UvA-DARE (Digital Academic Repository)

Fighting power, targeting and cyber operations

Ducheine, P.A.L.; van Haaster, J.

DOI

[10.2139/ssrn.2392373](https://doi.org/10.2139/ssrn.2392373)

Publication date

2014

Document Version

Submitted manuscript

[Link to publication](#)

Citation for published version (APA):

Ducheine, P. A. L., & van Haaster, J. (2014). *Fighting power, targeting and cyber operations*. (Amsterdam Law School Legal Studies Research Paper; No. 2014-10). Amsterdam Center for International Law, University of Amsterdam. <https://doi.org/10.2139/ssrn.2392373>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UNIVERSITY OF AMSTERDAM

FIGHTING POWER, TARGETING AND CYBER OPERATIONS

P.A.L. Ducheine

J. van Haaster

Amsterdam Law School Legal Studies Research Paper No. 2014-10

Amsterdam Center for International Law No. 2014-04

Amsterdam Center for International Law
University of Amsterdam

RESEARCH PAPER SERIES

ACIL Research Paper 2014-04

Fighting Power, Targeting and Cyber Operations

Paul Ducheine & Jelle van Haaster
Amsterdam Center for International Law

Cite as: ACIL Research Paper 2014-04,
available at www.acil.uva.nl and [SSRN](https://ssrn.com/abstract=2392373)

Fighting Power, Targeting and Cyber Operations

Paul Ducheine
Faculty of Military Sciences
Netherlands Defence Academy, Breda
University of Amsterdam
p.a.l.ducheine@uva.nl

Jelle van Haaster^{*}
Faculty of Military Sciences
Netherlands Defence Academy, Breda
University of Amsterdam
j.vanhaaster@uva.nl

Abstract

This article aims to contribute to the operationalisation of military cyber operations in general, and for targeting purposes (either in defence or offence) in particular. The position of cyber operations in military doctrine will be clarified, their contribution to fighting power conceptualised and the ramifications on targeting processes discussed.

Cyberspace poses unique challenges and opportunities; we distinguish new elements that may be utilized for 'targeting', namely: cyber objects and cyber identities. Constructive or disruptive cyber operations aimed at these non-physical elements provide new ways of attaining effects. Assessing the outcome of these cyber operations is, however, challenging for (military) planners. Intertwined network infrastructure and the global nature of cyberspace add to the complexity, but these difficulties can be overcome.

In principle, the targeting cycle is suitable for cyber operations, yet, with an eye to (a) effectiveness of offensive and defensive operations, and (b) legal obligations, special attention will be required regarding effects in general, and collateral damage assessment in particular.

Keywords: Cyberspace, Fighting power, Doctrine, Operations, Cyber operations, Targeting.

^{*} Colonel dr. Paul Ducheine MSc, LL.M. is Associate Professor of Cyber Operations, Legal Advisor (Netherlands Army Legal Service), lecturer and senior guest researcher at the University of Amsterdam. Lieutenant Jelle van Haaster, LL.M., is a Ph.D. candidate focusing on cyber operations at the Netherlands Defence Academy and University of Amsterdam. The authors are grateful to the publishers of the *Militaire Spectator*, for their kind permission to use portions of their article 'Cyber/operaties en militair vermogen' (org. Dutch), in: 182 *Militaire Spectator* (2013) 9, pp. 369-387.

1. INTRODUCTION

Cyber in its most general sense is heralded as a force-multiplier in the arsenal of both State and non-State actors.¹ Although the potency of 'cyber' is uncontested, there are questions with regard to the operationalisation of cyber means and methods. Since some of these questions remain unanswered, the use of 'cyber' in (military) operations is frequently cast aside or overlooked.² One of the issues leading to dismissal of 'the cyber option' is limited understanding of the effects and implications of the use of cyber-weapons for doctrinal thought and operational processes such as targeting. Understanding new means and methods is imperative for adequate appreciation and operationalisation of their potency in offensive, defensive and stability operations.

The goal of this article is to clarify the position cyber operations within military doctrine, conceptualize their contribution to fighting power and discuss potential ramifications on the targeting cycle, and by doing so, contributing to the debate regarding operationalisation of military cyber means and methods.

Contemporary military operations are not conducted stand-alone; they are means to an end and are conducted parallel to other (non-) military activities.³ In order to place the military instrument in its context, we will first briefly expand on instruments of State power, and focus on the conceptualization of fighting power and 'conventional' military operations (§2.). Before expanding on cyber operations, it is necessary to define the unique characteristics of cyberspace (§3.). Once cyberspace's landscape is examined, we will turn to cyber operations and their contribution to fighting power (§4. -5.). Lastly we will discuss the ramifications of conducting cyber operations on conventional targeting procedures (§6.).

¹ The current development of doctrine supports this notion, see for instance: U.S. DoD, *DoD Strategy for Operating in Cyberspace* (Washington DC: U.S.DoD, 2011).; Netherlands MoD, *The Defence Cyber Strategy* (The Hague: Netherlands MoD, 2012).; Russian MoD, *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space* [концептуальные взгляды на деятельность вооруженных сил российской федерации в информационном пространстве], trans. NATO CCDCOE, 2011).

² See for instance: Amber Corrin, "The Other Syria Debate: Cyber Weapons," few.com/articles/2013/09/04/cyber-weapons-syria.aspx (accessed 30 October, 2013).

³ NATO, *AJP-1(D): Allied Joint Doctrine* (Brussels: NATO Standardization Agency, 2010). Sections 107-110.

When describing and conceptualizing the position of cyber operations, Allied doctrine will be used, primarily focusing on doctrine published by the North-Atlantic Treaty Organization (NATO), but supplement it with doctrine publications by Allies. For military cyber operations we use the internationally commended definition stemming from the Tallinn Manual: “The employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace.”⁴ We will discuss the subtleties and implications of this definition in the course of this contribution.

2. THE MILITARY INSTRUMENT

In order to provide security and for the protection of other strategic vital interests, states may rely on their instruments of power: the integrated or joint military power (land, sea, air) as well as diplomatic, economic, and informational means.⁵ Apart from DIME-instruments,⁶ the NATO recognizes the “wide utility [of] civil capabilities” in contemporary operations.⁷ Thus, States nowadays have various instruments for achieving strategic goals to the detriment or in support of other States or non-State actors. The use of force is just one of those instruments, although it is quite different than other instruments.⁸

A. *Fighting Power*

Armed forces ‘produce’ and apply fighting power,⁹ consisting of three elements: the physical, moral and conceptual component (see figure 1).¹⁰

The physical component comprises first and foremost manpower and equipment that provide the “means to fight”.¹¹ Equipment consists of military platforms, systems, weapons and supplies of “operational or non-operational

⁴ Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013). p. 258.

