



UvA-DARE (Digital Academic Repository)

The Missing Component in Deterrence Theory: The Legal Framework

Ducheine, P.; Pijpers, P.

DOI

[10.2139/ssrn.3748348](https://doi.org/10.2139/ssrn.3748348)

Publication date

2020

Document Version

Author accepted manuscript

[Link to publication](#)

Citation for published version (APA):

Ducheine, P., & Pijpers, P. (2020). *The Missing Component in Deterrence Theory: The Legal Framework*. (Amsterdam Law School Legal Studies Research Paper; No. 2020-70), (Amsterdam Center for International Law; No. 2020-34). Amsterdam Center for International Law, University of Amsterdam. <https://doi.org/10.2139/ssrn.3748348>

General rights

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

Disclaimer/Complaints regulations

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



UNIVERSITY OF AMSTERDAM



THE MISSING COMPONENT IN DETERRENCE THEORY: THE LEGAL FRAMEWORK

Paul Ducheine

Peter Pijpers

Amsterdam Law School Legal Studies Research Paper No. 2020-70

Amsterdam Center for International Law No. 2020-34

The missing component in deterrence theory: The Legal Framework

Paul Ducheine and Peter Pijpers*

Abstract

This chapter takes the starting point that power to deter, consists of three components: (physical) capacities, concepts (strategy, plans, decision-making procedures) and will (moral, determination, audacity). In case one of these components is underdeveloped or not in place, (coercive) power fails. Modern technologies (e.g. ICT, AI) and strategic insights (e.g. the utility of soft and smart power) urge for a reinterpretation of the 'physical' component, and include cyber capacities as well as culture, knowledge or law(fare) as capacities (or power instruments), too. Moreover, and taking cyber capabilities as a test case, these developments put even more weight on the conceptual and moral components of power.

This chapter focusses on the legal framework as a key, but underrated, conceptual element of deterrent power. Using cyber threats as a case, it offers a legal framework enabling decision-makers to effectively generate deterrent power by showing which legal bases (should) undergird the employment of the variety of responses available to States. In democratic rule-of-law States, the principles of legitimacy and legality demand that the use of power (instruments) by States must be based on a legal basis and should respect other institutional features too.

Through two illustrative vignettes the generic value of the framework will be illustrated for the potential use of power instruments - diplomacy, information, military, economy, culture, legal, knowledge - in its various modalities, including cyber operations. This legal framework, though tailored to cyber capabilities, may be used as a starting point for conceptualising the legal framework for so-called cross domain and cross dimensional, or full spectrum deterrence.

Keywords

Legal framework – legal bases – deterrence – cyber operations – attribution - cyberspace

Table of content

1. INTRODUCTION	3
1.1. <i>East meets West</i>	3
1.2. <i>Cyberspace as a Strategic Opportunity?</i>	3
1.3. <i>Conceptual Considerations for Deterrence in Cyberspace</i>	4
1.4. <i>Aims and Structure</i>	5
2. POWER INSTRUMENTS	6
3. THE UNDERRATED CONCEPTUAL COMPONENT: LEGAL FRAMEWORK	8
4. LEGAL BASES.....	9
4.1. <i>Consent</i>	9
4.2. <i>Retorsion</i>	10
4.3. <i>Countermeasures</i>	11
4.4. <i>Plea of necessity</i>	12
4.5. <i>Self-Defence</i>	12
4.6. <i>Self-Defence post-2001</i>	14
5. OTHER PARAMETERS: INSTITUTIONAL ARRANGEMENT AND ATTRIBUTION	15
6. INSTRUMENTS - LEGAL BASES MATRIX	16
7. CONCLUSION.....	18
REFERENCES.....	19

P.A.L. Ducheine, B.M.J. Pijpers
University of Amsterdam
Amsterdam Centre for International Law, The Netherlands
e-mail: p.a.l.ducheine@uva.nl
b.m.j.pijpers@uva.nl

1. Introduction

The supreme art of war is to subdue the enemy without fighting.
Sun Zsu, 6th century BC

1.1. East meets West

Western States traditionally focus on the physical military instrument when conceptualising deterrence as a strategic function. The threat of military force, or its actual use, is a preferred *modus operandi* in Western strategic culture.¹ For Asian States such as China, force may be perceived differently in terms of instruments used, as well as in its modalities, and in concepts. Force and power may have an economic or diplomatic face, whilst the actual threat or use of military force is less prominent or takes virtual or symbolic shapes. Looking at China's Belt and Road Initiative, trade relations, loans, (lease)contracts, embassies, harbours, education, culture and indeed the positioning of armed forces, play important roles. Quite early, Chinese strategic thinkers like Sun Zsu, and more recently Qiao Liang and Wang Xiangsui, have stressed the importance of the information environment in strategic issues such as deterrence.² Although rather late, Western strategic interest – accelerated by ever growing opportunities and threats in cyberspace – in this sphere is growing fast.³

1.2. Cyberspace as a Strategic Opportunity?

Cyberspace has been described in many ways,⁴ ranging from 'a consensual hallucination'⁵ to a 'networked information infrastructure'.⁶ In short, cyberspace covers 'all entities that are or may potentially be connected digitally'.⁷ Cyberspace is central to the information environment, the sphere where information is presented, found, communicated, processed, handled and used upon which decision-making is based, followed by (in)action. The information environment entails a physical, a cognitive and a virtual dimension. To enable digital connections, cyberspace, as part of the information environment consists of three elements: (1) cyber identities, (2) cyber objects (i.e. software, data and protocols), and (3) the physical network layer entailing cyber infrastructure (i.e. hardware and (electromagnetic) connections).

¹ See Kitzen 2012a and 2012b; Ducheine and Osinga 2017.

² Qiao Liang and Wang Xiangsui 1999, p. 199.

³ Smeets and Soesanto (2020).

⁴ Most elaborate by Kuehl 2009, p. 28, who describes cyberspace as a 'global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'.

⁵ Gibson 2018, p. 51.

⁶ Koh 2012, p. 6.

⁷ See Netherlands Defence Cyber Strategy 2012 (UK version) "Cyberspace is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc.) present in this domain", (original Dutch) in: *Parliamentary Papers II 2011-2012*, 33 321, no. 1.

Cyberspace may be used in a number of ways. First of all, it offers a medium for information and communication. Secondly, it entails capacities that may be used as instruments of power: data, applications, procedures. Thirdly, these instruments may be directed at, or can engage with other actors in cyberspace. In military terms, one may find both weapons and targets, as well as a vector to connect weapons with the targets. In generic terms: cyber capacities may be used as instruments to engage with other cyber capacities in or through cyberspace.⁸

Not surprisingly, cyberspace has become the 5th domain of operations.⁹ In effect, the potency of cyberspace is related to the threat or use of (military) force, but also to the deliberate undermining of the understanding and autonomous decision-making of actors, hence the informational instrument of power.¹⁰

1.3. Conceptual Considerations for Deterrence in Cyberspace

Is deterrence possible in cyberspace? Cyberspace is not an instrument of power in itself, but an engagement 'arena' similar to the land or air domain. However, unlike land, sea and air, people are absent in cyberspace¹¹ and 'only' the virtual reflections of humans – cyber identities – engage in cyberspace. The dominant academic thinking tends to conclude that cyberspace is not fit for deterrence as a strategic function for States,¹² a view that appears at odds with the actual effects of on-line activities of numerous (State sponsored) Advanced Persistent Threats (APTs),¹³ or the considerations of US Cyber Command.¹⁴

But maybe the question is not whether cyberspace is fit for deterrence, but whether the constituent components of deterrent capabilities are fit for contemporary engagements. Power projection in cyberspace, whether for deterrence purposes or otherwise, is no longer merely focusing on military power, but on all instruments of power, including diplomacy, informational, cultural, financial or legal instruments.

