D-Day's Demise

The Impact of Hybrid Warfare on Traditional Operational Rationale

In this article we will describe how certain non-traditional means and methods could be used to undermine a military's capacity to respond effectively to an emerging threat. We will do so by focussing on the Netherlands and showing how some of its specific (non-military) vulnerabilities may be targeted by opponents using non-traditional means in an indirect manner. We will structure the sequence of events along an artificial 30-day period leading up to 'D-day'. Starting at D minus 30 (D-30), we have divided our actions into a preparation phase, a shaping phase, and an intensification phase. At each step we will discuss the means or methods used, the specific vulnerabilities exploited, and the likely consequences. We will show how the use of non-traditional means can be highly effective in disrupting a regular opponent and may fundamentally alter traditional operational rationale.

*First lieutenant (Army) Jelle van Haaster LL.M. and captain (Marine Corps) Mark Roorda LL.M.**

> *'In Strategy the longest way around is often the shortest way there. A direct approach to the object exhausts the attacker and hardens the resistance by compression, whereas an indirect approach loosens the defender's hold by upsetting his balance.' Liddell Hart*[1]

The term *hybrid warfare* has attracted significant attention, particularly since the Russian Federation's *de facto* annexation of Crimea and the subsequent instability in Eastern Ukraine. Its buzzword use is understandable, given the fact that neither Ukraine, NATO, nor the European Union seemed to have an appropriate response. While no single definition has been generally accepted, the Dutch Defence Minister described it as follows: 'I see it as the use of various covert and overt tactics, enacted with both military and non-military means. Besides the employment of conventional and irregular forces hybrid warfare includes intelligence and cyber operations and the application of economic power. It is not geographically limited. Hybrid methods serve to increase ambiguity, complicating decision making on the opposing side. […] And all of this is supported by a massive disinformation campaign to control the narrative or to dislodge the opponent's narrative.'[2] Hybrid warfare, so much is clear, combines many different instruments aimed at creating confusion and indecisiveness. Informa-

* Mark Roorda is a PhD candidate whose research deals with targeting and unmanned systems at the University of Amsterdam and the Faculty of Military Sciences in Breda. Jelle van Haaster is a PhD candidate researching the (future) utility of cyber operations at the University of Amsterdam and the Faculty of Military Sciences. The authors are indebted to brigadier-general professor dr. Paul Ducheine and colonel Han Bouwmeester for their feedback.

1 B.H. Liddell Hart, *The strategy of indirect approach* (London, Faber & Faber, 1941).

2 'Who's afraid of Hybrid Warfare?', address by the Netherlands Minister of Defence, J.A. Hennis-Plasschaert, at the Annual Baltic Conference on Defence (Tallinn, Estonia, 24 September 2015).

tion and disinformation are central aspects. It teaches us that there is more to contemporary conflict than regular combat operations. Still, NATO's response was (and is) predominantly one of showing traditional military muscle. Take, for example, the reinforcements to the Baltic air-policing mission, the naval exercises in the Baltic Sea, and the establishment of a Very High Readiness Joint Task Force. These are important signals from a reassurance and deterrence point of view, yet the range of opportunities is much broader. That is not to say that understanding of, and preparing for, regular conflict is not important. Surely, it is, and it will remain so. The challenge is that the predominance it takes seems to overshadow the idea that there is more to understand and prepare for.

In this article, we will address the use of the information environment and some non-traditional (and relatively simple and cheap) means and methods to 'shape the battlefield'. Our digital, transparent, and globally interconnected society has weaknesses that can be exploited by the military. We will deal with actions, both physical and non-physical, affecting the perception and responsiveness of the opponent. In other words, actions that are directed at the conceptual and moral components of military power, rather than the physical component. Moreover, we will focus on actions not necessarily directed against military capacities, but aimed at vulnerable elements of society having an indirect effect on the military. The purpose of this article is to create awareness about such means and methods, as they present both options for the military to use as well as vulnerabilities for an opponent to exploit.

Raising awareness is necessary since there still seems to be a tendency to think in terms of old-fashioned regular conflict. This assumption is hard to prove, yet we experience it continually in our day-to-day conversations with colleagues. Most agree that a hybrid threat would require a comprehensive response that goes beyond traditional military capabilities, yet most seem to be paying only lip service to it. This is, to a certain extent, understandable. Using non-traditional means to render effects is difficult. It requires a deeper understanding of the opponent's system, knowledge of sophisticated non-traditional means, and an ability to match the latter to the former. It requires thinking in second (or 'n') order effects, rather than in first order explosions and destruction. For the somewhat older soldiers, many of the modern possibilities did not even exist when they enlisted. And for the younger, it is commonly not what they thought they signed up for. Still, the use of non-traditional means and methods will become more important. And in our continuous efforts to effectively and efficiently influence the outcome of conflict, it is a subject we cannot afford to neglect.