⁵ Antulio J. Echevarria II, *Clausewitz and Contemporary War* (Oxford: Oxford University Press, 2007). p. 144.

⁶ NATO, *AJP-1(D)*. Sections 107-110.

⁷ *Ibid.* p. 1-3. Section 111.

⁸ Jachtenfuchs, *The Monopoly of Legitimate Force: Denationalization, Or Business as Usual?* p. 38.

⁹ British Army, *ADP: Operations* (Shrivenham: Development, Concepts and Doctrine Centre, 2010). p. 2-2.

¹⁰ NATO, *AJP-1(D)*. Sections 120-123.

¹¹ British Army, *ADP: Operations*. p. 2-31.

and deployable or non-deployable” nature.¹² Apart from material elements, the physical component also entails sustainability and (operational) readiness.¹³

The moral component¹⁴ involves “the least predictable aspect of conflict”, namely “the human element”.¹⁵ It entails “good morale and the conviction that the mission’s purpose is morally and ethically sound”.¹⁶ The moral component is rooted in three “priceless commodities: ethical foundations, moral cohesion and motivation”.¹⁷ In addition, effective leadership is vital.¹⁸

The conceptual component “provides the coherent, intellectual basis and theoretical foundation for the deployment of military units and troops”.¹⁹ The higher levels of doctrine (strategic and operational) “establish the philosophy

¹² Ibid. p. 2-32.

¹³ Netherlands MoD, *Netherlands Defence Doctrine* (NDD) (2013). p. 69.

¹⁴ The Netherlands Defence Doctrine (NDD) refers to a “mental component”, contrary to the NATO and British “moral component”.

¹⁵ British Army, *ADP: Operations*. p. 2-10.

¹⁶ NATO, *AJP-I(D)*. Section 121.

¹⁷ British Army, *ADP: Operations*. p. 2-11.

¹⁸ Netherlands MoD, *NDD*. p. 67.

¹⁹ Ibid. p. 71.

and principles underpinning the approach to conflict and military activity”.²⁰ Apart from guidance, “the conceptual component also plays a significant role in the preservation and development of the institutional memory and experience”²¹ through education, innovation and lessons learned.²²

Thus, fighting power entails the ability to effectively conduct military operations. However, fighting power is “more than just the availability of operational means (capacities); there must also be the willingness and ability to deploy these means (capability)”.²³ When properly developed, “capacities are elevated to capabilities” and they become fighting power.²⁴ Fighting power will then be employed effectively to achieve strategic goals, whether alone or in unison with other strategic instruments (the “comprehensive approach”).²⁵

B. Operation, the Manoeuvrist Approach and Comprehensiveness

Armed forces project fighting power through (military) operations. Operations vary in form, purpose, size and duration, and vectors (land, sea, air, space and cyberspace). This paragraph will focus on the conceptualization of administering fighting power through military operations. The Manoeuvrist Approach is vital in understanding the ratio of conducting military operations. This approach “focuses on shattering the adversary’s overall cohesion and will to fight, rather than his materiel [...] it is an indirect approach”.²⁶ The emphasis is on an adversary’s moral and conceptual component rather than the physical; the purpose is degrading the cohesion in components of an adversary’s fighting power.²⁷ In addition, the integration of various instruments, i.e. the Comprehensive Approach, is not only used at the strategic level, but in actual operations at lower levels as well.

Interpreted in a broader and more modern sense, operations entail influencing actors (as opposed to ‘the adversary’) by employing different instruments (in addition to the military instrument).²⁸ Contemporary conflict is characterized

²⁰ British Army, *ADP: Operations*. p. 2-5.

²¹ Netherlands MoD, *NDD*. pp. 70-71.

²² British Army, *ADP: Operations*. pp. 2-9, 2-10.

²³ Netherlands MoD, *NDD*. p. 66.

²⁴ Netherlands MoD, *NDD*. p. 66.

²⁵ NATO, *AJP-1(D)*. Sections 226-232.

²⁶ *Ibid.* Section 611.

²⁷ British Army, *ADP: Operations*. p. 2-6.

²⁸ Netherlands MoD, *NDD*. p. 108.

by a “[high] number of actors [...] intensified by our ‘open’ world, in which everyone can keep abreast of each military operation”.²⁹ Thus, operations are no longer primarily aimed at opponents, but at a wide range of actors, such as “population groups, parties, countries and organizations with which there is no physical interaction”.³⁰

Consequently, the military instrument is no longer the only and prime instrument in an area of operations. Activities should be tailored to increase and maintain support for friendly operations through employing various (DIME) instruments.³¹

Operations aim to decrease support for adversaries, and generate support from others.³² Figure 2 illustrates this conceptualization of influencing adversaries, neutral parties and supporters.

Figure 1 Employing instruments of State power

²⁹ Ibid.

³⁰ Netherlands MoD, *NDD*. p. 108.

³¹ Ibid.

³² Ibid.

Activities (operations) addressing adversaries are – by definition – *disruptive* in nature (figure 2 red arrows). An attempt is made to shatter overall cohesion, which only exists by virtue of clear lines of communication – whether information or leadership-wise. Or through ‘attacking’ or “addressing’ the moral and conceptual component. Without cohesion, morale and effective leadership, the opposing forces can more easily be conquered, destroyed or ‘outmanoeuvred’.

Operations addressing neutrals and supporters are *constructive* in nature. Their aim is to increase support for friendly operations. By influencing neutral actors, an attempt is made to convince them to join or support a friendly cause (figure 2 blue and grey arrows). The goal is to keep them neutral, but preferably turn them supportive. By reinforcing the power of supporters physically (e.g. through materiel and training), morally or economically (e.g. funds) the foothold within supportive groups can be increased (figure 2 blue and grey arrows).

C. Means to an effect

Activities conducted by armed forces are means to an end, namely: to achieve a predefined (strategic) kinetic or non-kinetic effect to the detriment or support of an actor. To that end, both “lethal and non-lethal means”, or physical and non-physical, means (hard-power and soft-power) can be applied.³³

Lethal and non-lethal effects, or physical and non-physical effects, are complementary and intertwined. For instance, destroying enemy materiel and personnel (physical component) will primarily cause physical effects, although it will also affect enemy morale (moral component), being a non-physical effect. (ref: Figure 2)

³³ NATO, *AJP-1(D)*, p. 6-3.

Figure 2 Means, targets and effects

D. Targets

Effects, whether physical or non-physical, are addressed at a target, or addressee.³⁴ Activities or operations are conducted against, or in support of, other actor's (fighting) power. Effects are achieved by engaging targets; these targets/addressees are derived from an actors' physical, moral and conceptual component.