Applying the instrument of power, including military power, (in deterrence contexts) requires the (demonstrated) capacity to perform, the will to act,¹⁵ but moreover a manner how to channel these capacities.¹⁶ These commonplace elements - capacities, concepts and will - are also encapsulated in military doctrine.¹⁷ Creating power presumes the existence

⁸ Whilst this generic view describes so-called hard cyber activities or operations, the present authors also recognize so-called soft cyber operations, where cyberspace is merely used a vector to communicate virtual or digitalised information (content) via cyber identities to real persons, in an effort to affect their psyche and consequently their autonomous decision-making process, individual or collective preferences and values.

⁹ See NATO Warsaw summit NATO 2016, bullet no. 70.

¹⁰ Ducheine and Pijpers 2020.

¹¹ Delerue 2019.

¹² Borghard and Lonergan 2017; Fischerkeller and Harknett 2017, p. 393; Taddeo 2018, pp. 352-353; Whyte 2016, pp. 100-101.

¹³ For an overview of these APTs, see the list produced by Mitre-Att&ck, at <https://attack.mitre.org/groups/>; and Booz Allen 2020.

¹⁴ US Cyber Command 2018.

¹⁵ Jakobsen 1998, Chapter 1; Jakobsen 2007, pp. 225-247.

¹⁶ Biddle 2006, pp. 190-191.

¹⁷ Fighting power comprises of (1) capacities, most often the so-called physical component (i.a. manpower, means), (2) a conceptual component (strategy, doctrine, planning), and (3) a moral

and effectiveness of these three components.. In case one of these components is underdeveloped or not in place, power fails.

For democratic states, the conceptual component includes an applicable legal framework which enables the use of these power instruments. Their common values¹⁸ dictate to respect and promote international law in their international relations,¹⁹ and respect for law in general when interacting with non-state actors.

This legal framework however, is an area that seems undervalued and less researched, at least in war studies and security studies, despite the fact that the legal framework is a crucial element of the conceptual component for (deterrence) operations in cyberspace or any physical domain. For the purpose of this treatise, the legal framework is considered an integral part of the holistic approach towards deterrence in operations as it should be when conducting research in these areas. Therefore, States will need to organise and structure their legal and institutional framework in order to deter others from engaging, threatening or attacking vital interests, in or through cyberspace.

1.4. Aims and Structure

The primary aim is to supplement the conceptual component of power by adding a concise legal framework for the use of all power instruments, be they military or otherwise, classic or modern. The approach taken departs from the premise that when the legal framework is not in place or underdeveloped, the conceptual component of power is flawed which in turn will have deteriorating impact on power itself. E.g. when, offensive cyber capabilities are in place, but actual legal bases haven't been analysed, realistic decision-making procedures are lacking, or competent bodies authorising the use of capabilities in response of threats haven't been designated, deterrence by punishment is illusive. For deterrence to be effective, credibility and clear communication demonstrating the will and ability to use capabilities is essential. Hence, without a legal framework in place, a deterrence strategy, with whatever means, will not be effective.

While such a framework is essential for the employment of all instruments of power, and certainly in a context of cross domain deterrence, this chapter focuses on the nexus of deterrence and cyberattacks. Taking deterrence against cyber threats as a case, a succinct matrix of options will be presented serving as a conceptual component to generate capabilities to dissuade opponents, offering insight in the available legal bases for each of the power instruments, recognizing the different faces or modalities that may be envisioned. Although at first glance, this approach may appear to focus on deterrence by punishment, it will become evident that deterrence by norms and/or entanglement may also be of relevance.²⁰

In addition, to the legal basis, other institutional elements, such as governance issues, will be addressed, involving questions such as 'who has the authority to decide to make use of

component (will, resilience, determination). See: NATO 2017, p. 1-16; UK Ministry of Defence 2017 p. 3-2; NL Defence Staff 2019, pp. 66 ff; Applied in Ducheine and Van Haaster 2014, p. 305.

¹⁸ See e.g. the Preamble to the Treaty of the European Union (6 October 2012); and the Preamble to the NATO Treaty (4 April 1949).

¹⁹ See e.g. the Preamble to the Charter of the United Nations (26 June 1945); and the Netherlands' position as expressed in *Parliamentary Papers II*, 2006-2007, 29 521 no. 41.

²⁰ Nye Jr 2016 pp. 58-62.

the instrument', who is responsible for the execution, who is accountable (for what part), how is oversight guaranteed, will be (briefly) addressed. As Jakobsen argued, effective coercion requires the demonstrated ability to quickly generate coercive power. Having thought through the appropriate governance framework is instrumental to that. To this end, the situation in the Netherlands' national legal framework will be used as a demonstration using so-called vignettes.²¹

Combining the international legal bases with the applicable national institutional or governance framework for the use of power instruments, also serves as a demonstration explaining the legal framework outside threats in cyberspace. In fact, it is argued, that the core of this legal framework may be used to prepare for deterrence in cross domain or full dimension situations. Hence, deterrence against opponents using military, economic or other threats, may benefit from this contribution supplementing or reinforcing the conceptual component of deterring power.

This chapter first briefly sets out the instruments of power (Sect. 2). Secondly, the components of power and the legal framework as a conceptual element therein are covered (Sect. 3). Next, the legal framework itself is analysed in two parts: the legal bases (Sect. 4) building on international law and other relevant elements (Sect. 5) building on the Netherlands' institutional arrangements, after which a matrix is presented offering legal options related to the instruments of power (Sect. 6)

2. Power Instruments

Power instruments are often briefly summarized as DIME: diplomacy, information, military, economy.²² In deterrence literature the military and diplomatic instruments have been dominant in the past. However, contemporary strategic theorists increasingly make use of concepts such as hybrid threats, unrestricted warfare, grey zone activities, information warfare, financial or economic warfare, cultural, ideological, political, virtual and cyber warfare. Other instruments, such as financial, intelligence, legal,²³ or culture and knowledge, might be added,²⁴ to fully grasp the instruments used to exert power in today's geopolitical arena.

Diplomacy is linked to foreign relations, it is generally about communicating and advocating national or international interests and values. Diplomacy gets a face through the work of diplomats, international governmental organisations but also through international agreements, resolutions, cooperation, coordination, norm development, alliances, treaties, customary law and soft law.²⁵ The military instrument, armed forces, may

²¹ As States will have different institutional and constitutional arrangements, this part of the legal framework using the Netherlands as a case in fact, serves as a demonstration.

²² Mann 2013, p. 502; Schroeder 2005, p. 2; UK Ministry of Defence 2011, pp. 1-6; US Joint Chiefs of Staff 2013, p. I-12.

²³ Van Haaster 2019, p. 64; Rodriguez ea 2020.

²⁴ Nye Jr 2013, pp. 7-10.

²⁵ See e.g. the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UNGGE) at <<https://www.un.org/disarmament/group-of-governmental-experts/>>; and the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), at <<https://www.un.org/disarmament/open-ended-working-group/>>.

be used in various ways, from (treaty based or ad hoc) peaceful cooperation based on shared values and norms, to armed conflict. The modalities used, the means and methods, may range from classic physical weaponry, to non-kinetic²⁶ (e.g. training and advisory capacity)²⁷ and new information related capabilities, including hard and soft cyber operations.²⁸

Economic power, as an instrument may also take various shapes, ranging from consensual (loans) to compulsory (sanctions),²⁹ and can be enlarged with the financial instrument of power. It covers both passive elements, e.g. a State's macro-economic characteristics as well as active measures (assets freeze, investments, etc.). On the institutional side, international economic relations, such as common markets, with its mechanisms and procedures in place, would be another facet.

