Chapter 25
The Missing Component in Deterrence Theory: The Legal Framework

Paul Ducheine and Peter Pijpers

Contents

Abstract This chapter takes the starting point that the 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 com-

P. Ducheine (✉) · P. Pijpers
Netherlands Defence Academy (NLDA), Breda, The Netherlands
e-mail: p.a.l.ducheine@uva.nl

P. Pijpers
e-mail: b.m.j.pijpers@uva.nl

P. Ducheine
University of Amsterdam, Amsterdam, The Netherlands

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_25

ponents 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

25.1 Introduction

"*The supreme art of war is to subdue the enemy without fighting.*"

Sun Zsu, 6th century BC

25.1.1 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

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

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]

25.1.2 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).

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

[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.

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]

25.1.3 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 cyberspace[11] 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.

---

[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, Bulletin 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-Attack, at https://attack.mitre.org/groups/; Booz Allen 2020.

[14]US Cyber Command 2018.

Applying the instruments 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 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 values[18] 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.

25.1.4 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 have not been analysed, realistic decision-making procedures are lacking, or competent bodies authorising the use of capabilities in response of threats have not been designated, deterrence by punishment is illusive. For deterrence to be

[15]Jakobsen 1998, ch 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 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.

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 (see Chap. 8 by Sweijs and Zilinck), 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 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. 25.2). Secondly, the components of power and the legal framework as a conceptual element therein are covered (Sect. 25.3). Next, the legal framework itself is analysed in two parts: the legal bases (Sect. 25.4) building on international law and other relevant elements (Sect. 25.5) building on the Netherlands' institutional arrangements, after which a matrix is presented offering legal options related to the instruments of power (Sect. 25.6).

[20]Nye 2016, pp. 58–62.

[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.

25.2 Power Instruments

Power instruments are often briefly summarized as DIME: diplomacy, information, military and 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 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-kinetic[26] (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.

---

[22]Mann 2013, p. 502; Schroeder 2015, p. 2; UK Ministry of Defence 2011, pp. 1–6; US Joint Chiefs of Staff 2013, p. 1–12.

[23]Van Haaster 2019, p. 64; Rodriguez et al. 2020.

[24]Nye 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.

[26]Ducheine 2015a.

[27]Wiltenburg 2019.

[28]Ducheine et al. 2017.

[29]Giumelli 2017.

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 instrument[33] 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 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

[30]Nye 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, 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 and Stevens 2011: compulsory power. See the four categories by Barnett and Duvall 2005, p. 43: compulsory, structural, institutional and productive power.

Facebook, Twitter and 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.

25.3 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 Sect. 25.1.3 and mindful of earlier academic and doctrinal work,[43] power requires (1) capacities, most often the so-called physical components (i.e. 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, and 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

[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 and Tencent). As on 31 March 2020. Market capitalization is calculated from the share price (as recorded on the 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".

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 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]

25.4 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 basis for *non-forceful action* (e.g. economic sanctions, or declaring diplomats *persona non grata*) is 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

[46]Ducheine and Pouw 2009, 2012a.

[47]Ducheine et al. 2020.

[48]See e.g. Ducheine and Pouw 2009, 2012b.

[49]Ducheine et al. 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.

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.

25.4.1 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 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]

25.4.2 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

[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.

[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.

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 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

[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 MPEFIL, 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.

[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".

"misleading a prospective intervening party by providing it with bogus or useless information or otherwise diverting cyber break-ins from their intended targets".[67]

25.4.3 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]

25.4.4 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.

---

[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 and Schmitt 2017.

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 to 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 other real possibility of taking action to address the damage caused or threatened exists, 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.

25.4.5 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:

---

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

[76]Schmitt 2013, p. 663,2014b: "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.

self-defence.[83] 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 Chapter are in-effective, not feasible or not

[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 2012, p. 443, 2015. See also Tallinn Manual 2013, Rules 13–17.

[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.

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 basis 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.

25.4.6 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 cyber-space,[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

[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.

[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). 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.

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 Netherlands[98] 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 financial system or prevents the government from carrying out essential tasks" could well be equated with an armed attack.[102]

25.5 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

[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 and Australia.

[100]France 2019, p. 8.

[101]See AIV/CAVV 2011, p. 21.

[102]See AIV/CAVV 2011, p. 21.

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.[106] 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 therefore unable to respond or deter at all. Detection capacities also require conceptual (i.a. legal) backing, before capabilities emanate. 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 it followed 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 address the responsible State (and author)[107] and if necessary, seek (legal) retribution.[108] But this 'naming and shaming' will not always follow suit;[109] 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.[110]

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

[103]See *supra* n 47.