Preparation phase: gathering intelligence

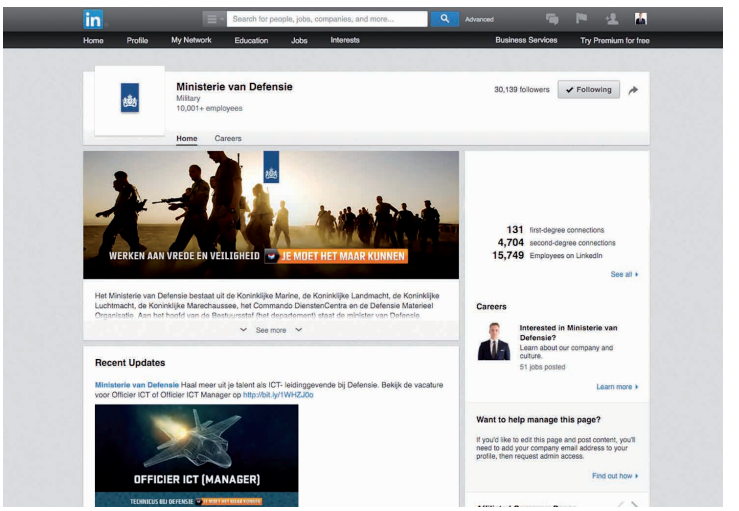
As with most operations, extensive planning and preparation is needed before being able to carry out concrete activities. An important part is gathering the necessary intelligence to identify those targets which render the most output when influenced. Creating an in-depth understanding of infrastructures and organisations enables effective and efficient use of resources. In our time schedule we have reserved D-30 to D-25 for gathering intelligence. Normally such preparations would exceed the thirty day timeframe, possibly beginning years in advance and continuing throughout. It is clear that the Internet serves as a valuable and accessible source for gathering information. Yet when taking into account the use of non-traditional means, what is militarily valuable proves to be more extensive. This section highlights two activities: mapping social networks and mapping technological networks.

D-30: Mapping social networks

We create large amounts of data as we embrace digital devices and increasingly extend our social and professional lives onto the Internet. Such data includes insights into location, social network(s), relationship status, political preferences, sexual preferences, shopping habits, devices used to browse the Internet and much more. By fusing these sources, for

instance by using data mining techniques, a comprehensive image of persons, groups and networks can be created. Even those who do not engage in online activities can be mapped as a consequence of their relations mentioning the person not online.[3] As social networks unveil ties between soldiers and their relatives, the relatives become known as part of the soldier's network and become a vector for influencing them.

A simple Linkedin query (search action) for 'Ministerie van Defensie' (i.e. the Netherlands Ministry of Defence) yields nearly 16,000 results for employees. A more specific Linkedin query for a specific combat vehicle on the 'Ministerie van Defensie' pool produces 31 persons who currently work or have worked with the platform. Similarly a query for 'system administrator' results in 41 persons. These queries can be performed on most social platforms and produce results that can consequently be used to target particular persons. By virtue of mapping social networks, an opponent may identify organisational structures, from brigades to individual soldiers in platoons. To put this to the test, in less than an hour we managed to find out 37 full names of the 96 crew members of an operational navy ship on mission in 2015, only by using public social networks. The exposure of names was not so much caused by military personnel itself, but by friends and relatives commenting on pictures shown on a public Facebook profile of the ship. Every crew name, including their relatives, could serve as a new vector for obtaining more information.



The Dutch Ministry of Defence page on Linkedin, listing 15,749 employees

D-28: Mapping technical networks

Besides social networks, technical networks can be similarly mapped for future use. These networks include operational platforms, office environments, military networks, civilian systems and their respective supply chains. Elements of interest of a target network are: (1) organisational aspects (e.g. culture, organisational structure, languages); (2) defensive processes and mechanisms (e.g. monitoring and response); and (3) technical aspects (e.g. systems, hostnames and misconfigurations).[4] Besides these digital aspects, the physical aspects of networks will also be mapped. Detailed information regarding the physical layout of vital infrastructure is listed online. An example is the Dutch emergency communication system C2000. While for security reasons the official antenna registers do not mention the C2000 antenna locations, a private website does.[5] There are numerous similar examples of other essential network infrastructure.[6]