Next to classic DIME instruments, others come to the fore: culture as a (soft) power element is often seen in action,³⁰ expressions of which are Radio Free Europe, China's Confucius institutes,³¹ Soros' Open Society Foundation.³² Lawfare, law used strategically as an alternative for the military instrument³³ in conflict situations,³⁴ is used in legal action: e.g. the US' indictments of foreign cyber operators,³⁵ or litigation between States.³⁶

Last but certainly not least, information as a power instrument – including intelligence – can be understood in several ways. First of all, it involves the relative value of information sources itself, whether physical, cognitive or virtual.³⁷ These sources may be observed by men and/or machine, upon which understanding and decision-making are based.³⁸ Large data sets containing personal information related to (large) groups, or traffic data, are also examples of power resources. This substantive facet may be used to affect other actors, e.g. through marketing.³⁹ Secondly, it entails structures to communicate, both in terms of procedures and as a medium or vector. This could be the world wide web as part of cyberspace, or the internet and the dark web. (Entry) control over these structures, may be used to exert power. One may think of communication channels (old media), Great Firewalls, but also Internet Exchanges, 5G networks, the glass fibre cable network covering the globe, satellites offering mobile internet to places without physical (cable) connectivity. Thirdly, institutions overseeing, designing, contributing to the flow of information may

²⁶ Ducheine 2015a.

²⁷ Wiltenburg 2019.

²⁸ Ducheine, Van Haaster and Van Harskamp 2017.

²⁹ Giumelli 2017.

³⁰ Nye Jr. 2013, pp. 10-14.

³¹ Young 2009; Łoś 2019.

³² See <<https://www.opensocietyfoundations.org/who-we-are>>.

³³ Sari 2020.

³⁴ Voetelink 2017.

³⁵ See i.a. US DOJ 2018b (GRU Indictment) and 2018a (IRA Indictment); New York Times 2018; New York Times, 2019; Bellinger 2020.

³⁶ ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment (Merits), [1986] ICJ Rep 14, 27 June 1986; ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996] ICJ Rep 226, 8 July 1996.

³⁷ See UK Ministry of Defence 2010, p. 2-5; and *supra* n 28.

³⁸ See *supra* n 28.

³⁹ In the terminology used by Bets & Stevens 2011: compulsory power. See the four categories by Barnett and Duvall 2005, p. 43: compulsory, structural, institutional and productive power.

offer a powerbase as well, e.g. the Internet Corporation for Assigned Names and Numbers (ICANN), or the Internet Engineering Task Force. Fourthly, information has a productive aspect as well: to generate debate, to reproduce and reinforce discourse or messaging, to construct and disseminate new information, whether malevolent or benevolent. Consider the (alleged) role of Facebook, Twitter, WikiLeaks in elections, or ordinary marketing.⁴⁰ As demonstrated, cyberspace is used to gather, transfer, handle and produce information, whilst virtual information (i.e. data, software, protocols) is also used as an instrument, as a vector and as a target to generate effects.

3. The Underrated Conceptual Component: Legal Framework

The commonplace understanding of power is as a capacity or attribute with which an actor is endowed, or as a resource to be exploited to achieve particular end.
David Betz & Tom Stevens

Power, described by Betz and Stevens,⁴¹ may be applied to promote and to protect the vital interests of States.⁴² As described in Section X.1.3 and mindful of earlier academic and doctrinal work,⁴³ power requires (1) capacities, most often the so-called physical components (i.a. manpower, means), (2) a conceptual component (strategy, doctrine, planning), and (3) a moral component (will, resilience, determination) to ensure effectiveness, and thus to be regarded a capability.⁴⁴ Power requires instruments, capacities, that may only be effective when ‘unlocked’ through strategy.⁴⁵

One essential part of the conceptual component, embedded in strategic notions, democratic principles and procedures, is the legal framework accompanying the foreseeable use of power instruments. In democratic rule-of-law States, the principles of legality demand that the use of power (instruments) by States must be based on such a legal framework. A first element in this legal framework is the legal basis for the legitimate employment of power instruments.⁴⁶ In addition, the legal framework, will also entail decision-making procedures describing the (legal and political) authority for the decision

⁴⁰ It is signalling that the seven largest publicly traded companies having the greatest market capitalization, are ICT companies (Microsoft, Apple, Amazon, Alphabet, Alibaba, Facebook, Tencent). As on 31 March 2020. Market capitalization is calculated from the share price (as recorded on selected day) multiplied by the number of outstanding shares. See Van Haaster 2019, p. 78, based on the Financial Times Global 500.

⁴¹ Betz and Stevens 2011, p. 42.

⁴² See *supra* n 10, p. 8.

⁴³ See Jakobsen 2011; NL Defence Staff 2019.

⁴⁴ The difference between *capacities* and *capabilities* is essential in this contribution. See by analogy NDD 2019, p. 66: “Fighting power is the ability to conduct military operations in an optimum NDD cohesive totality of functionalities and components. It is more than just the availability of means (capacities); there must also be the willingness and ability to deploy these means (capability). If this is properly developed, it then becomes fighting power, and capacities are elevated to capabilities.”

⁴⁵ Betz and Stevens 2011, p. 40: “strategy is the art of unlocking the power inherent in national capacities to effect outcomes in the national interest in contest with other strategists acting in their own national interests”.

⁴⁶ Ducheine and Pouw 2009; Ducheine and Pouw 2012a.

to use the designated assets,⁴⁷ the applicable legal regimes when these assets are used (i.a. rules of engagement),⁴⁸ and accountability and oversight mechanisms.⁴⁹

4. Legal Bases

Without a proper legal bases international action, law abiding, and legitimacy seeking States run the risk of producing (or threatening with) non-credible, thus non-deterrent action. Within the limits posed by international law, States are permitted to use power instruments in their international relations. When the use of these instruments falls short of the threshold on the use of force as defined in Article 2(4) of the UN Charter,⁵⁰ interstate action is governed by the general principles of territorial sovereignty,⁵¹ and respect for the political independence and territorial integrity, and inviolability of States.⁵²

Within this international law framework, various bases for non-forceful and forceful action indeed exist. The legal bases for *non-forceful action* (e.g. economic sanctions, or declaring diplomats *persona non grata*) are an essential part of the conceptual component as it offers three legitimate avenues for interaction with other States (and non-state actors). As States will generally seek to secure the (perceived) legitimacy of their acts, they will offer some form of clarification for non-consensual behaviour. Most often, these clarifications, or in other terms, legal bases, will be based on in the international law phenomena such as retorsion, countermeasures, or a plea of necessity.

Though the use of force itself is forbidden, international law relevant to interstate force, the *jus ad bellum*, offers another three exceptions to this rule that provide a legal basis for *forceful* (individual or collective) actions:⁵³ consent,⁵⁴ UN Security Council authorization, or self-defence (see below).⁵⁵ The legitimacy of these actions strengthens the conceptual component of power as it invigorates the normative justification for the action and moreover, it enhances the will the act. The various legal bases for response action will be described below.

4.1. Consent

Paradoxically as it may seem when considering deterrent capabilities, in some cases States might rely on a consensual basis to make use of its power instruments in international

⁴⁷ Ducheine, Arnold and Pijpers 2020.

⁴⁸ See e.g. Ducheine and Pouw 2009; Ducheine & Pouw 2012b.

⁴⁹ Ducheine, Van der Meulen and Moelker 2010.

⁵⁰ Article 2(4) 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.”

⁵¹ On this principle in cyberspace: Ziolkowski 2013, and Pirker 2013. See also Tallinn Manual 2013, Rule 4.

⁵² On this principle in cyberspace: Gill 2013.

⁵³ *Argumentum a maiore ad minus*.

⁵⁴ See e.g. the Tallinn Manual 2013, Rule 1, para. 8, following the notion of sovereignty, States ‘may consent to cyber operations conducted from its territory or to remote cyber operations involving cyber infrastructure that is located on its territory’.