In the physical domain objects and persons are 'targetable', constructively or disruptively (see Figure 3). Objects are tangible elements for instance military systems and supplies (see Figure 1). Persons vary from individuals to groups and may be hostile, neutral or supportive.

In the non-physical dimension the psyche of persons is targetable, with the purpose to influence the moral and conceptual component, as well as the cohesion between the components of (fighting) power. Yet again, either constructively or disruptively. By transmitting information an attempt is made to influence morale, mind-set and leadership. Besides that, the cognitive perception of the situation may be altered. Effects against an actor's psyche are primarily non-physical in nature, although they can cause (secondary) effects vis-à-vis persons. (see figure 3).

³⁴ We understand 'target' or 'addressee' in this regard as the entity against which the constructive or disruptive activity is addressed.

Figure 3 Target and effects

We have briefly described doctrinal viewpoints on (military) operations or activities. As mentioned before, new technical developments can result in new possibilities of conducting operations, but these developments may also pose risks. In the following part we will reflect on the influence of the digital domain or cyberspace and cyber operations on doctrinal thought.

3. CYBERSPACE

‘Cyberspace’, often referred to by popular media, is yet poorly understood. The exact meaning of cyberspace, however, is usually ill defined and unclear.³⁵ Before being able to touch upon cyber operations, it is necessary to briefly delve into the meaning of cyberspace. For the purpose of this contribution, the definition offered by Chatham House is used: “the global digital communication and information transfer infrastructure”.³⁶

With conventional domains (air, land, sea and space), cyberspace shares tangible elements,³⁷ but is unique as it entails virtual, more or less ethereal, elements as well. Cyberspace is frequently depicted as a three layer model

³⁵ Illustrative is the document *Securing America's Cyberspace, National Plan for Information Systems Protection: An Invitation to a Dialogue* (Washington, DC: The White House, 2000). The document equips 33 notions with a cyber prefix, there are only two cyber-terms defined.

³⁶ P. Cornish, D. Livingstone, D. Clemente & C. Yorke (2010). *On Cyber Warfare*, London: Chatham House, p. 1.

³⁷ U.S. Army, *TRADOC Pamphlet 525-7-8: Cyberspace Operations Concept Capability Plan 2016 2028* (Fort Eustis: TRADOC, 2010). p. 9.

with five sub-layers.³⁸ For our purpose, and in line with the analysis above, we will scale this down to two dimensions: (1) the physical and (2) the non-physical.

The physical dimension comprises people and objects, i.e. the physical network infrastructure (hubs, routers, cables) and hardware (computers, smartphones servers) etcetera.³⁹

Although based on physical elements, the distinguishing feature of cyberspace is the non-physical dimension. Virtual elements enable the transmission of data between objects (physical network infrastructure) and people.⁴⁰ Two virtual elements, being the ‘virtual reflection’ of tangible objects and people can be recognized: cyber objects and cyber identities.

Cyber objects are the logical elements enabling interoperability and communication between physical objects: protocols, applications, the domain name system,⁴¹ operating systems software,⁴² IP-addresses,⁴³ media access control (MAC) addresses,⁴⁴ encryption and other data.⁴⁵

Cyber identities are the digital/virtual identities of people, individuals, group, and organizations: e-mail account, social-media account, other virtual accounts, like phone numbers.⁴⁶ Cyber identities exist by virtue of the social and professional use of cyberspace.⁴⁷

³⁸ U.S. Army, *TRADOC Pamphlet 525-7-8*. p. 8; consisting of a physical, logical and social layer made up of the following five components: “geographic, physical network, logical network, cyber persona and persona” components.

There are also other approaches to layers of cyberspace. The Open Systems Interconnection (OSI) model describes seven layers, namely: the physical, data link, network, transport, session, presentation and application layer. The Transmission Control Protocol/Internet Protocol (TCP/IP) recognizes four layers, being: the link, Internet, transport and application layer. The United States Army in turn earmarks three layers, namely: the physical, logical and social layer.

³⁹ U.S. Army, *TRADOC Pamphlet 525-7-8*. p. 9.

⁴⁰ U.S. Army, *TRADOC Pamphlet 525-7-8*. p. 9.

⁴¹ DNS system: The system used to resolve IP addresses to comprehensible website names.

⁴² Operating system: The software enabling the functioning of hardware.

⁴³ IP address: The digital postal code of hardware.

⁴⁴ MAC address: The identification number/code of a particular device.

⁴⁵ Often referred to as the logical network layer.

⁴⁶ Often referred to as the cyber persona layer.

⁴⁷ David J. Betz & Tim Stevens (2011) *Cyberspace and the State*, Adelphi Series, 51:424.

The non-physical dimension is the essence of cyberspace's uniqueness. Without the non-physical dimension, cyberspace would not function nor exist. This exceptionality of cyberspace presents both opportunities and risks.

4. FIGHTING POWER IN CYBERSPACE

The question now is, how do these two 'cyber elements' relate to fighting power? This paragraph will therefore elaborate on the components of fighting power in cyberspace by reflecting on the physical, moral and conceptual component in cyberspace.

A. *Physical Component*

The physical dimension of cyberspace incorporates elements from the physical component of fighting power; it similarly envelops tangible objects and persons.

Tangible objects, as mentioned, relate to the network hubs (routers, servers and computers),⁴⁸ physical network infrastructure (such as optic fibre or copper wire)⁴⁹ and objects facilitating non-wired transmission between hubs (e.g. cell sites or mobile phone masts).⁵⁰ The notion of 'persons' relates to operators of objects and users of cyberspace, for example tweeters, followers and software developers and (governmental) 'hackers'.

The physical component also comprises education and training. Their training and education may include (joint and combined) cyber exercises,⁵¹ testing cyber capacities in a digital – preferably isolated – test range and supplementary education.⁵²

⁴⁸ U.S. Army, *TRADOC Pamphlet 525-7-8*, p. 9.

⁴⁹ Ibid. p. 9.

⁵⁰ Jason Andress & Steve Winterfeld, *Cyber Warfare*, 1st ed. (Waltham: Syngress, 2011). p. 120.

⁵¹ Such as the NATO exercises 'Locked Shields' and 'Cooperative Cyber Exercise'.

⁵² For an overview of basic safeguards: Charles Pfleeger & Shari Pfleeger, *Security in Computing*, 4th ed. (Boston: Pearson Education, 2006). p. 442-443.

Figure 4 Fighting power in cyberspace

B. Cyber objects and cyber identities?

Persons and objects in cyberspace communicate by using software, applications, accounts and protocols stemming from the non-physical dimension. These intangible entities differ from physical objects; hence their categorization within the fighting power concept is potentially problematic.

Cyber objects and cyber identities, merely being reflections of objects and persons, are non-physical and intangible though intrinsically linked to their physical counterparts, although not necessarily directly. They enable the working of cyberspace. This is demonstrated in Figure 6.

