2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

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 contributes to the operationalisation of military cyber operations in general, and for targeting purposes, either in defence or offence, in particular. The role of cyber operations in military doctrine will be clarified, its 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 used for targeting inter alia for active defence purposes, 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 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) the 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*

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 potential of 'cyber' is uncontested, there remain questions surrounding operationalising cyber means and methods. Since some of these questions remain

[*] 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 Board of Editors of the *Militaire Spectator*, for their kind permission to use portions of their article ęCyber-operaties en militair vermogenę (org. Dutch), in: 182 *Militaire Spectator* (2013) 9, pp. 369-387.

[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], available at ccdcoe.org/328 html.

unanswered, the use of cyber in military operations is frequently overlooked.[2] One of the issues leading to dismissal of ‘the cyber option’ is the limited understanding of the effects and implications of the use of cyber weapons in doctrinal thought and operational processes such as targeting. Understanding new means and methods is vital to adequate appreciation of, and operationalising their potential in offensive, defensive and stability operations.

Active cyber defence is generally conceived as ‘entailing proactive measures that are launched to defend against malicious cyber activities or cyber attacks’.[3] States tend to entrust their armed forces with a prominent role in securing cyberspace, and hence armed forces will prove crucial in taking proactive measures both domestically and internationally. Before being able to actually conduct cyber operations within the context of active cyber defence, the armed forces have to effectively incorporate cyber capacities within their organisations. Only then can these new capabilities be used effectively for the purposes stated, including active defence, offence and supportive roles.

This article will clarify the role of cyber operations in military doctrine, conceptualise its contribution to fighting power, and discuss potential ramifications on the targeting cycle. By doing so it will contribute to the debate regarding the operationalisation of military cyber means and methods.

Contemporary military operations are not conducted stand-alone; they are a means to an end and are conducted in parallel with other (non-) military activities.[4] In order to place the military instrument in its proper context, we will first briefly expand on instruments of State power and focus on the conceptualisation of fighting power and conventional military operations (§2). Before expanding on cyber operations, it is necessary to define the unique characteristics of cyberspace (§3), and once cyberspace’s landscape has been 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 for conventional targeting procedures (§6).

When describing and conceptualising the role of cyber operations, Allied doctrine will be used, primarily focusing on that published by the North-Atlantic Treaty Organisation (NATO), but supplemented with the doctrine publications of other 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.’[5] We will discuss the subtleties and implications of this definition in this contribution.

2. THE MILITARY INSTRUMENT

In order to provide security, and for the protection of vital strategic interests, States may rely on their instruments of power: integrated or joint military power on land, sea, and in the air, as well

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

[3] CCDCOE, ‘Latest News’, ccdcoe.org/cycon/home.html (accessed 14 March, 2014).

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

[5] Michael N. Schmitt (gen. ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press, 2013). p. 258.

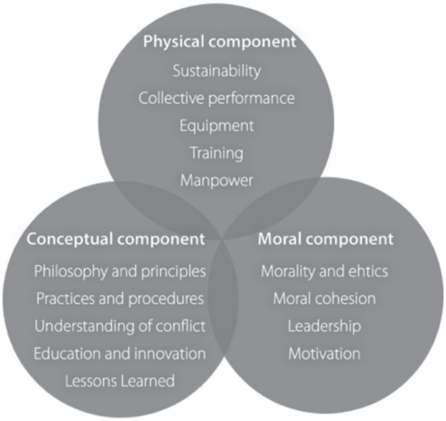
as diplomatic, economic, and informational means.[6] Apart from the diplomatic, informational, military, and economic instruments, the so-called DIME-instruments,[7] NATO recognises the 'wide utility [of] civil capabilities' in contemporary operations.[8] Thus, States nowadays have various instruments 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 from the other instruments.[9]

Fighting Power

Armed forces apply fighting power[10] consisting of three elements: the physical, moral, and conceptual components (see Figure 1).[11] The physical component comprises first and foremost the manpower and equipment that provide the 'means to fight'.[12] Equipment consists of military platforms, systems, weapons and supplies of 'operational or non-operational and deployable or non-deployable' nature.[13] Apart from material elements, the physical component also entails sustainability and (operational) readiness.[14]

The moral component[15] involves 'the least predictable aspect of conflict', namely 'the human element'.[16] It entails 'good morale and the conviction that the mission's purpose is morally and ethically sound'.[17] The moral component is rooted in three 'priceless commodities: ethical foundations, moral cohesion and motivation'.[18] In addition, effective leadership is vital.[19]

FIGURE 1. FIGHTING POWER



[6] Antulio J. Echevarria II, *Clausewitz and Contemporary War* (Oxford: Oxford University Press, 2007). p. 144.
[7] NATO, *AJP-1(D)*. Sections 107-110.
[8] Ibid. p. 1-3. Section 111.
[9] Jachtenfuchs, *The Monopoly of Legitimate Force: Denationalization, Or Business as Usual?* p. 38.
[10] British Army, *ADP: Operations* (Shrivenham: Development, Concepts and Doctrine Centre, 2010). p. 2-2.
[11] NATO, *AJP-1(D)*. Sections 120-123.
[12] British Army, *ADP: Operations*. p. 2-31.
[13] *Ibid*. p. 2-32.
[14] Netherlands MoD, *Netherlands Defence Doctrine* (NDD) (2013). p. 69.
[15] The Netherlands Defence Doctrine (NDD) refers to a 'mental component', contrary to the NATO and British 'moral component'.
[16] British Army, *ADP: Operations*. p. 2-10.
[17] NATO, *AJP-1(D)*. Section 121.
[18] British Army, *ADP: Operations*. p. 2-11.
[19] Netherlands MoD, *NDD*. p. 67.

The conceptual component 'provides the coherent, intellectual basis and theoretical foundation for the deployment of military units and troops'.[20] The higher levels of doctrine, the strategic and the operational, 'establish the philosophy and principles underpinning the approach to conflict and military activity'.[21] Apart from guidance, 'the conceptual component also plays a significant role in the preservation and development of the institutional memory and experience'[22] through education, innovation and lessons identified.[23]

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)'.[24] When properly developed, 'capacities are elevated to capabilities' and they become fighting power.[25] Fighting power will then be employed effectively to achieve strategic goals, whether alone or in unison with other strategic instruments; this is the 'comprehensive approach'.[26]

Operation, the Manoeuvrist Approach and Comprehensiveness

Armed forces project fighting power through military operations. Operations vary in form, purpose, size, duration, and vector: land, sea, air, space, and cyberspace. This section will focus on the conceptualisation of administering fighting power through military operations. The Manoeuvrist Approach is vital to understanding the rationale for 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'.[27] The emphasis is on the adversary's moral and conceptual component rather than on the physical; the purpose is to degrade cohesion in components of an adversary's fighting power.[28] The integration of various components – the Comprehensive Approach – is used not only at the strategic level, but also in actual operations at lower levels.