3 Emre Sarigol, David Garcia and Frank Schweitzer, 'Online Privacy as a Collective Phenomenon' (Dublin, Conference on Online Social Networks, October 1-2, 2014); Chloe Albanesius, 'Facebook Ireland Facing Audit Over Privacy, 'Shadow Profiles', *PC Magazine*, pcmag.com/article2/0,2817,2395109,00.asp (accessed July 14, 2015); Kate Knibbs, 'What's a Facebook Shadow Profile, and Why should You Care?', *Digital Trends*, digitaltrends.com/social-media/what-exactly-is-a-facebook-shadow-profile/ (accessed July 14, 2015); David Veldt, 'Is LinkedIn the Creepiest Social Network?', *Gizmodo*, gizmodo.com/is-linkedin-the-creepiest-social-network-498946693 (accessed July 14, 2015); The Archive Team, 'Friendster Snapchot Collection,' *Internet Archive*, archive.org/details/archive-team-friendster (accessed July 14, 2015); Jamie Condliffe, 'Even if You Don't use Social Networks, they Still Know Stuff about You', *Gizmodo*, gizmodo.com/even-if-you-dont-use-social-networks-they-still-know-s-1643246882 (accessed July 14, 2015).

4 Jelle van Haaster, Rickey Gevers and Martijn Sprengers, *Cyber Guerilla* (Boston: *Syngress*, forthcoming 2016), chapter three.

5 'C2000 Masten in Nederland,' *c2000masten.nl/* (accessed February 27, 2016).

6 See for instance: 'Waar Staan De GSM En UMTS Masten in Nederland?', *gsmmasten.nl* (accessed February 27, 2016); 'Overzichts Kaart,' *adslcentrale.nl*, adslcentrale.nl/index.php?dynamic_content=kaartje (accessed February 27, 2016); 'Wijkcentrales', *Hulpvanstudenten.nl*, hulpvanstudenten.nl/wijkcentrales/ (accessed February 27, 2016); 'Infrastructuur', *Nederland ICT*, destaatvantelecom.nl/#infrastructuur (accessed February 27, 2016).

PHOTO ELECTROSPACES.BLOGSPOT.NL

Telephones in use in the Dutch parliament, mentioned in a blog; further on in the blog they are described in detail

Telephone calls and (spear-)phishing mails to key-players – or other types of social engineering – may be used to fill knowledge gaps. Since many military personnel list their occupation on social platforms, it is easy for an opponent to select certain individuals, such as privileged users (administrators), leaders, or users of specific weapons platforms to be targeted to obtain more detailed information about technical networks.

Shaping phase: unhinging the opponent

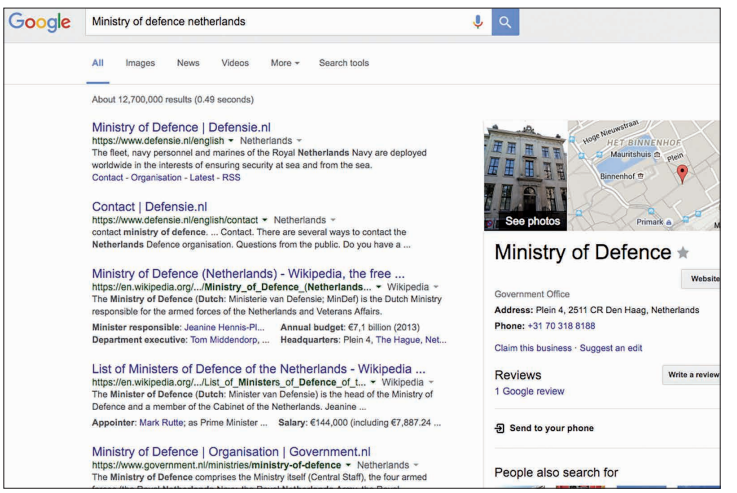
The information gathered will be used for preparing specific actions, which in our scenario will be undertaken from D-25 to D-5. The actions could be aimed at military entities directly or at civilian entities that render cascading effects on military capacity. We will focus on the latter. The activities aim to inhabit political and military decision-makers in adequately responding to actions at D-day through preventing (a) the possibility for claiming the right of (forceful) self-defence by remaining below the threshold of armed attack and (b) thwarting attribution attempts. The examples described below are merely a range of possible means and methods. Depending on the objectives, an opponent may choose to use these described activities or an entirely different set of capacities.

D-25: Political shock

At D-25, a media report creates a shock among political decision-makers. A message on a Darkweb forum claims that incriminating content has been downloaded from the parliamentary WiFi network. The media pick this up and urge the forum to disclose more detailed information. The forum's log files make clear that an iPhone on the parliamentary WiFi has been used to stream incriminating content. As a result, the media start to question press officers as to who watches this type of content during working hours. The lack of answers sparks speculation in traditional and social media.

From a technical perspective this type of action is made easy by the online information abundance. The types of phones used in the Dutch parliament are listed on a public blog and the project manager responsible for building the parliamentary WiFi is listed on another.[7] While

high-ranking officials are well protected, the project manager or contractor is not. His various social media profiles list intricate information about his preferences, social life, and relations, which may provide leverage or reveal possibilities to obtain it. Pressuring him to disclose information about the network yields the necessary insights into methods of manipulating the target phone via the network. Technology-wise it is relatively easy to perform and has been done before.[8] By conducting these kind of actions, political decision-makers are distracted from their actual jobs. Negative perceptions are easily created and difficult to eliminate. Although seemingly not a distinct military effect, it shifts the focus of military and non-military decision-makers to internal issues.



