UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Manoeuvring and Generating Effects in the Information Environment

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

DOI
10.1007/978-94-6265-189-0_9
Publication date
2017
Document Version
Author accepted manuscript
Published in
Netherlands Annual Review of Military Studies 2017

Link to publication

Citation for published version (APA):
Ducheine, P. A. L., van Haaster, J., & van Harskamp, R. (2017). Manoeuvring and Generating Effects in the Information Environment. In P. A. L. Ducheine, & F. P. B. Osinga (Eds.), *Netherlands Annual Review of Military Studies 2017: Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises* (pp. 155-179). (NL ARMS). Asser Press. https://doi.org/10.1007/978-94-6265-189-0_9

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.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:28 Nov 2021

UNIVERSITY OF AMSTERDAM

MANOEUVRING AND GENERATING EFFECTS IN THE INFORMATION ENVIRONMENT

P.A.L. Ducheine

Jelle van Haaster

Richard van Harskamp

Amsterdam Law School Legal Studies Research Paper No. 2017-30

Amsterdam Center for International Law No. 2017-25

Electronic copy available at: https://ssrn.com/abstract=2979287

Amsterdam Center for International Law
University of Amsterdam

RESEARCH PAPER SERIES

ACIL Research Paper 2017-25

Manoeuvring and Generating Effects in the Information Environment

Paul Ducheine, Jelle van Haaster, Richard van Harskamp
Amsterdam Center for International Law

Cite as: ACIL Research Paper 2017-25
available at SSRN

Forthcoming in: Ducheine, Paul A.L. & Osinga, Frans (eds.), *Winning Without Killing: The Strategic and Operation Utility of Non-Kinetic Capabilities in Crises*, Cham: Springer (2017)

Amsterdam Center for International Law, University of Amsterdam

Electronic copy available at: https://ssrn.com/abstract=2979287

Manoeuvring and Generating Effects in the Information Environment

Paul Ducheine, Jelle van Haaster, Richard van Harskamp[♣]

Is this the real life? Is this just fantasy?
Queen - Bohemian Rhapsody

Abstract This paper aims to offer a framework for States in general and armed forces in particular for generating effects in or through the information environment by answering the question: "How to generate effects in or through the information environment and therefore, how to manoeuvre in this information environment?" This environment is part of the larger operational environment and consists of three dimensions: the cognitive, virtual and physical. These dimensions in turn host certain layers and these hold targetable entities. States can create effects in this environment by wielding the instruments at their disposal (diplomacy, informational, military and economic) for various purposes (anticipation, prevention, deterrence, protection, intervention, stabilization and normalization). In order to be able to do so, States must organise and equip themselves for manoeuvring in the information environment. To show that indeed States can use this environment, this paper highlights some cases where an actor uses the information environment to great effect, being: the U.S. Election Information Campaign (2016) and the BlackEnergy operation (2015) in Ukraine. These cases are indicative of the potential of manoeuvring in the information environment by States and their armed forces.

Keywords Cyber Operations, Cyberspace, Cyber Warfare, Information Operations, Information Warfare, Psychological Operations, Non-Kinetic Effects, National Interests, Strategic Interests

Contents

[♣] P.A.L. Ducheine, J. van Haaster, R.H. van Harskamp
Amsterdam Centre for International Law, University of Amsterdam
Faculty of Military Sciences, Netherlands Defence Academy, Breda, The Netherlands
email: p.a.l.ducheine@uva.nl

Electronic copy available at: https://ssrn.com/abstract=2979287

9.1 Introduction

Early 2016, the US Secretary of Defense Ashton Carter affirmed that he had given US' Cyber Command "its first wartime assignment" in the war with ISIS.[1] Likewise, the UK's Secretary of State for Defence Michael Fallon MP confirmed that his country's offensive cyber capabilities are being deployed in this campaign against ISIS.[2] These statements combined with NATO's pronouncement to recognise cyberspace as a domain of operations,[3] have spearheaded the use of cyber operations during conflict. It is evident that the information environment, including cyberspace, is increasingly being used to project power, in war and peacetime. Current cyber capabilities, however, almost exclusively focus on the logic (software) and infrastructure (network) to be exploited for military purposes. For a brief period (2000s to early 2010s), these 'hard' cyberspace logic-focused operations have overshadowed the use of cyberspace for primarily influencing human cognition. Tantamount to this is that various cyberspace doctrines only briefly mention the use of cyber operations to affect the humans.[4] With the rise of so-called 'fake' news, election hacks, the hybrid warfare hype and regained attention for 'maskirovka',[5] 'soft' influence activities are once more in the limelight.[6]

Whether for strategic ends as part of a so-called 'hybrid threat' posed by States or terrorist campaigns,[7] or serving operational goals in a so-called comprehensive approach in recent counterinsurgency or stabilization operations,[8] it seems fair to conclude that information as a source of power, after its successes in the east,[9] enjoys a reappraisal in the Western Hemisphere after 2000.[10] Increasingly, States anticipate, or at least research the use of other than kinetic means, ways and strategies to solve its conflicts. This development is not limited to the cleverly timed release of content in

---

[1] Military.com 2016.

[2] Fallon 2016.

[3] NATO, Warsaw Summit Communiqué, 9 July 2016, para 70-71, <http://bit.ly/29wBtNW>.

[4] See for instance: The Joint Chiefs of Staff, 2013.

[5] Russian military deception, sometimes known as *Maskirovka*, is a military doctrine developed from the start of the twentieth century. The doctrine covers a broad range of measures for military deception, ranging from camouflage to denial and deception. See the Paper by Han Bouwmeester in: Ducheine P & Osinga F (2017 forthcoming) Netherlands Annual Review of Military Studies 2017 - Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises. Berlin/The Hague, Springer TMC Asser.

[6] Heickerö 2010, p. 20; Wirtz 2014, p. 21; Giles 2016, p. 26.

[7] Inter alia: Selhorst 2016, pp. 148-164; See also Han Bouwmeester in: Ducheine P & Osinga F (2017 forthcoming) Netherlands Annual Review of Military Studies 2017 - Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises. Berlin/The Hague, Springer TMC Asser.

[8] Inter alia: Ducheine 2015, pp. 201-220; See also Paper by Thijs Brocades Zaalberg Ducheine P & Osinga F (2017 forthcoming) Netherlands Annual Review of Military Studies 2017 - Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises. Berlin/The Hague, Springer TMC Asser.

[9] Kragh & Åsberg 2017; Lee, 2014.

[10] See Herrick 2016. pp. 99-112; Osinga and Russell 2013, pp. 308-309; Rid and Hecker 2009, pp. 132-133.

times war, but also involves the public acknowledgement of the potential of cyber capabilities to be used in (future) wars as well as to affect other states in times of peace. The use of capabilities in the information environment blurs the dichotomy of peace and war to the point of the distinction becoming obsolete.

This paper therefore aims to offer a framework for States in general and armed forces in particular for generating effects in or through the information environment by answering the question: "How to generate effects in or through the information environment and therefore, how to manoeuvre in this information environment?" It thereby contributes to this publication's overarching purpose to address the strategic and operational issues related to the various uses of non-kinetic capabilities by armed forces in pursuance of a State's goals, or in popular speech: *to fight without killing*.

To this end, first, the information environment itself will be analysed. Next, the purpose (the end) of manoeuvring in the Information Environment will be discussed, and, closely connected to the why of manoeuvring in the Information Environment, when this is envisioned. Thirdly, the means to do so will be addressed by subsequently analysing the physical, conceptual and moral component of fighting power required. Additionally, the ways to manoeuvre will then be discussed by providing a generic model, as well as by reviewing recent examples of manoeuvres in the Information Environment.

Before starting, three points of reference should be clarified. First, although initially departing from a military point of view, this paper will not restrict itself in this way. Therefore, the analysis presented will use the State as its point of departure, and will include civilian as well as military capabilities alike. Thus, apart from the fact that information as a part of instruments of power will be addressed, "information related capabilities", whether military or civilian, will be taken into consideration as well. Secondly, this papers aims to contribute to strategic as well as military operational notions of the subject of manoeuvring in the Information Environment. In doing so, references to state practice, inter alia that of the Netherlands armed forces, will be used. This practice, will serve as an example only, as the aim is to cover the themes in a generic international manner. Thirdly, although the requirement of the availability of intelligence is evident, this prerequisite will not be addressed in this paper.

9.2 Where? Manoeuvring in the Information Environment

An important aspect contributing to this paper's aim – to discern the opportunities of manoeuvring in the Information Environment – is delineating the Information Environment. Therefore, this section will first briefly outline the background of the Information Environment. Next, the dimensions and contents of the Information Environment will be derived from technological and military doctrinal analysis. Lastly, a conceptual model of the Information Environment involving the different dimensions (or layers), entities (or components) and (target) actors will be presented. This model will subsequently be used in this paper's analysis.

