# From Cyber Operations to Effects: Some Targeting Issues

Ducheine, P.; Gill, T.

**Publication date**
2018
**Document Version**
Final published version
**Published in**
Militair Rechtelijk Tijdschrift

Ministerie van Defensie

# From Cyber Operations to Effects: Some Targeting Issues

Versie 1

# Documentgegevens



**Originele versie:**
Citeertitel: From Cyber Operations to Effects: Some Targeting Issues
Permalink: http://puc.overheid.nl/doc/PUC_248377_11

**Soort document:**
Type: Publicaties - Beschouwing
Bron: Ministerie van Defensie

**Versie en datums:**
Versie: 1
Laatste wijziging: 17-08-2018

**Publicatiegegevens:**
Uitgever: Ministerie van Defensie
Kanaal: MRT
Vorm: origineel PUC document
Referentienummer: PUC_248377_11
Toegankelijkheid: Intern
Publicatiedatum: 17-08-2018
Taal: en

**Verrijking gepubliceerd bij document:**
Thema's:
- Jaargang 2018
- Beschouwing

# Inhoudsopgave

# From Cyber Operations to Effects: Some Targeting Issues

Brigadier General Prof. Dr. Paul Ducheine and Prof. Dr. Terry Gill[1]

1 Dr Terry Gill is Professor of Military Law at the University of Amsterdam and the Netherlands Defence Academy. Professor Gill is Director of the Research Programme "Role of Law in Armed Conflict & Military Operations" at the Amsterdam Center for International Law (ACIL). He is editor in chief of the Yearbook of International Humanitarian Law, member of the editorial boards of the Journal of Armed Conflict & Security Law, Journal of International Peacekeeping and Military Law Review. He was a member of the expert group convened by the ICRC and TMC Asser Institute on "Direct Participation in Hostilities", of the International Group of Experts which drew up the Tallinn Manual on the International Law Applicable to Cyber Warfare and of the Tallinn 2.0 Project on the application of international law to peacetime cyber security and is a board member of the International Society of Military Law and the Law of War (Brussels) and senior academic advisor to the Society's project on the drafting of "The International Law of Peace Operations". He is Chairman of the Study Group on The Conduct of Hostilities in the 21st Century of the International Law Association (London), He is author of numerous publications on the use of force, international humanitarian law and the law of military operations including the authoritative Handbook of the International Law of Military Operations published by Oxford University Press (1st ed 2010, 2nd ed. 2015). He teaches courses in international law relating to military operations, international humanitarian law and related topics at the University of Amsterdam and Netherlands Defence Academy and is a frequent guest lecturer at universities and other institutions inside and outside the Netherlands. Brigadier General Paul Ducheine (1965) is a Professor for Cyber Operations and Cyber Security at the Netherlands Defence Academy and a Professor in the Law of Cyber Warfare at the University of Amsterdam. Ducheine started his military career in 1983 at the Royal Military Academy and joined the Engineer Regiment (as a combat engineer) in 1987. In 1998 he joined the Army Legal Service. Prof. Ducheine holds degrees in Political Sciences (Amsterdam Free University, 1993) and Law (University of Utrecht, 1998). In 2008 he defended his PhD-thesis Armed Forces, Use of Force and Counter-Terrorism. A study of the legal aspects of the role of the armed forces in combating terror (org. Dutch) at the University of Amsterdam. He is one of the editors of Cyber Warfare: Critical Perspectives – NL ARMS 2012, TMC Asser Press (2012), and Fighting without killing, NLARMS 2017, TMC Asser Press/Springer verlag (2017). With Mike Schmitt (US Naval War College) and Frans Osinga (NLDA) he edited Targeting: Challenges of Modern Warfare (2015, TMC Asser Press).

# Introduction

Ladies and gentlemen, you've just heard Brigadier General Hans Folmer explain what the purpose of applying cyber capabilities could look like. He described a wartime situation and explained that there was a need to prevent the enemy from using a specific airfield and dispatching aircraft from there. The military process to plan action to that end, is called targeting. In classic circumstances, those planning and deciding on operations of this kind, joined in a targeting board, would for instances consider the use of cluster munitions to destroy the runway of the airfield, so that aircraft are unable to start (and land). Thus rendering the airfield (and its aircraft) useless. Or, if the state involved would not possess this type of weapons (as it is a party to the treaty banning the use of it), the targeteers would come up with a larger scale operations with other air delivered weaponry. The backlash of the latter would perhaps be that collateral damage might occur, or that it might hamper future operations of own troops.