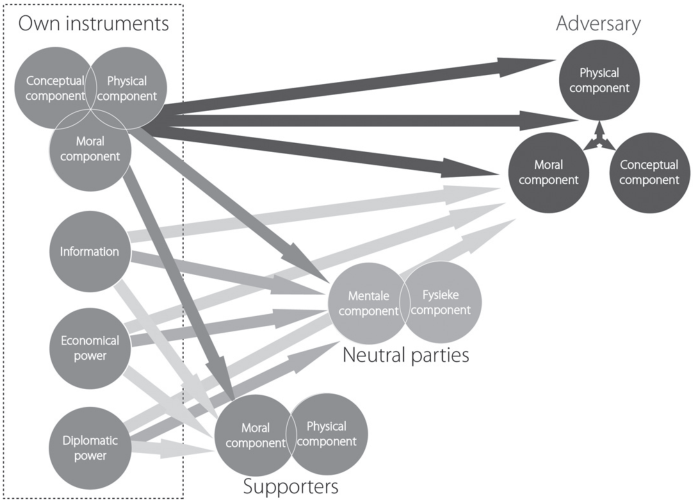
Interpreted in a broader and more modern sense, operations entail influencing actors, as opposed to the adversary, by employing different instruments in addition to the military instrument.[29] Contemporary conflict is characterised by a '[large] number of actors […] intensified by our "open" world, in which everyone can keep abreast of each military operation'.[30] Thus, operations are no longer primarily aimed at opponents, but at a wide range of actors including 'population groups, parties, countries and organisations with which there is no physical interaction'.[31]

Consequently, the military instrument is no longer the only or prime instrument in an area of operations. Activities should be tailored to increase and maintain support for operations by

[20] Netherlands MoD, *NDD*. p. 71.
[21] British Army, *ADP: Operations*. p. 2-5.
[22] Netherlands MoD, *NDD*. pp. 70-71.
[23] British Army, *ADP: Operations*. pp. 2-9, 2-10.
[24] Netherlands MoD, *NDD*. p. 66.
[25] Netherlands MoD, *NDD*. p. 66.
[26] NATO, AJP-1(D). Sections 226-232.
[27] *Ibid*. Section 611.
[28] British Army, *ADP: Operations*. p. 2-6.
[29] Netherlands MoD, *NDD*. p. 108.
[30] Netherlands MoD, *NDD*. p. 108.
[31] *Ibid*. p. 108.

employing various DIME instruments.[32] Operations aim to decrease support to adversaries, and generate support from others.[33] Figure 2 illustrates this conceptualisation of influencing adversaries, neutral parties, and supporters.

FIGURE 2. EMPLOYING INSTRUMENTS OF STATE POWER



Activities or 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 in terms of information or leadership or through attacking or addressing the moral and conceptual component. Without cohesion, morale, and effective leadership, opposing forces can more easily be defeated, destroyed, or outmanoeuvred.

Operations addressing neutrals and supporters are constructive in nature. Their aim is to increase support for one's own operations. By influencing neutral actors, an attempt is made to convince them to join or support the own cause (Figure 2, blue and grey arrows). The goal is to keep them neutral, but preferably to make them supportive. By reinforcing the power of supporters physically by, for example, materiel and training, the foothold within supportive groups can be increased either morally or economically (Figure 2, blue and grey arrows).

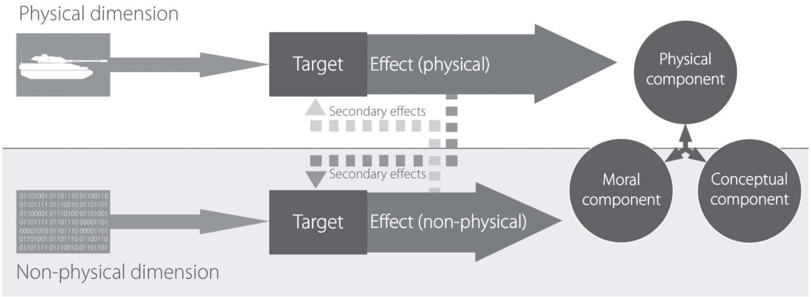
Means to an effect

Activities conducted by armed forces are a means to an end. They are intended to achieve a predefined kinetic or non-kinetic effect to the detriment or support of an actor. To that end, both lethal and non-lethal, physical and non-physical means can be applied.[34]

Lethal and non-lethal or physical and non-physical effects are complementary and intertwined. Destroying enemy materiel and personnel, part of the physical component, will primarily cause physical effects, but will also affect enemy morale, part of the moral component (see Figure 3).

[32] *Ibid*.
[33] *Ibid*.
[34] NATO, *AJP-1(D)*. p. 6-3.

FIGURE 3. MEANS, TARGETS AND EFFECTS



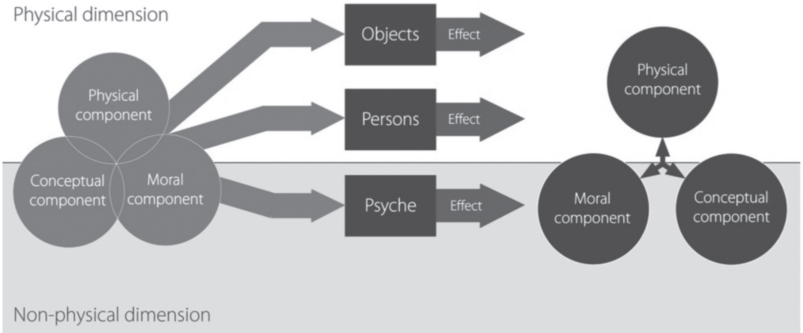
Targets

Effects, whether physical or non-physical, are addressed at a target, or addressee, the entity against which the constructive or disruptive activity is addressed. Activities or operations are conducted against, or in support of, other actors' power, including fighting power. Effects are achieved by engaging targets; these targets and addressees are selected from an actor's physical, moral, and conceptual component.