9.2.1 Doctrinal History of the information environment

The information environment is a construct often employed in publications regarding information operations. The capacities nowadays included under the ambit of information operations are long established in warfare. However, the integral coordination and application of these capacities is relatively new, that is, the early-90s.[11] Early doctrine described information operations as a new concept with "five core capabilities", being Electronic Warfare, Psychological Operations, Operational Security, military deception and Computer Network Operations.[12] The concept followed after the Second Gulf War (Desert Storm, 1991) was dubbed information war, later information warfare and finally replaced with the construct information operations.[13] These operations are conducted in the information environment, which is described as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[14]

Terminological issues regarding the concepts of scope and content of information operations, information activities, information domain and the information environment have plagued many discussions in this matter. These are not 'right or wrong' discussions, they revolve around being correct or doctrinally correct. Hence, these concepts are easily reconciled. The information domain, as often used in discussions, is referred to in doctrines as the information environment.[15] Although used interchangeably, from a doctrinal perspective they have different implications. An environment is a larger/higher concept than a domain, the US doctrine uses two environments: the traditional and the informational. Adjoined these two make up the operational environment.[16] In military doctrine, a domain is 'reserved' for acknowledged domains such as air, land, sea, space and cyberspace (see Figure 9.1).[17] In other words, the term information environment as will be used here, is doctrinally more precise; noting however, that amongst the military, the terms domain and environment are often used as synonyms.

[11] Office of the Chief of Naval Operations 1995; U.S. Army Training and Doctrine Command 1995; The Joint Chiefs of Staff 1998.

[12] U.S. Department of Defense 2003, p. 9.

[13] Bemis and Morgan 2008, pp. 19-21.

[14] The Joint Chiefs of Staff 2014. pp. I-2, I-3.

[15] North Atlantic Treaty Organization 2009. p. 1-1; The Joint Chiefs of Staff 2014. p. ix; UK Development, Concepts and Doctrine Centre 2010, p. 3-7; British Army 2010. p. 4-14.

[16] The Joint Chiefs of Staff 2014. p. x.

[17] An exception to this line of reasoning is the new doctrine for information operations that has replaced dimensions with domains, see: An exception to this line of reasoning is the new doctrine for information operations that has replaced dimensions with domains. See: North Atlantic Treaty Organization 2015. p. 1-2.

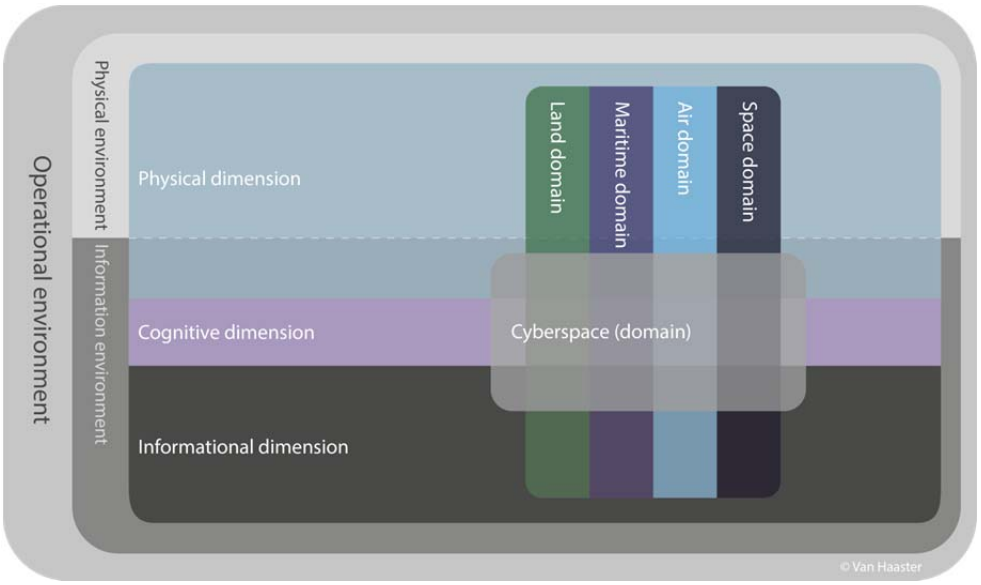

Figure 9.1 Relation between environments, dimensions and domains

9.2.2 A Model of the Informational Environment

Despite terminological differences, contemporary military doctrine agrees upon the dimensions of the information environment (see Figure 9.1), namely: physical, cognitive (psychological) and informational (virtual).[18] These "three interrelated dimensions […] continuously interact with individuals, organizations, and systems".[19] The physical dimension is "composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects".[20] The cognitive (US and UK) or psychological (NATO) dimension "encompasses the minds of those who transmit, receive, and respond to or act on information".[21] Lastly the virtual (UK and NATO) or informational (US) dimension "encompasses where and how information is collected, processed, stored, disseminated, and protected".[22]

The three dimensions making up the operational environment comprise seven layers (see Figure 9.2) that in turn comprise certain entities (see Figure 9.3).

[18] UK Development, Concepts and Doctrine Centre 2010, p. 2-5; The Joint Chiefs of Staff 2014, p. I-1; North Atlantic Treaty Organization, 2015, p. 1-2.
[19] The Joint Chiefs of Staff 2014, p. I-1.
[20] The Joint Chiefs of Staff 2014, p. I-2.
[21] The Joint Chiefs of Staff 2014, p. I-3.
[22] The Joint Chiefs of Staff 2014, p. I-3.

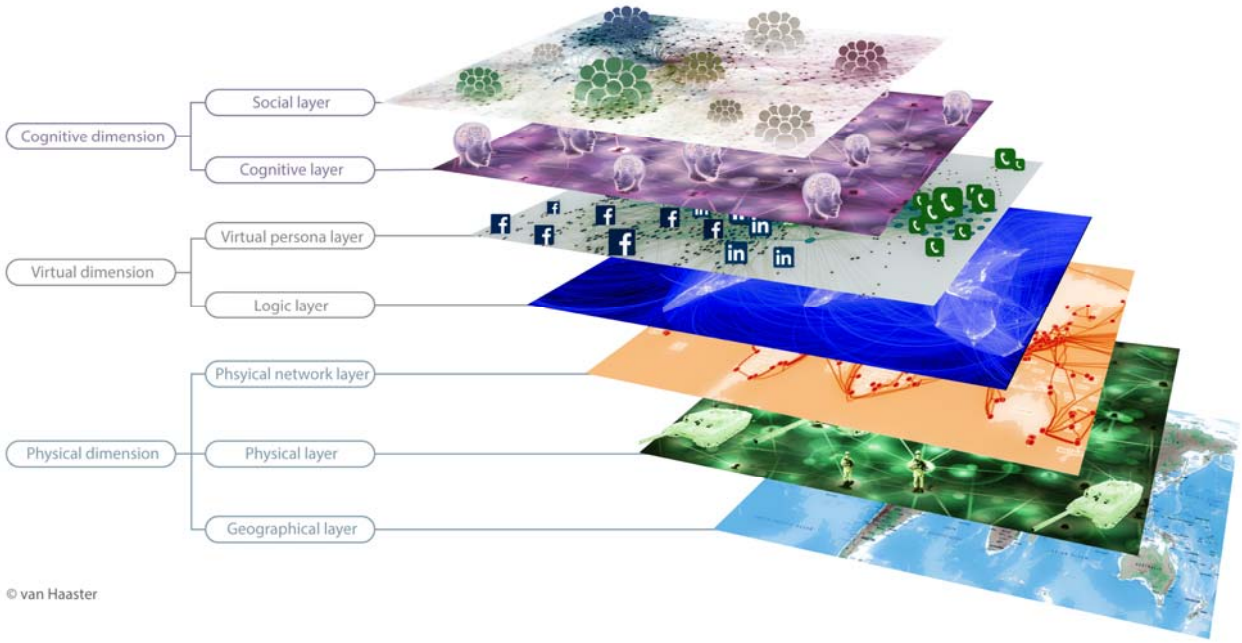

Figure 9.2 Dimensions and layers[23]

The physical dimension includes the geographical, physical network and physical layer; the virtual dimension envelops the logical and virtual persona layer and the cognitive dimension encompasses the cognitive and social layer. The layers subsequently hold various entities that are needed to operationalize the layer concept (see Figure 9.3); these entities can be affected via activities and/or operations.

