Cyber Warfare:
Critical Perspectives

Ministerie van Defensie

NL ARMS

Netherlands Annual Review of
Military Studies 2012

Cyber Warfare:
Critical Perspectives

Paul Ducheine, Frans Osinga, Joseph Soeters (eds.)

The Faculty of Military Sciences is part of the Netherlands Defence Academy.
This publication contributes to the faculty's academic Research Plan.

The views expressed in this publication are those of the authors and do not necessarily reflect the views of the Minister of Defence.

Word cloud: Jelle van Haaster
Cover and lay-out: Oasis Productions
Printed by: Wõhrmann Print Service

ISBN: 978 90 6704 341 0
NUR: 828

www.asserpress.nl

Foreword

It is an excellent tradition of the Faculty of Military Sciences of the Netherlands Defence Academy to publish the Netherlands Annual Review of Military Studies. NL ARMS shows the state of affairs of scientific research in military sciences and, moreover, the extent to which researchers of the Academy contribute to this corpus of knowledge. This year researchers of the Faculty of Military Sciences focus on current research in the cyber domain.

The Netherlands Ministry of Defence has, in line with other Dutch ministries, formulated a policy to intensify activities in the realm of cyber security and cyber warfare. It is the intention of the Ministry of Defence to dedicate in the coming years, and to an increasing extent, means to address issues of the cyber security of systems, and the role of cyber in warfare (both cyber warfare itself and the role of cyber in kinetic warfare).

In line with this policy the Faculty of Military Sciences is formulating a multidisciplinary research program in this field in order to scientifically support these efforts, of course in cooperation with other research institutes. This new research program will, in any case, entail research efforts in the field of legal and operational aspects of cyber warfare, but will also combine technical and non-technical aspects of cyber warfare.

The current issue of NL ARMS comprises the building blocks of this new research program. One finds in this publication reports of research activities of staff of the Faculty of Military Sciences related to aspects of cyber security and warfare.

Wouter van Rossum

Dean of the Faculty of Military Sciences
Netherlands Defence Academy

Table of Contents

FIVE

Towards a Legal Framework for Military Cyber Operations*

Paul Ducheine, Joop Voetelink, Jan Stinissen & Terry Gill

Contents

* In the preparation of this chapter, the authors used the article by P.A.L. Ducheine and J.E.D. Voetelink (2011), 'Cyberoperaties: naar een juridisch raamwerk', originally published in 180 *Militaire Spectator*, No. 6, p. 273-286. The authors are grateful to the publishers of the *Militaire Spectator* for their kind permission to use portions of that article in this contribution.

P. Ducheine, F. Osinga and J. Soeters (eds.), Cyber Warfare: Critical Perspectives
© 2012 T.M.C. Asser Press and Contributors

1. Introduction

1.1 *Attacks and War?*

Wikileaks' publication of US diplomatic cables in November 2010[1] was characterised by the US Government as 'an attack on America's foreign policy interests [and] an attack on the international community'.[2] A former policy advisor to the Canadian prime minister advocated the idea of the killing of WikiLeaks' founder, Julian Assange, as an act of 'defence' against the 'attack'.[3] Arguably, WikiLeaks' publication merely qualified a digital information campaign, which was, nevertheless, portrayed as 'attack'. Are we dealing with mere rhetoric, and should we consider this line of reasoning merely demagogic, or are we indeed witnessing 'attacks'? If so, are these 'attacks' isolated incidents? Apparently, they aren't, as the following examples demonstrate.

On the eve of the publication of the diplomatic communication, *Wiki Leaks.org* reported that its website suffered from a cyber attack through a so called *Distributed Denial of Service* (DDoS).[4] In response, WikiLeaks followers launched attacks against financial companies that appeared to be

[1] See <wikileaks.org/cablegate.html>, for an overview: <www.cablegatesearch.net/> (Accessed 4 April 2012).

[2] US Secretary of State, 'Remarks to the Press on the Release of Confidential Documents', 28 November 2010, <www.state.gov/secretary/rm/2010/11/152078.htm>.

[3] CBC News, 1 December 2010, 'Flanagan Regrets WikiLeaks Assassination Remark', <www.cbc.ca/politics/story/2010/12/01/flanagan-wikileaks-assange.html> (Accessed 9 December 2010).

[4] *NRC Handelsblad* 28 October 2010, 'WikiLeaks: slachtoffer van cyberaanval'. BBC News, 28 November 2010, 'Wikileaks Hacked ahead of Secret US Document Release', <www.bbc.co.uk/news/world-us-canada-11858637> (Accessed 5 April 2012).

non-supportive to WikiLeaks.[5] The battlefield also extended to the Netherlands when the website of the Public Prosecutor was brought down after the arrest of a Dutch hacker.[6] These activists' attacks back and forth are part of a wider and worldwide development in international relations, economic competition, espionage, crime and last but not least military innovation.

Iran suffered from a cyber attack through the infamous computer worm *Stuxnet* in September 2010,[7] allegedly ordered by the US President,[8] and apparently aiming to disrupt Iran's nuclear program.[9] Other and older illustrations are the cyber attacks against Estonia[10] and Georgia,[11] as well as the less well known explosion in the Siberian oil pipeline in 1982, presumably caused by the CIA that manipulated software that Russia had stolen from Canada.[12] More recently, the use of cyber weapons was considered a viable option against Libya by the US, however, this was not followed through for reasons of future international political and military consequences, as it might set a precedent to be followed by other States (or non-State actors).[13]

[5] *NRC Handelsblad* 8 December 2010, 'Duizend sites kopiëren alles van WikiLeaks'; BBC News 9 December 2010, 'Anonymous Hacktivists Say Wikileaks War to Continue', <www.bbc.com/news/technology-11935539> (Accessed 5 April 2012).

[6] *Volkskrant* 10 December 2010, 'Website OM plat na arrestatie hacker', <www.volkskrant.nl/vk/nl/3884/WikiLeaks/article/detail/1070943/2010/12/10/Website-OM-plat-na-arrestatie-hacker.dhtml> (Assessed 10 December 2010).

[7] *NRC Handelsblad* 27 September 2010, 'Iran: cyberaanval met computerworm afgewend'; *New York Times* 26 September 2010, 'A Silent Attack, but Not a Subtle One', <www.nytimes.com/2010/09/27/technology/27virus.html?_r=1&adxnnl=1&adxnnlx=1333648101-ftcOsY2tnApxgNOA3oJAtg#> (Accessed 5 April 2012).

[8] David E. Sanger, 'Obama Order Sped up Wave of Cyberattacks against Iran', *New York Times*, June 1, 2012, <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&hp> (Accessed 2 June 2012).

[9] *NRC Handelsblad* 16 November 2010, 'Kernreactors Iran mogelijk doelwit Stux net-worm', <beta.nrc.nl/nieuws/2010/11/16/kernreactors-iran-doelwit-stuxnet-worm /> (Accessed 9 December 2010); *New York Times*, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', 15 January 2011, <www.nytimes.com/2011/01/16/world/middle east/16stuxnet.html> (Accessed 19 January 2011).

[10] Brenner 2009, p. 3-6.

[11] Korns and Kastenberg 2009, p. 60; Tikk, Kaska and Vihul 2010.

[12] See Chapter 4 in this volume (Thomas Rid). Also: *The Economist*, 1 July 2010, 'Cyberwar: War in the Fifth Domain', <www.economist.com/node/16478792?story_id=16478792&fsrc=rss>. See also Rid 2012, p. 10.