⁵⁵ See e.g. Gill and Fleck 2015, Part II.

relations. This could be both non-forceful and forceful. International law enforcement cooperation might for instance provide for extraterritorial enforcement mechanisms,⁵⁶ enabling States e.g. to locate or attribute threats. When this information is made public, it could contribute to the legitimacy of the use of other instruments and modalities. A consensual basis could also be envisioned through treaty-based conflict-resolution or enforcement mechanisms, for which the treaty provides. For example, through international law enforcement cooperation to obtain forensic evidence from a foreign internet service provider's cloud server. Another example could be a Status of Forces Agreement, enabling armed forces operating abroad, to act in designated ways in response of e.g. threats to its forces.⁵⁷

4.2. Retorsion

A second basis States might select is retorsion which is defined as unfriendly, but internationally lawful acts, that do not require a prior violation of international law per se.⁵⁸ Unfriendly refers to the fact that retorsion is “wrongful not in the legal but only in the political or moral sense, or a simple discourtesy”.⁵⁹ Retorsion may be used to enforce (international) law, in case the triggering act was indeed a violation of the law. It may also be used to enforce soft law arrangements.⁶⁰ Notwithstanding its use in interstate relations, retorsion can also be used by and against qualified international organizations.⁶¹

State practice presents a great variety of measures of retorsion: each legislative, executive, administrative, etcetera measure that is permissible under international law and that “seems suitable to a State to redress the unwelcome, unfriendly, or illegal behaviour of another State”.⁶² Common forms can be found within various power instruments: protest; cancelling State visits; denying ships access to ports or to the exclusive economic zone; summoning ambassadors; declaring diplomats *persona non grata*;⁶³ “downgrading diplomatic intercourse to the technical level; recalling ambassadors for consultations of indefinite duration; severing diplomatic relations; terminating the payment of development

⁵⁶ Ducheine 2015b, p. 469: “Cross-border law enforcement responding to illegal (cyber) activity could be undertaken with respect to the territorial sovereignty of other States with the consent of that State”, with reference to Gill 2013, p. 229.

⁵⁷ See Boddens Hosang 2015; and Voetelink 2015.

⁵⁸ Max Planck Encyclopedia of Public International Law [MPEPIL]. Based on the Articles on State responsibility, chapeau to Chapter II of Part 3, para. 3. of the Commentary.

⁵⁹ MPEPIL, para 2. As stressed by (inter alia) the Netherlands' Cabinet: “This option is therefore always available to states that wish to respond to undesirable conduct by another state, because it is a lawful exercise of a state's sovereign powers. States are free to take these kinds of measures as long they remain within the bounds of their obligations under international law.” See *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47 (annex), p. 7. Via <<https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>>.

⁶⁰ Soft law being non-binding international arrangements, see MPEPIL, para 37: “a complex of norms lacking binding force, but producing significant legal effects nevertheless”.

⁶¹ To the extent that the latter have international legal personality and the capacity to act in the international sphere, see: MPEPIL, para 1.

⁶² MPEPIL, para 10.

⁶³ As was the case in response to Russia's meddling with the 2016 US Presidential elections, see: US White House 2016; Sanger 2016.

aid or the provision of military assistance; unilaterally imposing legally permissible economic sanctions such as an arms embargo; [...] suspending, terminating, or refusing to prolong a treaty; and withdrawing from an international organization in order to protest this organization's political activities.”⁶⁴

Retorsion by using cyber capabilities would be an option in a response to unfriendly (or unlawful) acts by other States,⁶⁵ e.g. by “limiting or cutting off the other state's access to servers or other digital infrastructure in its territory”,⁶⁶ or by “misleading a prospective intervening party by providing it with bogus or useless information or otherwise diverting cyber break-ins from their intended targets”.⁶⁷

4.3. Countermeasures

A third basis for response options consists of threatening or taking countermeasures. This involves actions taken in response to another State's violation of international law.⁶⁸ They may be defined as “pacific unilateral reactions which are intrinsically unlawful, which are adopted by one or more States against another State, when the former considers that the latter has committed an internationally wrongful act which could justify such a reaction”.⁶⁹ Countermeasures are used to induce compliance (and enforcement) of international legal obligations.

Unlike retorsion, countermeasures interfere with the target State's international legal rights, and are therefore subject to preconditions.⁷⁰ They require (1) a prior internationally wrongful act that (2) can be attributed to a State; (3) with the sole purpose to induce the wrongdoer's compliance; (4) they are limited to non-forceful and proportionate actions only; and (5) a prior demand to the wrongdoer is required.⁷¹ Finally, (6) countermeasures are not allowed once the unlawful act has ceased.⁷²

In terms of responding to prior cyber incidents that violate international law, countermeasures could be used to actively hack back when the location of the infrastructure is known, e.g. the GRU headquarters, to stop the violation,⁷³ or to initiate action against States that should have acted to stop their infrastructure from being to for the violation, but are not willing to do so.⁷⁴

⁶⁴ MPEPIL, para 10.

⁶⁵ Gill 2013, p. 230 and the accompanying notes; and Gill 1992, p. 105.

⁶⁶ *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47 (Annex), p. 7, stressing: “provided the countries in question have not concluded a treaty on mutual access to digital infrastructure in each other's territory”.

⁶⁷ Gill 2013, p. 236.

⁶⁸ Schmitt 2014a.

⁶⁹ Geiss and Lahmann 2013, p. 629.

⁷⁰ Schmitt 2013b, p. 678; Tallinn Manual 2013, Rule 9; also *Parliamentary Papers II*, House of Representatives, 2010-2011, 32 500 V, no. 166, p. 2.

⁷¹ See *supra* n 56, p. 470.

⁷² Geiss and Lahmann 2013, p. 638.

⁷³ *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47 (annex), p. 7: “a cyber operation could be launched to shut down networks or systems that another state is using for a cyberattack”. The ‘GRU’ is the military intelligence service of the Russian Federation.

⁷⁴ See the debate covered in the commentaries to Rule 20-25 in the Tallinn Manual 2.0 2017.

4.4. Plea of necessity

In addition, States facing ‘grave and imminent peril’ to its ‘essential interests’ might, when the strict conditions are met, rely on a plea of necessity in response. Unlike countermeasures, action based on this plea does not require a prior internationally wrongful act to which it is responding, and the author responsible for this act could – next to States – also be a non-state or an unknown entity.⁷⁵ Once again, the preconditions are very strict. The threshold is high, as it requires (1) a situation of ‘grave and imminent peril’ to (2) ‘essential interests’ of the victim State.⁷⁶ Moreover, action may (3) not involve the use of force,⁷⁷ should be (4) proportional, and it (5) requires attribution to the author of the (threatening) act who should be (6) addressed first ordering him/her to desist.

The crucial notion of essential interests of States is “vague in international law”.⁷⁸ What is essential, is contextual and will depend from State to State. Grave and imminent peril to a State’s essential interest, refers to actual harm and to threats: “the damage does not already have to have taken place, but it must be imminent and objectively verifiable”.⁷⁹ Moreover, damage caused or threatened could be physical or non-physical, e.g. “situations in which virtually the entire internet is rendered inaccessible or where there are severe shocks to the financial markets” could be viewed as cases in which necessity may be invoked.⁸⁰ Alongside the strict conditions, the plea also gives leeway, as “establishing the existence of a situation of necessity does not require a State to determine the precise origin of the damage or whether another State can be held responsible for it.”⁸¹ Nevertheless, the necessity may only be invoked when no “no other real possibility of taking action to address the damage caused or threatened, and provided there is no interference with the essential interests” of other States “or of the international community as a whole”.⁸²

In terms of cyberspace, closing down an intrusive cyber operation (e.g. ransomware) against central medical infrastructure or key financial technology (e.g. iDeal) caused by cyber criminals operating from an unknown jurisdiction so that international law enforcement cooperation is futile, could be a scenario to be used.

4.5. Self-Defence

Next to retorsion, countermeasures and a plea of necessity, States may in extreme situations of an armed attack, resort to yet another self-help mechanism: self-defence.⁸³

⁷⁵ Schmitt 2014b; Geiss and Lahmann 2013. Tallinn Manual 2.0 2017, Rule 26.

⁷⁶ Schmitt 2014b; Schmitt 2013, p. 663: “In the cyber context, the plea of necessity is most likely relevant when cyber operations threaten the operation of critical cyber infrastructure.”

⁷⁷ See *supra* n. 56, p. 470.

⁷⁸ Tallinn Manual 2.0 2017, p. 135.

⁷⁹ *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47 (annex), p. 8.

⁸⁰ *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47 (annex), p. 8.