The geographical layer includes geographical locations, the physical layer physical objects and persons, the physical network layer physical network infrastructure (i.e. routers, cables, computers), the logical virtual objects (e.g. software), the virtual persona layer virtual personas (e.g. social media profiles and mail accounts), the cognitive layer encompasses human psyche (e.g. will, perception and behaviour) and the social layer networked/interacting groups or audiences.[24] These entities are interconnected and interrelated; affecting one will affect others too.

[23] Based on: UK Development, Concepts and Doctrine Centre 2010, p. 2-9; The Joint Chiefs of Staff 2013, p. I-3; Ducheine and Van Haaster 2014; Dekkers, Benten and Dijkstra 2016.

[24] See for a more detailed description of these entities: Ducheine and Van Haaster 2014, pp. 303-327; [Dutch] Ducheine and Van Haaster 2013, pp. 368-387; UK Development, Concepts and Doctrine Centre 2010, p. 2-9; U.S. Army 2010, pp. 8-9.

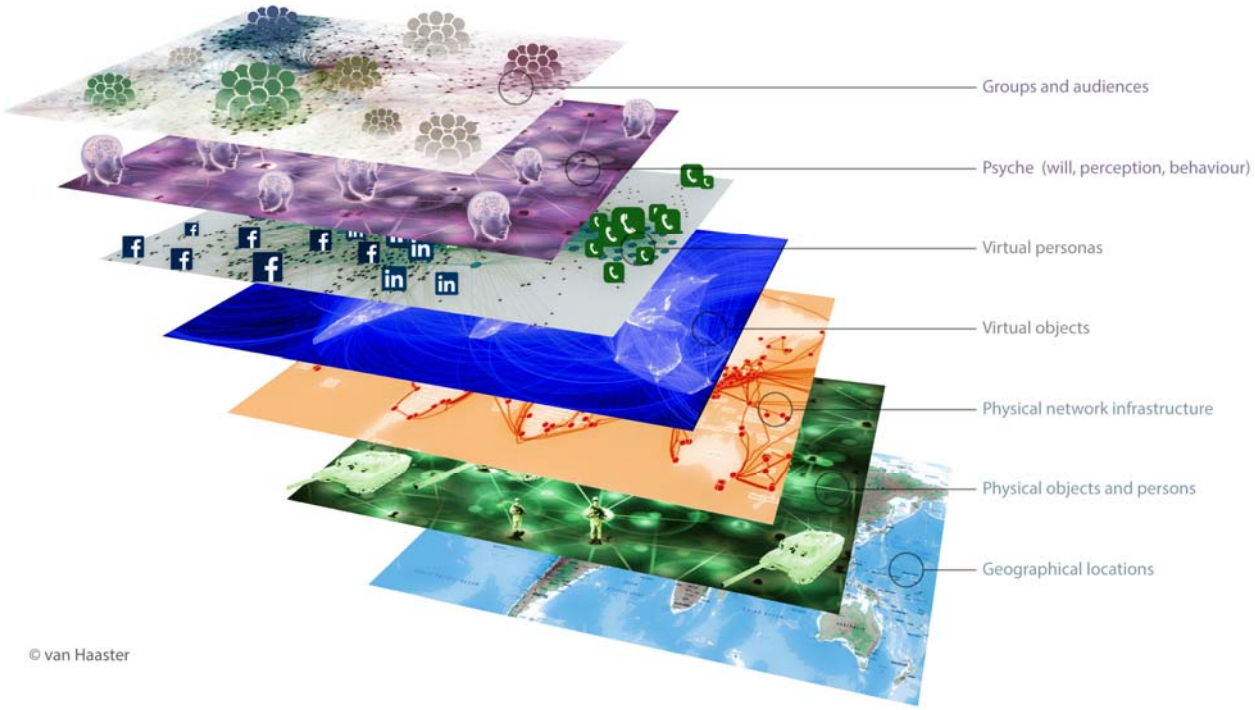

Figure 9.3 Entities

A current surge towards human-machine interfaces has further blurred the distinct differences between virtual and cognitive/physical aspects of humans.[25] Similarly, the rise of artificial intelligence (AI), although still nascent, is starting to blur the difference between physical or virtual objects and a virtual 'AI' persona.[26] In the present authors' opinion, society will increasingly be confronted with hybrid entities, humans linked with hardware and software, virtual objects with an individual virtual persona.

9.3 Why? Pursuing, Promoting and Securing National Interests

The purpose, the 'why' of manoeuvring, is to pursue, promote, secure or defend national interest in times of peace and in war. For the military, this may too easily sound as "winning wars" or to "accomplish missions", the real strategic goal is a higher one. This actual purpose may be stated explicitly in a Grand Strategy,[27] in so-called White Papers,[28] or in policy documents issued by various functional departments.[29] Sometimes, purpose is implied in or can be deduced from ad hoc documents or statements. In the Dutch situation, two complementary policy documents define the Netherlands' national security ambition, encompassing five vital and three strategic interests.[30] Jointly, they cover territorial integrity, physical security, economic security, ecological security, social and political stability and the international legal order.

[25] See for example: Anthony 2014; Hewitt 2014; Regalado 2014.

[26] See for instance: Abadi and Andersen 2016; Rayner 2016; Suzuki, Inaba and Takeno 2005.

[27] Inter alia The White House 2015.

[28] See the French White Paper [Livre Blanc] on Defence and National Security 2013.

[29] Such as the various National Cyber Security Strategies, at <https://ccdcoe.org/cyber-security-strategy-documents.html>.

[30] Netherlands National Security Strategy 2006; Netherlands Ministry of Foreign Affairs 2013.

Whether to promote or advocate national vital and strategic interests in peacetime, or to secure or defend them in times of war or conflict, all available instruments of power provide the means enabling States in doing so. These instruments of power are quite often referred to by the acronym DIME: diplomacy, information, military and economy.[31] The synchronized and harmonised application of these instruments of power is caught in terminology such as the 'whole of government' or 'comprehensive approach'.[32] Ideally, a proper and well-coordinated use of DIME offers synergic advantages compared to the stand-alone or side-by-side employment of separate instruments. Jointly (or separately), the DIME-instruments contribute to strategic functions in international relations.[33] In the Dutch situation these strategic functions encompass anticipation, prevention, deterrence, protection, intervention, stabilization and normalization.[34]

Though much is expected from cyber capabilities and manoeuvring in the IE, given the scarce number of publicly known demonstrations available for research, the contribution, if any, to these strategic functions is subject of much speculation, and - luckily also - research.[35] In the meantime, the effectiveness of military cyber capabilities and manoeuvres in the Information Environment may be derived by learning from experiences and lessons drawn in other fields where these capabilities are more widely used. This might prove problematic as this involves quite different paradigms,[36] however, extracting (or copying) means, methods, modus operandi and concepts from other fields of application may end up illustrative.[37]

The general idea is that manoeuvring in the information environment will offer advantages and reveal capabilities for States to be used alongside or in combination with other instruments, thus supplementing kinetic military capabilities.

9.4 Doing What in the Information Environment

This notion is reflected in Figure 9.4, where physical as well as non-physical activities and operations (Figure 9.4: white arrows) are aimed at objects, persons, network infrastructure, virtual objects, virtual personas, psyche and audiences in order to influence via the cognitive dimension to create an effect in a target actor (Figure 9.4: actor B). These activities or operations are directed vis-à-vis or

[31] US Joint Forces Staff College / National Defense University.

[32] UK Ministry of Defence, 2014 p. 4-1.

[33] South African Defence Review 2015; In a similar way: US Department of Defense 2013, pp. I–10 – I–11.

[34] [In Dutch] Netherlands Ministry of Defence 2010, p. 193; Jordan et al 2008; Netherlands Ministry of Defence 2013; Based on the strategic functions defined in the French White Papers [Livre Blanc] on Defence and National Security as of 2007.

[35] For a constructive attempt: Siedler 2016, pp. 23-36; Also: Healey 2013; Raitsasalo 2015; Geers 2010, pp. 298–303; Libicki 2009; Lindsay 2013, pp. 365–404; Kuehl 2009.

[36] Ducheine 2015a, pp. 211-232.