[104]See *supra* n 48.

[105]See *supra* n 49.

[106]Rid and Buchanan 2015; Bijleveld 2018.

[107]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.

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

[109]Finnemore and Hollis 2019.

[110]US White House 2016; UK Foreign and Commonwealth Office 2020.

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 political[111] or operational[112] 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.

25.6 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 25.1 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,[113] a few fictitious examples for the

Table 25.1 Legal bases matrix

Legal basis instrument	Consent	Retorsion	Countermeasures	Plea of necessity	Self-defence
Diplomacy	1	2			
Information and knowledge (incl. Intelligence)	3	4	5	6	7
Military	8	9*	10*	11*	12
Economy and financial	13	14	15	16	
Culture	17	18			
Legal	19	20	21	22	

The * stand for: non-violent/non-forceful action only
(*Source* Ducheine and Pijpers)

[111] See *supra* n 47.

[112] See e.g. Smeets and Work 2020.

[113] Fictitiously ranging from 1 to 22 in the matrix (Table 25.1).

Table 25.2 Vignette for option 2—Halt diplomatic consultations (Retorsion)

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

(*Source* Ducheine and Pijpers)

Table 25.3 Vignette for option 5—Counter-Intelligence operation (countermeasures)

Instrument	Informational (intelligence)
Action	Take control of C2-server
Paradigm	Countermeasures
Authority	Minister home affairs
Legal basis	Countermeasures
Action by	Intelligence service (AIVD)
Oversight	Parliament (CIVD) and CTIVD

(*Source* Ducheine and Pijpers)

Netherlands' institutional and constitutional setting, including the EU framework, will serve to demonstrate the logic and value of the matrix.[114]

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 and Table 25.2).[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 (see Table 25.2).

Another vignette involves a counter-intelligence operation (see option 5, and Table 25.3). Based on authorisation by the Minster 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.

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

[115]See e.g. Van der Meer 2018.

25.7 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. Accessed 1 May 2020

Algemene Rekenkamer (2019) Strengthening the digital defences: the cyber security and critical water structures. ARK, The Hague. 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. The Washington Post. https://www.washingtonpost.com/opinions/2020/04/23/suing-china-over-coronavirus-wont-help-heres-what-can-work/. Accessed 23 April 2020

Betz D J, Stevens T (2011) Cyberspace and the state: toward a strategy for cyber-power. Adelphi Series, 424. International Institute for Strategic Studies (IISS). Online via. http://dx.doi.org/10.1080/19445571.2011.636954

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

Bijleveld A (2018) We have to steer the cyber domain, before it steers us (keynote speech). Militair Rechtelijk Tijdschrift. https://puc.overheid.nl/mrt/doc/PUC_248478_11/1/. Accessed 23 April 2020

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

Boddens Hosang J F R, 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. Accessed 1 May 2020

Borghard E D, Lonergan S W (2017) The Logic of Coercion in Cyberspace. Security Studies 26.3, pp 452–481

Barnett M, Duvall R (2005) Power in International Politics. International Organisation 59.1:39–75

Delerue F (2019) Reinterpretation or contestation of international law in cyberspace? Israel Law Review, 52.3, pp 295–326

Ducheine P A L (2015a) Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting. In: Ducheine P, Schmitt M N, Osinga F P B (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 P A L (2015b) Military Cyber Operations. In: Gill T D, Fleck D (eds) The Handbook of the International Law of Military Operations, 2nd edn. Oxford University Press, Oxford, Chapter 23, pp 456–475

Ducheine P A L, Arnold K L, Pijpers B M J (2020) Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces. https://ssrn.com/abstract=3540732. Accessed 1 May 2020

Ducheine P A L, Osinga F (2017) Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises, NL ARMS Netherlands Annual Review of Military Studies 2017. TMC Asser Press, The Hague

Ducheine P A L, Pijpers B M J (2020) The Notion of Cyber Operations. In: Tsagourias N, Buchan R (eds) The Research Handbook on the International Law and Cyberspace, 2nd edn. forthcoming. Edward Elgar, Cheltenham. https://ssrn.com/abstract=3575755. Accessed 1 May 2020

Ducheine P A L, Pouw E H (2009) Operation Change of Direction: A Short Survey of the Legal Basis and the Applicable Legal Regimes. In: De Weger M J, Osinga F P B (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 P A L, Pouw E H (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 P A L, Pouw E H (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 P A L, Van der Meulen J, Moelker R (2010) Legitimacy and Surveillance: Shifting Patterns of External Control. In: Soeters J, van Fenema P C, Beeres R (eds) Managing Military Organizations: Theory and Practice. Routledge, London, pp 29–41