Figure 5 The physical dimension hosts persons and physical objects, in this case a person and his smartphone. By using his smartphone (step 1), a person can manifest itself on the Internet (step 2). Apart from the smartphone's physical elements facilitating data-exchange (e.g. antenna), there are non-tangible elements representing the smartphone in cyberspace, which we call 'cyber objects', such as the IP and MAC address, IMEI number identifying the smartphone, IMSI number identifying the user, operating systems and other software. By making use of the Internet to create (social-media) accounts (step 3), a person creates his cyber identity.

C. Conceptual and moral component

Cyber and regular operations alike, require doctrinal and operational preparation. The novel challenges and opportunities of cyber operations have to be grasped before being able to effectively employ cyber capacities.

These lessons have to be integrated in (military) training and education. Apart from being well trained and educated, armed forces require motivated

personnel. Most importantly, cyber operators and developers have to possess a 'military mind-set'.⁵³ These elements are incorporated in the conceptual and moral component.

In order to adequately utilize the armed forces, military planners need to understand the inherent cohesion between the components of fighting power. Apart from that, planners have to be able to assess the potential contribution of cyber operations and cyber capacities to instruments of State power, fighting power and (military) operations.

Before being able to so, military planners should have working knowledge of the interrelated dimensions of cyberspace. Such understanding is necessary in order to comprehend the links between social, technical and (military) operational processes. Once proficient, the armed forces can further tread within the non-physical realm through cyber means and methods.

D. Business as usual?

We have introduced distinguishing features of cyberspace, namely, the non-physical dimension, cyber objects and cyber identities. Some would argue that these features are not new; they fit easily within effect-based operations, information operations and they are 'merely' an example of a soft power instrument.

Though cyber operations may conceptually share similarities with these operations, they differ capability and target-wise. As such, cyber operations are truly novel and different from other operations. The very existence of cyber objects and cyber identities results in a vast range of new possibilities, these opportunities have to be grasped, which requires awareness, acceptance and adaptation.

Other striking difference are the concepts of time and space. Cyber operations can be conducted at the speed of light. People (i.e. their physical form) and tangible objects reside within a geographically delimited State. By manifesting themselves through cyber objects and cyber identities, however, their reach extends globally.

⁵³ Andress & Winterfeld, pp. 61-69.

Cyber object and cyber identity can – in principle – be traced back to their physical counterparts, however, defending or striking back with cyber operations may prove to be politically, legally and technically challenging.

E. Cyber fighting power

This paragraph set out to discuss the place of ‘cyber’ within fighting power. The concept of fighting power, as we have interpreted it, can accommodate cyber capabilities. We find cyber in the physical, conceptual and moral component in the form of persons (operators, developers and users), tangible objects (e.g. physical network infrastructure) and psyche (for instance a military mind-set).

Cyber is unique with regard to the non-physical dimension of cyberspace, which includes new elements we have dubbed ‘cyber objects’ and ‘cyber identities’. These elements can be used to utilize cyberspace. We will discuss how to employ these elements in the following paragraph briefly.

5. CYBER OPERATIONS

We understand cyber operations to be “the employment of cyber capabilities with the prime purpose of achieving [military] objectives in or by the use of cyberspace”.⁵⁴ Similar to conventional operations, the goal of cyber operations is to achieve an effect, namely: influencing actors in or through cyberspace.

As suggested in the definition, actors can be influenced *in* or *through* cyberspace. Effects can be achieved *in* cyberspace by creating constructive or disruptive effects vis-à-vis the physical or non-physical dimension of cyberspace with using both kinetic and non-kinetic means. Conversely, constructive and disruptive effects can also be attained *through* cyberspace by, for instance, employing social-media applications to influence persons or by employing malware against aerial-defence systems. Cyber operations can achieve these effects stand-alone or parallel to other operations.⁵⁵

⁵⁴ Schmitt, *Tallinn Manual*, p. 258

⁵⁵ Terry D. Gill & Paul A. L. Ducheine, ‘Anticipatory Self-Defense in the Cyber Context’, 89 *US NWC International Law Studies* (2013), pp. 438-471.

A. *Phasing & Purposes*

Figure 6 Phases in cyber operations

Cyber operations have different phases; each having a different purpose. Although there are different approaches towards naming phases and sub-phases,⁵⁶ the general tenure is illustrated in figure 6. Cyber operations do not necessarily undergo each and every phase; it differs per operation. If the goal is to gather information regarding vulnerabilities by scanning a system or network,⁵⁷ it will stop at the reconnaissance phase (figure 7 operation A). Whereas an operation aimed at penetrating and creating a foothold in the system might undergo phases one up until five (figure 7 operation B). A fully-fledged cyber operation intended to implant, retrieve or steal a particular piece of information from a network might go through all six phases (figure 7 operation C).

⁵⁶ Andress & Winterfeld, p. 171: Recon, scan, access, escalate, exfiltrate, assault, sustain; Lech J. Janczewski & Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism* (Hershey: Information Science Reference, 2008). p. xv: Reconnaissance, penetration, identifying and expanding internal capabilities, damage system or confiscate data, remove evidence.

⁵⁷ For instance by using Nmap (Network Mapper), which enables users discover vulnerabilities within networks.

Figure 7 Cyber operations and effects

B. *Target/ addressee and effects*

Similar to regular operations, cyber operations are addressed at a target in order to attain a designated effect. New possibilities arise since there are new elements that can be targeted, i.e. cyber identities and cyber objects. The overall goal, however, remains influencing supportive, neutral and opposing actors.

Cyber operations are conducted against cyber identities and cyber objects, resulting into a predefined effect vis-à-vis an actor. If successful, they result into a direct effect against these two cyber elements. But, through targeting cyber objects and cyber identities, secondary effects are generated against (or in support of) persons, objects and psyche (see figure 8).

For instance, by addressing a Twitter account of a commander (cyber identity) the direct effect is a change within the cyber identity. The secondary effect, an alteration of his state of mind, is achieved when the commander consumes the particular piece of information on his Twitter feed, which may (or may not) result in a psychological effect (psyche). Another example is targeting the control system (cyber object) of an industrial machine, initially the control system software is altered, but it secondarily results in a physical effect, for instance operating failure.

The effects achievable through cyber operations are diverse; constructive and disruptive. However, even without conducting constructive or disruptive cyber operations, the mere availability of unprecedented quantities of

information in cyberspace reinforces the intelligence position of every actor. We will briefly discuss how cyber identities and cyber objects can be utilized to generate such effects.

C. Constructive effects

Constructive effects can be achieved through by utilizing cyber identities and cyber objects.