In the physical dimension objects and persons are targetable, constructively or disruptively (see Figure 4). Objects are tangible elements, for instance military systems and supplies. People vary from individuals to groups and may be hostile, neutral, or supportive.

In the non-physical dimension, the psyche of people is targetable, with the purpose of influencing the moral and conceptual components, as well as the cohesion between the components of fighting power, either constructively or disruptively. By transmitting information, an attempt is made to influence morale, mind-set, and leadership. Besides this, 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 (see Figure 3).

FIGURE 4. TARGET AND EFFECTS



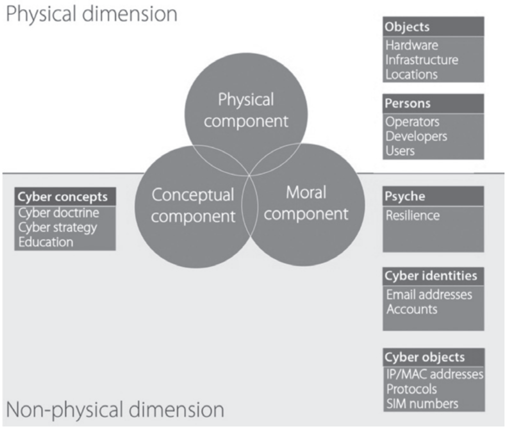
We have briefly described doctrinal viewpoints on military operations or activities. New technical developments can result in new possibilities for conducting operations, but these developments may also pose risks. In the next part we will reflect on the influence of the digital domain, or cyberspace, and cyber operations on doctrinal thinking.

3. CYBERSPACE

Cyberspace, often referred to by the popular media, is as yet poorly understood. The exact meaning of cyberspace is usually ill defined and unclear.[35] Before being able to touch on 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]

Cyberspace shares tangible elements with conventional domains of air, land, sea, and space,[37] but is unique as it also contains virtual, more or less ethereal, elements. Cyberspace is frequently depicted as a three layer model with five sub-layers.[38] For our purposes, and in line with the analysis above, we will scale this down to two dimensions: the physical and the non-physical. The physical dimension comprises people and objects, the physical network infrastructure such as hubs, routers, and cables, and the hardware such as computers, smartphones, and servers.[39]

FIGURE 5. FIGHTING POWER IN CYBERSPACE



[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.

[38] U.S. Army, *TRADOC Pamphlet 525-7-8*. p. 8, consisting of a physical, logical, and social layer comprising of the following five components: 'geographic, physical network, logical network, cyber persona and persona'. There are also other approaches to layers of cyberspace. The Open Systems Interconnection (OSI) model describes seven layers: the physical, data link, network, transport, session, presentation, and application layers. The Transmission Control Protocol/Internet Protocol (TCP/IP) recognises four layers: the link, internet, transport, and application layers. The United States Army in turn recognises three: the physical, logical, and social layers.

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

Although based on physical elements, the distinguishing feature of cyberspace is the non-physical dimension. Virtual elements enable the transmission of data between objects in the physical network infrastructure and people.[40] Two virtual elements, the 'virtual reflection' of tangible objects and people, can be recognised: 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 and virtual identities of people, individuals, groups, and organisations: e-mail accounts, social-media accounts, and other virtual accounts such as phone numbers.[46] Cyber identities exist by virtue of the social and professional use of cyberspace.[47]

The non-physical dimension is the essence of cyberspace's uniqueness. Without the non-physical dimension, cyberspace would not 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 section will therefore elaborate on the components of fighting power in cyberspace by reflecting on the physical, moral, and conceptual components in cyberspace.

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 relate to the network hubs, the routers, servers, and computers;[48] the physical network infrastructure, such as optic fibre or copper wire;[49] and objects facilitating non-wired transmission between hubs, such as cell sites or mobile phone masts.[50] The notion of 'persons' relates to operators of objects and users of cyberspace; for example tweeters, followers, software developers, and 'hackers'. The physical component also comprises education and training. Training and education may include conducting cyber exercises,[51] testing cyber capacities in a digital and preferably isolated test range, and supplementary education.

Cyber objects and cyber identities?

Persons and objects in cyberspace communicate using software, applications, accounts, and

[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.

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

[49] *Ibid*. p. 9.

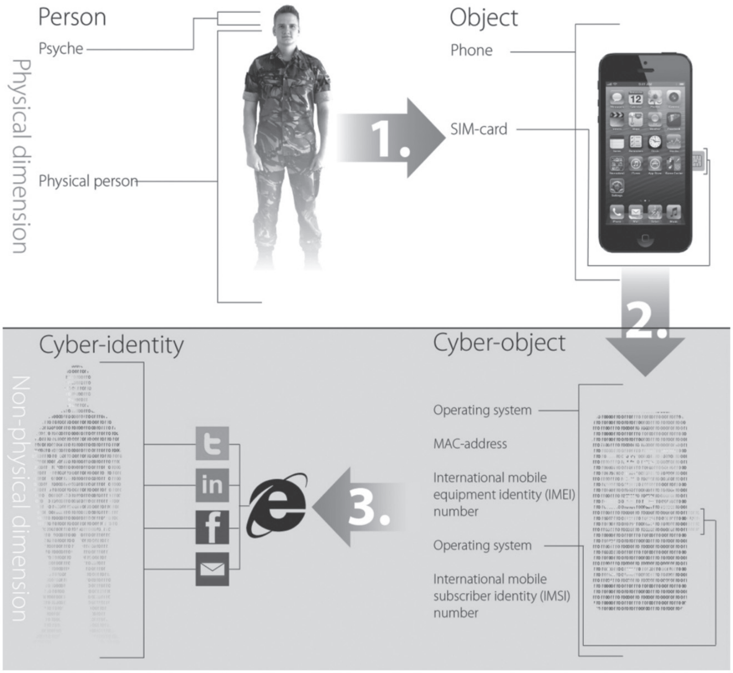
[50] Jason Andress & Steve Winterfeld, *Cyber Warfare*, 1st ed. (Waltham: Syngress, 2011). p. 120.