[37] See for instance: Ducheine and Van Haaste, 2014, pp. 303-327; Learning from intelligence services, law enforcement agencies, criminal organisations, marketing, psychology and social behaviour studies, and of course from international relations and strategic studies, offers a temporary indication of the utility of operations and activities in the information environment.

via these intermediate entities seeking premeditated and designated effects (Figure 9.4: red arrow), which may influence other actors or interests - in turn other actors may respond. Despite western military culture and its prevalence to physical action,[38] NATO's information operations doctrine acknowledges that "the cognitive/psychological domain is the most important as it consists of cognition and emotions, which affect an individual's decision-making".[39]

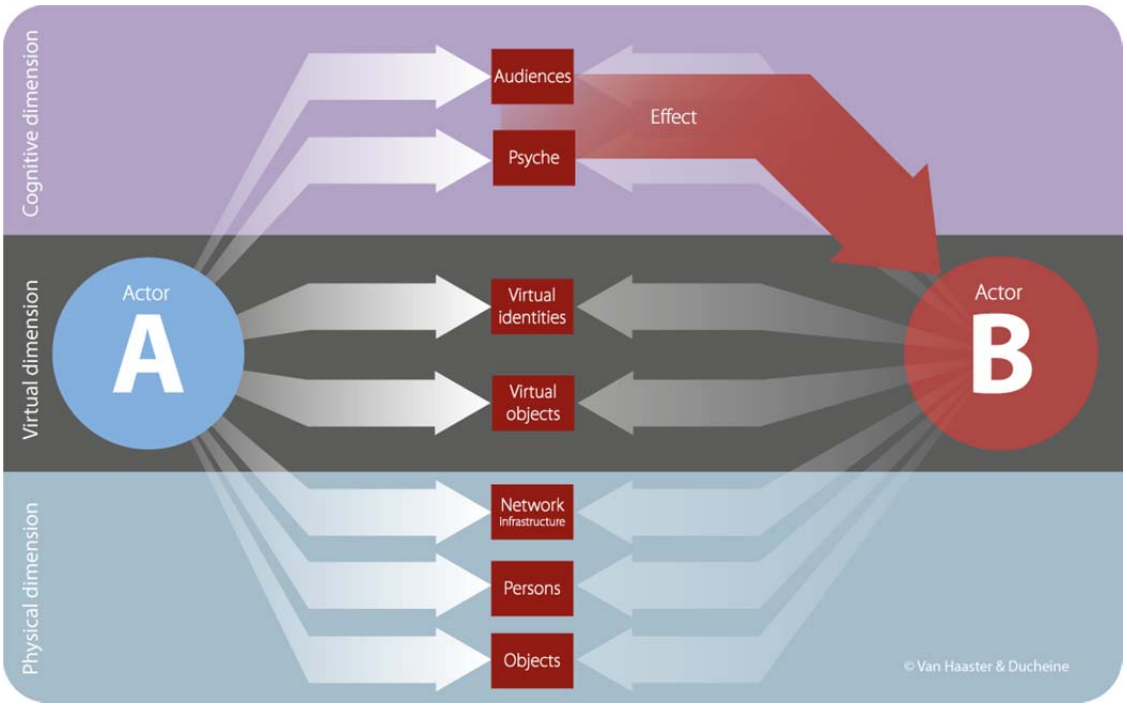

Figure 9.4 Creating effects[40]

The activities specifically tailored to affecting the cognitive dimension are known as "information operations" and/or "information activities". From a NATO perspective information operations (InfoOps or IO) are "a staff function to analyse, plan, assess and integrate information activities"; information activities being "actions designed to affect information or information systems".[41] The US perspective to information operations is that they entail the "integrated employment, during military operations, of information-related capabilities in concert with other lines of operation".[42] The UK has a similar terminological approach to information operations, namely as a "coordinated military activity undertaken to affect decision-makers".[43] As NATO's information activities are labelled information operations in UK and US doctrine, it depends per State what the scope of

[38] See Ducheine 2015b, pp. 201-220.

[39] North Atlantic Treaty Organization 2015, p. 1-2; See also Manoeuver warfare doctrine and the Air/Land battle concept.

[40] See for a more detailed description of these entities: See for a more detailed description of these entities: Ducheine and Van Haaster 2014, pp. 303-327; UK Development, Concepts and Doctrine Centre 2010, p. 2-9; U.S. Army 2010, pp. 8-9.

[41] North Atlantic Treaty Organization 2015, p. 1-5.

[42] The Joint Chiefs of Staff 2014, p. GL-3.

[43] UK Joint Doctrine & Concepts Centre 2002, p. 1-2; UK Development, Concepts and Doctrine Centre 2007, p. 1-2.

information operations and/or activities is. The following section will discuss the requirements needed to actually do so, for manoeuvring in the information environment.

9.5 Requirements for Manoeuvring in the Information Environment

Before being able to manoeuvre in the information environment, States as well as forces require the capability to project military power into this environment. One of the ways of thinking about capability is through the concept of power as it is used in military doctrine, namely: fighting power. Fighting power consists of three components, the conceptual, physical and moral.[44]

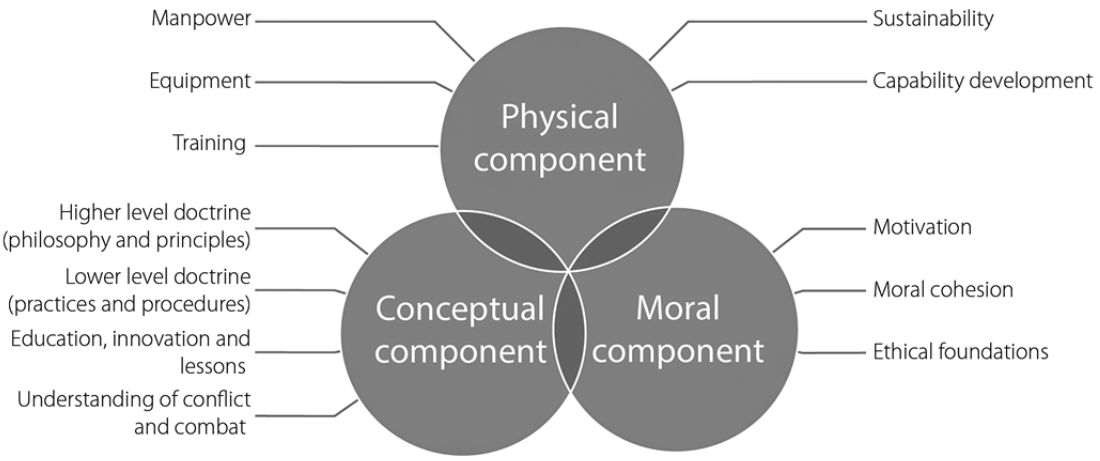

Figure 9.5 (Fighting) power components[45]

Although a Western view of fighting power, it also reflects how other, non-Western, actors reflect on military capabilities.[46] The conceptual component encompasses "the ideas behind how to operate and fight". The moral component comprises "people's will and ability to get people to operate and fight". And the physical component entails the "means to operate and fight".[47] The aspects of these components required for projecting fighting power are depicted in Figure 9.5. In the present authors' opinion, these three components apply to other instruments of power as well. Power of whatever kind requires means, a proper concept as well as the will and dedication to use those means accordingly. The next subsections will discuss the ramifications on the components of fighting power when organising for manoeuvring in the information environment.

9.5.1 Conceptual component

Apart from the proper mind-set as an essential part of the moral component and the capacities as part of the 'physical' component just described, capacities wilfully employed also require ideas, concepts, to generate credible capabilities. The conceptual component comprises, amongst other,

[44] British Army 2010, p. 2-2; Netherlands Ministry of Defence 2013, p. 66.

[45] Based on figure 2.1 in British Army 2010, p. 2-2; Netherlands Ministry of Defence 2013, p. 66.

[46] See for instance: Ministry of Defence of the Russian Federation 2003, pp. 69-82; Security Council of the Russian Federation 2010, pp. 40-44; Li 1999, pp. 146-174.

[47] British Army 2010, p. 2-2.

higher- and lower-level doctrine; education, innovation and lessons; and understanding of conflict and combat.[48] It also encompasses strategies on the use of power and the pursuance of national interest.

States and non-state actors have promulgated grand strategies or issued ad hoc strategic guidance, expressing strategic or operational concepts of thinking regarding the use of instruments of power. These ideas often apply to regular geopolitical settings to the use of power, whether in or outside crises and war. Concepts can be found on the political-strategic, military-strategic, or on the operational and tactical military level of deployments. The idea is that the purpose of the use of instruments of power, including the military, will be guided, explicitly or implied, by a stated or deducted concept on the use of power.

It is evident that the synchronised and harmonised wielding of the instruments of power to create synergy is more complicated than using them separately. Despite criticism related to the effectiveness this comprehensive approach,[49] States already employ instruments in this manner; or, when confronted with a comprehensive (and or hybrid) application of adversaries' power, are forced to or starting to adhere a similar approach. This goes for the constituent elements of the military as well. Full spectrum and joint operations, using all dimensions of the Operational Environment are once more becoming more accepted and used.[50] Increasingly, military targeting procedures developed for classical physical engagement, are being used for operations in the information environment.[51]

Despite this progress, doctrine regarding the Information Environment is sometimes immature or even non-existent.[52] It is telling that NATO is trying to close the conceptual gap in this respect by pushing hard for its first allied joint publication on cyber operations. The Tallinn Manual on the international law of cyber warfare, supported by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE),[53] was the first to shed light on the legal ramifications of the deployment of cyber capabilities in war. The follow-up process generated a second manual applicable to cyber operations in peacetime too.[54] In addition, numerous reports on strategic communication, information operations and hybrid threats have been published by others.[55] The challenge will be to orchestrate and deconflict the overlaps in doctrine and concepts.