[13] *New York Times*, 17 October 2011, 'U.S. Debated Cyberwarfare in Attack Plan on Libya', <www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html> (Accessed 5 April 2012). As a public initiative, the Cyber Security Forum Initiative provided an overview of Libyan cyber capabilities and vulnerabilities:

1.2 *Cyber Security in the Netherlands*

Cyber operations, often referred to as the 'fifth domain' of warfare, have reached the top of the political and military agenda in the Netherlands, as they have elsewhere.[14] The Dutch Parliament urged the Government to set up an interdepartmental cyber security strategy and to initiate constructive contributions in the realm of cyber warfare within NATO, to which Government responded.[15] First of all, the Dutch Government delivered its *National Cyber Security Strategy* (NCSS) to parliament in February 2011.[16] Subsequently, the Cyber Security Council, co-chaired by a public and a private executive, was established in June 2011.[17] Most recently, the Governmental Cyber Emergency Response Team (GovCERT) was integrated into the newly set up National Cyber Security Centre (NCSC), a public-private interagency effort to concentrate knowledge and expertise.[18] The NCSC was immediately involved in the aftermath of the DigiNotar incident (in which a private cyber firm had failed to adequately protect digital signatures with which it had been entrusted).[19]

Unmistakably, the developments in the cyber domain and the increasing awareness of potential and actual cyber threats and developments in cyber warfare are also of importance to the Netherlands Armed Forces and the Netherlands Ministry of Defence (MoD), as they relate to threats on the one hand, and to (active or passive) protection against these threats and attacks on the other. By concluding that 'the response capabilities in the cyber realm will be enhanced, *inter alia* within the MoD, the Government

CSFI, *Project Cyber Dawn v1.0 – Libya*, (April 17, 2012) <www.unveillance.com/latest-news/project-cyber-dawn-libya-released-for-public-viewing/> (Accessed 5 April 2012).

[14] Fifth domain aside land, water, air and space. See Tettero and De Graaf 2010. See also Bosch, Luiijf and Mollema 1999.

[15] Motion filed by R. Knops c.s., *Parliamentary Papers* [Kamerstukken] II, 2009/10, 32 123 X, No. 66. Progress in 32 123 X, No. 89; 26 643, No. 149 and 164. See also the motion filed by M. Hernandez, *Parliamentary Papers* II, 2010/11, 32 500X, No. 76.

[16] *Parliamentary Papers* II, 2010/11, 26 643, No. 174.

[17] 'Cyber Security Council Invested' (30 June 2011), <english.nctb.nl/current_topics/press_releases/2011/press-release-110630.aspx?cp=92&cs=25472> (Accessed 12 April 2012).

[18] 'National Cyber Security Centre (NCSC) Combines Knowledge and Expertise' (2 January 2012), <english.nctb.nl/current_topics/press_releases/2012/press_release-120112.aspx?cp=92&cs=25472> (Accessed 2 January 2012).

[19] BBC News, 5 September 2011, Fake DigiNotar web certificate risk to Iranians, <www.bbc.com/news/technology-14789763> (Accessed: 7 April 2011). See the dossier (in Dutch) at: <www.govcert.nl/dienstverlening/Kennis+en+publicaties/dossier-diginotar>.

indicated a general policy related to the strategic decision-making process within the MoD.[20] The Minister of Defence is to launch a Defence Cyber Strategy encompassing 'cyber intensifications'.[21] In his Defence White Paper *Defence after the Financial Crisis*, he already stated that 'the MoD will reinforce its digital resilience in the years to come, and will develop the capacity to execute cyber operations'.[22] Simultaneously, a strategic framework for cyber operations has to be developed, as was rightfully advocated by Tettero and De Graaf.[23] The need for such a strategy was also pointed out in the British study by Chatham House, *On Cyber Warfare,* which indicated that the lack of a strategy for cyber operations could serve as a catalyst for hostile cyber operations.[24] In addition, it was fully recognised that such a strategy would have to contain a legal framework as well.[25] Parts of this framework for cyber security in general were presented in December 2011,[26] whilst the Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law were requested to advice on legal questions of cyber warfare. The joint advice *Cyber Warfare* was delivered in December 2011,[27] and Government appears to endorse most of its conclusions and advice.[28]

Advancing on the foundation provided in the Defence Cyber Strategy, including its indicated legal framework for military cyber operations, this chapter strives to stimulate thoughts and analysis and provide some guidelines for further development. Firstly, some issues related to the strategic context that are relevant to the legal framework will be introduced. Secondly, the conceptual legal framework itself will be presented. Thirdly, the legal bases for the conduct of cyber operations will be reviewed, and finally, the legal regimes that apply during the execution phase of these operations will be examined.

[20] *Parliamentary Papers* II, 2010/11, 26 643, No. 174.

[21] *Parliamentary Papers* II, 2010/11, 26 643, No. 174.

[22] *Parliamentary Papers* II, 2010/11, 32 733, No. 1, p. 19: 'Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld', 8 April 2011.

[23] Tettero and De Graaf 2010.

[24] Cornisch 2010, p. 21-22.

[25] Tettero and De Graaf 2010, p. 247.

[26] *Parliamentary Papers* II, 2011/12, 26 643, No. 220 (annex): 'Juridisch kader cyber security'.

[27] AIV and CAVV 2011, see <www.aiv-advice.nl>.

[28] *Parliamentary Papers* II, 2010/11, 33 000 X, No. 79, annex, 6 April 2012.

2. The Strategic Context

The Dutch target for its National Cyber Security Strategy is rather challenging, as cyber security has various characteristics, of which nine are particularly relevant in the legal realm. First, the features of threats will be addressed, followed by remarks associated with the protection against and response to these threats. Next, attributes of the cyber battlefield that influence both attacking and defending parties will be examined and finally the strategic and constitutional embedding of military cyber operations will be discussed.

2.1 *Threats*

Cyber threats are of a very diverse nature, since they encompass (a combination of) ideological, criminal, financial, political, economic, cultural and military infringement on national and international security.[29] Alongside States, a great diversity of non-State actors are the sources of these threats, including, amongst others, criminals, pressure groups, terrorists, rebels, commercial enterprises (including private intelligence services) and, last but not least, hackers and activists (and the combination of the latter two: 'hacktivists'). Moreover, cyber threats may be overt as well as covert, the latter being the rule and as a result of that, attribution is one of the main obstacles before an adequate response to these threats becomes possible.

2.2 *Protection and Response*

Given the plurality of threats and its authors, the envisioned cyber security strategy logically embraces several policy areas and includes both public and private actors,[30] and is therefore comprehensive. Thus, cyber security calls for a comprehensive (multidisciplinary and interdepartmental) and interagency approach.[31] Given the characteristics of the threats as well as the 'battlefield' (see below), governments alone are incapable of responding adequately as they are heavily dependent upon private partners such as internet providers. Therefore, public-private partnership is required, and this feature is demonstrated by the public-private co-chair of the Cyber

[29] Tettero and De Graaf 2010, p. 242.

[30] Tettero and De Graaf 2010, p. 242.

[31] Demonstrated by the fact that the *Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010* was signed by three ministers (Security & Justice; Economic Affairs, Agriculture & Innovation; and Defence). See *Parliamentary Papers* II 2010/11, 28 684, No. 292 (Annex).

Security Council,[32] as well as in the 'information knots' within the National Infrastructure for the fight against Cyber Crime (NICC) program.[33] Moreover, an international effort in cyber security is imperative as the World Wide Web and digital communication are an intrinsic part of globalisation and the fading of (physical) boundaries.

2.3 *The Virtual Battlefield*

The virtual battlefield affects both one's own as well as cyber operations conducted by (potential) opponents. Although digital communication relies on physical infrastructure located within sovereign states, cyber communication is hardly hampered by physical and sovereign boundaries as it is a virtual domain, albeit with physical components located in states.[34] Some states are particularly vulnerable as they host so called internet hubs that are crucial to the structure of internet.[35] Furthermore, cyber operations can involve non-kinetic methods of warfare, notwithstanding their potential of causing (severe) physical consequences.

Apart from these features, two other are of relevance for the Defence Cyber Strategy: the strategic framework and the constitutional objectives of the Netherlands Armed Forces.

2.4 *The Strategic Framework?*

Logically, the NCSS should fit within the framework of a comprehensive national security strategy including both an international and a national dimension. Such a Grand Strategy is at present non-existent in an explicit format in the Netherlands. Instead, the Netherlands has only developed its *National Security Strategy*, which has a primarily domestic focus.[36] This 'national' strategy is just a partial one, since it only refers to five vital national interests,[37] thereby erroneously omitting the sixth vital interest, i.e. the 'international legal order'.[38] Given the constitutional duty vested upon Government 'to promote the international legal order',[39] the

[32] Co-chaired by the National Coordinator for Counterterrorism and Security, E. Akerboom, and the CEO of Royal KPN, E. Blok.

[33] *Parliamentary Papers* II, 2009/10, 30 821, No. 10, p. 3-4.

[34] See for the example: Haaster 2012.

[35] The Amsterdam Internet Exchange is one of the main hubs in the world, see i.a. <en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size>.

[36] *Nationale Veiligheidsstrategie,* see *Parliamentary Papers* II 2006/07, 30 821, No. 1.