[51] Such as NATO CCDCOE's exercise 'Locked Shields' and NATO's Cyber Exercise 'Cyber Coalition'.

protocols stemming from the non-physical dimension. These intangible entities differ from physical objects; hence their categorisation within the fighting power concept is potentially problematic.

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

FIGURE 6. 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 HIMSELF 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, FOR EXAMPLE, SOCIAL-MEDIA ACCOUNTS (STEP 3), A PERSON CREATES HIS CYBER IDENTITY.



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 cyber capacities can be effectively employed. 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 need to have a military mind-set, which includes for example basic knowledge of 'strategy and tactics'.[52] These elements are incorporated in the conceptual and moral component.

In order to adequately use the armed forces, military planners need to understand the inherent cohesion between the components of fighting power and be able to assess the potential contribution of cyber operations and cyber capacities to instruments of State power, fighting power and operations. To be able to do so, military planners should have sufficient knowledge of the interrelated dimensions of cyberspace. Such understanding is necessary in order to comprehend the links between social, technical, and operational processes. Once proficient, the armed forces can further tread within the non-physical realm through cyber means and methods.

Business as usual?

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

Although cyber operations may conceptually share similarities with these operations, they differ in capability and targeting and 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, acceptation, and adaptation.

Another striking difference is in the concepts of time and space. Cyber operations can be conducted at the speed of light. People and tangible objects reside within a geographically delineated State. By manifesting themselves through cyber objects and cyber identities, their reach extends globally.

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

Cyber fighting power

This section discusses 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 components in the form of persons, be they operators, developers, or users; tangible objects such as the physical network infrastructure; and the psyche; for example, the 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 access cyberspace. We will briefly discuss how to employ these elements in the following paragraph.

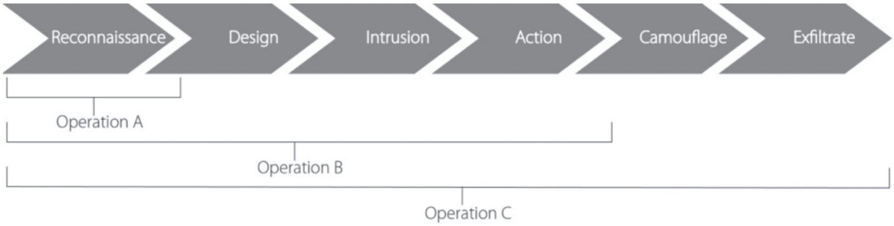
[52] Andress & Winterfeld, p. 63.

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'.[53] Similar to conventional operations, the goal of cyber operations is to achieve an effect, to influence actors in or through cyberspace.

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, 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 people or employing malware against aerial-defence systems. Cyber operations can achieve these effects stand-alone or in parallel with other operations.[54]

FIGURE 7. PHASES IN CYBER OPERATIONS



Phasing and Purposes

Cyber operations, like all military operations, have different phases, each having a different purpose. Although there are different approaches towards naming phases and sub-phases,[55] the general consensus is illustrated in Figure 7. Cyber operations do not necessarily undergo each and every phase; it varies between operations. If the goal is to gather information regarding vulnerabilities by scanning a system or network,[56] the cyber operation 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 phase one through to phase 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).

Target/addressee and effects

As with regular operations, cyber operations are addressed at a target in order to attain a desired effect. New possibilities arise since there are new elements that can be targeted: cyber identities and cyber objects. The overall goal, however, remains to influence supportive, neutral, and opposing actors.

[53] Schmitt (gen. ed.), *Tallinn Manual*, p. 258.

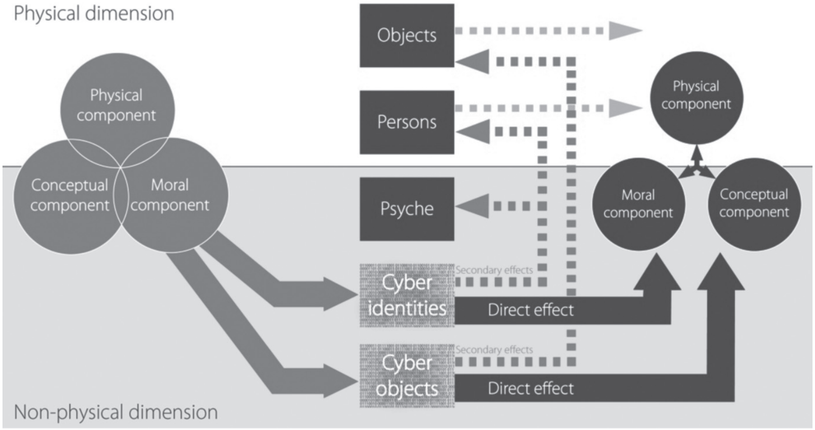
[54] Terry D. Gill & Paul A. L. Ducheine, 'Anticipatory Self-Defense in the Cyber Context', 89 *US NWC International Law Studies* (2013), pp. 438-471.

[55] 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.

[56] For instance by using Nmap (Network Mapper), which enables users to discover vulnerabilities within networks.

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

FIGURE 8. CYBER OPERATIONS AND EFFECTS



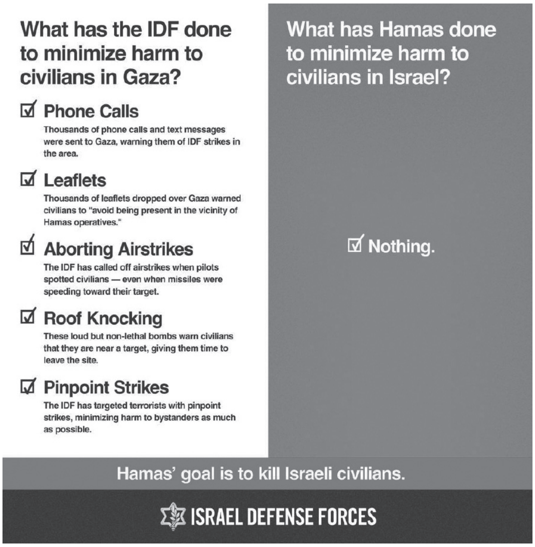
For instance, by addressing the Twitter account of a commander which forms part of his cyber identity, the direct effect is a change in that cyber identity. The secondary effect, an alteration of his state of mind, is achieved when the commander consumes the particular piece of information on his Twitter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

The effects achievable through cyber operations are diverse, both the constructive and the 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 used to generate such effects.