⁸¹ *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47 (annex), p. 8.

⁸² *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47 (annex), p. 8.

⁸³ See *supra* n 56, p. 472, Rule 23.05. For more details on self-defence: Gill 2015, esp. pp. 214 – 216; and Gill and Ducheine 2015; Gill and Ducheine 2012, p. 443. See also Tallinn Manual 2013, Rules 13–17.

Before the terrorist attacks of 2001, international law accepted that States that are the victim of violent activities that reach the threshold of an armed attack,⁸⁴ may respond with lawful measures of self-defence against the author(s) of that armed attack, “provided it does so in conformity with the other material (necessity and proportionality)⁸⁵ and procedural requirements of exercising self-defence (reporting to the Security Council).”⁸⁶

Whether violent activities or operations qualify as an armed attack ‘depends on its scale and effects’. Based on Article 51 UN Charter and customary law, an armed attack has been defined as “a use of force which originates from outside the target State’s territory, rising above the level of a small scale isolated armed incident or criminal activity, which is directed against a State’s territory, its military vessels or aircraft in international sea or airspace or lawfully present on another State’s territory, or in certain situations directed against its nationals located abroad.”⁸⁷

Analysing its elements, an armed attack, first of all, involves the use of force, normally understood to be military force. It might be ‘produced’ through conventional, nuclear or other means and methods of warfare.⁸⁸ Second, it requires a significant use of force, usually measured in terms of “scale and effects”,⁸⁹ as it is generally viewed as a more serious form of the use of force.⁹⁰ Third is the transnational or cross-border aspect of an armed attack. Normally, armed attacks are conducted by the armed forces of a State, launching or conducting a military operation against targets in or belonging to another State.

In accordance with the principle of necessity, self-defence is a forceful measure of last resort, that is, when no consent could be reached, and collective enforcement measures under Chapter VII of the UN Charter are in-effective, not feasible or not opportune. Moreover, the self-defence response should be proportional.⁹¹ In the context of this field of the *jus ad bellum*, proportionality has a distinct meaning.⁹² Contrary to common misunderstanding, proportionality in self-defence does *not* require a response in kind. In other words, self-defence is a proper legal bases for cross domain deterrence, as e.g. a classic armed attack could trigger a self-defence response with cyber capabilities, and vice versa, a digital armed attack could be followed by a conventional military response.

⁸⁴ See article 51 UN Charter. See also its customary law basis in Gill 2015, pp. 214 ff (Rule 8.02).

⁸⁵ See Tallinn Manual 2013, Rule 14 on necessity and proportionality.

⁸⁶ See *supra* n 56, p. 472.

⁸⁷ Gill and Ducheine 2012, p. 443. Also: Gill 2015, p. 213, Rule 8.01.

⁸⁸ See: ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996] ICJ Rep 226, 8 July 1996.

⁸⁹ CJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua vs. United States), Merits, 27 June 1986, paragraph 195. Also: Gill 2015, p. 216, Rule 8.03: “a reasonably significant use of force”.

⁹⁰ See Article 2(4) UN Charter.

⁹¹ Gill 2015, p. 221, Rule 8.04.

⁹² Gill and Ducheine 2012, p. 450 “Proportionality in the context of self-defense refers to the requirement that measures of self-defense must not exceed those required under the circumstances to repel the attack and prevent further attacks from the same source in the proximate future and that they must be roughly commensurate to the scale and aims of the overall attack. Hence, the scale and nature of the attack will determine what is required to repel or, if necessary, over-come it and prevent a continuation”. On the various meanings of proportionality, see Van den Boogaard 2019.

4.6. Self-Defence post-2001

The classic interpretation of an armed attack however, has evolved as a result of the 9/11 terrorist attacks against the United States, and the 2015 terrorist attacks in France, including the subsequent responses that were based on self-defence. Next to States, non-states actors potentially qualify as the author of an armed attack too.⁹³ Moreover, an armed attack could be ‘produced’ or generated by non-military means and alternative methods, such as hijacked airliners. In addition, an armed attack could also comprise a series of smaller attacks, launched by a single author against the same target State, when these attacks are reasonably related in geographic and temporal terms.⁹⁴ These new insights, combined with current practises in cyberspace,⁹⁵ have forced States to review their security strategies and stances in international relations, including international law.

Witnessing the interdependence of societies, economies, households and humans created through and with cyberspace, it is notable that States as well as non-state actors have proven to possess capabilities which can threaten or affect vital interests.⁹⁶ As noted by Boddens Hosang and Ducheine, “launching cyber operations that potentially equal the effects of an armed attack, as was the case on 9/11, either by State or non-state actors, is not just a theoretical chance or risk.”⁹⁷ In recognition of this, the Netherlands⁹⁸ and France, take the view that cyber-attacks could qualify as armed attack,⁹⁹ including the option of purely non-physical consequences of the attack. France notes that a “cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to paralyse whole swathes of the country’s activity, trigger technological or ecological disasters and claim numerous victims.”¹⁰⁰ The Netherlands’ government, based on its advisory councils, recognizes that “disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks”¹⁰¹ could indeed qualify as an armed attack. Notably, a cyber operation targeting “the entire

⁹³ See *supra* n 46.

⁹⁴ Boddens Hosang and Ducheine 2020, pp. 14-15: “This would require that the series of attacks can, firstly, be attributed at all, and, secondly, be attributed to a common author. Hence, it involves (i) the capability of detecting an attack, (ii) the capability of technical or ‘forensic’ attribution of the attacks, and (iii) the capability of legal attribution of the attacks to a common author (operating from abroad).⁹⁴ Thirdly, the series of attacks should be directed against targets in or belonging to a single State. Fourthly, the series of attacks are – somehow – related in terms of time and location. And fifthly, the series of attacks, or the attack as whole, constitutes force of sufficient gravity in terms of scale and effects as to qualify as an armed attack”. Also: Gill and Ducheine 2012. See i.a. UN Doc. S/2001/947 (Letter dated 7 October 2001 from the Chargé d’affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations Addressed to the President of the Security Council), p. 1.

⁹⁵ See *supra* n 10.

⁹⁶ See *supra* n 94, p. 13, referring to WRR 2019; Algemene Rekenkamer 2019; Dutch Safety Board 2020.

⁹⁷ See *supra* n 94, p. 13.

⁹⁸ *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47, p. 8 (see *supra* n 59). For the Advisory Report it follows: AIV/CAVV 2011.

⁹⁹ In general terms, this is also the explicit view of NATO, the United Kingdom, Estonia, Australia.

¹⁰⁰ France 2019, p. 8.

¹⁰¹ See AIV/CAVV 2011, p. 21.

financial system or prevents the government from carrying out essential tasks” could well be equated with an armed attack.¹⁰²

5. Other Parameters: Institutional Arrangement and Attribution

In addition to the legal basis as part of the legal framework that contributes to the conceptual component of power (instruments), two other legal elements are relevant in order to generate effective capabilities with the designated capacities: the institutional set-up and the ability to attribute. Once again, in case these elements are not in place, producing (or threatening with) action with power instruments would be non-credible and ineffective, as opponents would be (or could be) aware of the missing link to transform capacities into effective capabilities.