[37] Territorial, physical, ecologic, economic security, and political & social stability. Ref: footnote 36.

[38] Ducheine 2008, p. 20.

[39] See Art. 90 of the Netherlands Constitution which reads: 'The Government shall promote the development of the international legal order.'

non-existence of a Grand Strategy and the domestic focus of the National Security Strategy seem curious, as 'the Netherlands undoubtedly has a significant interest in promoting international security and cooperation'.[40]

Moreover, considering the international components of the other vital interests (i.e. economic security, and the political and social stability) as well as being the sixteenth largest economy and the ninth export nation worldwide,[41] the international legal order is one of the prerequisites for the other vital interests and can therefore not be neglected.

This gap in the Netherlands strategic framework could potentially leave the door open for hostile cyber operations.[42] Recent events in North Africa and the Middle East have demonstrated the effects of social and digital media upon political stability and international (legal) order.

Nevertheless, the MoD will have to develop its Defence Cyber Strategy, which ought to be drawn for the NCSS and the National Security Strategy. As shown in Figure 1, the deficiency caused by the non-existent Grand Strategy could hamper the development of a comprehensive and effective Defence Cyber Strategy.

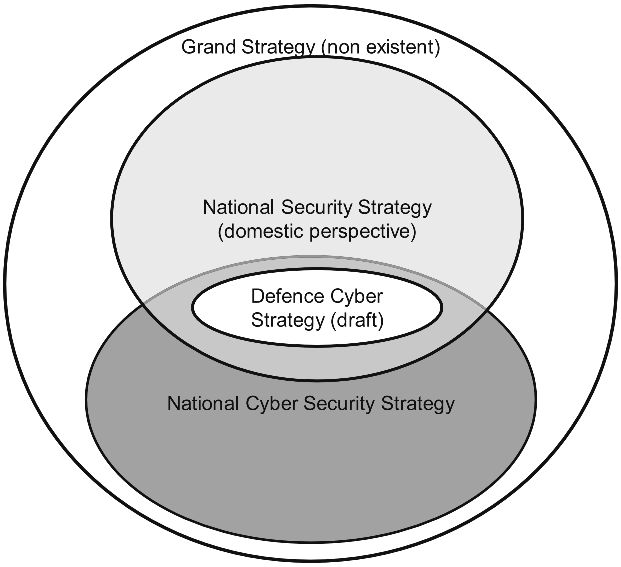
Grand Strategy (non existent)
National Security Strategy (domestic perspective)
Defence Cyber Strategy (draft)
National Cyber Security Strategy

Figure 1. Strategic framework

[40] *NRC Handelsblad*, Commentaar, 8 April 2011.

[41] *NRC Handelsblad*, Commentaar, 8 April 2011.

[42] Cornish et al. 2010, p. 21-22.

2.5 *Constitutional Embedding: Which Operations?*

The Defence Cyber Strategy will be guided by (*inter alia*) the triple objectives of the armed forces as provided in Article 97(1) of the Dutch Constitution:

> There shall be armed forces for [1] the defence and [3] protection of the [other vital] interests of the Kingdom, and [2] in order to maintain and promote the international legal order.

This triple objective implies that the MoD and the armed forces are to execute cyber operations as part of their three main tasks,[43] and consequently, that military cyber operations will be part of the widest spectrum available, ranging from military defence of the territory [1] and missions abroad [2], to domestic support for national civil authorities for law enforcement purposes [3], as well as for intelligence gathering. Therefore, these operations may be passive/defensive as well as active/offensive and will logically also encompass digital (counter) intelligence operations, as well as domestic and international operations in which the armed forces are involved.[44]

It is therefore advocated by the present authors, that military cyber operations should be extensively defined as they refer to (military) *operations in the digital domain, including offensive, defensive, passive and active activities as well as intelligence operations, domestically and abroad.*[45]

3. Military Legal Framework

Considering the aforementioned strategic context, and the characteristics and the constitutional framework for military operations, a design of the legal framework *in militaribus* will be presented below. The framework consists of two constituents: the legal bases for military cyber operations, and the legal regimes applicable to the execution of those operations. Before embarking upon the two components, it is necessary to address another conceptual element first, namely the appropriate paradigm for the conduct of cyber operations.

[43] Ducheine 2012.

[44] Tettero and De Graaf 2010, p. 241.

[45] Ducheine and Voetelink 2011, p. 277.

3.1 *Which Paradigm?*

It is vital to realise that cyber security in general, and cyber operations in particular fit into a wide range of paradigms ranging from (internet) governance to warfare. In our view, six paradigms are of relevance to military cyber operations:

- (ICT-)governance;
- protection & security;
- intelligence;
- law enforcement;
- crisis response operations;
- war.

Each of the paradigms provides the purpose, the perspectives, and the doctrine underlying specific types of cyber operations. By analogy, counter terrorism operations can be conducted within the paradigm of law enforcement (i.e. regular police operations), but exceptionally also as war (e.g., Enduring Freedom).[46] Applying this approach to cyber operations, it follows that military operations related to international crisis management and armed conflict would be based on military principles and doctrine, including where relevant, the international legal framework for the use of force, and would be governed by the law of armed conflict (LOAC or international humanitarian law), and executed by applying military manuals and doctrines.

However, again by analogy, counter terrorism should not be viewed exclusively as either war or law enforcement, instead it should employ and be part of a multidisciplinary comprehensive approach.[47] It is also realistic to conclude that a single minded restrictive approach doesn't readily fit cyber operations either.

Instead, one should realise that cyber operations are part of a fluid spectrum ranging from the monitoring of governmental networks by CERTs, to active protection by shutting down sites once they are under 'attack', followed by criminal investigations into the source of the 'attacks' where criminal activity was reasonably suspected, combined with intelligence operations to *inter alia* ascertain the nature of the threat posed and identify the source of the threat, possibly resulting in a military response in situations which rose to the level of a use of armed force by a foreign

[46] Ducheine 2008, p. 45.

[47] Ducheine 2008, p. 559.

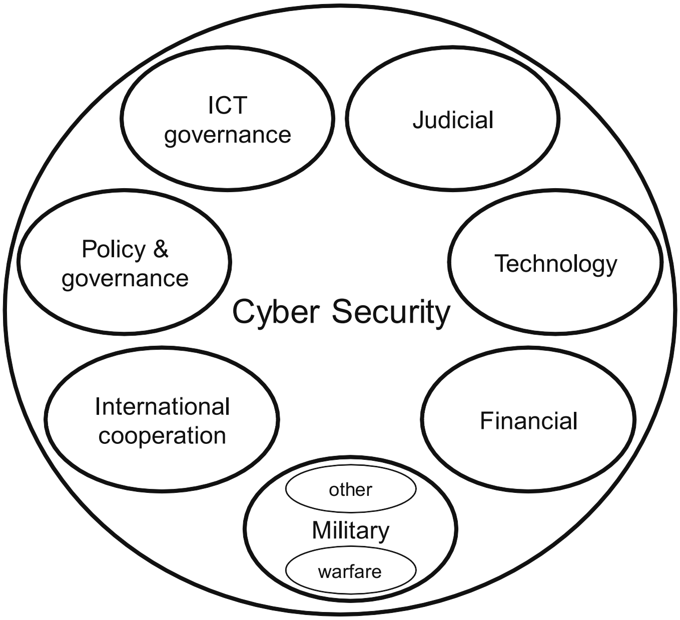

Figure 2. A multidisciplinary and comprehensive response to cyber threats

power or organised armed group, even resulting, in exceptional cases, in participation in an armed conflict. In addition, it is clear that concepts as human rights, privacy and ICT regulations & governance would play a role throughout the whole spectrum. Moreover, although the present chapter and publication are written from a military professional perspective, it should also be made clear that only those operations conducted or supported by armed forces that amount to 'warfare' in the strict sense, only fit as 'cyber warfare', and, even more important, that most cyber security responses will be civil and therefore non-military, as is characterised in Figure 2.

Therefore, it is advocated that an integral or complementary attitude is required, implying that cyber operations can potentially fit into multiple paradigms, and that the constituent parts of the legal framework, instead of a particular paradigm will be defining the outcome.