Yet, despite familiarities and old wine in new bottles, those planning and executing operations, military or otherwise, will be faced with biases and preferences. These can partly be addressed in the conceptual component, for instance through training and education. However, organisational cul-

[48] British Army 2010, pp. 2-3 to 2-10.

[49] See for instance: Clingendael Conflict Research Unit 2012, pp. 2-3.

[50] For a Dutch example of this process: National Coordinator for Security and Counterterrorism, 2016.

[51] Ducheine and Van Haaster 2014, pp. 303-328; Ducheine 2015b, pp. 201-220; Pratzner 2015, pp. 78-95.

[52] See for example: North Atlantic Treaty Organization 2015; The Joint Chiefs of Staff 2014.

[53] Schmitt 2013; Also: Ducheine 2015c, pp. 456-475.

[54] Schmitt 2017; Also: Ziolkowski 2013; For an early Dutch effort: Ducheine 2012, p. 116.

[55] See for instance: Echevarria II 2016.

ture will have a say too, as will rivals or even opponents that are the subject (targets) of operations, of the use of power. In addition, organisations and people have their conceptual comfort zones. Of course this applies to both sides of the model just presented (Figure 9.4: Actor A and B).

Preferences, when properly exploited, may turn into weaknesses. This applies to issues of overlapping competences, seems, or lacunas too. Seems and overlapping competences will cause friction, therefore coordination is required. In addition to these doctrinal and organisational issues, legal competences, including its seems, overlaps and voids, may also offer opportunities to be exploited. In this respect, one of the characteristics of a holistic approach is demonstrated by the Russian Federation. Whilst manoeuvring below the threshold of armed conflict as stated in the UN Charter, Russia embraces 'bespredel' (denial), 'maskirova', or proxies and non-military instruments, exploiting these seems, overlaps and gaps, to avoid responses from actors targeted and affected.

9.5.2 Physical component

The physical component comprises manpower, equipment, training, sustainability and capability development. Although the concept of fighting power is sufficiently general to be equally applicable to all operations, both traditional and information, the scope of these elements will change.

Manpower comprises the people engaged in information operations. As with most operations, various roles or tasks exist, depending on the purpose of operations. Given the numerous types of information operations,[56] the manpower required is increasingly diverse. Depending on the goal of an information operation, manpower could include regular soldiers (e.g. for physical destruction or deception), cyber operators (e.g. developers, hackers, forensics), press affairs officers, legal advisors, linguists, cultural advisors, financial advisors, political advisors, psychologists, analysts, etcetera. In addition, many other specialties such social-media experts, web designers, content developers, webcare, marketers will be needed to manoeuvre in the information environment.

This non-kinetic expertise could be present in peacetime military organisations, although it will take some effort to orchestrate and reinforce the specialities before being able to create effects in the information environment. For instance, the social media experts, content developers, public affairs officers, psychologists and marketers reside in the non-operational, often civilian, parts of the defence organisation, whilst the psychological operations teams and cyber operators are located in the operational, military parts of the military. Currently, in the Dutch context, a single authority that can wield these capacities although being envisioned, is still lacking. Thus, the issue is less about the manpower; instead, it is about organising the manpower into an organisation that can be orchestrated.

[56] NATO and US doctrine earmark the following operations to be capabilities to be employed under the ambit of information operations: Psychological operations; presence, posture and profile; operations security; information security/information assurance; deception; electronic warfare/joint electromagnetic spectrum operations; physical destruction; key-leader engagement; computer network operations/ cyberspace operations; civil-military cooperation/civil-military operations; strategic communication; joint interagency coordination; public affair; space operations; military information support operations and intelligence

On the equipment part, all essential parts can be found in the physical network layer of the information environment, ICT-infrastructure and hardware, as well as in the virtual layer. The latter comprising virtual persona (digital accounts), ICT-software (operating systems, firmware, applications), protocol and scripts, as well as content (information and data). Information and data may be available in the physical dimension or in the cognitive and informational/virtual dimension. Hence, the classical physical component comprises truly physical as well as virtual elements such as software, data, virtual identities. Seemingly hard to reconcile, this concept is demonstrated by the value of datasets and information, often coined the 'new gold' in modern information societies.[57]

9.5.3 Moral component

The moral component, which epitomises the moral qualities needed to conduct (military) operations, comprises three important elements: "ethical foundations, moral cohesion and motivation".[58] The elements are equally, if not more important when manoeuvring in the information environment important. The pinnacle, however, is adopting the mind-set and willingness of targeting, that is affecting actors in situations of war and peace. This is even more important as soon as it becomes evident that States are being targeted or affected by all instruments of power by other actors and States 24/7, not only during conflict and rivalry, but in this respect predominantly in peacetime as well.

Manoeuvring in the information environment blurs the lines between armed conflict and peace in a geographical and temporal sense. As states and non-state actors can, enabled by information technologies, increasingly and more easily affect others from within their borders, the geographical delimitation of in and outside theatre will vanish, however, from a mind-set perspective only, not from the legal perspective. Also militaries often still talk of and use 'lines of departures', marking the temporal division between pre-operation and the start of an operation (on 'D-day' at 'H-hour').[59] Manoeuvring in the information environment requires a different attitude, which may involve "stop [thinking] in terms of D-days and lines of departure at all".[60] Operations aimed at shaping the environment should not be preserved for the small timespan before an operation; instead it should be done continuously, taking into account all instruments of power in a synchronised and harmonised manner: before, during and after conflict.[61] These activities should involve aspects such as "developing situational understanding; developing options to influence audiences; persuading and empowering other actors to make choices that are advantageous; and conducting limited offensive actions in order to keep adversaries off-balance."[62] Governments wishing to employ their military instrument of power in the information environment should prepare itself and its

[57] Smit-Kroes 2011; Singh 2013.

[58] British Army 2010, p. 2-11.

[59] North Atlantic Treaty Organization 2014, p. 2-D-5.

[60] Van Haaster and Roorda 2016, p. 185.

[61] See the Paper by Han Bouwmeester Ducheine P & Osinga F (2017 forthcoming) Netherlands Annual Review of Military Studies 2017 - Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises. Berlin/The Hague, Springer TMC Asser.

[62] British Army 2010, p. 5-21.

military for doing so. In addition, on the strategic level, society and government should be prepared to actively promote their strategic and vital interests comprehensively throughout the whole spectrum of peace and war.

At the same time, Governments, society and militaries should be resilient and beware for being targeted 24/7.[63] Traditionally military resilience is established with security training aimed at creating understanding and awareness.[64]. These measures are, however, primarily focused on military personnel and facilities and less on their surroundings (family, friends and other connections). As social-media permeates every aspect of real and virtual life and society, adversaries can easily uncover the network surrounding individual soldiers and hurt them where they can be hurt most.[65] The so-called 'attack surface' of soldiers extends as they can be influenced more easily on different fronts and dimensions: physically, cognitively and virtually. Traditionally, military personnel primarily faced physical peril on a battlefield, whilst within the paradigm of information manoeuvre the will face many *Dantean* risks on moral, conceptual and physical levels, not only personally, but in their social environments such as their family as well.[66] Although this already happened on a small scale in modern warfare,[67] recent developments suggest an increase in these types of activities.

9.6 Examples

This section will discuss two recent examples of manoeuvres in the information environment, in doing so this section will reflect on the model forwarded in Figure 9.2. It will discuss the context of the case, the purpose and ways of trying to achieve an effect and whether or not it was successful in doing so. The first example, the U.S. election information campaign of 2016, was selected for its distinct strategic purpose and envelops not only cyber means and methods but also other information activities. The second is an operation with a disruptive physical effect induced by social engineering and cyber activities, namely the Black Energy case.

9.6.1 Information campaign 'U.S. election hacks' (2016)

Before, during and in the wake of the 2016 U.S. elections there were many allegations regarding Russian interference in the democratic process, amongst others from the U.S. Intelligence Community (IC). Following his election, the president-elect's sceptical approach as to the IC's allegations resulted in the Office of the Director of National Intelligence (ODNI) releasing a declassified report on Russian activities during the elections, which offers a glance into the allegedly Russian activities during the election.[68] Using open-source information, other sources arrived at the same conclusion: It is very likely that Russian agencies have interfered in the U.S. elections.[69]

[63] See for example National Cyber Security Centre 2016.
[64] Often referred to as operations (OPSEC), personal (PERSEC), communications (COMSEC) and information security (INFOSEC).
[65] Van Haaster and Roorda 2016. p. 183.
[66] Alighieri 1982.
[67] Hughes 2015; Herridge 2014.
[68] U.S. Office of the Director of National Intelligence 2017.
[69] See for instance: Rid 2016; Gilsinan and Calamur 2017; Taub 2017.