1) Cyber identities

By utilizing cyber identities actors can be influenced. Constructive effects can consist of attempts to induce alignment-shift within neutral actors (both individuals and groups) or reinforce the position of supporters. In order to do so, armed forces can use own social-media accounts to broadcast general information or interact with the accounts of neutral and supportive actors. Through these channels, armed forces can explain the ratio behind military operations, counter false information (i.a. lawfare), provide practical information regarding (military) operations, or generate support (see figure 9). The purpose of these activities is keeping neutral actors neutral at the least and (further) increase support for a mission.

The infographic is divided into two main columns. The left column, titled 'What has the IDF done to minimize harm to civilians in Gaza?', lists five actions with checkmarks: Phone Calls, Leaflets, Aborting Airstrikes, Roof Knocking, and Pinpoint Strikes. Each action is followed by a brief description of the measure. The right column, titled 'What has Hamas done to minimize harm to civilians in Israel?', contains a single entry with a checkmark: 'Nothing.' At the bottom, a red banner states 'Hamas' goal is to kill Israeli civilians.' Below this, a black banner features the Israel Defense Forces logo and name.

What has the IDF done to minimize harm to civilians in Gaza?	What has Hamas done to minimize harm to civilians in Israel?
☒ Phone Calls Thousands of phone calls and text messages were sent to Gaza, warning them of IDF strikes in the area.	
☒ Leaflets Thousands of leaflets dropped over Gaza warned civilians to "avoid being present in the vicinity of Hamas operatives."	
☒ Aborting Airstrikes The IDF has called off airstrikes when pilots spotted civilians — even when missiles were speeding toward their target.	☒ Nothing.
☒ Roof Knocking These loud but non-lethal bombs warn civilians that they are near a target, giving them time to leave the site.	
☒ Pinpoint Strikes The IDF has targeted terrorists with pinpoint strikes, minimizing harm to bystanders as much as possible.	

Hamas' goal is to kill Israeli civilians.

ISRAEL DEFENSE FORCES

Figure 8 Utilizing cyber identities: IDF⁵⁸

2) *Cyber objects*

Cyber objects can be constructively used to influence neutral actors and supporters. Such effects can be generated through providing neutral and supportive actors the tools needed to protect networks (e.g. antivirus software, virus definitions/signatures and known exploits); tools to better utilize cyberspace (e.g. data mining software, social media management software and tools for intelligence purposes); and tools needed to exploit adversary vulnerabilities (e.g. malware, root kits and botnets).

D. *Disruptive effects*

Whereas constructive effects are generated to influence and support friendly actors, armed forces attempt to generate disruptive effects against an adversary (armed forces, groups or individuals).

1) *Cyber identities*

Adversary cyber identities – such as spokespersons, commanders and their (most influential) supporters – can be targeted. One of the means is decreasing their credibility, for instance by countering the validity of what they publish, highlighting false facts or claims and generally question their legitimacy. In order to do so, own cyber identities can be used to engage and interact with adversary cyber identities with the purpose of nullifying their influence.

Apart from decreasing credibility, friendly cyber identities can be used to psychologically influence adversary cyber identities. Through publishing information regarding upcoming military operations, which may or may not be true, a psychological effect may be generated (see figure 10).⁵⁹

⁵⁸ Tweet @IDFSpokesman (and IDFBlog.com) during Second Gaza War (Operation *Pillars of Defence*), via: <idfblog.com/wp-content/uploads/2012/11/checklistinfographic.jpg>, accessed 26 Feb 2013.

⁵⁹ Tweet @IDFSpokesperson, via <twitter.com/IDFSpokesperson/status/268780918209118208>, accessed 12 January 2014.

Figure 10 IDF notifying Hamas operators of impeding action

Adversary cyber identities can also be personally addressed, a message tailored to the specific strengths and weaknesses of a target will undoubtedly affect the psyche of the person 'behind' a cyber identity (such as a threat as illustrated in figure 11).⁶⁰

Figure 9 Kenyan police threatening terrorists during the Westgate shopping mall siege in Nairobi after terrorists claimed to still occupy the mall via Twitter

Adversary cyber identities can also be blocked or hijacked. The easiest way of blocking a cyber identity is requesting the (social-) media company to do so,⁶¹ but there are other means that supersede the companies' authority.⁶² Adversary cyber identities can also be hijacked, for instance through (automatically) 'guessing' credentials⁶³ or employing social engineering techniques (e.g. phishing and pharming).⁶⁴ Once hijacked, the adversaries' identity can be used at the discretion of a (military) commander. He could use it in order to deceive adversaries, publish (false) information to the benefit of

⁶⁰ Tweet @PoliceKE, via: <twitter.com/PoliceKE/status/382161864106737664>, accessed 12 January 2014.

⁶¹ See for instance: Bill Gertz, "User Suspended: Twitter Blocks Multiple Accounts of Somali Al-Qaeda Group during Kenya Attack," freebeacon.com/user-suspended/ (accessed January 8, 2014).

⁶² For instance reporting a user 'en masse' will result in account suspension.

⁶³ For example by making use of 'brute force' attacks employing tools such as THC Hydra ('Hydra') and John the Ripper ('John') to automatically guess credentials.

⁶⁴ Andress & Winterfeld, p. 141.

own goals,⁶⁵ or he could 'just' deactivate and thereby nullify the influence of the account.

2) *Cyber objects*

Cyber objects belonging to an adversary – for instance operating systems, malware and other software or data – can be utilized and exploited. Cyber objects can be externally denied to an adversary by employing (distributed) denial of service attacks, known as (D)DOS. When successful, these types of attacks render a cyber object inoperable and inaccessible,⁶⁶ consequently resulting in decreased operability of the connected physical object.⁶⁷ Yet again, it is paramount to comprehend the potential effects of a DOS attack in advance, otherwise such a cyber operation may cause unintended side effects of regional, national or international nature.

Apart from denying access externally, adversary cyber objects can be hijacked by employing certain attack techniques and tools.⁶⁸ Once an attacker has access to a cyber object, the attacker can gather information inside the system and utilize this information in order to gain control over the cyber object. If the attacker successfully takes control over a cyber object, for instance a control system of an air defence turret (object), he can manipulate the control system (cyber object) and consequently operate the object at his commanders' bidding. Through gaining control over cyber objects a commander can generate a variety of effects in an area. The cyber objects could be used for future (cyber) operations (e.g. in the form of botnets), used to control physical objects (e.g. operating systems of military platforms) or create other physical effects (e.g. denying an area by opening a floodgate).

⁶⁵ Cnaan Liphshiz, "Israeli Vice Prime Minister's Facebook, Twitter Accounts Hacked," jta.org/2012/11/21/news-opinion/israel-middle-east/israeli-vice-prime-ministers-facebook-twitter-accounts-hacked (accessed January 8, 2014); Grace Wyler, "AP Twitter Hacked, Claims Barack Obama Injured in White House Explosions" businessinsider.com/ap-hacked-obama-injured-white-house-explosions-2013-4 (accessed January 8, 2014).