3.2 *Legal Bases and Regimes*

The legal framework itself comprises two distinct constituent parts: legal bases and legal regimes.[48] As in any other military operation, an 'adequate'

[48] See also Koninklijke Landmacht 2009, p. 42, Para. 2702; Ducheine and Pouw 2012a and 2012b.

legal basis is required before it is decided upon and undertaken. Legal bases can be found in international law (*ius ad bellum*), for instance, in the form of an authorisation by the UN Security Council, or in domestic national law for operations which were wholly conducted within the national legal framework(such as the Act on Intelligence and Security Services 2002). The second part of the framework, legal regimes, refers to those rules that are applicable once an operation commences. One could think of the law of armed conflict (hereafter: LOAC), human rights law, and criminal codes. Although they can't be considered 'law', for the purpose of this chapter, operational and political guidelines governing the use of force, known as Rules of Engagement (ROE), national caveats, or Tactical Directives et al will also be addressed under the header of 'legal regimes'.

Both constituent parts – legal bases and legal regimes – make up the legal framework for military cyber operations, covering the whole spectrum of (pro-)active, passive, offensive and defensive cyber operations (see Figure 3).

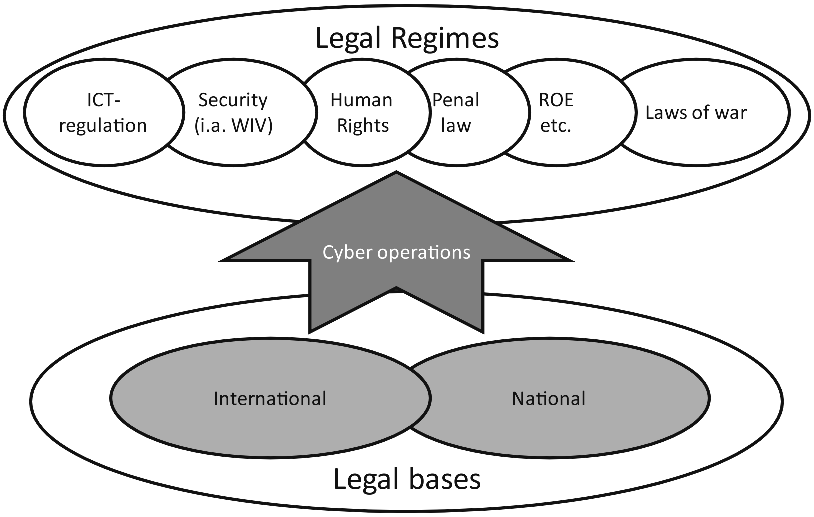

Figure 3. Legal Framework for Cyber Operations

3.3 *The Challenge*

The comprehensive framework might be clear, the challenge, however, is recognising, defining, interpreting and when necessary supplementing the parts of the framework, which is not a straightforward task. The role of ICT law regulating international data traffic, for instance, is alien to military operations up to date, and the experience and knowledge of the classic military legal advisor (the Legad), would likely be insufficient in that respect. It will be essential to widen knowledge in this field of law in the near future, be it autonomously, or through a joint venture with other partners.[49] International (ICT related) Treaties, EU and Council of Europe directives, decisions and resolutions of other international organisations (*inter alia* UN, ITU, UN Security Council, G8, OECD, OSCE, NATO and (W)EU), will inevitably play a role.

Hence, cyber operations differentiate from more traditional military operations (see above)[50] and demand – if and when necessary – a reinterpretation or supplement to the existing and familiar legal framework. At this moment, the specific legal framework for the developing cyber domain is rather incomplete, as law often lags behind technical and/or social developments. Until full development is reached, cyber operations will have to be planned and executed within the existing legal framework, a method not unfamiliar to the government and the armed forces as we all know from our experiences with new threats as modern terrorism. Like the latter, cyber threats also disregard physical borders, the primacy of state actors in international law, and challenge the classic rules of attribution.

Within the confines of this chapter, completeness would be an illusion. Therefore, those parts were selected which – according to the present authors – required interpretation or accommodation, ranging from analysis to mere demarcation. The presented order follows the constituent parts of the framework (see Figure 3): national and international legal bases and subsequently the legal regimes.

4. National Legal Bases

4.1 *Intelligence and Security Services Act 2002*

Based on the Intelligence and Security Services Act,[51] the General Intelligence and Security Service[52] and the Military Intelligence and Security Service[53] have the authority to collect intelligence referring to threats posed by opponents and countries.[54] The collection of intelligence is partly done by using open sources and partly by using so called special authorities (Art.

[49] See *inter alia*: Lodder and Boer 2012.

[50] Todd 2009, p. 68.

[51] Wet inlichtingen en veiligheidsdiensten 2002, hereafter: WIV.

[52] Algemene inlichtingen en veiligheidsdienst, hereafter: AIVD.

[53] Militaire inlichtingen en veiligheidsdienst, hereafter: MIVD.

[54] Art. 7 WIV.

18 WIV). The MIVD for example is authorised to tap and record electronic messages and network data exchange (Art. 25), intercept international satellite communication (Art. 26 and 27) and break into computer systems (Art. 24).

An important characteristic of the WIV is the fact that it has no extraterritorial effect.[55] This means that, while the MIVD has a task in collecting intelligence on other countries, Dutch law does not provide an explicit basis for operations *on the territory* of these countries.[56]

Another characteristic is that the WIV defines tasks and responsibilities with regard to intelligence collection; meaning the WIV is primarily defensive in nature. An important question is whether or not the WIV also authorises the intelligence services to conduct offensive cyber operations, for example by injecting viruses or worms, or facilitating 'exploitation'. As yet, the latter does not seem to be the case.[57]

4.2 *Protection of Military Infrastructure*

The Act on the Use of Force by Guards of Military Objects[58] authorises the use of force while guarding and securing military objects.[59] Force is defined as: 'any significant force against persons or subjects'.[60] The most important application of the *Rijkswet* is the physical guarding and securing of military objects, such as: military radio stations, direction finders, antennas, transmitters and communication centres.[61]

This enumeration has a typical signals orientation. It remains to be seen if data centres, servers and internet hubs in use by the armed forces, as well as those located at civilian sites, can be included under the same denomi-

[55] CTIVD 2007a, p. 1, see: <www.ctivd.nl/?Overige_activiteiten>.

[56] See *inter alia* CTIVD 2007b, p. 54. However, there is no prohibition (in international law) of purely intelligence gathering (as opposed to other types of covert ops) in international law.

[57] Dutch Government reaction to AIV and CAVV's report on *Cyber Warfare*, dated 6 April 2012, *Parliamentary Papers* II, 2011/12, 33000 X, No. 79.

[58] Rijkswet geweldgebruik bewakers militaire objecten, *Stb.*2003, 134, hereafter: the *Rijkswet*.

[59] Art. 1 and 2 *Rijkswet*.

[60] Art. 1 Decree on the Use of Force by Defence Personnel in the Conduct of Guarding and Securing [Besluit geweldgebruik defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak], 2003, June 17, *Stb*. 2003, 282.

[61] Annex A(7) to the Decree on designation of objects to be guarded and secured [Bijlage A(7) bij Rijksbesluit houdende aanwijzing van te bewaken en te beveiligen objecten], Stcrt. 2000, 185, p. 16.

nator.[62] Another question is whether or not a defensive cyber operation, for example, countering a hostile cyber attack against our data systems, falls within the scope of the *Rijkswet*. The operation should then be regarded as use of force and be allowed as means of force. As yet the *Rijkswet* primarily only authorises securing physical objects using the defined traditional – physical – means of force.[63]

4.3 *Police Act 1993*

Based on the Police Act 1993, the Royal Military Constabulary[64] is mandated – among other tasks – to conduct the police task within the Netherlands' Armed Forces and at locations controlled by the Ministry of Defence (Art. 6). Part of this police task is to investigate and prevent criminal activity such as cyber crime, espionage, blackmail, violation of a pledge of secrecy, etc.[65] Criminal offences in this area are (*inter alia*) hacking,[66] spamming or DDoS (bombing),[67] installing ettercaps,[68] and the destruction of data by defacing a website, spreading viruses, worms and Trojan Horses.[69]

As part of military assistance to the (civil) police, the Royal Military Constabulary and other parts of the Armed Forces can assist the civilian police in the cyber domain.[70] For example, Intelligence, Surveillance, Target Acquisition & Reconnaissance (or ISTAR) means can be temporarily placed at the disposal of the civilian police for investigations, prevention or termination of cyber crime or cyber terrorism.

