon is unleased in a civilian cyber-network with the same software-components?
3. Evaluate the military necessity of the attack.
4. Consider whether the military advantage gained is proportional to possible damage done to civilian lives or property.
5. If possible, program the weapon so that it can distinguish between a civilian network and military network.

22) Gervais "Cyber Attacks and the Laws of War", Berkeley Journal of International Law, volume 30, Issue 2, Article 6, 2012, p. 571.

Conclusion

These five points are all standard points of consideration in laws of armed conflict but in this particular case, we urge that specific software components rather than entire networks be viewed as the appropriate target of a cyber-attack. Targeting software components rather than networks will help ensure that collateral effects are given the proper considerations, and that the proportionality calculations can be done as accurately as possible, which together will allow cyber operations to unfold squarely within the norms of LoAC.

This potential problematic issue also urges the various nations Cyber Commands to consider if they have sufficient technical competences to make such targeting possible. If they don't have the sufficient cyber capabilities, then this is a call to increase cyber capabilities.

It should be stressed that these recommendations are not a call to outlaw cyber-attacks on software-components with a dual-military-civilian use. Rather, the goal is to sensitize the cyber research community to the need to make additional considerations before launching such an attack, especially since we have such limited experience with CNA.

The decision-making process to attack should be made like any other conventional attack. The military commander has the final say, but the decision should be made in close consultation with military legal advisors, technical experts and even public affairs officers. When practical knowledge is so limited, it becomes even more important to consult subject-matter experts. We have little in the way of practical experience to refer back to. As the attack can have serious consequences for the civilian population (legal or otherwise), the decision may benefit from the involvement of public affairs professionals. All these considerations are in order that the decision must be based on a sound and thorough analysis of such a complex operation. The final responsibility will still be with either the military leadership or the political leadership like any conventional or nuclear attack.

In our scenario, NATO may not be responsible for the accidental transference of Borodino. However, they are certainly responsible for the civilian lives lost at the train accident. This has to be considered against the anticipated military advantage gained by the attack.

The attack by NATO would probably be legal with the current knowledge, experience and technology.

Nevertheless, this might change. Given how easy it is to transfer a virus or malware between computers and systems, it can be increasingly more difficult to deny the responsibility for such an eventuality.

Finally, we must remember article 57 precautions in attack (2) (ii). The attacker shall *take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss or civilian life, injury to civilians and damage to civilian objects*.

In the very near future, this may well include CNA refraining from targeting software components that also have a civilian use.

Bibliography

Gervais, M., "Cyber Attacks and the Laws of War", Berkeley Journal of International Law, 30(2), 6, 2012.

Geneva Conventions of 1949, their Commentaries and Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Joint Chiefs of Staff, Joint Publication 3-60, Joint Targeting I-10 (2007).

Lachow, I., "The Stuxnet Enigma: Implications for the Future of Cybersecurity", *Georgetown Journal of International Affairs*, 2011, pp. 118-126.

Militærmanual om folkeret for danske væbnede styrker i internationale militære operationer, september 2016.

Rogers, A.V.P., "Law on the Battlefield", Melland Schill Studies on international law, 2012 edition

Solis, G.D. "The Law of Armed Conflict" Cambridge University Press 2010 edition

Tallinn Manual on the International Law Applicable to Cyber Warfare, *Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. General editor Michael N. Schmidt, Cambridge: Cambridge University Press, 2013

Yde, I., The Law of Cyber Armed Conflict: *Translating Existing Norms of International Humanitarian Law into Cyber Language*. Copenhagen: Royal Danish Defence College, August 2013.