The current Google site listing for the query 'Ministry of Defence Netherlands.' This listing may change as a consequence of SEO methods

D-23: Google search results

Around D-23, Google's and other search engines' site listings regarding the conflict gradually change. Google's algorithms have replaced the websites at the top of the listing by a set of other websites. Everybody querying Google for keywords related to the conflict or 'Netherlands armed forces' is presented with new top-listed websites. While normally the official armed forces website is the top result, it has now been replaced by websites belonging to other organisations. These websites apparently offer an alternative view on news regarding the Dutch armed forces and issues regarding security and policy. By using professional-looking videos, images and reports these websites explain the different viewpoints on the conflict.[9] Although the content cannot be attributed to a specific party, the tone and wording suggest that the opponent is behind these websites.

These actions are made possible via a marketing technique called search engine optimization (SEO). After typing keywords, algorithms decide which websites are most relevant and calculate the position of websites in the listing. The purpose of SEO is to rank as high as possible in search engine listings. A website's relevance is ranked by using factors such as activity on page (e.g. reviews, reactions, interaction), site visits, returning visitors, and the bounce rate.[10] Companies specialized in SEO aim to optimize a website's ranking by offering reactions, clicks, likes, followers, fans and members for a website. Prices range from five dollars for automated actions to thousands of dollars for manually typed content.[11] The purpose of this action is to gain attention for the opponent's narrative and degrade the armed forces' ability to express their own

7 'Wifi-Netwerk,' *Tweede Kamer der Staten-Generaal*, jaarverslag2011.tweedekamer.nl/informatiseren/wifi-netwerk (accessed February 27, 2016); Gerard Weideveld, 'Draadloos Internet in De Tweede Kamer', gerardweideveld.nl/index.php?page=wifi (accessed February 27, 2016); 'The Phones of the Dutch Prime Minister,' *Electrospaces*, electrospaces.blogspot.nl/2014/11/the-phones-of-dutch-prime-minister.html (accessed February 27, 2016).

8 See for instance: Carolyn Thompson, 'Innocent Man Accused of Child Pornography After Neighbor Pirates His Wifi,' *The Associated Press*, huffingtonpost.com/2011/04/24/unsecured-wifi-child-pornography-innocent_n_852996.html (accessed February 28, 2016).

9 See for instance: ОКеям Нет, 'Я Русский Оккупант', youtube.com/watch?v=T65SwzHAbes (accessed February 27, 2016); ОКеям Нет, 'Россия Снова Агрессор', youtube.com/watch?v=JLesB4EQQrI (accessed February 27, 2016).

10 The bounce percentage is the percentage of visitors leaving the website shortly after arriving on the homepage.

11 See for instance: Fiverr, 'Results for 'Google Review'', fiverr.com/search/gigs?acmpl=1&sub_category=67&category=2&utf8=%E2%9C%93&search_in=category&source=guest-hp&locale=en&query=google+review&page=1&layout=auto (accessed February 27, 2016); Pro_girl, 'Viral Promotion to 5.000.000', *Fiverr*, fiverr.com/pro_girl/tweet-your-game-to-3-250-000-facebook-320k-twitter?context=advanced_search&context_type=rating&pos=4&funnel=8758f0c5-68f5-4a78-b6f6-cd8125734a82; (accessed February 27, 2016); *AudienceGain*, 'Social Media Marketing that really Works!', audiencegain.com/ (accessed February 27, 2016).

message. Google receives approximately 100 queries for 'Ministerie van Defensie' (Netherlands Ministry of Defence) a day.[12] By routing those visitors to other websites and presenting them with the alternative narrative, support for the Ministry of Defence may erode.

D-22: E-government services

The government-issued digital identity service (DigiD), used as authentication for Dutch governmental online services, suddenly goes off-line. It is hit by yet another distributed-denial of service (DDoS) attack, in which millions of devices (a Botnet) send void data to the servers, causing an overload.[13] Regular users cannot reach the DigiD website as it is struggling to handle all the void requests coming from the Botnet. The National Cyber Security Centre (NCSC) is notified and requested to help mitigate the DDoS attack. As the centre has been struggling to fill job vacancies and is committed to other cases, the NCSC advises the DigiD representative on hiring a company which specializes in DDoS-mitigation. By rerouting the void data to the servers of the specialized company the DDoS is warded off. The attack, however, has resulted in many people unable to access tax, social benefits, governmental invoicing and customs services.