[62] Art. 2 of the Decree on designation of objects to be guarded and secured [Rijksbesluit houdende aanwijzing van te bewaken en te beveiligen objecten] gives the possibility to designate objects on a temporary basis; see: Ducheine 2005.

[63] Art. 3 jo. Art. 6 Decree on the Use of Force by Defence Personnel in the Conduct of Guarding and Securing [Besluit geweldgebruik defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak], 2003 June 17.

[64] Koninklijke Marechaussee, KMar.

[65] See also the file Cybercrime: <www.ejure.nl/articles/dossier_id=175/id=55/show.html> (Accessed 11 January 2011).

[66] Computer integrity violation [computervredebreuk], Art. 138a Criminal Code [Wetboek van Strafrecht].

[67] Art. 138b Criminal Code.

[68] Devices to tap or disturb network traffic. See: Destruction of information technology [vernielen van een geautomatiseerd werk], Art.161sexties and 161septies Criminal Code. See: <www.win.tue.nl/~aeb/linux/hh/cybercrime.html> (Accessed 11 January 2011).

[69] Destruction of computer data [vernielen van computerdata], Art. 350a and 350b Criminal Code.

[70] Through Art. 58-60 Police Act 1993.

4.4 *Summary: National Legal Bases*

The current national legal bases for cyber operations are mainly defensive and law and order oriented. In principle, national law does not provide a legal basis for offensive operations, either in the Netherlands, or abroad. There is however a variety of (pro) active, preventive and repressive options. The recent developments in cyber security in a number of cases have not yet been converted to laws and regulations.

5. International Legal Bases

Under the *ius ad bellum* offensive and defensive cross-border military operations are not permitted because of the inter-state prohibition of the use of force, as laid down in Article 2(4) of the UN-Charter:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

This provision prohibits extraterritorial operations, including cyber operations, insofar these operations can be conceived as 'use of force'. This issue is problematic as international law does not provide for a definition of this term.[71] It is generally accepted that use of force encompasses armed, i.e. military, physical force.[72] The extent of this force is not relevant.[73] Actions are judged by the results or effects:[74] they are considered use of force if they directly cause death, injury or physical damage to property.

5.1 *Armed Force?*

The key question is, of course, whether cyber operations can qualify as armed force and are thus covered by the prohibition of the use of force. This question causes a problem as cyber operations are difficult to compare with traditional, kinetic military operations in the physical world, given the dimension in which cyber operations take place. Moreover, damage is often not physical in character. Schmitt, therefore, uses criteria like sever-

[71] For an overview of views on force within the meaning of Art. 2(4) of the UN-Charter, see Waxman 2011, p. 426-430.

[72] See, *inter alia*, Ducheine 2008, p. 130-131; Barkham 2001, p. 71.

[73] Ducheine and Pouw 2010, p. 10.

[74] Brown 2006, p. 187. Furthermore, a criminal law approach was proposed that focuses on the genesis of a cyber attack; Todd 2009, p. 70.

ity, immediacy, directness, invasiveness, measurability and presumed legitimacy to determine if the foreseeable consequences of cyber operations approximate armed force.[75] As the Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV) concluded in their joint advice on Cyber Warfare, a cyber attack qualifies as use of force 'if the consequences are comparable to those caused by an attack with conventional or unconventional weapons'.[76] Not every cyber activity qualifies as use of force and is allowed as long as it does not infringe other rules of international law.[77]

Cyber operations that do amount to armed force and fall within the prohibition of the use of force, can only be justified by one of the three exceptions allowed for under international law: consent, military enforcement measures under Chapter VII of the UN-Charter and self-defence against an armed attack (see below). These three exceptions constitute the so called 'adequate mandate under international law' as the Dutch Government recently reiterated.[78]

5.2 *Consent*

Cyber operations abroad, even if amounting to the use of force, are permissible with the consent of the foreign state involved.[79] During crisis management operations the host state can grant permission using a *Status of Forces Agreement* or a *Memorandum of Understanding*. It goes without saying that the execution of the operation is subject to constraints and host state law. These constraints determine the legal regime that applies to the operation, e.g. in the form of ROE (see below).

5.3 *Military Enforcement Measures*

In the absence of consent (and if the cyber operation amounts to the use of force) another exception to the ban on force would be required in order to be lawful. One such exception can be found in the UN Charter, specifically in the provisions relating to the maintenance and restoration of international peace and security under the primary responsibility of the Security Council. Hence, a possible legal basis can exist whenever the UN Security Council has authorised military enforcement measures under

[75] See Schmitt 1999, p. 914-916.

[76] AIV and CAVV 2011, p. 21. See footnote 27.

[77] Like, for instance, the sovereignty or non-intervention principle of the UN-Charter.

[78] Government programme *Samen Werken, Samen Leven*, Balkenende IV, in: *Parliamentary Papers* II, 2006/07, 29 521, No. 41, p. 2 et seq.

[79] As a result of the consensual basis, these operations do not infringe upon the principles of sovereignty, non-intervention and the prohibition of the use of force.

Chapter VII of the UN-Charter. The Security Council can decide to take these kinds of measures in case of 'any threat to the peace, breach of the peace, or act of aggression'.[80] It is for the Security Council to decide if a *hostile* cyber operation constitutes such a threat to the peace and/or to authorise 'all necessary measures', potentially including cyber measures involving the use of force as part of military enforcement measures. The Council also has the power to implement measures not involving the use of force, including cyber measures, for example, in the context of embargos aimed at cutting communications, or preventing financial or economic transactions by a targeted State.[81]

The UN Security Council resolution that authorises enforcement measures and contains the phrase 'to use all necessary means' implies the permission to use military force (including cyber operations), to carry out its mandate. These do not require the consent of the State or entity against which they are directed.

5.4 *Self-Defence*

Without consent or authorisation by the UN Security Council, a State may invoke the 'inherent' right of individual or collective self-defence if 'an armed attack occurs'.[82] Self-defence is only permitted under strict conditions that raise pressing questions in the cyber domain.

Firstly, an armed attack is required. This constitutes one of the most controversial questions in the *ius ad bellum*, partly because of the lack of a definition.[83] Ruys uses the following definition:

> An armed attack consists in the deliberate use of armed force against a State, producing, or liable to produce, serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property.[84]

Generally, the definition includes a threat that is instant, overwhelming, leaving no choice of means, and no moment of deliberation.[85] Furthermore, a series of smaller and related attacks cumulatively can be considered an armed attack.[86]

[80] Art. 39 UN-Charter.
[81] Art. 41 UN-Charter.
[82] Art. 51 UN-Charter.
[83] See *inter alia* Ruys 2010.
[84] Ruys 2010, p. 542, based on Dinstein 2005, p. 193.
[85] Often referred to as 'pre-emptive self-defence'.
[86] Ducheine 2008, p. 221.

The crucial issue is, of course, whether (a hostile) cyber operation can be considered to amount to an armed attack. Cyber operations aimed against Estonia and Georgia did not qualify as such.[87] In an advisory report to the Dutch government it was noted that:

> if a cyber attack leads to a significant number of fatalities or causes substantial physical damage or destruction to vital infrastructure, military platforms or installations or civil property, it could certainly be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter.[88]

Also, an organised cyber attack on vital functions of the state could conceivably be qualified as such 'if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state'.[89]

Secondly, once the qualification as an armed attack is clear, the next issue – attribution – arises. As the *Stuxnet* attack demonstrates, cyber activities are difficult to trace back to the author or attacker. However, attribution is required to determine the addressee of self-defence. Logically, that is against the attacker, provided it can be identified, of course.[90]

6. National Legal Regimes

Within the national legal domain, laws and regulations (such as the Police Act) can often provide the legal basis as well as the legal regime for domestic operations.[91] The AIVD and the MIVD, for example, derive their mandate from the WIV (being the legal basis), but this law also provides the legal regime for the execution of the AIVD's/MIVD's mandate.

A comparable situation arises with regard to the protection of military objects and with regard to the police tasks of the Royal Military Constabulary. When cyber operations are launched, they will be regulated by 'use of force provisions' in these respective laws, characterised by their primary focus on the 'classic' kinetic use of force. As a result, the application of these laws is not painless in case of 'offensive' operations, as the

[87] Tikk, Kaska and Vihul 2010.

[88] AIV and CAVV 2011, p. 21. Endorsed by the Netherlands' Government, see footnote 56.

[89] AIV and CAVV 2011, p. 21.