Related to the legal basis and to the tasking of responsible State organs, and impacting on the decision-making procedure thereto, is the paradigm governing the potential or real response. So, rules concerning the roles, mandates and responsibilities of services and State organs i.a. the Ministry of Foreign Affairs, Ministry of Trade and Development Aid, Economic Affairs, Police, Public Prosecutors, armed forces etc, ought to be in place. It also entails decision-making procedures describing the (legal and political) authority to order the use of the designated assets.¹⁰³ Moreover, it involves the legal regimes applicable when these assets are to be used, i.a. rules of engagement, should be clear.¹⁰⁴ Likewise, accountability and oversight mechanisms will have to be in place.¹⁰⁵

Next, a four-tiered attribution framework, is required. First, threats or harmful cyber incidents need to be detected. Without adequate detection, States are unaware of threats or actual damaging situations in cyberspace, and therefor unable to respond or deter at all. Detection capacities also require conceptual (i.a. legal) backing, before capabilities emanates. Hence, it should be clear who is tasked with what kind of detection or surveillance responsibilities, as well as how detection is handled and communicated to what authorities. For that reason, surveillance and/or investigative powers should be available to the relevant services. Second, technical attribution is needed: a technical forensic inquiry is required to assess e.g. what malware was used, how it operates, from which IP-address or cyber identity it came from, what path did it follow and who authored it and has sent it. Obviously, this will require investigative powers. Third, through legal attribution the actors who bear responsibility for the incident may be designated. This relates to the burden of proof and affiliating the perpetrator e.g. an APT to a State or subject to State control. The so-called Articles on States Responsibility are the key legal concept in this realm. The final part is political attribution in which a State may choose to use political communication to

¹⁰² See AIV/CAVV 2011, p. 21.

¹⁰³ See *supra* n 47.

¹⁰⁴ See *supra* n 48.

¹⁰⁵ See *supra* n 49.

address the responsible State (and author)¹⁰⁶ and if necessary, seek (legal) retribution.¹⁰⁷ But this ‘naming and shaming’ will not always follow suit;¹⁰⁸ it will often be conducted discreetly and not in public especially if the relation with the perpetrator is sensitive or if it is a friend rather than a foe. It should be noted however, that political attribution is not required to stem from digital forensics and/or legal attribution. Often the political attribution is a solitary and unilateral act.¹⁰⁹

The concepts (and rules) for these three forms of attribution should be available, clear and ready to be used, exercised if possible. In case essential parts of this framework are lacking, outdated, not well known or badly rehearsed, the conceptual component is suboptimal, and credibility, hence also effectiveness, of the deterrent instrument could be at stake. For example, with its Defence Cyber Command, cyber capacities in the Netherlands are available. Moreover, the ambition to use these capacities in a deterrent posture had been expressed publicly. However, when the meaning of what an armed attack entails, is unclear, or when political¹¹⁰ or operational¹¹¹ decision-making procedures to actually use these capacities in self-defence would be missing, no credible, hence no effective capability is around. As that would be the same when the political will to actually use the capacities of the Defence’s Cyber Command, is lacking.

6. Instruments - Legal Bases Matrix

While the analysis of the legal framework above was presented in the context of cyber capabilities and threats, this framework is generic and essential to all democratic rule-of-law States. The matrix in Table 1 is composed of the various power instruments as previously described. It conveys how states can resort to specific legal bases when considering employing instruments of power. The numbered boxes offer realistic combinations of instruments/modalities and legal basis. The numbering refers to a vignette below. While space restriction precludes covering each of the available options,¹¹² a few fictitious examples for the Netherlands’ institutional and constitutional setting, including the EU framework, will serve to demonstrate the logic and value of the matrix.¹¹³

¹⁰⁶ See e.g. The Netherlands considers Russia’s GRU responsible for cyber-attacks against Georgia, at <<https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia>>.

¹⁰⁷ See e.g. the indictments against the Internet Research Agency by the US Department of Justice: US DOJ 2018a.

¹⁰⁸ Finnemore and Hollis, 2019.

¹⁰⁹ US White House 2016; UK Foreign and Commonwealth Office 2020.

¹¹⁰ See *supra* n 47.

¹¹¹ See e.g. Smeets and Work 2020.

¹¹² Fictitiously ranging from 1 to 22 in the matrix (Table 1).

¹¹³ As States will have different institutional and constitutional settings, these vignettes based on the Dutch background serve as an example only.

Legal Basis	Consent	Retorsion	Counter-measures	Plea of Necessity	Self-Defence
Instrument					
Diplomacy	1	2			
Information & Knowledge (incl. Intelligence)	3	4	5	6	7
Military	8	9*	10*	11*	12
Economy & Financial	13	14	15	16	
Culture	17	18			
Legal	19	20	21	22	

Table 1: Legal Bases Matrix¹¹⁴

In scenario one, based on the Cabinet’s decision, the Minister of Foreign Affairs has ordered a negotiation team on bilateral trade cooperation with State B to pause consultations (see option 2 above and Table 2).¹¹⁵ The decision came after the annual report by one of the Intelligence Services revealed that B was caught in an attempt to exfiltrate stolen intellectual property. The Minister just announced this in parliament, who have formulated questions to learn more details. Using the matrix, this example can be expressed as the following vignette: (see Table 2).

Instrument	Diplomacy
Action	Halt consultations
Paradigm	Diplomacy
Authority	Cabinet/MFA
Legal Basis	Retorsion
Action by	MFA
Oversight	Parliament

Table 2: Vignette for option 2 - Halt diplomatic consultations (Retorsion)

¹¹⁴ The * stand for: non-violent/non-forceful action only.

¹¹⁵ See e.g. Van der Meer 2018.

Another vignette involves a counter-intelligence operation (see option 5 above and Table 3). Based on authorisation by the Minister of Home Affairs, the General Intelligence and Security Service (AIVD), has taken control over a command and control server located in State B that was used by one of B's proxies, to steer a large botnet threatening to overload C2000 communications. The Minister has informed the Parliamentary Intelligence Committee (CIVD), and the Review Committee on the Intelligence and Security Services (CTIVD) is aware of the operation and will evaluate the legitimacy of the operation in the coming year.

Instrument	Informational (Intelligence)
Action	Take control of C2-server
Paradigm	Counter-Intelligence
Authority	Minister Home Affairs
Legal Basis	Counter Measures
Action by	Intelligence Service (AIVD)
Oversight	Parliament (CIVD) & CTIVD

Table 3: Vignette for option 5 – Counter Intelligence operation (Counter measures)

7. Conclusion

Contemporary conflicts are no longer exclusively fought in the military domain, if they ever were. Other arenas and instruments of power have come to the fore. Next to military power, economic, diplomatic, cultural, legal and especially informational means are important in today's world in which physical confrontation is often absent or less relevant, *inter alia* due to the emergence of cyberspace as an omnipresent domain of engagement.

In order to effectively apply State power, through whatever instrument, the capacities need to be in place as well as the will to apply them. An often-overlooked factor however is the conceptual component: a clear idea on how to apply the instruments, the relevance of which only increases with the widening set of instruments of power States may consider, or be forced to employ, such as cyber operations.

For democratic states the conceptual component fundamentally includes the legal framework and proper and well-established institutional arrangements.

The legal framework, often undervalued, generates the conceptual legitimate basis for executing operations, including deterrence operations. It includes the legal basis in terms of proper authority and decision-making procedures, legal regimes, accountability and oversight mechanisms. Moreover, the framework must not merely exist, it must be trained in a cross-domain setting, because in case essential parts of the legal framework are lacking, outdated, not well known or badly rehearsed, the conceptual component is suboptimal, and credibility, hence also effectiveness, of the deterrent instrument could be at stake.

Although this framework was set up within cyberspace and with cyber threats as a starting point, the argument is that in its generic shape, this legal framework is relevant outside cyberspace in expressing the State's will and for countering outside threats. The framework itself, composed of international legal bases and other national legal elements, is presented here in a matrix, combining all instruments of powers, and applicable legal bases enabling the actual or potential use of those instruments in their various modalities.

The matrix also demonstrates that other strategic functions could benefit from the idea that power entails capacities, concepts to use it, and the actual will to do so. The examples demonstrated that threats from one domain could be countered by responses in another domain. The legal framework thus may empower the ambition to effectuate so-called cross domain deterrence.

References

AIV/CAVV (2011) Advisory Council on International Affairs/Advisory Committee on Issues of Public International Law. Cyber Warfare. Advisory Report no. 77/22. Online at: www.aiv-advice.nl or www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare.