Orchestrating a DDoS is cheap: with as little as five dollars for a couple of minutes up to 500 dollars for a month one can hire a Botnet and cause extensive damage. These costs are minimal compared to the financial and reputational damage caused by a DDoS attack. Apart from the primary damage caused by downtime, DDoS mitigation for large services can cost thousands of dollars a month and even more when hired on an ad hoc basis. Apart from that, the results of these actions may feed the sentiment that the government is not able to provide (online) security for its citizens. There are many examples of large-scale attacks aimed at similar systems, and DDoS attacks have been proven successful in crippling DigiD and other large networks.[14]

D-20: Spambots

Social networks users notice that messages pertaining to the conflict receive comments offering 'a more nuanced view on the conflict' – in fact, the narrative of the opponent. After posting a tweet with the hashtag #conflict a comment is posted from another account with a link to a *YouTube* video in which someone explains the underlying reasons for the conflict.[15] *Facebook* pages belonging to national and international press agencies and other social media have a similar experience. After having posted an item, a well written comment is uploaded offering a more nuanced perspective on the developments in the conflict. These comments are supplemented with video, images, and audio, all well designed and tailored to a specific platform.

Due to the vast amount of posts on social media, sending response messages to influence a target audience requires automated systems, for instance spambots (automated content distribution systems) or specialized units.[16] Using spambots to send content has certain disadvantages: messages will be generic and not

12 Google Trends, 'Explore: Ministerie Van Defensie + Defensie', Google Trends, google.com/trends/explore#q=Ministerie%20van%20Defensie%2C%20Defensie&cmpt=q&tz=Etc%2FGMT-1 (accessed February 28, 2016).

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

14 Brian Krebs, 'Six Nabbed for using LizardSquad Attack Tool', krebsonsecurity.com/tag/lizard-stresser/; Brian Donohue, 'How Much Does a Botnet Cost?', *Threatpost*, threatpost.com/how-much-does-botnet-cost-022813/77573/ (accessed December 25, 2015); William Turton, 'Lizard Squad's Xbox Live, PSN Attacks were a 'Marketing SCheme' for New DDoS Service', *The Daily Dot*, dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/ (accessed December 25, 2015).

15 Twitter uses hashtags (#) to categorise content, allowing users to quickly select their subject of choice and to position their own content within the various categories by adding a hashtag to their post.

16 Ukraine Today, 'Inside Kremlin Propaganda Machine: Russian Blogger Exposes Russia's Internet Troll Factory', youtube.com/watch?v=L5w3Ib1cyJM (accessed February 27, 2016); Dmitry Volchek and Daisy Sindelar, 'One Professional Russian Troll Tells All', *Radio Free Europe Radio Liberty*, rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html (accessed February 27, 2016); Kevin Morris, 'Russia's Spy Agency Invests $1 Million in Spam-Bot Army', *The Daily Dot*, dailydot.com/news/svr-spy-agency-storm-13-propaganda-bots/ (accessed February 27, 2016); '#ColumbianChemical Hoax: Trolling the Gulf Coast for Deceptive Patterns', Recorded Future, recordedfuture.com/columbianchemicals-hoax-analysis/ (accessed February 27, 2016); Adrian Chen, 'The Agency', *The New York Times*, nytimes.com/2015/06/07/magazine/the-agency.html?_r=0 (accessed February 27, 2016).

specifically tailored to a target group. Users and platform administrators are likely to notice large amounts of generic messages, which will result in these messages being deemed spam and possibly being blocked. Yet, the effect is countered by the sheer number of messages; if from hundreds of thousands messages only a small percentage makes it through human and logic spam filters, it still reaches many more people than manually achievable. Using specialised units to send messages – like the Russian Troll Factory, the British 77th brigade (the 'Facebook Warriors') or departments within intelligence agencies – is considerably more work than using Spambots, but these messages can be tailored to a specific target group or individual.[17] The purpose of such actions is to influence domestic or foreign societies as a whole or specific target groups within them. As many are online and have social media profiles, targeting these profiles with content expressing the opponent's narrative serves to highlight his cause and degrade support for others.[18]

D-18: Press hoax

Press agencies launch a report about the disconcerting state of our military materiel. The equipment is said to be faulty, not providing adequate safety to personnel, and unable of countering modern adversaries on the battlefield. It is unclear who has written the report, but it describes the failing state of the materiel in detail: helmets and vests lack bullet-resistant properties, weapons systems are prone to software errors and misfires and the latest GPS update has gone wrong. Various stakeholders respond by demanding answers why we send our soldiers to a conflict without adequate materiel. Soldiers express unease when they read coverage on the subject. Even though their superiors guarantee the adequacy of the equipment – emphasising the media's tendency for exaggeration – the thought lingers when they put on their helmets and vests.