[90] Ducheine 2008, p. 570.

[91] Besides that civil and human rights play an important role.

'force' in both cases is defined as: 'any significant use of force against persons or subjects'.[92]

For the Royal Military Constabulary's police tasks, the Code of Criminal Procedure is relevant. Armed Forces providing military assisting under the Police Act will have to adhere to the Police (use of force) regulations. Also, the Police and Criminal Justice privacy regulations and regulations on reporting and archiving are relevant in this respect.

In general, generic national legislation such as constitutional rights (human rights),[93] or the Personal Data Protection Act,[94] as well as specific legislation dealing with, for example, criminal prosecution (Police Data Act), are also of relevance for the legal regime.[95]

It is clear that not all these aspects can be discussed in detail in this chapter. We confine ourselves to the conclusion that the Dutch national legal regime often depends on the basis of the operation and sometimes is characterised by physical and/or kinetic preoccupation.

7. International Legal Regimes

For the sake of brevity, the review of international legal regimes is restricted to the Law of Armed Conflict, human rights law, and the (non-legal) regimes of Rules of Engagement, and Status of Forces Agreements. International information law and the patchwork of other international efforts to control cyber operation will not be covered.[96]

7.1 *Law of Armed Conflict*

The Law of Armed Conflict (LOAC) has developed well before cyber operations came into existence, resulting in issues of interpretation and application as a result. However, LOAC has effectively dealt with issues like

[92] 'Elke dwangmatige kracht van meer dan geringe betekenis, uitgeoefend op personen of zaken', see Art.1 of respectively the Official Instruction for the Police, the Military Police and the Special Investigation Officer [Ambtsinstructie voor de politie, de Koninklijke marechaussee en de buitengewoon opsporingsambtenaar]; and the Decree on the Use of Force by Defence Personnel in the Conduct of Guarding and Securing [Besluit geweldgebruik defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak].

[93] For example Art. 10 Dutch Constitution dealing with the Right to Privacy.

[94] Wet bescherming persoonsgegevens.

[95] For a (partial) overview: *Parliamentary Papers* II, 2011/12, 26 643, No. 220 (annex): Juridisch kader cyber security.

[96] For a survey of legal mechanisms created by the UN, NATO, the Council of Europe and other international organisations, see: Hathaway et al. 2012, p. 48 et seq. See also Tikk 2010.

these before. Although aerial weapons came into use during World War I, a specific treaty dealing with combat in the third dimension has yet to be concluded. Yet, it is beyond doubt that LOAC applies to aerial warfare, and by this analogy LOAC is also applicable to the fifth dimension (once the threshold of armed conflict has been reached).

LOAC has always been adaptive in character. The basic principles – military necessity, humanity, proportionality, distinction and chivalry – apply in all armed conflicts and thereby function as a safety net; LOAC is in practice technology independent and thus applicable to new developments like cyber operations.[97]

Nevertheless, the application of LOAC raises various questions. Obviously, the most important one is whether LOAC applies to cyber operations. In two situations that question can be answered in the positive. First, when cyber operations as such amount to an armed conflict, and secondly, when cyber operations are part of an armed conflict and can be regarded as hostilities. Both situations are elaborated upon in the next paragraphs.

7.1.1 Cyber Operations as Such: Armed Conflict?

Once an armed conflict exists, LOAC automatically applies to the parties involved.[98] The key question is when an armed conflict exists.[99] International law does not define this term either. The existence of an armed conflict must be based on facts. Although the views of the parties involved on that matter are relevant, they are not conclusive.[100] The case-law of the International Criminal Tribunal for former Yugoslavia proves that:

> an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.[101]

Two cumulative conditions must be met.[102] First, actual hostilities must take place. (In the case of a non-international armed conflict (NIAC) these hostilities should be of sufficient intensity).[103] Secondly, they must be carried out by opposing organised armed groups (for NIACs: capable of

[97] Kruit 2009, p. 450 et seq.

[98] ICTY (1995), *Tadic (Appeal: jurisdiction)*, § 70.

[99] See ICRC 2008.

[100] Ducheine and Pouw 2010, p. 46.

[101] ICTY (1995), *Tadic (Appeal: jurisdiction)*, § 70.

[102] Especially in the context of a non-international armed conflict. See Ducheine 2008, p. 474.

[103] For an international armed conflict (between States): the force should exceed the threshold of minor or isolated armed incidents (AIV and CAVV 2011, p. 23); for non-

undertaking military operations over longer periods of time). It goes without saying that the non-kinetic nature of cyber operations affects the answer to the question whether cyber operations amount to an armed conflict, resulting in the application of LOAC.

7.1.2 Cyber Operations during Armed Conflict

If cyber operations as such are conducted as part of an existing armed conflict,[104] the next question is whether cyber operations can be regarded as hostilities. Most rules relating to hostilities[105] take the term attack as starting point, which is defined as: 'acts of violence against the adversary, whether in offence or in defence'.[106] Attacks can be launched from land, sea or air.[107] Two issues come to mind. Firstly, whether (all) attacks in the fifth dimension are covered by the general provisions on hostilities? That would be logical given the purpose of LOAC. Secondly, whether cyber operations can be regarded as 'acts of violence'? If not, some provisions on hostilities do not apply. To the extend they do, they will be governed by the rules pertaining to the conduct of hostilities.

Assuming that cyber operations can be construed as attacks and are governed by the general rules on hostilities, the application of these rules encounters obstacles as well. In the next paragraphs the application of the principles of distinction and proportionality, as well as the issue of neutrality will be reviewed.

7.1.3 Distinction and Military Targets

Belligerent parties must distinguish between the civilian population and combatants and between civilian objects and military objectives.[108] In the classical practice of war this distinction is sometimes hard to make. *Dual use* objects, like infrastructure, radio stations, power plants, communication satellites and computer networks, can have both a military as a civilian

international armed conflict this threshold is higher, see: Ducheine and Pouw 2012b, p. 72-73.

[104] It is expected that cyber operations will not solely take place in cyberspace but will be part of military operations that include other dimensions as well; see AIV and CAVV 2011, p. 12.

[105] See API, Part IV Civilian Population – Section I General Protection against Effects of Hostilities.

[106] Art. 49(1) API.

[107] Art. 49(3) API.

[108] Art. 48 API. This so called Basic Rule restates the customary principle of distinction and has been labeled as one of the cardinal principles of the law of armed conflict; see Schmitt 2011, p. 90-91.

function. Cyber operations put more pressure on this principle as cyber operations use *dual use* objects, like the internet.

7.1.4 Proportionality and Collateral Damage

The prohibition of *disproportionate* attacks obliges the attacking party to consider method, time and place of the attack and to carry out a *collateral damage assessment.*[109] As a rule, this proportionality test is onerous during normal operations.[110] Cyber operations are no exception to that rule, with the danger of disengagement of rules. Some cyber operations may cause less civilian casualties and less physical damage than traditional, kinetic attacks. Especially when faced with *dual use* objects, that aspect may be a consideration to launch an attack using cyber means, that would otherwise be prohibited on account of the principles of distinction and proportionality.[111]

7.1.5 Neutrality

Cyber operations will be partly conducted via the internet and, because of its international structure, will involve infrastructure and internet nodes in neutral states.[112] Neutrality law (dated 1907!) establishes that the territory of 'neutral Powers' is inviolable and cannot be used by the belligerents.[113] The use of internet facilities (due to the transit of data traffic) in or through a neutral State would be in conflict with neutrality law.

Possibly, an exception in The Hague Convention V offers a solution, as 'telegraph or telephone cables or of wireless telegraphy apparatus' belonging to companies or private individuals may be used.[114] Therefore, the use of internet nodes and connections in another State may not directly violate neutrality law.[115]

During the cyber attacks in the 2008 war, Georgia moved its internet activities abroad[116] and made use of the services and facilities of local companies abroad without the explicit permission or consent of the States

[109] Compare Art. 51(5)(b) API.

[110] For a case study and analysis, see: Baron and Ducheine 2010.

[111] Kelsey 2008. Also Haaster 2012.

[112] Kelsey 2008, p. 1441.

[113] Art. 1 and 2 of the *Convention V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land*; The Hague, 18 October 1907 (2 *AJIL* (1908) Supplement 117-27).

[114] Art. 8.

[115] See: Owens, Dam and Lin 2009, p. 270.