Constructive effects

Constructive effects can be achieved by using cyber identities and cyber objects.

FIGURE 9. USING CYBER IDENTITIES: IDF



What has the IDF done to minimize harm to civilians in Gaza?

☑ **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.

☑ **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.

What has Hamas done to minimize harm to civilians in Israel?

☑ Nothing.

Hamas' goal is to kill Israeli civilians.

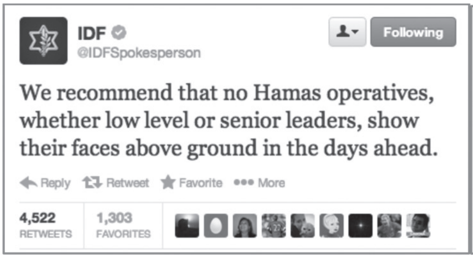
ISRAEL DEFENSE FORCES

1) Physical support

By physically supporting neutral and supportive actors, their capacity to act in cyberspace can be reinforced. Cyber capacity depends strongly on the qualitative state of networks and underlying infrastructure. By providing infrastructure, for instance computers, mobile phone masts, routers, and servers, the position of other actors in cyberspace can be reinforced and their perception or situational awareness influenced to the benefit of the sponsor. Similarly, deploying a Computer Emergency Response Team (CERT) to assist actors in securing theirs networks reinforces the position of those actors and alters their perception and situational awareness. Physical support, or the prospect thereof, could result in an increased foothold within supportive actors or an alignment shift by neutral entities.

FIGURE 10. IDF NOTIFYING HAMAS OPERATORS OF IMPEDING ACTION

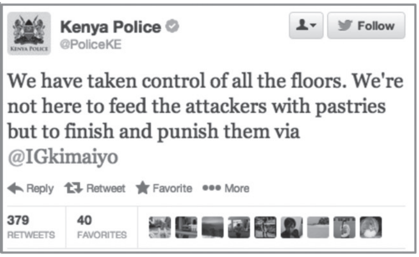
FIGURE 11. KENYAN POLICE THREATENING TERRORISTS DURING THE WESTGATE SHOPPING MALL SIEGE IN NAIROBI AFTER TERRORISTS CLAIMED TO STILL OCCUPY THE MALL VIA TWITTER



IDF
@IDFSpokesperson

We recommend that no Hamas operatives, whether low level or senior leaders, show their faces above ground in the days ahead.

4,522 RETWEETS 1,303 FAVORITES



Kenya Police
@PoliceKE

We have taken control of all the floors. We're not here to feed the attackers with pastries but to finish and punish them via @IGkimaiyo

379 RETWEETS 40 FAVORITES

2) Cyber identities

By using cyber identities, actors can be influenced. Constructive effects can consist of attempts to induce alignment-shift within neutral actors, both individuals and groups, or to reinforce the positions of supporters. In order to do so, armed forces can use social-media accounts to broadcast general information or interact with the accounts of neutral and supportive actors. Through these channels they can explain the rationale behind military operations, counter false information,[57] provide practical information regarding operations, or generate support (see Figure 9). The purpose of these activities is keeping neutral actors neutral at the least and increasing support for a mission.

3) 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 such as antivirus software, virus definitions, and signatures and known exploits; tools to better use cyberspace such as data mining software, social media management software, and tools for intelligence purposes; and tools needed to exploit adversary vulnerabilities such as malware, root kits, and botnets.

Disruptive effects

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

1) Physical disruption

By physically disrupting cyber capacities belonging to neutral and supportive actors, their capability to act in cyberspace is reduced. Cyber capacity and capability strongly depend on the quality of networks and infrastructure. A network can most easily be disrupted when armed forces have access to the physical network infrastructure.[58] Actors that are able to gain access to or target network infrastructure are capable of disrupting network traffic by methods 'that predate the internet by decades', namely '[c]utting the […] lines'.[59] However, there are other benefits when operators have physical access to network infrastructure: there are no firewalls to be circumvented and they can install, uninstall, and reverse-engineer hardware and software.

2) 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 questioning their legitimacy. In order to do so, cyber identities can be used to engage and interact with the adversaries' cyber identities for the purpose of nullifying their influence.

Apart from decreasing credibility, friendly cyber identities can be used to psychologically

[57] See for instance: J. Voetelink, 'Lawfare,' *Militair Rechtelijk Tijdschrift* 106, no. 3 (2013), 69-79.; Charles J. Dunlap Jr, 'Lawfare Today: A Perspective,' *Yale Journal of International Affairs* 3 (2008), 146.

[58] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. (New York: Syngress, 2014). p. 137.

[59] Carol Matlack, 'Cyberwar in Ukraine Falls Far Short of Russia's Full Powers,' Bloomberg Business Week, businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers (accessed March 11, 2014).; See also: Reuters, 'Ukrainian Authorities Suffer New Cyber Attacks,' Reuters, reuters.com/article/2014/03/08/us-ukraine-cricis-cyberattack-idUSBREA270FU20140308 (accessed March 11, 2014).; Andress and Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. p. 139.

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).[60]

Adversaries' cyber identities can also be personally addressed, and a message tailored to the specific strengths and weaknesses of a target will undoubtedly affect the psyche of the person 'behind' a cyber identity (see Figure 11).[61]

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,[62] but there are other means that supersede the companies' authority.[63] Adversary cyber identities can also be hijacked, for instance through 'guessing' credentials[64] or employing social engineering techniques such as phishing and pharming.[65] Once hijacked, the adversary's identity can be used at the discretion of a commander. He could use it in order to deceive adversaries, publish false information to the benefit of own goals,[66] or he could just deactivate and thereby nullify the influence of the account.

3) Cyber objects

Cyber objects belonging to adversaries such as operating systems, malware and other software or data can be used and exploited.

a) Monitoring

Armed forces can gather information about an adversary's cyber objects by collecting information about their networks. Before being able to do so, the mission's cyberspace landscape has to be mapped. This 'map' would include the types of machines used, software versions, port configurations, active or live machines, interdependencies, and the general network environment. By employing software such as Nmap, such information can be gathered.[67] When armed forces have mapped the network environment in an area of operations, this information can be used to increase situational awareness of cyber activities and to earmark weak spots.

b) External manipulation

Should operational circumstances require cyber objects to be denied, denial of service attacks (DOS) can be employed. In order to be able to conduct an effective DOS attack, armed forces should possess a so-called 'botnet', which is a network of computers capable of spawning

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

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

[62] 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).