The report in this case is, of course, forged by the opponent. The Dutch television show Rambam was able to prove that media outlets, when fed with newsworthy scoops, tend to go

The television show RamBam was able to get a foothold in the media with various fake press releases

for rapid publication instead of time-consuming fact checking. It did so by manipulating news sources via fake press releases citing fictional persons and research.[19] The lack of fact checking and verification opens a window for anyone wishing to influence target groups via the (conventional) press by simply drafting a press release and forging supplementary materials (e.g. a report or website). The purpose of this activity here is to degrade the confidence soldiers have in their equipment and to reduce their trust in their military and political leadership. As it is distributed through domestic media channels, the message seems more credible than foreign news sources.

D-15: GPS spoofing and jamming

Several days later, devices using GPS (e.g. smartphones, tablets, cars, planes) in the vicinity of Schiphol International Airport are showing positions that are off by miles. In

17 '77th Brigade', *British Army*, army.mod.uk/structure/39492.aspx (accessed February 27, 2016); Glenn Greenwald and Andrew Fishman, 'Controversial GCHQ Unit Engaged in Domestic Law Enforcement, Online Propaganda, Psychology Research', theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/ (accessed February 27, 2016).

18 See for a general overview of non-kinetic targeting capabilities Paul Ducheine, *Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting*, in: P. Ducheine, M. Schmitt and F. Osinga (eds), *Targeting: The Challenges of Modern Warfare* (The Hague, Springer, 2015).

19 'Rambam: Persberichten', *NPO*, npo.nl/rambam/05-03-2012/VARA_101280224 (accessed February 27, 2016).

SOURCE: HTTP://WWW.THEGUARDIAN.COM/UK/AL-SWEADY-INQUIRY

One of the images used in the Al Sweady allegations and resulting inquiry, which lead the armed forces to produce a 24 million pound report regarding the incident in 2009

subsequent days, other military and civilian airports are hit by similar GPS malfunctions. All air traffic is halted in order to get to the bottom of the GPS anomaly, as it is unclear whether the error is external (spoofing)[20] or internal (e.g. software failure). The aviation authority is alerted and conducts an investigation. It finds that someone is probably spoofing GPS signals around airports, but they do not have definitive answers and advocate caution.

GPS spoofing has been around for decades in the domain of military electronic warfare (EW), yet in recent years it has regained attention.[21] As GPS has become commonplace, the potential effects of manipulating it increase. The knowledge and material needed to spoof GPS signals proliferate, increasing the likelihood of such an action. Jamming and spoofing devices are available from as little as 100 dollars up to 20,000 dollars for more sophisticated versions.[22] There are cases where GPS-jamming has been used in the vicinity of an airport to disrupt systems and this will probably happen more often in the future.[23] Although many soldiers believe that the military GPS system is more robust than its civilian counterpart, it is prone to many similar weaknesses.

The first apparent effect of spoofing GPS is financial damage. Planes are grounded and many man-hours are committed to investigate the cause. In one case in the United States, it took the Federal Aviation Authority two years to locate a GPS jammer.[24] A less apparent effect, though with much more impact, is the distrust in the construct of the GPS system. GPS is perceived as a robust, faultless system on which we rely many times a day. The goal of the opponent is to weaken our trust in this system, also creating doubt with regard to its military use. The impact of not being able to rely on GPS will most likely have major consequences for the armed forces' overall effectiveness.

D-9: Victim blog

At D-9, a WordPress blog appears online in which a man claims to be tortured by Dutch troops in Afghanistan. He indicates that he will use the blog to release information about his torture and does not seek redress; he merely wants to share his story. As the blog gains momentum, more and more visitors read his story and speak out against the atrocities. The level of detail in the blogs attracts even more visitors who in turn share it on different social networks. Within a couple of days the number of blog visitors has skyrocketed and conventional media pick up on the story. As the Ministry of Defence lacks the proper tools to monitor online activities and sentiment, its communications directorate is only alerted when conventional media start covering the story. As they are trying hard to verify the allegations, soldiers are questioned on- and offline by their social network whether these practices are common in the Dutch military.

20 Spoofing is generating customised (often erroneous) information in order to fool a system, for instance by forging GPS packets listing a different location that the legitimate GPS packets.

21 Tyler Nighswander et al., 'GPS Software Attacks' (Raleigh, ACM, October 16-18, 2012).

22 'New Products', *Jammer4u.co.uk*, jammer4uk.com/contact-ezp-13.html (accessed March 15, 2016); 'GPS Jammers', *JammerfromChina*, jammerfromchina.com/categories/GPS_Jammers/?price_min=13980&price_max=17463&sort.

23 Glen Gibbons, 'FCC Fines Operator of GPS Jammer that Affected Newark Airport GBAS', *Engineering Solutions from the Global Navigation Satellite System Community*, insidegnss.com/node/3676 (accessed February 28, 2016).