[116] Estonia, Poland and the US; see: Korns and Kastenberg 2009, p. 60.

involved.[117] Thus, Georgia managed to withstand the cyber attack and to maintain communication with its troops.

7.2 *Human Rights Law*

The application of human rights treaties is primarily limited to the territory of States parties to these treaties. Increasingly, extraterritorial behaviour of states has an effect on individuals abroad, leading to the important question whether cyber operations fall within the reach of these human rights instruments. That seems to be the case if a state, by conducting military operations, exercises effective control over a certain area. Control can take different forms.[118] Firstly, as an occupying force under the LOAC, and secondly, when a state exercises public authority with the consent of another state that normally exercises that control.[119] Thirdly, through a mandate of the UN Security Council, as was the case with KFOR and UNMIK in Kosovo.

As soon as geographic effective control exists, all military operations in that area are governed *inter alia* by human rights law (sometimes alongside the rules of LOAC). That rule also applies to cyber operations to which human rights law automatically apply, such as law enforcement operations carried out both domestically and abroad.

7.3 *ROE and SOFAs*

The third 'legal' regime concerns Rules of Engagement (ROE).[120] The NATO ROE catalogue – MC 362 – places 'cyber' ROE under the heading of 'Information Operations' and 'Electronic Warfare'. Since 2000 the US *Standing Rules of Engagement* include specific instructions on cyber operations.[121] One of the ROE-issues concerns the (geographic) scope of the ROE. The question is if ROE that normally defines the *Area of Operations* would allow the use of information systems belonging to parties that are not involved in the conflict or operation.

Arrangements on the (legal) status of troops stationed abroad and their privileges, like the use of facilities in respect of communication, are usually laid down in Status of Forces Agreements (SOFAs).[122] Obviously,

[117] Korns and Kastenberg 2009, p. 66-67.

[118] Ducheine 2008, p. 405.

[119] This situation is referred to above as the third normal exception.

[120] ROE are operational and/or political guidelines governing the use of force.

[121] See the Annex on Information Operations. Currently: SROE/SRUF (Standing Rules for the Use of Force); O'Donnell and Kraska 2003, p. 143.

[122] This applies to situations that states are not engaged in an armed conflict with each other. In such a conflict situation the status of the forces in enemy territory follows from the law of armed conflict.

existing, long-term SOFAs (e.g., the NATO-SOFA) did not take cyber operations into account, but future SOFAs will be affected by the developments in the field of cyber operations.

8. Conclusion

The Netherlands already have faced operations in the cyber domain. The purpose of this chapter was to stimulate further thinking and provide some tools for analysis in an effort aimed towards advancing the legal framework related to military cyber operations. Regarding the framework itself, two cautionary remarks are deemed fit.

First of all, the legal framework runs the risk of being ineffective and incomplete as long as the overarching strategic framework is incomplete itself. There is a need for an explicit overarching Grand Strategy encompassing both an international alongside a national dimension, which unfortunately does not yet exist. The present *National Security Strategy* has a primarily domestic focus and fails to address the international legal order as a vital national interest.

Secondly, as the *National Cyber Security Strategy* celebrates its first anniversary, the *Defence Cyber Strategy* should be ready to see the light. This strategy on military cyber operations should fit seamlessly into both existing strategic concepts. In addition, the *Defence Cyber Strategy* should take into account the international legal order as (the missing) sixth vital national interest, not only because of the constitutional roots but because of the second constitutional purpose of the armed forces (and the second main task) as well.

Before reconsidering the framework itself, it was argued that cyber operations could be explained and covered by more than one paradigm at the same time. Hence, it is also realistic to conclude that a monistic approach is not suitable for cyber operations. Instead, one should realise that cyber operations are part of a fluid spectrum, and therefore, require an integral or complementary approach, implying that cyber operations (at the same time could) fit into multiple paradigms, and that the constituent parts of the legal framework instead of the paradigm, will be defining the outcome. Furthermore, it is obvious that the majority of the cyber security measures will be civil in nature, with a small role for the military, and thereby limiting the role of cyber warfare proper.

Nevertheless, the legal framework comprises the legal bases for operations and the legal regimes applicable during the operations. Clearly, an operation could have more than one legal basis, as well as the execution of the operation will be covered by multiple legal regimes.

The existing legal framework is largely based on classic, defensive, reactive tasks and appears to be rather monodisciplinary. Laws and regulations relevant for the military or international treaties are still kinetically orientated, as cyber is not fully developed yet. In national legal bases and legal regimes that issue calls for reconsideration and modification when necessary, e.g., in the field of security and intelligence.

International legal bases and legal regimes are by nature adaptive and flexible. Still, the non-kinetic character of cyber operations generates serious questions in this field as well. Within the *ius ad bellum* two questions are relevant: do cyber operations constitute armed force and are they thus prohibited under Article 2(4) UN-Charter? And, can they amount to an armed attack, justifying states to respond in self-defence? Within the Law of Armed Conflict similar issues arise: when has a cyber operation sufficient 'intensity of force' to be labelled as an armed conflict? Are cyber activities true 'hostilities'? And, what will a *collateral damage assessment* result in?

By introducing cyber operations the Netherlands Armed Forces enter a new arena, which, in spite of the new and advanced technology, is beyond doubt not beyond the scope of legal regulation: the law also applies during (cyber)war.[123]

9. References

AIV and CAVV (2011): Advisory Council on International Affairs (AIV) & Advisory Committee on Issues of Public International Law (CAVV), *Cyber Warfare* (report No. 77/22, 2011), see <www.aiv-advice.nl>.

Barkham, J. (2001), 'Information Warfare and International Law on the Use of Force', in: 34 *New York University Journal of International Law and Politics*, No. 1, p. 57-113.

Baron, W. and P.A.L. Ducheine (2010), 'De luchtaanval in Kunduz – Targeting en oorlogsrecht', in: 179 *Militaire Spectator*, No. 10, p. 493-506.

Bosch, J.M.J., H.A.M. Luiijf and A.R. Mollema (eds.) (1999), *NL ARMS 1999, Information Operations*, Breda: KMA.

Brenner, S.W. (2009), *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford: OUP.

Brown, D. (2006), 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict', in: 47 *Harvard International Law Journal*, No. 1, p. 179-221.

Cornisch, P. et al. (2010), *On Cyber Warfare*, Chatham House.

CTIVD (2007a), Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten [Supervising Committee on Intelligence and Security Serv-

[123] After the maxim of the Netherlands Army Legal Service: *Et inter arma vigent leges.*

ices], Report study day CTIVD 27 October 2007, *Inlichtingenactiviteiten in het buitenland*, p. 1, see: <www.ctivd.nl/?Overige_publicaties>.

CTIVD (2007b), Jaarverslag 2006-2007 [Annual Report 2006-2007], see: <www.ctivd.nl>.

Dinstein, Y. (2005). *War, Aggression and Self-Defence*, Cambridge: University Press.

Ducheine, P.A.L., (2005), 'Geweldgebruik op grond van de Rijkswet geweldgebruik bewakers militaire objecten: de definitie van een "militair object" en extraterritoriale werking?', in: 98 *Militair Rechtelijk Tijdschrift*, No. 2, p. 45-55.

Ducheine, P.A.L. (2008), *Krijgsmacht, Geweldgebruik & Terreurbestrijding* (diss. UvA) Nijmegen: Wolf Legal Publishers.

Ducheine, P.A.L. (2012), 'Parliamentary Involvement in the Netherlands' Military Operations Abroad', in S. Hardt, L. Verhey and W. van der Woude (eds.), *Parliaments and Military Missions*, Groningen: Europa Law Publishing, p. 15-32.

Ducheine, P. and E. Pouw (2010), *ISAF operaties in Afghanistan: oorlogsrecht, doelbestrijding in counterinsurgency, ROE, mensenrechten & ius ad bellum*, Nijmegen: Wolf Legal Publishers.

Ducheine P.A.L. and E.H. Pouw (2012a), 'Legitimizing the Use of Force: Legal Bases for Operation Enduring Freedom and ISAF', in J. van der Meulen et al. (eds.), *Mission Uruzgan: Collaborating in Multiple Coalitions for Afghanistan*, Amsterdam: AUP 2012, p. 33-46.

Ducheine P.A.L. and E.H. Pouw (2012b), 'Controlling the Use of Force: Legal Regimes', in J. van der Meulen et al. (eds.), *Mission Uruzgan: Collaborating in Multiple Coalitions for Afghanistan*, Amsterdam: AUP, p. 67-80.