Brigadier General Folmer also presented another line of action. By tampering digitally with the airfield's flight control system, aircraft would be unable to start (and land) as well. This cyber operation could nullify the amount of collateral damage and as it has only temporary effects, would guarantee future use of the airfield by own troops.

Today, targeting boards, at least in a number of states, have this alternative offered through cyber capabilities at hand. The process and procedures to consider these cyber capabilities is the same targeting process as is used in the classic situations. And it contains the same legal questions derived from the law of armed conflict (of international humanitarian law) as in the classic cases. The same basic questions, that is, with some new or not yet touched upon more detailed issues at hand.

My goal [Ducheine], is to briefly introduce this targeting process in the first place and then take you through the legal basic questions accompanying its various phases. Professor Gill will then elaborate on some of the general and specific legal issues involved.

The next lectures by Dr. Heather Harrison-Dinniss and mr. Joost Bunk will specifically deal with the issue of data as an object and its protection under IHL or other regimes such as intellectual property.

Just to iterate in order to prevent misinterpretation: we're at war and IHL applies. In particular, the rules on hostilities, or in other words, the some called targeting rules in principle apply. These rules centre on the notion of attack (art. 49 API).

# Targeting

As mentioned in the airfield case by Hans Folmer, all targeting starts with the 'why'. The first phase of targeting involves stating the purpose, the end or goal of the action(s) to be taken. In the second phase potential targets that could be engaged with some kind of (military) action in order to contribute to that stated end will be listed. The weaponry will be considered in the third phase: what's in the arsenal? What are the effects of those weapons? And will it be effective against the target(s)? Then, in the fourth phase, one of the weapons will allocated for a specific target. Phase five comprises the actual attack that will be launched, which will be evaluated (phase six) to see whether the attack was successful and generated the designated effect, thus contributing to the very purpose of the actions taken. If and when necessary, the procedures will be followed once more.

Just to remind you, this targeting process, or the targeting cycle, is based on a rational decision-making (and planning) model. The process itself can take up to months in preparation when pre-planned strategic campaigns are involved. But it could also be a matter of seconds when tactical opportunities arise on the battlefield.