[63] For instance reporting a user '*en masse*' will result in account suspension.

[64] 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.

[65] Andress & Winterfeld, p. 141.

[66] 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).

[67] Nmap (Network Mapper) enables users to scan networks to collect information regarding port configuration, vulnerabilities, operating systems and active machines. Source: Nmap, 'About,' nmap.org (accessed March 11, 2014).

large amounts of data on command.[68] Creating a botnet would require some preparation, since malware has to be written or bought, distributed, and executed.[69] Alternatively, a botnet can also be taken over,[70] leased or bought from a botnet owner.[71] Besides that, armed forces can persuade supporters to partake in a Distributed DOS (DDOS) attack against an adversary by providing the tools, for instance software called Low- or High-Orbit Ion Cannon,[72] and the target's IP-addresses.[73] No matter the method, when successful these attacks render a cyber object inoperable and inaccessible.[74] That may consequently result in decreased operability of the connected physical object.[75] Effects are achieved by targeting adversary cyber objects with a DOS attack. Targets could include official websites, command and control systems, logistical support systems, third-party suppliers' systems, financial services for military personnel, and connected tactical operating systems. It is important to comprehend the potential effects of a DOS attack in advance, otherwise these cyber operations may have unintended side effects of a regional, national, or international nature.

c) Intrusion and internal manipulation

Apart from denying access to cyber objects externally, a wider range of actions can be conducted from the inside. Internal manipulation requires access to a cyber object's 'back-end', hence an operator has to force entry. In order to do so, an operator can crack easy passwords using brute force techniques.[76] If unsuccessful he can also resort to social engineering techniques such as phishing.[77]

Apart from these methods, access can be forced by exploiting software vulnerabilities if an exploit is available for a specific vulnerability.[78] Well-known exploitable vulnerabilities, or

[68] Andress and Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. pp. 216-217.

[69] Ramneek Puri, 'Bots & Botnet: An Overview,' *SANS Institute 2003* (2003). pp. 1-2.; Nicholas Ianelli and Aaron Hackworth, 'Botnets as a Vehicle for Online Crime,' *CERT Coordination Center* 1 (2005), 15-31. pp. 16-17.

[70] Ryan Vogt, John Aycock and Michael J. Jacobson Jr, 'Army of Botnets,' *Network and Distributed System Security Symposium*, no. February (2007). p. 2.

[71] See for instance: Yuri Namestnikov, 'The Economics of Botnets,' *Kapersky Lab* (2009).

[72] 'The original LOIC Tool was built by Praetox Technologies as a stress testing application. The tool performs a simple DoS attack, by sending a sequence of TCP (Transmission Control Protocol), UDP (User Datagram Protocol) or HTTP (Hyper-Text Transfer Protocol) requests to a target host.' Source: Aiko Pras et al., *Technical Report 10.41: Attacks by 'Anonymous' WikiLeaks Proponents Not Anonymous* (Enschede: University of Twente, Centre for Telematics and Information Technology, [2010]).

[73] Steve Mansfield-Devine, 'Anonymous: Serious Threat Or Mere Annoyance?' *Network Security January* (2011), 4-10. p. 7.

[74] 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).

[75] 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).

[76] Such as (THC-)Hydra and John (the Ripper). 'Hydra' and 'John' are tools enabling an attacker or pentester to automatically and systematically guess passwords (brute force) and automatically try a list of potential credentials (dictionary attack).

[77] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques and Tools for Security Practitioners*, 1st ed. (Waltham: Syngress, 2011). pp. 103-105.

[78] Matthijs R. Koot, Personal communication entailing comments on Dutch Article 'Militair Vermogen en Cyberoperaties' (Fighting Power and Cyber Operations), November, 2013.

‘exploits’, are available online either in databases[79] or enclosed in specific software.[80] Apart from applications and databases, specialised companies sell less- or unknown exploits to the highest bidder.[81] By employing brute-forcing tools, social engineering techniques, and exploits an operator can gain access to an adversary’s cyber object.

Once an attacker has access to a cyber object, he can gather information inside the system and use this information to gain control over the cyber object. If the attacker successfully takes control over the cyber object, for instance a control system of an air defence turret, he can manipulate the object and subsequently operate it at his commander’s bidding. Through gaining control over cyber objects, commanders can generate a variety of effects. The cyber objects could be used for future operations in the form of botnets, or used to control physical objects such as the operating systems of military platforms, or create other physical effects such as denying an area by opening a floodgate.

d) Destruction

Manipulation of cyber objects affects functions and functionality. Destroying a cyber object would result in function failure. Yet, destruction in the physical domain seems easier than in the non-physical domain. Would it, for instance, be possible to destroy or erase cyber objects? Often there are back-ups and redundant applications; erasure of cyber objects would only be complete once they are entirely removed. In most cases, it would be hard to completely erase applications and thus it would only lead to temporary failure, i.e. until back-ups are used to restore the system.

e) Human manipulation

As made clear in recent publications, content can also be used to manipulate and deceive, or in a more accepted terminology, to influence people.[82] As Greenwald demonstrates, information, true or false, may be provided as content on social media, blogs, and websites, all of which are cyber objects. Not only human perception and situational awareness may thus be affected, in addition their reputation could be challenged and, ultimately, destroyed.[83]

So?

Military and other goals can be achieved by using cyber identities and cyber objects to exert effect on other actors’ cyber objects and identities. There are many other ways of using these unique features of cyberspace; we have merely scratched the surface of possible uses of cyber

[79] See for example: Exploit Database, ‘Windows Exploits,’ exploit-db.com/platform/?p=windows (accessed March 14, 2014).; Shodan Exploits, ‘Windows XP Exploits,’ Shodan HQ, exploits.shodan.io/?q=windows+xp (accessed March 14, 2014).

[80] See for example Metasploit, an application used for scanning, selecting exploits for the scanned system, equipping an exploit with a payload and executing it on a target system. Source: Rapid 7, ‘The Attacker’s Playbook: Test Your Network to Uncover Exploitable Security Gaps with Metasploit.’ rapid7.com/products/metasploit/ (accessed March 14, 2014).