24 Ibid.

Social media tend to pick-up on stories regarding, amongst others, (social) injustice. Sharing the story is seen as expressing sympathy towards the victim. As such, a blog tailored to invoke these feelings among readers is likely to be read and shared. It is very difficult for a large organisation to debunk allegations in due time. Often verification and formulation of an official comment takes time; the damage is done well before the Ministry is able to respond. In the case of British troops being falsely accused of murdering, torturing and mistreating Iraqis in 2004 for instance, the armed forces produced a 24 million pound report regarding the case in 2009.[25] The cost of creating the blog is virtually non-existent compared to efforts required to refute a story. By creating such blogs, negative sentiment towards the armed forces can be created, mobilised, or increased among domestic and international audiences.

D-7: Targeting relatives

Starting at D-7, the soldier's friends and family receive alarming messages. Spouses, boyfriends, girlfriends, sons, and daughters all receive messages, some via e-mail, others via WhatsApp. These messages ask questions about the motivations of their relatives to be in the torturous, ill-equipped military and tell them to urge their relatives to discontinue any military activity. If disregarded, the message reads, harm will come to them or their loved ones.

As the opponent has mapped the armed forces and the social network of soldiers, he can use it for manipulation. One way is to send direct messages to the soldier's relatives via different media. These activities involve considerable planning, sophisticated data mining techniques, man power and tools for content distribution, yet are feasible, especially when supported by state actors. The purpose of this type of action is to unsettle soldiers through their family and friends. Although many soldiers have accepted the fact that they can be subjected to risks, their relatives have not necessarily come to grips with that reality. By targeting and unsettling his home environment the soldier may be distracted from his core business, reducing his effectiveness.

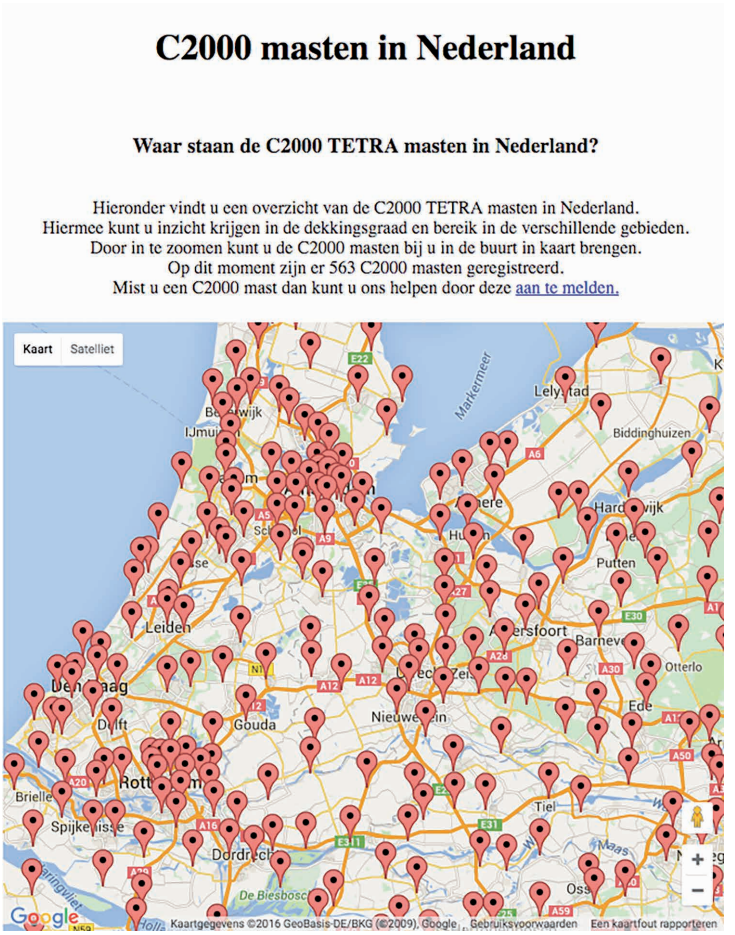
Image of an area point of presence, used for aggregating thousands of Internet connections whilst being protected with a simple lock

Intensification phase: tipping the balance

The aforementioned activities remain well below the threshold of an armed attack and most of them may be conducted from outside the target nation's territory. They are aimed at unhinging the security ecosystems, yet are probably not sufficient to tip them over. In the remaining five days to D-day, the actions are combined with physical activities, performed

Although many soldiers have accepted the fact that they can be subjected to risks, their relatives have not necessarily come to grips with that reality

25 'Al-Sweady Inquiry: Iraqis Mistreated but UK Troops did Not Murder Insurgents', *The Guardian* (accessed February 28, 2016), theguardian.com/uk-news/2014/dec/17/al-sweady-inquiry-uk-troops-mistreated-iraqi-prisoners-not-murder.