⁶⁶ Pfleeger & Pfleeger, *Security in Computing*. pp. 427-433; See e.g.: Eduard Kovacs, "DDOS Attack on DigiD Impacts 10 Million Dutch Users," news.softpedia.com/news/DDOS-Attack-on-DigiD-Impacts-10-Million-Dutch-Users-348791.shtml (accessed October 30, 2013).

⁶⁷ Such as financial traffic services and online payment services, see also: Don Eijndhoven, "On Dutch Banking Woes and DDoS Attacks," argentconsulting.nl/2013/04/on-dutch-banking-woes-and-ddos-attacks/ (accessed January 8, 2014).

⁶⁸ Andress & Winterfeld, pp. 100-106.

E. So?

In sum, (military) goals can be achieved by using cyber identities and cyber objects vis-à-vis other actors' cyber objects and identities. There are many other modes of utilizing these unique features of cyberspace; we have merely scratched the surface of possible uses of cyber identities and objects. The wide range of possibilities and opportunities opens up cyberspace as operating (or "warfighting")⁶⁹ domain for armed forces, States, (belligerent) groups, individuals and other actors.

'Regular' targeting procedures have crystalized over the years and are firmly rooted in most modern armed forces. New means and methods – such as cyber means and methods – pose challenges to the targeting procedures armed forces employ. In the next paragraph we will discuss ramifications on contemporary targeting procedures as a result of the emergence of cyber operations.

6. TARGETING

A. Targeting in general

As stated, military operations are executed in order to affect other actors with a view to higher strategic objectives. Actors can be influenced by applying fighting power (and other instruments) vis-à-vis an addressee or a target during operations, in short: through 'targeting'. Targeting is "the process of selecting and prioritizing targets and matching the appropriate response to them"⁷⁰ with the purpose of determining "effects necessary to accomplish operational objectives; [selecting] targets that achieve those effects; and [selecting] or [tasking] the means, lethal or non-lethal, with which to take action upon those targets".⁷¹ A target can be "an area, structure, object, person, organization, mindset, thought process, attitude or behavioural pattern".⁷²

⁶⁹ The Joint Chiefs of Staff [JCS], *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* p. 18; The Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* p. 3.

⁷⁰ British Army, *ADP: Operations*. p. 5-13; JCS, *Joint Publication 3-60: Joint Targeting* (Washington, DC: JCS, 2007). p. viii.

⁷¹ Giulio Di Marzio, "The Targeting Process: This Unknown Process (Part 1)," *NATO Rapid Deployable Corps Italy Magazine*, no. 13 (2009), 11-13. p. 13.

⁷² British Army, *ADP: Operations*. p. 5-13.; JCS, *JP3-60*. p. viii.

Before touching upon the ramifications of cyber operations on the targeting process, it is necessary to briefly describe the targeting processes. The

targeting process is a cyclic process and consists of distinct phases (Figure 11).⁷³

Desired end-state and objectives provide initial input. Together with guidelines issued (i.a. ROE) they comprise the *first phase* of the process that is initiated in order to achieve an effect leading to the (partial) achievement of an object or

Figure 11 Targeting cycle

end-state.

In the *second phase* targets are selected, developed and prioritized by systematically examining potential targets,⁷⁴ resulting in a target list with various potential targets that may contribute to achieving an end-state or objective.

The *third phase* entails evaluating available capabilities in order to determine available options,⁷⁵ and matching the potential target nominations from phase two “with [available] weapons or other capabilities to create the desired effects on the target(s)”.⁷⁶ Critically important throughout the whole targeting process, primarily in this phase, is the collateral damage estimate and assessment.⁷⁷ Weapons or capabilities may not cause collateral damage disproportional to the military advantage gained.

After phase one till three, the appropriate commander may decide on executing an operation against a target, and tasking orders can be “prepared

⁷³ Most often, six phases are recognized; See also: USAF, "Air Force Pamphlet 14-210" fas.org/irp/doddir/usaf/afpam14-210/part01.htm (accessed January 8, 2014). Section 1.5.1.

⁷⁴ JCS, *JP3-60*, p. II-4.

⁷⁵ JCS, *JP3-60*, p. II-10.

⁷⁶ Ibid. p. II-11.

⁷⁷ See Art. 52(2) AP I.

and released to the executing components and forces”,⁷⁸ weapons/capabilities can be allocated and forces be assigned to the operation in *phase four*.

Phase five, execution, follows after further mission planning and taking precautionary measures to i.a. verify information, minimize collateral damage, and issues warning (when appropriate and feasible). Phase five results in the actual operation against the target.⁷⁹

Phase six is aimed at collecting information “about the results of the engagement [in order] to determine whether the desired effects have been created”.⁸⁰ The output from phase six can serve as input for phase one, since after assessing effects it might prove necessary to readjust guidelines or conduct a follow-up action against the target.

The targeting process, being an operations instrument, is complemented with a legal considerations derived from the law of armed conflict (LOAC) obligations. Without going into details, the questions and issues involved are: is the target a military objective, is collateral damage expected, is the collateral damage assessed to be excessive to the military advantage anticipated, is mitigation of collateral damage by ‘tweaking’ means and methods possible, are precautionary measures feasible.

B. Targeting (in) cyberspace

Faced with unique cyber elements (cyber identities and objects) in the virtual or non-physical domain, the ramifications of targeting in or through cyberspace will now be addressed. Since targeting of the physical dimensions of cyberspace (people and objects) is well known and covered by the process just presented, we will focus on discussing targeting cyber identities and objects during cyber operations.

1) Phase one: Effects and guidelines

Phase one of targeting cyber elements does not differ from ‘regular’ targeting; cyber operations are extra means to an effect, just like other (military) operations and activities. Cyber operations are ‘merely’ an addition to the

⁷⁸ Ibid.

⁷⁹ Ibid.

⁸⁰ Ibid. p. II-18.

commander's arsenal for generating effects, although it is evident that proper concepts, personnel, equipment, mindset and training e.a. are required.

2) *Phase two: Target development*

As demonstrated, new non-physical elements are available as capabilities as well as targets or addressees: cyber objects and cyber identities. As the targeting process is designed for both lethal and non-lethal targeting, and recognizes the application of 'soft power' against the psyche of actors, the process can – in principle – incorporate both physical and non-physical targets.

Questions may – and do – arise however regarding the feasibility of targeting cyber identities and cyber objects in operations and the ratio for doing so. For instance, it is fairly obvious that adversary cyber objects and cyber identities may be targeted (in accordance with LOAC and ROE),⁸¹ but can we similarly target cyber objects and cyber identities of supportive or neutral groups and individuals?