[81] Mathew J. Schwartz, ‘Blackhole Botnet Creator Buys Up Zero Day Exploits,’ Information Week, informationweek.com/security/vulnerabilities-and-threats/blackhole-botnet-creator-buys-up-zero-day-exploits/d/d-id/1108075? (accessed March 14, 2014).; Andy Greenberg, ‘Shopping for Zero-Days: A Price List for Hackers’ Secret Software Exploits,’ Forbes, forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ (accessed March 14, 2014).

[82] Glenn Greenwald, ‘How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations’, The Intercept (24 February 2014), https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/ (accessed 15 March 2014).

[83] Although described in the context of disruptive effects, this method is also available for constructive purposes.

identities and objects. The wide range of possibilities and opportunities opens up cyberspace as an operating or 'warfighting'[84] domain for armed forces, States, belligerent groups, individuals, and other actors.

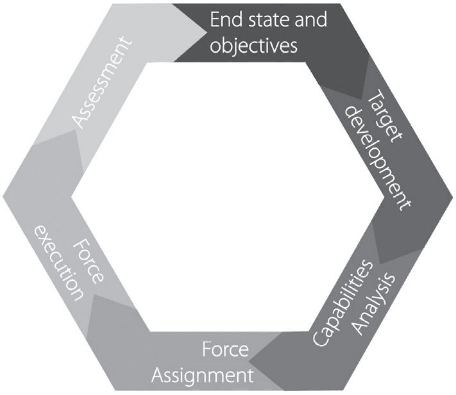
Targeting procedures have crystallised over the years and are firmly rooted in most modern armed forces. New means and methods, such as those involving cyber, pose challenges to the targeting procedures armed forces employ. In the next section we will discuss ramifications for contemporary targeting procedures as a result of the emergence of cyber operations.

6. TARGETING

Targeting in general

Military operations are executed in order to produce an effect on other actors with a view to higher strategic objectives. Actors can be influenced by applying fighting power and other instruments against an addressee or target during operations – in short, through targeting. Targeting is 'the process of selecting and prioritizing targets and matching the appropriate response to them'[85] with the purpose of determining the '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'.[86] A target can be 'an area, structure, object, person, organisation, mind-set, thought process, attitude or behavioural pattern'.[87] Before touching on the ramifications of cyber operations for targeting, it is necessary to briefly describe the targeting process. The targeting process is a cyclic process and consists of distinct phases (See Figure 12).[88]

FIGURE 12. TARGETING CYCLE



[84] 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.

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

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

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

[88] Most often, six phases are recognised; 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.

Desired end-states and objectives provide initial input. Together with guidelines issued such as Rules of Engagement, they comprise the *first phase* of the process that is initiated in order to achieve an effect leading to the achievement of an object or end-state.

In the *second phase* targets are selected, developed and prioritised by systematically examining potential targets,[89] 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 options,[90] and matching the potential targets from phase two 'with [available] weapons or other capabilities to create the desired effects on the target(s)'.[91] Critically important throughout the whole targeting process, primarily in this phase, is the collateral damage estimate and assessment.[92] Weapons or capabilities may not cause collateral damage disproportionate to the military advantage anticipated.

From phase one to three, the commander may decide to execute an operation against a target, and tasking orders can be 'prepared and released to the executing components and forces',[93] weapons or capabilities can be allocated, and forces assigned to the operation in *phase four*.

Phase five, execution, follows after further mission planning and taking precautionary measures to verify information, minimise collateral damage, and issue warnings when appropriate and feasible. Phase five results in the actual operation against the target.[94]

Phase six is aimed at collecting information 'about the results of the engagement [in order] to determine whether the desired effects have been created'.[95] The output from phase six can serve as input for phase one, since after assessing effects it might prove necessary to adjust guidelines or conduct a follow-up action against the target.

The targeting process, being an operations instrument, is complemented by legal considerations derived from the law of armed conflict (LOAC). 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, and are precautionary measures feasible.

Targeting in cyberspace

Faced with unique cyber identities and cyber 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 is well known and covered by the process just presented, we will focus on discussing targeting cyber identities and objects during cyber operations.

[89] JCS, *JP3-60*. p. II-4.
[90] JCS, *JP3-60*. p. II-10.
[91] *Ibid*. p. II-11.
[92] See Art. 52(2) AP I.
[93] JCS, *JP3-60*. p. II-11.
[94] *Ibid*.
[95] *Ibid*. p. II-18.

1) Phase one: Effects and guidelines

Phase one of targeting cyber elements does not differ from regular targeting; cyber operations are a means to an end, just like other military operations and activities. Cyber operations are merely an addition to the commander's arsenal for generating effects, although it is evident that proper concepts, personnel, equipment, mind-set, and training are required.

Guidelines relevant to the context and conduct of cyber operations will accompany stated purposes. With an eye to the legitimacy of cyber operations they will, like other operations, be restricted for operational, political and legal reasons. It is to be expected that States, unilaterally or in coalition, will somehow express their position on the applicability and application of LOAC and human rights law to these operations. Whether or not using manuals as a point of departure, before employing cyber capabilities States will issue guidance to their troops. In addition to LOAC interpretations and positions, as in conventional operations it is commonplace to issue ROE relevant to these weapons and operations. For instance, by the use of a 'weapon release matrix' for cyber capacities, by restricting the use of cyber operations to designated digital domains or networks, or by authorising specific cyber weapons.

2) Phase two: Target development

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

Questions arise regarding the feasibility of targeting cyber identities and cyber objects in operations and the rationale for so doing. For instance, it is fairly obvious that an adversary's cyber objects and cyber identities may be targeted subject to LOAC and ROE,[96] 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. Apart from combating opponents through force, operations are aimed at diminishing support for adversaries by targeting the hearts and minds of the local population.[97] By supporting the local population through humanitarian aid (e.g. water, food, medical care), security (e.g. training local police, patrolling the area, combatting lawlessness) and economic aid (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 present a logical target for constructive cyber operations, as adversaries do for disruptive cyber operations.

3) Phase three: Capabilities Analysis

Phase three aims to find 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

[96] 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.

[97] 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.

operations against cyber objects and cyber identities, potentially followed by secondary effects against people and physical objects. This differs from kinetic targeting, where lethal force may destroy people or objects as the direct physical effect, and a secondary non-physical effect may occur.