C2000MASTEN.NL

A private website lists the C2000 mast locations in detail, even though official registers do not mention them for security reasons

by proxy forces such as the 'Little Green Men' in Crimea. These activities have in common with the actions of the shaping phase that they are not aimed at military forces directly, but at vital processes needed to support security force responses. During the intensification phase vital communication systems will be targeted in order to degrade coordination and synchronisation. We will briefly list some possible activities.

D-5: Sabotaging aggregation points

Most communication depends on Internet access, even many modern telephone services rely on Voice over IP (VoIP), using the Internet or other IP-networks to transport voice. Sabotaging critical network components such as aggregation points or data centers may serve to disable Internet traffic locally, regionally or nationally. The inconspicuous small buildings that house such points are often secured with simple digital locks which are no match for agents with military hardware. Once inside, network traffic can be selectively denied or fully shut down. Sabotaging only two or three aggregation points in The Hague – the locations are identified in the preparation phase – would affect several Ministries, including Defence and Security & Justice. Destroying network infrastructure will prevent governmental decision-makers, military and non-military, from effectively coordinating countermeasures.

D-3: Sabotaging C2000

Similar possibilities exist for disabling the emergency response communications network C2000, which, among others, is used by police, firefighters, ambulances, customs, military police, guard services of military bases, and intelligence services. Although the network is redundant to some extent, the physical protection of the masts – a single fence – is limited. Once over the fence, a cable can be cut that runs openly from top to bottom. Concentrating on the Western, most urbanized part of the Netherlands, populated by more than 7 million people and home of the Dutch Parliament, the biggest port of Europe and Schiphol International Airport, a small team of 20 proxy forces could easily disable the 150-200 masts overnight. While the network design anticipates power failures – an emergency battery can provide up to four hours of power – there is no fail-safe for cut cables. The six mobile backup masts would be rendered completely useless given their range limitations. Since both voice and data communication rely on the system, there is no other alternative than using cell phones, severely hampering coordination.

D-1: 'Coup de grâce'

Depending on the effectiveness of earlier activities, a *coup de grâce* may be necessary to

26 The AMS-IX is one of the biggest aggregation points on the Internet and responsible for exchanging data between Internet Service Providers (ISPs) and other businesses.

make the disarray complete. Focussing on vital infrastructure, the options are numerous, yet when balancing effectiveness and feasibility, two stand out: the Amsterdam Internet Exchange (AMS-IX) and high-voltage electricity stations. Security measures for both are not designed with military-trained agents in mind. Unplugging the AMS-IX, one of the largest Internet exchange points, will at a minimum leave large parts of Western Europe with a degraded Internet connection.[26] Similarly, sabotaging a high-voltage electricity station will disrupt many services and facilities. On March 27, 2015, a technical malfunction in a power station in Diemen resulted in a series of effects in most of the provincies of North Holland and Flevoland: A loss of utilities such as electricity for businesses and private homes, hot water and heating, cancellations of air traffic, stand-still of public transport, traffic jams, and local Internet failure.

Conclusion

Within the information environment, the use of both physical and non-physical actions can be highly useful in affecting an adversary's perception and his ability to respond appropriately. Transparency and connectivity are valuable assets in modern society, yet at the same time they offer unique vulnerabilities to exploit, increasing our so-called 'attack surface'. Actions do not necessarily have to be aimed directly at the components of military power to have a cascading effect on them. This indirect approach has multiple advantages for the attacker: problems in attribution may confuse and delay decision-makers, keeping actions below the threshold of an armed attack and exploiting fault lines in responsibilities hampers response mechanisms, and it is relatively simple and cheap compared to the results that are attainable. Low-scale, non-traditional means and methods (in the information environment) may have a significant impact on operational readiness and responsiveness of military forces. Creating decision-maker overload, undermining the credibility of military forces, instilling doubts as to purpose and capacity, and hampering effective communications, all contribute to eroding fighting power. When faced with all these activities and effects, how effective will our forces be on D-day?

Bear in mind that the examples we have used are at the low-end of sophistication and relatively easy, cheap, and accessible. Combining them with higher-end cyber activity, such as hacking into military or civilian operating systems of vital infrastructure, would render exponential results. Not to speak of integrating regular and irregular military activity for destructive effects.

Perhaps we should stop thinking in terms of D-days and lines of departure at all

This article is not an appeal to stop thinking in terms of regular combat operations, but a plea to stop doing so exclusively. At the outset of our exercises we commonly kick off with our full military potential, everything prepared and ready to go. But how realistic is that? Chances are that our military fighting power has already been degraded by the opponent well before any D-day or line of departure. Because shaping operations in the information environment may be conducted continuously, perhaps we should stop thinking in terms of D-days and lines of departure at all. ■