Algemene Rekenkamer (2019) Strengthening the digital defences: the cyber security and critical water structures. ARK, Den Haag, via <https://english.rekenkamer.nl/publications/reports/2019/03/28/strengthening-the-digital-defences-the-cyber-security-of-critical-water-structure>

Bellinger III J (2020) Suing China over the coronavirus won't help. Here's what can work. In: The Washington Post, (23 April 2020), via <https://www.washingtonpost.com/opinions/2020/04/23/suing-china-over-coronavirus-wont-help-heres-what-can-work/>

Betz DJ, Stevens T (2011) Cyberspace and the state: toward a strategy for cyber-power (Ser. Adelphi series, 424) International Institute for Strategic Studies (IISS). Online via

Biddle, S (2006) Military Power: Explaining Victory and Defeat in Modern Battle, 5th ed, Princeton University Press

Boddens Hosang JFR (2015) Force Protection, Unit Self-Defence, and Personal Self-Defence: Their Relationship to Rules of Engagement. In: Gill TD, Fleck D (2015) [eds.] The Handbook of the International Law of Military Operations, (2nd ed.) Oxford University Press, Oxford, Chapter 24, pp. 476-501

Boddens Hosang JFR, Ducheine PAL (2020) Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats (SSRN forthcoming), pp. 14-15

Booz Allen (2020) Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations, at <https://www.boozallen.com/c/insight/publication/the-logic-behind-russian-military-cyber-operations.html>

Borghard ED, Lonergan SW (2017) The Logic of Coercion in Cyberspace. In: *Security Studies*. Taylor & Francis, 26(3), pp. 452–481.

Barnett M, Duvall R (2005) Power in International Politics. In: *International Organisation* 59(1):39-75

Delerue F (2019) Reinterpretation or contestation of international law in cyberspace? In: *Israel Law Review*, 52(3), pp. 295–326.

Ducheine PAL (2015a) Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting' in: Ducheine P, Schmitt MN, Osinga FPB (eds) *Targeting: Challenges of Modern Warfare*. TMC Asser Press, The Hague, pp. 201-220. Online SSRN draft at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474091>.

Ducheine PAL (2015b) Military Cyber Operations. In: Gill TD, Fleck D (2015) [eds.] *The Handbook of the International Law of Military Operations*, (2nd ed.) Oxford University Press, Oxford, Chapter 23, pp. 456-475

Ducheine PAL, Arnold KL, Pijpers BMJ (2020) Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces. Online at <https://ssrn.com/abstract=3540732>

Ducheine PAL, Osinga F (eds)(2017) *Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, NLARMS Netherlands Annual review of Military Studies 2017. TMC Asser Press-The Hague

Ducheine PAL, Pijpers BMJ (2020) The Notion of Cyber Operations. In: Tsagourias N, Buchan R (eds) *The Research Handbook on the International Law and Cyberspace*, 2nd edition forthcoming. Edward Elgar, Cheltenham, online at <https://ssrn.com/abstract=3575755>

Ducheine PAL, Pouw EH (2009) Operation Change of Direction: A Short Survey of the Legal Basis and the Applicable Legal Regimes. In: De Weger MJ Osinga FPB e.a. (eds) *Complex operations: Studies on Lebanon (2006) and Afghanistan (2006-present)*. NL Arms - Netherlands Annual Review of Military Studies 2009. Netherlands Defence Academy, Breda, pp. 51-96

Ducheine PAL, Pouw EH (2012a) Legitimizing the Use of Force. In: Van der Meulen J, Vogelaar A, Beeres R, Soeters J (eds) *Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan*. AUP, Amsterdam, Chapter 3, pp. 33-46

Ducheine PAL, Pouw EH (2012b) Controlling the Use of Force: Legal Regimes. In: Van der Meulen J, Vogelaar A, Beeres R, Soeters J (eds) *Mission Uruzgan: Collaborating in multiple coalitions for Afghanistan*. AUP, Amsterdam, Chapter 5, pp. 67-80

Ducheine PAL, Van der Meulen J, Moelker R (2010) Legitimacy and Surveillance: Shifting Patterns of External Control. In: Soeters J, van Fenema PC, Beeres R (eds) *Managing Military Organizations: Theory and Practice*. Routledge, London, pp. 29-41

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

Ducheine PAL, Van Haaster J, Van Harskamp R (2017) Manoeuvring and Generating Effects in the Information Environment. In: Ducheine P, Osinga F (eds) *Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, NLARMS Netherlands Annual review of Military Studies 2017. TMC Asser Press-The Hague, pp. 155-180, online SSRN version: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2979287>

Dutch Safety Board (2020) Patient safety during IT outages in hospitals, , Onderzoeksraad voor de Veiligheid, The Hague, via <https://www.onderzoeksraad.nl/en/media/attachment/2020/2/13/patient_safety_during_it_outages_in_hospitals.pdf>

Finnemore M, Hollis DB (2019) Beyond Naming and Shaming: Accusations and International Law in Cybersecurity, online at <https://ssrn.com/abstract=3347958>

Fischerkeller MP and Harknett RJ (2017) Deterrence is Not a Credible Strategy for Cyberspace, In: *Orbis*. Foreign Policy Research Institute, 61(3), pp. 381–393.

France (2019) International law applied to operations in cyberspace. Online at <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf>

Geiss R, Lahmann H (2013) Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention. In: Ziolkowski K (ed) *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. NATO CCDCOE, Tallinn, pp. 621-658. Available at SSRN: <<https://ssrn.com/abstract=2462950><

Gibson W (2018) *Neuromancer*, Ace. New York - 320 p. 22cm: Penguin Press.

Gill TD (1992) The Forcible Protection, Affirmation and Exercise of Rights by States under Customary International Law. In: *Netherlands Yearbook of International Law* 23:105-173.

Gill TD (2013) Non-Intervention in the Cyber Context. In: Ziolkowski K (ed) *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. NATO CCDCOE, Tallinn, pp. 217-238

Gill TD (2015) Legal Basis of the Right of Self-Defence Under the UN Charter and Under Customary International Law. In: Gill TD, Fleck D (2015) [eds.] *The Handbook of the International Law of Military Operations*, (2nd ed.) Oxford University Press, Oxford, Chapter 8, pp. 213-224

Gill TD, Ducheine PAL (2012) Anticipatory Self-Defence in Cyber Warfare. In: Schmitt M (ed) *Cyber War and International Law*, 89 *International Law Studies* 2012, pp. 438-471, via <<https://digital-commons.usnwc.edu/ils/vol89/iss1/6/>>.

Gill TD, Ducheine PAL (2015) Rescue of Nationals. In: Gill TD, Fleck D (2015) [eds.] *The Handbook of the International Law of Military Operations*, (2nd ed.) Oxford University Press, Oxford, Chapter 12, pp. 240-243

Gill TD, Fleck D (2015) [eds.] *The Handbook of the International Law of Military Operations*, (2nd ed.) Oxford University Press, Oxford

Giumelli F (2017) Winning Without Killing: The Case for Targeted Sanctions. In: Ducheine P, Osinga F (eds) *Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, NLARMS Netherlands Annual review of Military Studies 2017. TMC Asser Press-The Hague, pp. 91-106

Jakobsen PV (1998) *Western Use of Coercive Diplomacy After the Cold War*, MacMillan, London.

Jakobsen PV (2007) Coercive Diplomacy, in Alan Collins, *Contemporary Security Policy*, Oxford University Press, pp. 225-247

Jakobsen PV (2011) Pushing the limits of military coercion theory, in: *International Studies Perspectives* 12:153–170

Kitzen M (2012a) Close encounters of the tribal kind: the implementation of co-option as a tool for de-escalation of conflict: the case of the Netherlands in Afghanistan's Uruzgan Province. *Journal of Strategic Studies* 35(5):713–734

Kitzen M (2012b) Western military culture and counter-insurgency, an ambiguous reality. *Scientia Militaria: South African Journal of Military Studies* 40(1):123–134

Koh HH (2012) International Law in Cyberspace. In: *Faculty Scholarship Series*, 4854, pp. 1–9.

Kuehl DT (2009) From Cyberspace to Cyberpower. In Kramer, F. D., Starr, S. H., and Wentz, L. K. (eds) *Cyberpower and National Security*. University of Nebraska Press, pp. 24–42. doi: 10.2307/j.ctt1djmhj1.7.