Collateral damage estimation and assessment is crucial in targeting decisions. Apart from LOAC obligations, collateral damage or 'unintended effects'[98] 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 globalised character of (social) media and increasing possibilities for 'citizen journalism',[99] and 'lawfare' to be used to discredit operations and reputation,[100] planners seek to effectively assign capabilities to targets, whilst minimising collateral damage.[101]

Thus, the collateral damage assessment of direct non-physical and secondary physical effects when targeting cyber identities and cyber objects will become increasingly important.[102] 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 must 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

Of special interest during cyber operations is the issue of precautionary measures.[103] Care has to be taken to avoid unintended effects throughout the operation. Afterwards the effects can be assessed, and unlike regular operations, the effects of some cyber operations may be easier to quantify through other cyber operations. For example, the effects of conducting a constructive cyber operation such as influencing the perception of the local population can be assessed through monitoring the increase in positive sentiment on social media.[104]

7. CONCLUSION

We set out to operationalise military cyber operations, conceptualise their contribution, and discuss their ramifications for the targeting cycle. Having discussed the instruments of State

[98] JCS, *JP3-60*. p. I-11.

[99] Stuart Allen & Einar Thorsen, *Citizen Journalism: Global Perspectives* (New York: Peter Lang Publishing, 2009). p. ix-xi; See e.g. compromising '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).

[100] 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.

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

[102] 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.

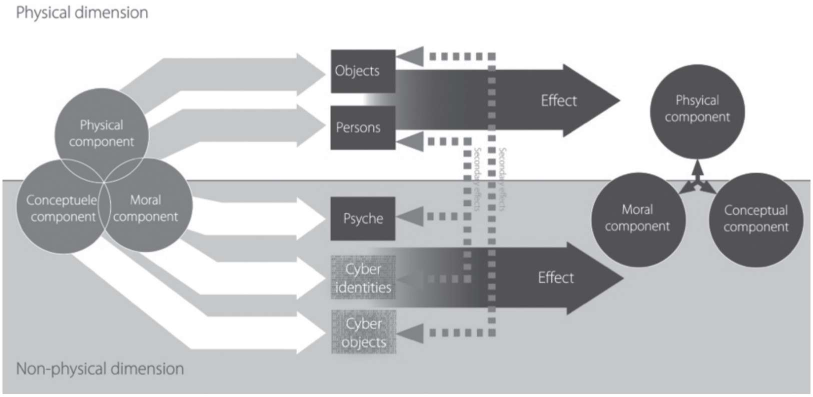
[103] Schmitt, *Tallinn Manual*, p. 159ff; Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack', in: 89 *USNWC ILS* (2013), pp. 198 ff; Paul Walker, 'Organizing for Cyberspace Operations: Selected Issues', in: 89 *USNWC ILS* (2013), pp. 341 ff.

[104] In order to do so data mining tools can be employed to collect, verify, cluster, and display the sentiment within a specific population.

power, the military instrument of 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. As such, cyber operations enhance capabilities for offensive and defensive purposes, including so called active defence.

Operationalisation of cyber means and methods 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 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.

FIGURE 13. FIGHTING POWER AND CYBER OPERATIONS



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

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.

Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd ed. New York: Syngress, 2014.

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.

Betz, David J. and 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.

Cornish, P., D. Livingstone, D. Clemente and 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.

Dunlap Jr, Charles J. 'Lawfare Today: A Perspective,' *Yale Journal of International Affairs* 3 (2008), 146.

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/.

Exploit Database. 'Windows Exploits', accessed March 14, 2014, exploit-db.com/platform/?p=windows.

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.

Greenberg, Andy. 'Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits.' Forbes, accessed March 14, 2014, forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Ianelli, Nicholas and Aaron Hackworth. 'Botnets as a Vehicle for Online Crime.' *CERT Coordination Center* 1, (2005): 15-31.

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.

Jensen, Eric Talbot. '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.

Namestnikov, Yuri. 'The Economics of Botnets.' *Kapersky Lab* (2009).

Nmap. 'About.', accessed March 11, 2014, nmap.org.

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.

Mansfield-Devine, Steve. 'Anonymous: Serious Threat Or Mere Annoyance?' *Network Security* January, (2011): 4-10.

Matlack, Carol. 'Cyberwar in Ukraine Falls Far Short of Russia's Full Powers.' Bloomberg Business Week, accessed March 11, 2014, businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers.

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,' accessed March 20, 2014, ccdcoe.org/328.html.

Murphy, John F., '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 Organisation. *Allied Joint Publication 1(D): Allied Joint Doctrine.* Brussels: Nato Standardization Agency, 2010.

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

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

Pras, Aiko, Anna Sperotto, Giovane Moura, Idilio Drago, Rafael Barbosa, Ramin Sadre, Ricardo Schmidt, and Rick Hofstede. *Technical Report* 10.41: *Attacks by 'Anonymous' WikiLeaks Proponents Not Anonymous*. Enschede: University of Twente, Centre for Telematics and Information Technology, 2010.

Puri, Ramneek. 'Bots & Botnet: An Overview.' *SANS Institute 2003* (2003).

Rapid 7. 'The Attacker's Playbook: Test Your Network to Uncover Exploitable Security Gaps with Metasploit.', accessed March 14, 2014, rapid7.com/products/metasploit/.

Reuters. 'Ukrainian Authorities Suffer New Cyber Attacks.' Reuters, accessed March 11, 2014, reuters.com/article/2014/03/08/us-ukraine-cricis-cyberattack-idUSBREA270FU20140308.

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

Schmitt, Michael N. (gen. ed.) *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.

Schwartz, Mathew J. 'Blackhole Botnet Creator Buys Up Zero Day Exploits.' Information Week, accessed March 14, 2014, informationweek.com/security/vulnerabilities-and-threats/blackhole-botnet-creator-buys-up-zero-day-exploits/d/d-id/1108075?.

Shodan Exploits. 'Windows XP Exploits.' Shodan HQ, accessed March 14, 2014, exploits.shodan.io/?q=windows+xp.

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.

Voetelink, J. 'Lawfare,' *Militair Rechtelijk Tijdschrift* 106, no. 3 (2013), 69-79.

Vogt, Ryan, John Aycock, and Michael J. Jacobson Jr. 'Army of Botnets.' *Network and Distributed System Security Symposium* no. February (2007).

Walker, Paul. '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.