Ducheine, P.A.L. and J.E.D. Voetelink (2011), 'Cyberoperaties: naar een juridisch raamwerk', in: 180 *Militaire Spectator*, No. 6, p. 273-286.

Haaster, J. van (2012), *Het Juridisch Slagveld 2.0*, Bachelor-thesis Krijgswetenschappen, Breda: NLDA.

Hathaway, O.A. et al. (2012), 'The Law Of Cyber-Attack', forthcoming in: *California Law Review*, <www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf>, p. 48 et seq.

ICRC (2008) ICRC Opinion paper (March 2008) – 'How Is the Term "Armed Conflict" Defined in International Humanitarian Law?', see: <www.icrc.org/web/eng/siteeng0.nsf/html/armed-conflict-article-170308> (17 September 2008).

Kelsey, J.T.G. (2008), 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', in: 106 *Michigan Law Review*, No. 7, p. 1427-1451.

Koninklijke Landmacht (2009), *Land Doctrine Publicatie – Militaire doctrine voor het landoptreden (LDP-1).*

Korns S.W. and J.E. Kastenberg (2009), 'Georgia's Cyber Left Hook', in: 38 *Parameters*, No. 4, p. 60-76.

Kruit, P.J.J. van der (ed.)(2009), *Handboek militair recht*, Nijmegen: Wolf Legal Publishers.

Lodder, A.R. and L.J.M. Boer (2012), 'Cyberwar? What War? Meer in het bijzonder: welk recht?', in: 38 *Justitiële verkenningen*, No. 1, p. 52-67.

O'Donnell B.T. and J.C. Kraska (2003), 'Humanitarian Law: Developing International Rules for the Digital Battlefield', in: 8 *Journal of Conflict and Security Law*, No. 1, p. 133-160.

Owens, W.A., K.W. Dam and H.S. Lin (eds.) (2009), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, DC: The National Academies Press.

Rid, T. (2012), 'Cyber War Will Not Take Place', in: 35 *Journal of Strategic Studies*, No. 1, p. 5-32.

Ruys, T. (2010), *'Armed Attack' and Article 51 of the UN Charter – Evolutions in Customary Law and Practice*, Cambridge: University Press.

Schmitt, M.N. (1999), 'Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework', in: 37 *Columbia Journal of Transnational Law*, p. 885-937.

Schmitt, M.N. (2011), 'Cyber Operations and the Jus in Bello: Key Issues', in R. Pedrozo and D.P. Wollschlaeger (eds.), *International Law and the Changing Character of War*, International Law Studies Vol. 87, Newport: Naval War College, p. 89-112.

Tettero M.A.D. and P. de Graaf (2010), 'Het vijfde domein voor de krijgsmacht', in: 179 *Militaire Spectator*, No. 5, p. 240-248.

Tikk, E. (2010), *Frameworks for International Cyber Security*, Tallinn: CCDCOE

Tikk, E., K. Kaska and L. Vihul (2010). *International Cyber Incidents: Legal Considerations*. Tallinn: CCDCOE.

Todd, G.H. (2009), 'Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition', in: 64 *Air Force Law Review*, p. 65-102.

Waxman, M.C. (2011), 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)', in: 36 *The Yale Journal of International Law*, No. 2, p. 421-459.

Contributors

Dr. Floribert H. Baudet is Associate Professor of Strategy (Section Military History and Strategy) at the Netherlands Defence Academy (Faculty of Military Sciences).

Dr. Robert J.M. Beeres is Associate Professor of Defence Accounting Control & Economics at the Netherlands Defence Academy (Faculty of Military Sciences) and at Nyenrode Business Universiteit.

Dr. Myriame T.I.B. Bollen is Associate Professor in organisation studies at the Netherlands Defence Academy and a member of the Board of the Faculty of Military Sciences. Since 2004, she is a visiting professor at the Baltic Defence College, Estonia.

Lieutenant-Colonel A.J.H. (Han) Bouwmeester MSc MMAS is an operational concept developer and a core member of the Cyber Defence project team at NATO's Allied Command Transformation in Norfolk (VA, USA).

Dr. Theo B.F.M. Brinkel is acting Head of the International Securities Studies at the Netherlands Defence Academy (Faculty of Military Sciences).

Dr. Elly Broos is Assistant Professor of Human Resource Management at the Netherlands Defence Academy (Faculty of Military Sciences).

Colonel dr. Paul A.L. Ducheine LL.M. is Associate Professor of Cyber Operations at the Netherlands Defence Academy (Faculty of Military Sciences), (guest) lecturer in Military Law at the University of Amsterdam, and researcher at the Amsterdam Centre of International Law. More at: <home.medewerker.uva.nl/p.a.l.ducheine/>.

P. Ducheine, F. Osinga and J. Soeters (eds.), Cyber Warfare: Critical Perspectives
© 2012 T.M.C. Asser Press and Contributors

Dr. Paul C. van Fenema is Associate Professor of Management & Organisation at Netherlands Defence Academy (Faculty of Military Sciences). More at: <www.paulcvanfenema.com>.

Colonel ir. J.M. (Hans) Folmer MSS is the Commanding Officer of Task Force Cyber at the Netherlands Ministry of Defence.

Professor dr. Terry D. Gill is Professor of Military Law at the University of Amsterdam and the Netherlands Defence Academy (Faculty of Military Sciences).

Henk de Jong MA is an Assistant Professor of Military History at the Netherlands Defence Academy (Faculty of Military Sciences).

Professor dr. ir. Robert E. Kooij is principal scientist at TNO (Netherlands Organisation for Applied Scientific Research) and part-time professor Robustness of Complex Networks at the Delft University of Technology.

Dr. Sean Lawson is an Assistant Professor, Department of Communication, University of Utah. More: <www.seanlawson.net>.

Dr. ir. Roy H.A. Lindelauf is an Assistant Professor of Military Operational Art & Sciences at the Netherlands Defence Academy (Faculty of Military Sciences).

Professor dr. Jan S. van der Meulen is an Associate Professor at the Netherlands Defence Academy (Faculty of Military Sciences), as well as a professor of military-societal studies at Leiden University (Faculty of Social and Behavioural Sciences).

Dr. René Moelker is Associate Professor of Sociology at the Netherlands Defence Academy (Faculty of Military Sciences).

Dr. Herman Monsuur is Associate Professor of Mathematics and Operations Research at the Netherlands Defence Academy (Faculty of Military Sciences).

Air-Commodore prof. dr. Frans P.B. Osinga is Professor of Military Operational Art & Sciences, and Chair of the War Studies Department at the Netherlands Defence Academy (Faculty of Military Sciences).

Dr. Thomas Rid is a Reader in War Studies at King's College London and a non-resident fellow at the Center for Transatlantic Relations at the School for Advanced International Studies (SAIS), Johns Hopkins University, Washington, DC. More at: <thomasrid.org>.

Dr. Maarten G.D. Rothman is Associate Professor of International Security Studies at the Netherlands Defence Academy (Faculty of Military Sciences).

Professor dr. Joseph M.M.L. Soeters is Professor of Management and Organisation Studies at the Netherlands Defence Academy and Tilburg University, and Chair of the Department of Management, Organisation and Defence Economics (Faculty of Military Sciences).

Lieutenant-colonel Jan F. Stinissen LL.M. is a Senior Analyst to NATO's Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia.

Lieutenant-colonel Nico W.A. Timmermans is Assistant Professor of Military Operational Art & Sciences at the Netherlands Defence Academy (Faculty of Military Sciences).

Dr. Giliam G. de Valk is Associate Professor Intelligence & Security Studies at the Netherlands Defence Academy (Faculty of Military Sciences), and lecturer at the University of Amsterdam (Faculty of Science – Institute for Interdisciplinary Studies).

Professor dr. ir. Piet F.A. Van Mieghem is Professor of Telecommunication Networks and chairman of the section Network Architectures and Services (NAS) at the Delft University of Technology.

Lieutenant-colonel Joop E.D. Voetelink LL.M. is an assistant professor of Military Law at the Netherlands Defence Academy (Faculty of Military Sciences).

Prof. dr. Ad L.W. Vogelaar is Professor of Military Behavioural Sciences at the Netherlands Defence Academy (Faculty of Military Sciences).