The "influence campaign" encompassed the following goals: "[…] to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."[70] The campaign was carefully staged; starting with cyber operations aimed at collecting intelligence in March 2016, directed at, amongst other, "both major US political parties."[71] Having obtained the requisite intelligence, selected content was publically disclosed in data dumps and "exclusives to media outlets" via the Romanian hacker 'Guccifer 2.0', DCLeaks.com and WikiLeaks.[72] The compromising material, also known as "*Kompromat*",[73] was used to target various individuals involved in the election, for example the Democratic National Committee's (DNC) chair Debbie Wasserman Schultz,[74] the chairman of the 2016 Hillary Clinton presidential campaign John Podesta,[75] and most prominently Hilary Clinton.[76] Although the definitive answer as to the impact of the campaign on the result remains to be seen, some have called this campaign – somewhat alarmist –the "political equivalent of 9/11".[77]

The information campaign aimed at the 2016 U.S. election is an example of how states can contribute to the strategic function 'prevention' (see 9.3), which encompasses "active steps intended to prevent a threat occurring to [State] interests".[78] It shows how States can manoeuvre in the information environment to achieve a strategic goal, namely: a preferential outcome at the political-strategic level. The means to influence the target audience, that is, the U.S. electorate, are diverse. As with all activities, the prime target is to influence psyche, in this case the perception as to which candidate is qualified for presidential office. Influencing psyche in this case involved using and exploiting virtual personas (e.g. using Guccifer 2.0, DCLeaks, and trolls whilst exploiting the Clinton, Podesta and Wasserman Schultz mail accounts) and virtual objects (e.g. exploiting databases and mail servers whilst using websites and blogs to disclose the finds). As to the effectiveness of the campaign there is much yet unresolved, apart from a general state of confusion as to what has actually occurred before, during and after the elections. Considering that the ODNI has deemed undermining public faith in the US democratic process and denigrating Secretary Clinton to be the goals of the campaign, for now it seems that the influence campaign was successful. As such, it is a well-documented example of manoeuvring in the information environment to achieve strategic ends.

9.6.2 'BlackEnergy' operation (2015)

Whereas the U.S. elections case was primarily aimed at discrediting persons via virtual personas and in the preparatory stages included 'hard' cyber operations, the Black Energy example could be characterised as a 'hard' cyber operation aimed at affecting software and hardware. This sub-section will briefly discuss the context of the case, the purpose, the means involved and the effectiveness.

---

[70] U.S. Office of the Director of National Intelligence 2017, p. 1.
[71] U.S. Office of the Director of National Intelligence 2017, p. 2.
[72] U.S. Office of the Director of National Intelligence 2017, pp. 2-3; Rid, 2016.
[73] Rid, 2016.
[74] Martin and Rappeport 2016; Shear and Rosenborg 2016.
[75] WikiLeaks 2016a.
[76] WikiLeaks 2016b.
[77] Morell and Kelly 2016.
[78] Netherlands Ministry of Defence 2010, p. 15.

BlackEnergy is the name of malware previously used by criminals (from 2007 on) and later by advanced persistent threat (APT) groups (2014).[79] Currently BlackEnergy has become synonymous with the power outage in Ukraine December 23, 2015. Some use BlackEnergy to refer to the APT group using BlackEnergy whilst generally it is used to refer to the specific strand of malware and/or the Ukraine outage.[80] The BlackEnergy operation of 2015 was significant as it heralded "ICS [industrial control system] attacks going mainstream".[81]

The operation was conducted amidst of geo-political tensions between Russia and Ukraine regarding the Crimean annexation (2014). Within that geopolitical context there are series of events that could be considered relevant for this operation,[82] however, there is one event that can be considered a catalyst for conducting this operation: the Crimean blackout November 21 (2015). The Crimean blackout was caused by the destruction/sabotage of "four electricity transmission towers" on Ukrainian territory resulting in a blackout in Crimea.[83] There is speculation "that the subsequent blackouts [by the BlackEnergy operations] in Ukraine were retaliation for the attack on the [towers]" – albeit not the original motivation as the operation started six months before the Crimean blackout.[84]

The operation consisted of a preparation stage of obtaining access to networks via spear-phishing from 2014 to mid-2015; the mails contained malicious Office files (first Excel, later Power Point and Word).[85] Using macros in Office, an "old-school method from the 90's",[86] the 2015 BlackEnergy operation targeted railway, mining, media and power sectors in Ukraine[87] and ICS/SCADA and energy companies worldwide.[88] After rising tensions in the region, from mid-2015 the operation has geared towards obtaining control over the regional *Prykarpattya Oblenergo* and *Kyivoblenergo* energy providers in Ukraine.[89]

After gaining access to the corporate networks, the attackers "conducted extensive reconnaissance, exploring and mapping the networks" and, as a textbook example, targeted the Windows Domain Controllers.[90] By doing so the attackers "acquired legitimate credentials" that facilitated remote access via a virtual private network (VPN) to industrial control systems – including, amongst other, the electrical breakers.[91] After laying the groundwork, the attackers took additional steps in order to extend the blackout period for maximum effect. In order to thwart the recovery operation the

[79] F-Secure 2014; Kaspersky 2016a.
[80] Kaspersky 2016a.
[81] Van Haaster, Gevers and Sprengers 2016, p. 72.
[82] See: Zetter 2017. She lists other causes such as Ukrainian parliament considering privatisation of privately owned power companies in Ukraine of which some are owned by a powerful Russian oligarch.
[83] BBC 2015; Radio Free Europe/Radio Liberty 2015; Russia Today 2015.
[84] Zetter 2017.
[85] Cys-Centrum 2016; Kaspersky 2016b.
[86] Zetter 2017.
[87] Trend Micro 2016.
[88] Kaspersky 2016b.
[89] Zetter 2017.
[90] Van Haaster, Gevers and Sprengers 2016. p. 62.
[91] U.S. Department of Homeland Security ICS-CERT 2016.

attackers had overwritten firmware on "serial-to-Ethernet converters" – the link between logical (SCADA) and physical control systems – in order to "prevent [company] operators from sending remote commands to re-close breakers once a blackout occurred."[92] Besides that, they "reconfigured the uninterruptible power supply [UPS]" for the companies control centres, resulting in the company operators manning the control centre would also lack power in the event of an outage.[93]

At around 15:30 on December 23 the attackers "launched a telephone denial-of-service attack [from Moscow] against customer call centres to prevent customers from calling in to report the outage", "entered the SCADA networks through the hijacked VPNs and sent commands to disable the UPS [and] began to open breakers".[94] After completion the attackers used KillDisk, "a disk wiping malware",[95] to erase files and corrupt the master boot record, "rendering systems inoperable" and deleting tracks.[96] The attack resulted in a population of "around 1.4 million […] left without electricity for a few hours".[97]

The BlackEnergy operation of 2015 could be seen as an example of how States can manoeuvre in the information environment. Assuming Russia's involvement, focussing on the virtual dimension, the author-State could have sought a strategic goal, namely: retaliate against a target-State in order to dissuade it from future activities harming the interests of the author-State. This is an example of the strategic function 'intervention' as the author-State aims to "enforce a change in the behaviour of one or more parties that threaten the interests of the [State]".[98] In this case, although speculative, Russia responding in kind to Ukraine for allowing the sabotage of Crimea's power supplies. By exploiting virtual personas (mail accounts targeted in the spear-phishing campaign) the attackers gained access to the network and were able to escalate access to the domain controller, control systems and SCADA systems (virtual objects) and gain control over physical network infrastructure (serial-to-Ethernet converters) and 'regular' physical energy infrastructure (objects). By doing so the author-State creates a blackout, aimed to send the message: "you think you can take away the power [in Crimea]? Well I can take away the power from you."[99]

13.7 Conclusion

This paper has sought to answer the question: "How to generate effects in or through the information environment and therefore, how to manoeuvre in this information environment?" First this paper has discussed the information environment construct. This environment, a part of the larger operational environment consist of three dimensions, the cognitive, virtual and physical. These dimensions in turn host certain layers and these hold targetable entities. Departing from that conceptual model of the information environment, this paper has turned to how to manoeuvre in that environment. First the 'why' was discussed, considering the potential there are many incentives for a State to use this environment. A State can create effects in the information environment by wield-

[92] Zetter 2017.
[93] Zetter 2017.
[94] Zetter 2017.
[95] Trend Micro 2016.
[96] U.S. Department of Homeland Security ICS-CERT 2016.
[97] ESET 2016.
[98] Netherlands Ministry of Defence 2010, p. 15.
[99] Zetter 2017.

ing the instruments at its disposal (diplomacy, informational, military and economic) for various purposes, for instance strategic functions (anticipation, prevention, deterrence, protection, intervention, stabilization and normalization). In order to be able to do so, it must organise and equip itself for manoeuvring in the information environment, this paper has used the components of fighting power in order to highlight critical elements required for creating effects. Lastly, this paper has highlighted the U.S. Election Information Campaign (2016) and the BlackEnergy operation (2015) as examples of manoeuvring in the information environment in order to achieve strategic goals. These cases demonstrate that the use of and manoeuvring in the information environment might indeed contribute to achieving effects and strategic goals.