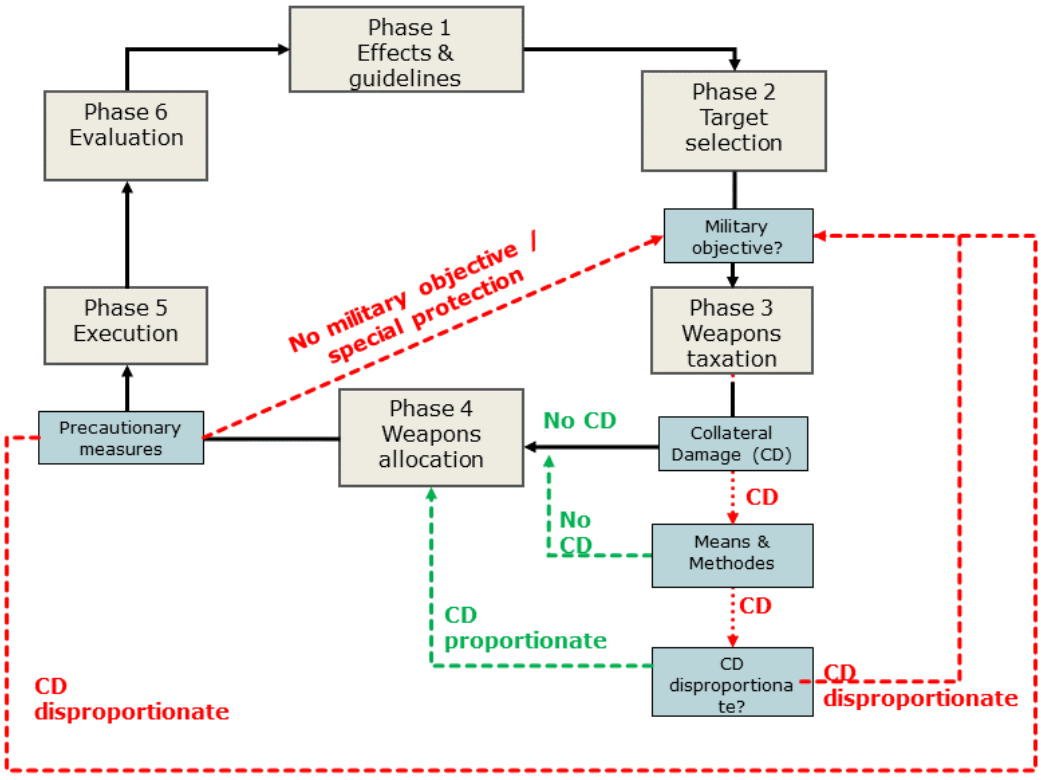


*Figure 1 : Targeting cycle with its legal (IHL) issues*

During this targeting cycle, the staff officers combined in a targeting board and the commander who bears ultimate responsibility for the decision to (and how to) attack, are confronted which legal questions posed to them, as they are to adhere to the law of armed conflict when planning and conducting attacks. These legal questions are imposed through the so-called targeting rules, and they find their background in the principles of the law of armed conflict. The principles involved are: military necessity, humanity, distinction, proportionality and the obligation to take precautionary measures, and, finally, chivalry.

These principles and the more detailed targeting rules are part and parcel of the targeting cycle. When integrating the two – the targeting cycle and the legal issues – the targeting cycles can be amended to contain the legal questions related to targeting derived from the law of armed conflict (see Figure 1).

The first issue after having defined the goal (phase 1) and having listed the potential targets (phase 2) is which of these potential targets qualify as "military objectives" (ex art. 52 API), as "attacks shall be limited strictly to military objectives".[2]

After that, when potential weapons are reviewed (phase 3), the question will be posed whether collateral damage (CD, ex art. 57 API) can be expected once the particular weapon is used against the legitimate target (i.e. a military objective). When no foreseeable collateral damage is expected, the weapon can be allocated to the legitimate target (phase 4). Quite often however, CD is to be foreseen.

Then, as part of one of the precautionary measures (ex art. 57 API), the question arises how this CD can be mitigated through changes in the choice of means (weapons) and/or methods of attacks. When tweaking of means and methods of attack nullifies the foreseeable CD expected, phase 4 (allocation) can be pursued. If and when this is not the case, the question will be posed whether this attack "may be expected to cause [collateral damage, that] would be excessive in relation to the concrete and direct military advantage anticipated".[3] If the attack is not expected to generate a disproportional (or "excessive") amount of CD, allocation (phase 4) will commence. When the attack is disproportionate, the attack shall be "cancelled or suspended".[4] As a result, the targeting cycle has to start all over.

After weapons have been allocated to a legitimate target ("military objective") in phase 4, the remaining precautionary measures, such as last minute verification and identification, warning, and last-minute actual checking of the CD estimation are to be taken. This could result in last-minute aborting the attack. After the attack (phase 5), the battle damage assessment is made (phase 6) and evaluation takes place.

This integration of the targeting cycle and the targeting rules apply to all attack in the meaning of article 49 API. Regardless of the weapons, or technique, used. This integrated cycle with targeting rules is thus to be used when the targeting board and the commander responsible for planning and executing the operations against general Folmer enemy airfield. Both when classic weapons are considered, and also when cyber capabilities are contemplated. In the first case, this is definitely a matter a legal obligation. In the latter, this will most likely be a matter of policy, as the debate on the applicability of the targeting rules to cyber operation is still continuing.[5]

This will now be explained by Prof. Gill in general terms.