Parallels can be drawn from contemporary conflict; operations not only address adversaries, but a wide range of other actors as well (see § **Error! Reference source not found.**). Apart from combatting opponents through force, operations are aimed at diminishing support for adversaries by 'targeting' (or addressing) the hearts and minds of the local population.⁸² Through supporting local population via humanitarian help (e.g. water, food, medical care), security (e.g. training local police, patrolling the area, combatting lawlessness) and economical help (e.g. microcredits) an attempt is made to influence them to the benefit of the deployed force. Nowadays, the local population is increasingly online and thus would pose a logical 'target/addressee' for constructive cyber operations, as are adversaries for disruptive cyber operations.

3) *Phase three: Capabilities Analysis*

⁸¹ E.g. Noam Lubell, 'Lawful Targets in Cyber Operations - Does the Principle of Distinction Apply?', in: 89 *US Naval War College International g (USNWC ILS)* (2013), pp. 252 ff.

⁸² U.S. Army and U.S. Marine Corps, *Army Field Manual 3-24/ Marine Corps Warfighting Publication 3-33.5: Counterinsurgency* (Washington, DC: United States Army, 2006). p. A-5; British Army, *ADP: Operations*. p. 5-2; Netherlands MoD, *NDD*. p. 68.

Phase three basically aims at finding the right ‘tools for the job’. Since cyber identities and cyber objects are connected to the physical dimension (people and objects) direct and secondary effects are achievable. Direct effects, either constructive or disruptive, are feasible through cyber operations against cyber objects and cyber identities, potentially followed by secondary effects against people and physical objects. This differs from the kinetic targeting, where lethal force may destroy people or objects as the direct physical effect, and a secondary non-physical effect may occur (see § 5. B)

The collateral damage estimate and assessment is crucial in targeting decisions. Apart from LOAC obligations, collateral damage (or “unintended effects”)⁸³ is crucial with an eye to strategic objectives and long term effects, for instance the perceived legitimacy of, and popular support for, operations and the military. Due to the globalized character of (social-) media, increasing possibilities for ‘citizen journalism’,⁸⁴ and ‘lawfare’ used to discredit operations and reputation,⁸⁵ planners seek to (a) effectively assign capabilities to targets, whilst (b) minimizing collateral damage.⁸⁶

Thus, the collateral damage assessment of direct non-physical and secondary physical effects when targeting cyber identities and cyber objects will become increasingly important.⁸⁷ First of all, the anticipated military advantage should be assessed, and secondly, the collateral damage expected should be qualified and quantified. Finally these two should be ‘weighed’, and the collateral damage may not be ‘excessive’. This three tiered collateral damage assessment, complicated as it is in kinetic operations, will require research and training in cyberspace before it is usable at all.

4) *Phases four-six*

⁸³ JCS, *JP3-60*. p. I-11.

⁸⁴ Stuart Allen & Einar Thorsen, *Citizen Journalism: Global Perspectives* (New York: Peter Lang Publishing, 2009). p. ix-xi; See e.g. the compromise of ‘Operation Neptune Spear’ (or the raid on Bin Laden) on Twitter: Melissa Bell, “Sohaib Athar’s Tweets from the Attack on Osama Bin Laden,” <washingtonpost.com/blogs/blogpost/post/sohaib-athar-tweeted-the-attack-on-osama-bin-laden--without-knowing-it/2011/05/02/AF4c9xXF_blog.html> (accessed January 9, 2014).

⁸⁵ E.g. John F. Murphy, ‘Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?’, in: 89 *USNWC ILS* (2013), pp. 309ff.

⁸⁶ Netherlands MoD, *NDD*. p. 99; NATO, *AJP-1(D)*. p. 2-10. Section 221; British Army, *ADP: Operations*. p. 3-7.

⁸⁷ Schmitt, Michael N., *The Law of Cyber Warfare: Quo Vadis?* (September 4, 2013). 25 *Stanford Law & Policy Review*, (2014- Forthcoming), at SSRN: <<http://ssrn.com/abstract=2320755>>, p. 22.

Of special interest during cyber operations is the issue of precautionary measures:⁸⁸ *inter alia*, due care has to be issued to avoid non-intended effects throughout the operation. Afterwards the effects can be assessed, contrary to 'regular' operations, effects of some cyber operations may be easier to quantify through (other) cyber operations. For example, effects of conducting a constructive cyber operation (e.g. influencing the perception of the local population) can be assessed through monitoring the increase of positive sentiment on social-media.⁸⁹

7. CONCLUSION

We set out to operationalise military cyber operations, conceptualize their contribution and discuss the ramifications on the targeting cycle. Having discussed the instruments of state power, the military instrument itself, fighting power, is composed of various activities both military and non-military, forceful and non-forceful, and kinetic and non-kinetic. Cyber operations fit within today's concepts of fighting power, including the manoeuvrist and comprehensive approaches; they are an addition to contemporary instruments.

Operationalisation of cyber means and methods however, still requires considerable effort. Whilst fighting power in cyberspace requires 'ordinary' elements like manpower, materiel, motivation, training, concepts and doctrine, the unique characteristics of cyberspace may still pose challenges, as unique non-physical elements, cyber objects and cyber identities, are present. These virtual elements not only offer new means and methods of (constructively or disruptively) influencing supportive, neutral and adversary actors, but require research and conceptualisation as well.

⁸⁸ Schmitt, *Tallinn manual*, p. 159ff; Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack', in: 89 *USNWC ILS* (2013), pp. 198 ff; Paul Walker, 'Organizing for Cyberspace Operations: Selected Issues', in: 89 *USNWC ILS* (2013), pp. 341 ff.

⁸⁹ In order to do so data mining tools can be employed to collect, curate, cluster and display the sentiment within a specific population.

Figure 12 Fighting power and cyber operations

Targeting procedures can incorporate new ways of influencing actors, since it recognizes kinetic and non-kinetic targeting, through physical and non-physical means, resulting in physical and non-physical effects. Assessing distinctiveness, effects/effectiveness (primary and follow-on effects), and collateral damage however, may still prove to be difficult. This will require proper research, tooling and training. We conclude with an overview of the position of cyber operations amongst 'regular' operations (see figure 13).

V5: 6513 –904 biblio= 5609 words + 1371 notes = 6980 words.