References

Abadi M, Andersen DG (2016) Learning to Protect Communications with Adversarial Neural Cryptography. https://arxiv.org/pdf/1610.06918.pdf. Accessed 4 March 2017

Alighieri D (Dante) (1982) The Inferno translated by John Ciardi. Signet Classics, London

Anthony S (2014) The First Human Brain-to-Brain Interface has been Created in the Future, Will we all be Linked Telepathically? (3 September 2014) extremetech.com/extreme/188883-the-first-human-brain-to-brain-interface-has-been-created-in-the-future-will-we-all-be-linked-telepathically. Accessed 14 January 2015

BBC (2016) Crimea Power Blackout: Russia Accuses Ukraine of Sabotage (30 Nov 2015) bbc.com/news/world-europe-34967093 Accessed 10 February 2017

Bemis J, Morgan G (2008) Exposing the Information Domain Myth. In: Air & Space Power Journal 22(3):19-21

British Army (2010) Army Doctrine Publication: Operations. Development, Concepts and Doctrine Centre, Shrivenham

Clingendael Conflict Research Unit (2012) CRU Policy Brief: How to make the Comprehensive Approach Work. Clingendael, The Hague

Cys-Centrum (2016) Киберугроза Blackenergy2/3. История Атак На Критическую Ит Инфраструктуру Украины (Cys-CentrumFebruary 10) cys-centrum.com/ru/news/black_energy_2_3. Accessed 4 March 2017

Dekkers PAP, Benten C, Dijkstra H (2016) Advisory Report: Information as Weapon, Vector and Target. Ministry of Defence, The Hague.

Ducheine P (2015a) Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting' in: Ducheine P, Schmitt M, Osinga F (eds) Targeting: Challenges of Modern Warfare,: TMC Asser Press/Springer, The Hague/Berlin, pp 201-220

Ducheine P (2015b) The Notion of Cyber Operations. In: Tsagourias N, Buchan R (eds) Research Handbook on International Law and Cyber Space,: Edward Elgar Publishing, Cheltenham, pp 211-232

Ducheine P (2015c) Military Cyber Operations. In: Gill TD, Fleck D (eds) Handbook of the International Law of Military Operations (2nd ed) Oxford University Press, Oxford, pp 456-475

Ducheine P, Haaster J van (2013) Cyber-Operaties en Militair Vermogen. In: *Militaire Spectator* 182(9):368-387

Ducheine P, Haaster J van (2014) Fighting Power, Targeting and Cyber Operations. In: Brangetti P, Maybaum M, Stinissen J (eds) Proceedings of the 6th International Conference on Cyber Conflict, NATO CCD COE, Tallinn, pp 303-328

Fallon M (2016) Secretary of State for Defence Michael Fallon MP at The Second International Cyber Symposium (21 October 2016) <youtube.com/watch?v=6TqQTVkYHYc>. Accessed 16 February 2017

Farrell T, Osinga F, Russel JA (2013) Military Adaptation in Afghanistan.: Stanford University Press, Stanford

F-Secure (2014) BlackEnergy & Quedagh: The Convergence of Crimeware and APT Attacks. F-Secure, Helsinki <https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf> Accessed 4 March 2017

French White Paper [Livre Blanc] on Defence and National Security (2013) <http://www.defense.gouv.fr/content/download/215253/2394121/file/White%20paper%20on%20defense%20%202013.pdf> Accessed 4 March 2017

Geers K (2010) The Challenge of Cyber Attack Deterrence. In: Computer Law & Security Review 26(3):298-303

Giles K (2016) Russia's New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power. Chatham House, London

Kragh M, artin Åsberg S (2017) Russia's strategy for influence through public diplomacy and active measures: the Swedish case. In: *Journal of Strategic Studies* (5 Januari 2017) http://dx.doi.org/10.1080/01402390.2016.1273830. Accessed 4 March 2017

Libicki M (2009) Cyberdeterrence and Cyberwar. RAND, Santa Monica

Gilsinan K, Calamur K (2017) Did Putin Direct Russian Hacking? and Other Big Questions. In: The Atlantic (6 January 2017) www.theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/. Accessed 6 January 6 2017

Healey J (ed)(2013) A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association

Herrick D (2016) The Social Side of 'Cyber Power'? Social Media and Cyber Operations. In: Pissanidis N, Rõigas H, Veenendaal M (eds), Proceedings of the 8th International Conference on Cyber Conflict Cyber Power. NATO CCD COE Publications, Tallinn, pp 99-112

Herridge C (2014) Army Warns US Military Personnel on Threat to Family Members. In: Fox News (2 October 2014) foxnews.com/politics/2014/10/02/army-warns-us-military-personnel-on-isis-threat-to-family-members.html. Accessed 15 November 2016

Heickerö R (2010) Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. FOI, Stockholm

Hewitt J (2014) New Brain Implant Tech from Blackrock is Making 'Mind Over Matter' a Reality. In: extremetech.com (18 December 2014) www.extremetech.com/extreme/194935-new-brain-implant-tech-from-blackrock-is-making-mind-over-matter-a-reality. Accessed January 14, 2015

Hughes C (2015) Jihadis Threaten to Slaughter British Soldiers' Wives and Families as Police Issue Social Media Warning. In: Mirror (31 July 2015) www.mirror.co.uk/news/uk-news/jihadis-threaten-slaughter-british-soldiers-6173859. Accessed November 15, 2016

Netherlands Ministry of Foreign Affairs (2013) International Security Strategy - A secure Netherlands in a secure world. www.government.nl/latest/news/2013/06/21/a-secure-netherlands-in-a-secure-world [Kamerstukken II 2012-13, 33 694, nr. 1, Internationale Veiligheidsstrategie]

Jordan D et al (2008) Understanding Modern Warfare. Cambridge University Press, Cambridge

Kaspersky (2016a) BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents. In: Kaspersky Lab (28 Janaury 2016) https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/. Accessed 10 February 2017

Kaspersky (2016b) Newly Discovered BlackEnergy Spear-Phishing Campaign Targets Ukrainian Entitities. In: Kaspersky Lab (28 January 2016) usa.kaspersky.com/about-us/press-center/press-releases/2016/newly-discovered-blackenergy-spear-phishing-campaign-targets-uk. Accessed 10 February 2017

Lee S (2014) China's 'Three Warfares': Origins, Applications, and Organizations. In: Journal of Strategic Studies 37(2):198-221, http://dx.doi.org/10.1080/01402390.2013.870071

Siedler RE (2016) Hard Power in Cyberspace: CNA as a Political Means. In: Pissanidis N, Rõigas H, Veenendaal M (eds) Proceedings of the 8th International Conference on Cyber Conflict Cyber Power. NATO CCD COE Publications, Tallinn, pp 23-36

Kuehl D(2009) From cyberspace to cyberpower: Defining the problem. In: Kramer F, Starr S, Wentz L (eds) Cyberpower and National Security. Potomac Books, Licoln

Li N (1999) The PLA's Evolving Campaign Doctrine and Strategies. In: Mulvenon JC, Yang RH (eds) The People's Liberation Army in the Information Age. RAND, Santa Monica, pp 146-174

Lipovsky R, Cherepanov A (2016) BlackEnergy Trojan Strikes again: Attack Ukrainian Electric Power Industry. In: ESET (4 Janauary 2016) welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/. Accessed 10 February 2017

Lindsay JR (2013) Stuxnet and the Limits of Cyber Warfare. In: *Security Studies*, 22(3):365-404

Martin J, Rappeport A (2016) Debbie Wasserman Schultz to Resign D.N.C. Post. In: The New York Times (35 July 2016) nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html. Accessed 8 February 2017

Ministry of Defence of the Russian Federation (2003) Aktual'nyye Zadachi Razvitiya Vooruzhënnykh Sil Rossiyskoy Federatsii [The priority tasks of the development of the Armed Forces of the Russian Federation] Ministry of Defence of the Russian Federation, Moscow