Ducheine P A L, 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 P A L, 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, NL ARMS 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. https://www.onderzoeksraad.nl/en/media/attachment/2020/2/13/patient_safety_during_it_outages_in_hospitals.pdf. Accessed 1 May 2020

Finnemore M, Hollis D B (2019) Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. https://ssrn.com/abstract=3347958. Accessed 1 May 2020

Fischerkeller M P, Harknett R J (2017) Deterrence is Not a Credible Strategy for Cyberspace, In: Foreign Policy Research Institute (ed) Orbis 61.3, pp 381–393

France (2019) International law applied to operations in cyberspace. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf. Accessed 1 May 2020

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 SSRN: https://ssrn.com/abstract=2462950

Gibson W (2018) Neuromancer, Ace. Penguin Press, New York, p 22

Gill T D (1992) The Forcible Protection, Affirmation and Exercise of Rights by States under Customary International Law. Netherlands Yearbook of International Law 23:105–173

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

Gill T D, Ducheine P A L (2012) Anticipatory Self-Defence in Cyber Warfare. In: Schmitt M (ed) Cyber War and International Law. 89 International Law Studies 2012, pp 438-471. https://digital-commons.usnwc.edu/ils/vol89/iss1/6/

Gill T D, Ducheine P A L (2015) Rescue of Nationals. In: Gill T D, Fleck D (eds) The Handbook of the International Law of Military Operations, 2nd edn. Oxford University Press, Oxford, Chapter 12, pp 240–243

Gill T D, Fleck D (eds) (2015) The Handbook of the International Law of Military Operations, 2nd edn. 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, NL ARMS Netherlands Annual Review of Military Studies 2017. TMC Asser Press, The Hague, pp 91–106

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

Jakobsen P V (2007) Coercive Diplomacy. In: Collins A (ed) Contemporary Security Policy. Oxford University Press, pp 225–247

Jakobsen P V (2011) Pushing the limits of military coercion theory. 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 ambigious reality. Scientia Militaria: South African Journal of Military Studies 40.1:123–134
Koh H H (2012) International Law in Cyberspace. Faculty Scholarship Series, 4854, pp 1–9
Kuehl D T (2009) From Cyberspace to Cyberpower. In: Kramer F D, Starr S H, Wentz L K (eds) Cyberpower and National Security. University of Nebraska Press, pp 24–42. https://doi.org/10.2307/j.ctt1djmhj1.7
Łoś R (2019) U.S. and China: Hard and Soft Power Potential. International Studies. Interdisciplinary Political and Cultural Journal 22(1):39–50. 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]. https://opil.ouplaw.com/home/mpil. Accessed 1 May 2020
NATO (2016) Warsaw Summit Communiqué, (July), pp 1–30
NATO (2017) Allied Joint Doctrine - AJP 01
Nye Jr J S (2013) Hard, Soft, and Smart Power. In: Cooper A F, Heine J, Thakur R (eds) The Oxford Handbook of Modern Diplomacy, pp 1–17
Nye Jr J S (2016) Deterrence and Dissuasion in Cyberspace. International Security, 41.3:44–71
New York Times (2018) Italy Orders Seizure of Migrant Rescue Ship, 20 November 2018. https://www.nytimes.com/2018/11/20/world/europe/italy-aquarius-seizure-order.html. Accessed 1 May 2020
New York Times (2019) U.S. Seizes North Korean Ship for Violating Sanctions, 9 May 2019 https://www.nytimes.com/2019/05/09/us/politics/wise-honest-north-korea-ship-seized.html. Accessed 1 May 2020
NL Defence Staff (2019) Netherlands' Defence Doctrine. Ministry of Defence, The Hague. https://english.defensie.nl/downloads/publications/2019/06/27/netherlands-defence-doctrine. Accessed 1 May 2020
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, pp 194–199
Qiao L, Wang X (1999) Unrestricted Warfare. PLA Literature and Arts Publishing House, Beijing. https://archive.org/details/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/mode/2up
Rid T, Buchanan B (2015) Attributing Cyber Attacks. Journal of Strategic Studies 38(1–2):4–37
Rodriguez C A, Walton T C, Hyong C (2020) Putting the "fil" into "dime": growing joint understanding of the instruments of power. Joint Force Quarterly 97.2:121–128
Sanger D E (2016) Obama Strikes Back at Russia for Election Hacking. In: New York Times (29 December 2016) https://www.nytimes.com/2016/12/29/us/politics/russia-electon-hacking-sanctions.html. Accessed 1 May 2020
Sari A (2020) Hybrid threats and the law: Concepts, trends and implications. Hybrid Centre of Excellence Trend Report 3 (April) https://www.hybridcoe.fi/wp-content/uploads/2020/05/Hybrid-CoE-Trend-Report-3.pdf. Accessed 1 May 2020
Schmitt M N (2013a) Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, Cambridge
Schmitt M N (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 M N (2014a) 'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law. Virginia Journal of International Law 54 https://ssrn.com/abstract=2353898. Accessed 1 May 2020