Łoś R (2019) U.S. and China: Hard and Soft Power Potential. In: *International Studies. Interdisciplinary Political and Cultural Journal* 22(1):39-50. Online at <<https://doi.org/10.18778/1641-4233.22.03>>.

Mann M (2013) The Sources of My Sources. *Contemporary Sociology: A Journal of Reviews* 42(4):499-502

Max Planck Encyclopedia of Public International Law [MPEPIL]. Online at: <<https://opil.ouplaw.com/home/mpil>>.

NATO (2016) *Warsaw Summit Communiqué*, (July), pp. 1–30.

NATO (2017) *Allied Joint Doctrine - AJP 01*.

- Nye Jr. JS (2013) Hard, Soft, and Smart Power. In: Cooper, A. F., Heine, J., and Thakur, R. (eds) *The Oxford Handbook of Modern Diplomacy*, pp. 1–17.
- Nye Jr. JS (2016) Deterrence and Dissuasion in Cyberspace. In: *International Security*, 41(3), pp. 44–71.
- New York Times (2018), Italy Orders Seizure of Migrant Rescue Ship, 20 Nov 2018, at <<https://www.nytimes.com/2018/11/20/world/europe/italy-aquarius-seizure-order.html>>
- New York Times (2019), U.S. Seizes North Korean Ship for Violating Sanctions, 9 May 9 2019, at <https://www.nytimes.com/2019/05/09/us/politics/wise-honest-north-korea-ship-seized.html>;
- NL Defence Staff (2019) Netherlands' Defence Doctrine. Ministry of Defence, The Hague. Online via <<https://english.defensie.nl/downloads/publications/2019/06/27/netherlands-defence-doctrine>>
- Pirker B (2013) Territorial Sovereignty and Integrity and the Challenges of Cyberspace. In: Ziolkowski K (ed) *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. NATO CCDCOE, Tallinn, 194–199
- Qiao Liang, Wang Xiangsui, *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999, via <https://archive.org/details/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/mode/2up>.
- Rid T, Buchanan B (2015) Attributing Cyber Attacks In: *Journal of Strategic Studies* 38(1–2), 4–37
- Rodriguez CA, Walton TC, Hyong C (2020) Putting the "fil" into "dime": growing joint understanding of the instruments of power. In: *Joint Force Quarterly* 97(2):121-128
- Sanger DE (2016) Obama Strikes Back at Russia for Election Hacking. In: *New York Times* (Dec. 29), at <<https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html>>
- Sari A (2020) Hybrid threats and the law: Concepts, trends and implications. Hybrid Centre of Excellence Trend Report 3 (April), via <https://www.hybridcoe.fi/wp-content/uploads/2020/05/Hybrid-CoE-Trend-Report-3.pdf>
- Schroeder R (2015) Introduction: the IEMP model and its critics. In: Hall JA, Schroeder R (eds) *An Anatomy of Power: The Social Theory of Michael Mann*. Cambridge University Press, Cambridge, pp. 1-16
- Schmitt MN (ed)(2013a) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, Cambridge

Schmitt MN (2013b) 'Cyber Activities and the Law of Countermeasures', in: Ziolkowski K (ed.) *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. NATO CCDCOE, Tallinn, pp. 659-690

Schmitt MN (2014a) 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. In: *Virginia Journal of International Law* 54. Available at SSRN: <https://ssrn.com/abstract=2353898>

Schmitt MN (2014b) Normative Voids and Asymmetry in Cyberspace. In: *Just Security* (29 December), at <<http://justsecurity.org/18685/normative-voids-asymmetry-cyberspace>>

Schmitt MN (ed)(2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge University Press, Cambridge

Smeets M, Work JD (2020) Operational Decision-Making for Cyber Operations: In search of a Model, In: *The Cyber Defense Review* (March), via <<https://cyberdefensereview.army.mil/About-CDR/>>.

Smeets M, Soesanto S (2020) Cyber Deterrence Is Dead. Long Live Cyber Deterrence! In: *Council on Foreign Affairs*, pp. 1–6.

Taddeo M (2018) 'The Limits of Deterrence Theory in Cyberspace', *Philosophy and Technology*. *Philosophy & Technology*, 31(3), pp. 339–355. doi: 10.1007/s13347-017-0290-2.

Tallinn Manual (2013), see Schmitt (2013).

Tallinn Manual 2.0 (2017), see Schmitt (2017).

UK Ministry of Defence (2010) *Joint Doctrine Publication 04: Understanding a (JDP 04)* (1st ed). DCDC, Swindon, online at: <<http://knowreqts.yolasite.com/resources/1.3%20%20JDP04%20Understanding.pdf>>.

UK Ministry of Defence (2011) *Joint Doctrine Publication 0-01: British Defence Doctrine*

UK Ministry of Defence (2017) *Land operations - ADP AC 71940*. Centre Land War Doctrine

UK Foreign and Commonwealth Office (2020) Press release UK condemns cyber actors seeking to benefit from global coronavirus pandemic.

US Cyber Command (2018) *Achieve and Maintain Cyberspace Superiority*.

US DOJ (2018a) Department of Justice: Internet Research Agency Indictment. At <<https://www.justice.gov/file/1035477/download>>.

US DOJ (2018b) Department of Justice: GRU Indictment. At <<https://www.justice.gov/file/1080281/download>>.

US Joint Chiefs of Staff (2013) Joint Publication 1: Doctrine for the Armed Forces of the United States

US White House (2016) Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29), at <https://perma.cc/C83Z-SQSL>

Van den Boogaard JC (2019) Proportionality in international humanitarian law (PhD-University of Amsterdam) via: <<https://hdl.handle.net/11245.1/57363698-c6b8-458d-9033-0fd9cfc9bb91>>.

Van der Meer S (2018) State-level responses to massive cyber-attacks: a policy toolbox, Clingendael Policy Brief (December), via <https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf>

Van Haaster J (2019) On cyber: the utility of military cyber operations during armed conflict (PhD University of Amsterdam) NLDA, Breda, online at <https://pure.uva.nl/ws/files/37093787/Thesis.pdf>

Voetelink J (2015) Status of forces: criminal jurisdiction over military personnel abroad. TMC Asser Press, The Hague

Voetelink JED (2017) Reframing Lawfare. In: Ducheine P, Osinga F (eds)(2017) Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises, NLARMS Netherlands Annual review of Military Studies 2017. TMC Asser Press-The Hague

Whyte C (2016) Ending cyber coercion: Computer network attack, exploitation and the case of North Korea. In: Comparative Strategy. Taylor & Francis, 35(2), pp. 93–102. doi: 10.1080/01495933.2016.1176453.

Wiltenburg IL (2019) Security force assistance: practised but not substantiated. In: Militaire Spectator 188(2):88-99. Online at <[https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire Spectator 2-2019 Wiltenburg.pdf](https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire_Spectator_2-2019_Wiltenburg.pdf)>.

WRR (2019) Netherlands Scientific Council for Government Policy. Preparing for Digital Disruption (Summary), WRR-report no. 101. WRR, Den Haag, via <<https://english.wrr.nl/topics/digital-disruption/documents/reports/2019/09/24/preparing-for-digital-disruption>>

Young N (2009) The Cultural Crusades. In: New Internationalist 423:8–10, online at <https://newint.org/features/2009/06/01/culture>

Ziolkowski K (2013) General Principles of International Law as Applicable in Cyberspace. In: Ziolkowski K (ed.) Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy. NATO CCDCOE, Tallinn

Brigadier-General Dr. Paul Ducheine, LL.M. MSc is Professor of Cyber Operations at the Netherlands Defence Academy (NLDA) and Endowed Professor of Military Law of Cyber Operations and Cyber Security at the University of Amsterdam.

Colonel Peter Pijpers LL.M. MSc is Associate Professor for Cyber Operations at the NLDA and PhD Candidate at the University of Amsterdam.