Military.com (2016) Cyber Command Gets First Wartime Assignment in Fight ISIS (5 April 2016) military.com/daily-news/2016/04/05/cyber-command-gets-first-wartime-assignment-in-fight-isis.html. Accessed February 16, 2017

Morell M, Kelly S (2016) Former CIA Acting Director Michael Morell: "This is the Political Equivalent of 9/11". In: The Cipher Brief (11 December 2016) thecipherbrief.com/article/exclusive/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091. Accessed February 8, 2017

National Coordinator for Security and Counterterrorism (2016) Magazine Nationale Veiligheid en Crisisbeheersing, 14(5) https://www.nctv.nl/binaries/Magazine Nationale Veiligheid en Crisisbeheersing 2016 5_7 interactief_tcm31-234692.pdf. Accessed 4 March 2017

National Cyber Security Centre (2016) Cyber Security Assessment Netherlands. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html. Accessed 4 March 2017

Netherlands National Security Strategy (2006) [Strategie nationale veiligheid], in: Parliamentary Papers II [Kamerstukken II] 2006-07, 30 821, nr. 2

Netherlands Ministry of Defence (2010). Future Policy Survey: Summary and Conclusions. Ministry of Defence, The Hague

Netherlands Ministry of Defence (2013) Netherlands Defence Doctrine. Ministerie van Defensie, Den Haag

North Atlantic Treaty Organization (2009) Allied Joint Publication 3.10: Allied Joint Doctrine for Information Operations. North Atlantic Treaty Organisation, Brussels

North Atlantic Treaty Organization (2014) Allied Administrative Publication 06: NATO Glossary of Terms and Definitions (English and French). NATO Standardization Agency, Brussels

North Atlantic Treaty Organization (2015) Allied Joint Doctrine for Information Operations (Edition A Version 1 ed). NATO, Brussels

North Atlantic Treaty Organization (2016) *Warsaw Summit Communiqué*. North Atlantic Treaty Organisation, Brussels

Office of the Chief of Naval Operations (1995) *OPNAV Instruction 3430.26: Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W)*

Orenstein D (2013) Brown Unveils Novel Wireless Brain Sensor (28 February 2013) In: news.brown.edu/articles/2013/02/wireless. Accessed 14 January 2015

Pratzner P (2015) The Current Targeting Process. In: Ducheine P, Schmitt M, Osinga F (eds), *Targeting: Challenges of Modern Warfare*,: TMC Asser Press/Springer, The Hague/Berlin, pp 77-97

Radio Free Europe/Radio Liberty (2016) Pylon 'Blown Up' in Ukraine, Causing Crimea's Blackout. In: Radio Free Europe/Radio Liberty (22 November 2015) www.rferl.org/a/ukraine-crimea-blackout-state-of-emergency/27379758.html. Accessed 10 February 2017

Ragalado A (2014) Military Funds Brain-Computer Interfaces to Control Feelings. In: MIT Technology Review (29 May 2014) <technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/. Accessed 14 January 2015

Raitasalo J (2015) Hybrid Warfare: where's the beef? In: War on the Rocks (23 April 2015) http://warontherocks.com/2015/04/hybrid-warfare-wheres-the-beef>, Accessed 4 March 2017

Rayner A(2016) Can Google's Deep Dream Become an Art Machine? In: The Guardian (28 March 2016) theguardian.com/artanddesign/2016/mar/28/google-deep-dream-art. Accessed 9 November 2016

Rid T (2016) How Russia Pulled Off the Biggest Election Hack in U.S. History. In: Esquire (20 October 2016) www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/. Accessed 8 February 2017

Rid T, Hecker M (2009) War 2.0: Irregular Warfare in the Information Age. Praeger Security International, London

Russia Today (2016) State of Emergency, Blackout in Russia's Crimea After Transmission Towers in Ukraine Blown Up. In: rt.com/news/323012-crimea-blackout-lines-blown-up/. Accessed 10 February 2017

South African Defence Review (2015) in: http://www.dod.mil.za/documents/defencereview/Defence%20Review%202015.pdf. Accessed 4 March 2017

Security Council of the Russian Federation (2010) Military Doctrine Russian Federation [ОЕННАЯ ДОКТРИНА РОССИЙСКОЙ ФЕДЕРАЦИИ].: Security Council of the Russian Federation, Moscow

Sellhorst AJC (2016) Russia's Perception Warfare - The development of Gerasim-ov's doctrine in Estonia and Georgia and its application in Ukraine. In: *Militaire Spectator* 185(4)148-164, www.militairespectator.nl/thema/strategie-operaties/artikel/russias-perception-warfare. Accessed 4 March 2017

Shear MD, Rosenberg M (2016) Released Emails Suggest the D.N.C. Derided the Sanders Campaign. In: The New York Times (3 July 2016) nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html. Accessed 8 February 2017

Smit-Kroes N (2011) Data is the new Gold - Opening Remarks, Press Conference on Open Data Strategy, European Commission, Brussels (12 December 2011) https://ec.europa.eu/digital-single-market/en/news/data-new-gold. Accessed 1 March 2017

Singh A (2013) Is Big Data the New Black Gold? In: Wired.com (undated) https://www.wired.com/insights/2013/02/is-big-data-the-new-black-gold/. Accessed 1 March 2017

Suzuki T, Inaba K, Takeno J (2005) Conscious Robot that Distinguishes between Self and Others and Implements Imitation Behavior. Springer, Berlin

Taub A (2017) 'Kompromat' and the Danger of Doubt and Confusion in a Democracy. In: The New York Times (15 january 2017) nytimes.com/2017/01/15/world/europe/kompromat-donald-trump-russia-democracy.html. Accessed 8 February 2017

UK Development, Concepts and Doctrine Centre (2007) Joint Doctrine Publication 3-45.1: Media Operations. The Development, Concepts and Doctrine Centre, Shrivenham

UK Development, Concepts and Doctrine Centre (2010) Joint Doctrine Publication 04: Understanding. Ministry of Defence, Shrivenham

UK Joint Doctrine & Concepts Centre (2002) Joint Warfare Publication 3-80: Information Operations. Ministry of Defence, Shrivenham

U.S. Army (2010) Cyberspace Operations Concept Capability Plan 2016-2028. The U.S. Training and Doctrine Command, Fort Eustis

U.S. Army Training and Doctrine Command (1995) TRADOC Pamphlet 525-69: Military Operations Concept for Information Operations. Department of the Army, Fort Monroe

U.S. Department of Defense (2003) Information Operations Roadmap. Department of Defense, Washington DC

U.S. Department of Homeland Security (2016) Alert (IR-ALERT0H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure. ICS-CERT. ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. Accessed 10 February 2017

U.S. Joint Chiefs of Staff (1998) Joint Publication 3-13: Joint Doctrine for Information Operations. The Joint Chiefs of Staff, Washington, DC

U.S. Joint Chiefs of Staff (2013) Joint Publication 3-12 (R): Cyberspace Operations. The Joint Chiefs of Staff, Washington, DC

U.S. Joint Chiefs of Staff (2014) Joint Publication 3-13: Information Operations (20 November 2014). The Joint Chiefs of Staff, Washington, DC

U.S. Joint Forces Staff College / National Defense University (no date) Elements of National Power. In: http://jfsc.ndu.edu/Portals/72/Documents/library/Bibliographies/Elements_of_National_Power.pdf. Accessed 1 March 2017

U.S. National Security Strategy (2015) The White House (February 2015) http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf. Accessed 1 March 2017

U.S. Office of the Director of National Intelligence (2017) Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. U.S. Office of the Director of National Intelligence, Washington, DC

Van Haaster J, Gevers R, Sprengers M (2016) Cyber Guerilla. Syngress, Boston

Van Haaster J, Roorda MP (2016) D-Day's Demise: The Impact of Hybrid Warfare on Traditional Operational Rationale. In: Militaire Spectator 185(4):175-185

WikiLeaks (2016a) Hillary Clinton Email Archive. In: wikileaks.org/clinton-emails/. Accessed 8 February 2017

WikiLeaks (2016b) The Podesta Emails. In: wikileaks.org/podesta-emails/. Accessed 8 February 2017

Wilhoit K (2016) KillDisk and BlackEnergy are Not just Energy Sectory Threats. In: Trend Micro (11 February 2016) blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/. Accessed 10 February 2017

Wirtz JJ (2014) Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In: Geers K (ed) Cyber War in Perspective: Russian Aggression against Ukraine.: CCD COE, Tallinn

Zetter K (2016) Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. In: Wired (3 March 2016) wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Accessed 8 February 2017