Schmitt M N (2014b) Normative Voids and Asymmetry in Cyberspace. Just Security (29 December 2014). http://justsecurity.org/18685/normative-voids-asymmetry-cyberspace. Accessed 1 May 2020
Schmitt M N (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn. Cambridge University Press, Cambridge
Schroeder R (2015) Introduction: the IEMP model and its critics. In: Hall J A, Schroeder R (eds) An Anatomy of Power: The Social Theory of Michael Mann. Cambridge University Press, Cambridge, pp 1–16
Smeets M, Soesanto S (2020) Cyber Deterrence Is Dead. Long Live Cyber Deterrence! Council on Foreign Affairs, pp 1–6
Smeets M, Work J D (2020) Operational Decision-Making for Cyber Operations: In Search of a Model. The Cyber Defense Review (March). https://cyberdefensereview.army.mil/About-CDR/. Accessed 1 May 2020
Taddeo M (2018) The Limits of Deterrence Theory in Cyberspace. Philosophy & Technology 31.3:339–355. https://doi.org/10.1007/s13347-017-0290-2
Tallinn Manual (2013), see Schmitt M N (2013a)
Tallinn Manual 2.0 (2017), see Schmitt M N (2017)
UK Ministry of Defence (2010) Joint Doctrine Publication 04: Understanding a JDP 04, 1st edn. DCDC, Swindon. http://knowreqts.yolasite.com/resources/1.3%20%20JDP04%20Understanding.pdf. Accessed 1 May 2020
UK Foreign and Commonwealth Office (2020) Press release—UK condemns cyber actors seeking to benefit from global coronavirus pandemic
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
US Cyber Command (2018) Achieve and Maintain Cyberspace Superiority
US DOJ (2018a) Department of Justice: Internet Research Agency Indictment https://www.justice.gov/file/1035477/download. Accessed 1 May 2020
US DOJ (2018b) Department of Justice: GRU Indictment. https://www.justice.gov/file/1080281/download. Accessed 1 May 2020
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 (29 December 2016) https://perma.cc/C83Z-SQSL. Accessed 1 May 2020
Van den Boogaard J C (2019) Proportionality in international humanitarian law .PhD, University of Amsterdam. https://hdl.handle.net/11245.1/57363698-c6b8-458d-9033-0fd9cfc9bb91. Accessed 1 May 2020
Van der Meer S (2018) State-level responses to massive cyber-attacks: a policy toolbox. Clingendael Policy Brief (December). https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf. Accessed 1 May 2020
Van Haaster J (2019) On cyber: the utility of military cyber operations during armed conflict. PhD, University of Amsterdam, NLDA, Breda. https://pure.uva.nl/ws/files/37093787/Thesis.pdf. Accessed 1 May 2020
Voetelink J (2015) Status of forces: criminal jurisdiction over military personnel abroad. TMC Asser Press, The Hague
Voetelink J E D (2017) Reframing Lawfare. 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
Whyte C (2016) Ending cyber coercion: Computer network attack, exploitation and the case of North Korea. Comparative strategy, 35.2:93–102. https://doi.org/10.1080/01495933.2016.1176453
Wiltenburg I L (2019) Security force assistance: practised but not substantiated. Militaire Spectator 188(2):88-99. https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/MilitaireSpectator2-2019Wiltenburg.pdf

WRR (2019) Netherlands Scientific Council for Government Policy. Preparing for Digital Disruption (Summary), WRR-report no. 101. WRR, The Hague. https://english.wrr.nl/topics/digital-disruption/documents/reports/2019/09/24/preparing-for-digital-disruption. Accessed 1 May 2020

Young N (2009) The Cultural Crusades. New Internationalist 423:8–10 https://newint.org/features/2009/06/01/culture. Accessed 1 May 2020

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

Paul Ducheine (Ph.D.) is an active serving general officer of the Netherlands Army and Professor of Cyber Operations at the Netherlands Defence Academy (NLDA), as well as Endowed Professor of Military Law of Cyber Operations and Cyber Security at the University of Amsterdam.

Peter Pijpers is Associate Professor for Cyber Operations at the Netherlands Defence Academy and Ph.D. Candidate at the University of Amsterdam.