2 Article 52 Additional Protocol I tot he Geneva Conventions, 1977 (API).

3 Art. 57 (2) b API.

4 Art. 57 (2) b API.

5 See the Tallinn Manual.

# A Brief Overview of the Main Controversies

The question of whether international humanitarian law (or the law of armed conflct as it is widely referred to in military circles) applies in cyber-space was supposed to have been resolved, but controversy remains on that issue.[6] But assuming it does (and from our viewpoint it is impossible to see how it could not if cyber were employed in an armed conflict in either a stand-alone capacity or more probably alongside other means and methods of warfare), then certain other controversies remain. One of the most seemingly intractable of these is the question as to whether data is an "object" in the context of Article 49 of Additional Protocol I. The Group of Experts which drew up the Tallinn Manual could not reach consensus on this issue and various points of view have been put forward by other commentators , one of whom, Dr. Harrison Dinniss, will elaborate on her views in more detail presently.

The issue may seem for the non-lawyer perhaps a bit technical and arcane at first sight, but is of real importance in a practical sense. Put simply: if data is not an object, then the rules of IHL relating to targeting as set out above by my colleague Brigadier General Prof. Ducheine are not applicable to cyber operations which affect data without causing any directly related secondary physical injury to persons or damage to physical objects. Which rules would then be applicable are open to question, but in any case, the principles of proportionality, precautions in attack and so forth would be irrelevant in the absence of related physical effects resulting from tampering with or corrupting data. That means of course, that the permissible scope for many types of operations would be much wider. To take the example of the neutralization of an airfield by cyber means used by Brigadier General Folmer earlier, such an operation would not constitute an attack in the sense of Art. 49 AP I unless it caused the aircraft to crash. Simply making an airfield unusable by cyber means, without any directly related physical effects would be outside the scope of targeting principles if data did not constitute an object in itself. So this debate is really about whether a whole range of cyber actions in an armed conflict are subject to targeting law or not.

Several main positions have emerged on this issue. One is the majority opinion of the Group of Experts in the Tallinn Manual. This states in a nutshell that neither the text of Article 49, nor the Commentary thereto would include data as constituting an object for the purposes of determining whether its neutralization, alteration or removal would amount to an 'attack'.[7] This follows in the majority view expressed in the commentary from a textual interpretation of the word 'object' , which denotes in that view something with physical properties and is tangible in the "real" world. Another view expressed is that this is too restrictive and that data should be considered an object when its destruction or neutralization would have severe consequences for the civilian population even though these fell short of physical harm to persons or physical objects. This view has been put forward *inter alia* by Kubo Mačák, who argues that the term 'object' should be interpreted more expansively and that a teleological interpretation of Article 49 AP I is therefore called for to enhance the protection of the civilian population and internet infrastructure. [8] Other views include those of Dr. Harrison Dinniss who argues that while data as such may not constitute an object the systems data which operate the system as a whole do and that destruction thereof should fall within the ambit of 'attack'.[9] Still another is to be found in the writings of various commentators who argue by analogy that other intangibles such as intellectual property or electricity are regulated and protected by other branches of the law. Essentially what all these critiques of majority position in the Tallinn Manual is that they disagree with the outcome of excluding data from the general protection offered by the law of targeting in AP I. In this view an attack which would affect all or some data without any physical effects,

6 See Report by Group of Governmental Experts on Developments on the Field of Information and Telecommunications in the Context of International Security, A68/98 24 June 2013 and the subsequent failure of the UN GGE to reach agreement on the application of international law and the use of force and international humanitarian law to cyber space. https://www.un.org/disarmament/topics/informationsecurity/

7 See Tallinn Manual 2.0 , Rule 92 and commentary thereto.

8 K. Macak, Military Objectives 2.0: the Case for Interpreting Computer Data as Objects under International Humanitarian Law. *Israel Law Review*, *48*(1), 55-80.

9 H. Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge University Press (2012).

but causing damage or destruction to the data with potential negative impact on the civilian population is or at least should be included in the notion of attack and covered by considerations of proportionality and precautions in attack.

This is as of yet, an unresolved issue, but one with real consequences. It remains to be seen how State practice and possibly other factors such as positions taken by the UN or by an international court or the preponderance of academic opinion may affect the outcome of this controversy. In the meantime, it remains somewhat a grey area in the application of international law to cyberspace.