BIBLIOGRAPHY

- Allen, Stuart and Einar Thorsen. *Citizen Journalism: Global Perspectives*. New York: Peter Lang Publishing, 2009.
- Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques and Tools for Security Practitioners*. 1st ed. Waltham: Syngress, 2011.
- Antoci, Angelo, Fabio Sabatini, and Mauro Sodini. "See You on Facebook: The Effect of Social Networking on Human Interaction." *European Research Institute on Cooperative and Social Enterprises* (2010).
- Bell, Melissa. "Sohaib Athar's Tweets from the Attack on Osama Bin Laden." , accessed January 9, 2014, washingtonpost.com/blogs/blogpost/post/sohaib-athar-tweeted-the-attack-on-osama-bin-laden--without-knowing-it/2011/05/02/AF4c9xXF_blog.html.
- David J. Betz & Tim Stevens (2011) *Cyberspace and the State*, Adelphi Series, 51:424.
- British Army. *Army Doctrine Publication: Operations*. Shrivenham: Development, Concepts and Doctrine Centre, 2010.
- Clausewitz, Carl von. *On War, Translated and Edited by Michael Howard and Peter Paret*. Princeton: Princeton University Press, 1976.
- P. Cornish, D. Livingstone, D. Clemente & C. Yorke (2010). *On Cyber Warfare*, London: Chatham House.
- Corrin, Amber. "The Other Syria Debate: Cyber Weapons." , accessed 30 October, 2013, fcw.com/articles/2013/09/04/cyber-weapons-syria.aspx.
- Coyle, Cheryl L. and Heather Vaughn. "Social Networking: Communication Revolution Or Evolution?" *Bell Labs Technical Journal* 13, no. 2 (2008): 13-17.
- Di Marzio, Giulio. "The Targeting Process: This Unknown Process (Part 1)." *NATO Rapid Deployable Corps Italy Magazine* no. 13 (2009): 11-13.

Echevarria II, Antulio J. *Clausewitz and Contemporary War*. Oxford: Oxford University Press, 2007.

Eijndhoven, Don. "On Dutch Banking Woes and DDoS Attacks." , accessed January 8, 2014, argentconsulting.nl/2013/04/on-dutch-banking-woes-and-ddos-attacks/.

Gertz, Bill. "User Suspended: Twitter Blocks Multiple Accounts of Somali Al-Qaeda Group during Kenya Attack." , accessed January 8, 2014, freebeacon.com/user-suspended/.

Gibson, William. "Burning Chrome." *Omni* (July, 1982): 72-107.

Gibson, William. *Neuromancer*. New York: Berkley Publishing Group, 1984.

Gill, Terry D. and Paul A. L. Ducheine. "Anticipatory Self-Defense in the Cyber Context." *United States Naval War College International Law Studies* 89, (2013): 438-471.

Jachtenfuchs, Markus. "The Monopoly of Legitimate Force: Denationalization, Or Business as Usual?" *European Review* 13, no. 1 (2005): 37-52.

Janczewski, Lech J. and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Hershey: Information Science Reference, 2008.

Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack', in: 89 *United States Naval War College International Law Studies* (2013), p. 198.

Kovacs, Eduard. "DDOS Attack on DigiD Impacts 10 Million Dutch Users." , accessed October 30, 2013, news.softpedia.com/news/DDOS-Attack-on-DigiD-Impacts-10-Million-Dutch-Users-348791.shtml.

Liphshiz, Cnaan. "Israeli Vice Prime Minister's Facebook, Twitter Accounts Hacked." , accessed January 8, 2014, jta.org/2012/11/21/news-opinion/israel-middle-east/israeli-vice-prime-ministers-facebook-twitter-accounts-hacked.

Noam Lubell, 'Lawful Targets in Cyber Operations - Does the Principle of Distinction Apply?', in: 89 *United States Naval War College International Law Studies* (2013), p. 252.

Miller, Daniel and Don Slater. *The Internet: An Ethnographic Approach*. Oxford: Berg, 2000.

Ministry of Defence of the Russian Federation. *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space* [концептуальные взгляды на деятельность вооруженных сил российской федерации
в информационном пространстве]. Translated by NATO Cooperative Cyber Defence Centre of Excellence 2011.

John F. Murphy, 'Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?', in: 89 *United States Naval War College International Law Studies* (2013), p. 309.

William Gibson: No Maps for these Territories. Directed by Neale, Mark. New York: Docurama Films, 2000.

Netherlands Ministry of Defence. *The Defence Cyber Strategy*. The Hague: Netherlands Ministry of Defence, 2012.

Netherlands Ministry of Defence. *Netherlands Defence Doctrine*. Den Haag: Ministerie van Defensie, 2013.

North Atlantic Treaty Organization. *Allied Joint Publication 1(D): Allied Joint Doctrine*. Brussels: Nato Standardization Agency, 2010.

Pfleeger, Charles and Shari Pfleeger. *Security in Computing*. 4th ed. Boston: Pearson Education, 2006.

Plato. "□λαιβιάδης." In *Plato with an English Translation VII*, edited by Lamb, W. London: William Heinemann Ltd., 390-342 B.C.

Rheingold, Howard. *The Virtual Community: Homesteading on the Electronic Frontier*. Reading: Addison-Wesley Publishing Company, 1993.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

- Schmitt, Michael N. "The Law of Cyber Warfare: Quo Vadis?" (September 4, 2013). *Stanford Law & Policy Review*, Vol. 25, 2014, Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2320755>, p. 22.
- The Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*. Washington, DC: Office of the Chairman, 2006.
- The Joint Chiefs of Staff. *Joint Publication 3-60: Joint Targeting*. Washington, DC: The Joint Chiefs of Staff, 2007.
- The Joint Chiefs of Staff. *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*. Washington, DC: Office of the Chairman, 2004.
- The White House. *Securing America's Cyberspace, National Plan for Information Systems Protection: An Invitation to a Dialogue*. Washington, DC: The White House, 2000.
- United States Air Force. "Air Force Pamphlet 14-210: Intelligence Targeting Guide." , accessed January 8, 2014, fas.org/irp/doddir/usaf/afpam14-210/part01.htm.
- United States Army. *Cyberspace Operations Concept Capability Plan 2016 2028*. Fort Eustis: The United States Training and Doctrine Command, 2010.
- United States Army and United States Marine Corps. *Army Field Manual 3-24/ Marine Corps Warfighting Publication 3-33.5: Counterinsurgency*. Washington, DC: United States Army, 2006.
- United States Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC: United States Department of Defense, 2011.
- Paul Walker, 'Organizing for Cyberspace Operations: Selected Issues', in: 89 *United States Naval War College International Law Studies* (2013), p. 341.
- Weber, Max. "Politics as a Vocation." Chap. Hans H. C. Wright Mills, In *From Max Weber: Essays in Sociology*, edited by Gerth, Hans H. and Charles Wright Mills. London: Routledge, 1918.

Wyler, Grace. "AP Twitter Hacked, Claims Barack Obama Injured in White House Explosions

". , accessed January 8, 2014, businessinsider.com/ap-hacked-obama-injured-white-house-explosions-2013-4.