Decision-Making and Parliamentary Control for International Military Cyber Operations by the Netherlands Armed Forces

Ducheine, P.A.L.; Arnold, K.L.; Pijpers, B.M.J.

DOI
10.2139/ssrn.3540732
10.1007/978-94-6265-395-5_5

Publication date
2021

Document Version
Author accepted manuscript

Published in
Military Operations and the Notion of Control Under International Law

UNIVERSITY OF AMSTERDAM

DECISION-MAKING AND PARLIAMENTARY CONTROL FOR INTERNATIONAL MILITARY CYBER OPERATIONS BY THE NETHERLANDS ARMED FORCES

P.A.L. Ducheine

K.L. Arnold

B.M.J. Pijpers

Amsterdam Law School Legal Studies Research Paper No. 2020-07

Amsterdam Center for International Law No. 2020-06

Decision-making and parliamentary control for international military cyber operations by the Netherlands armed forces

Paul Ducheine, Kraesten Arnold and Peter Pijpers♠

Abstract
This chapter focuses on the highly pertinent issues of political decision-making, the provision of information to parliament and parliamentary control related to the international 'deployment' of military cyber capabilities by the Netherlands armed forces. These military cyber operations will be based on the threefold purpose taken from the Constitution: defending the Kingdom, including collective defence; maintaining and promoting the international legal order; and protecting other (vital) interests of the Kingdom.

The chapter's main conclusions are, first, that in all cases, the deployment of cyber capabilities is a political decision that rests with the government. Therein, the government always takes note of the Chief of Defence's (CHOD) military advice and the Military Intelligence and Security Service's (MIVD) assessment. Second, in all cases, a proper international legal basis and mandate for the cross-border deployment of cyber capabilities is required. Notwithstanding government's supreme authority over the armed forces, in all cases, the deployment of cyber capabilities by the government is also subject to parliamentary control and oversight, although the way in which it does so differs according to the purpose or core task concerned.

The chapter concludes that the decision-making, information procedure and parliamentary control usually adheres to the standard model, based on the Article 100 of the Constitution for 'maintaining and promoting the international legal order' as the basic modus operandi warranting a normal political control and accountability process. The procedure for deployments related to self-defence formally differs from the so called Article 100 procedure, but in terms of substance displays many similarities with it. The same applies to the expeditionary protection of other vital interests of the Kingdom.

The procedure is different for specific operations in cyberspace that are classified as 'special operations' owing to their 'substantial political and military risks and the need for strict secrecy'. The decision to deploy is made by the Ministerial Core Group on Special Operations (MKSO), which determines when and to what extent to involve or inform the rest of the government. It also decides how and when parliament should be informed. This evidently impacts on the features of parliamentary control.

♠ This chapter is an updated and supplemented version of the article published in Dutch: P. Ducheine & K. Arnold, 'Besluitvorming bij cyberoperaties' in: Militaire Spectator, Vol 184, 2015-2, pp. 56-70 <http://www.militairespectator.nl/thema/recht-cyberoperations/artikel/besluitvorming-bij-cyberoperaties>. The authors wish to thank Colonel RNLAF (ret.) Dr. Joop Voetelink once again for his suggestions.

In short, although the government ultimately decides whether or not to commit military cyber capabilities to cross border military operations, its decision is subject to regular parliamentary control and oversight.

Contents

P.A.L. Ducheine, B.M.J. Pijpers
Netherlands Defence Academy & University of Amsterdam, The Netherlands
e-mail: p.a.l.ducheine@uva.nl
b.m.j.pijpers@uva.nl
K.L. Arnold
Netherlands Defence Academy, The Netherlands
e-mail: KL.Arnold@mindef.nl

1.1. Introduction

The establishment of the Defence Cyber Command marks an important step in the Netherlands' military development in cyberspace.[1] Since the end of 2015, the government could rely on digital capability as part of fighting power comprising capacities as well as conceptual and moral components. After all, no capability without capacities, whilst

[1] See: Ducheine, van Haaster & van Harskamp 2017, pp. 159-161.

capacities are useless without the political will to deploy them or if the appropriate decision-making procedures have not been identified. However, the core question is, whether the ubiquitous attributes of cyberspace and cyber operations induce alterations in the existing procedures? In this chapter, we analyse and describe the various procedures for political decision-making on the deployment of these cyber capabilities and for informing parliament.

With the establishment of the Defence Cyber Command (DCC) on 25 September 2014, the then Minister of Defence, Jeanine Hennis-Plasschaert, gave a further impulse to the Defence Cyber Strategy launched by her predecessor at the Netherlands Defence Academy in June 2012.[2] Among the strategy's six focal points, the following three have attracted the most attention: strengthening the digital resilience of the Defence organisation (defensive element); developing the military capability to conduct cyber operations (offensive element); and strengthening intelligence capabilities in the digital domain (intelligence element).[3]

While defensive measures and efforts to strengthen the digital intelligence capabilities of the Defence Intelligence and Security Service (MIVD) were already underway,[4] the DCC's planned 'military capabilities' had to wait for its official launch, gaining the status of being fully operational capable. In those days, and maybe still today, several issues need to be addressed and resolved. These issues were first discussed at a meeting on cyber warfare, between the Minister of Defence and the Permanent Parliamentary Committees on Defence, Foreign Affairs, the Interior, and Security and Justice, on 26 March 2014.[5]

Many of the questions raised at this meeting concerned the legitimacy and legality of cyber operations.[6] This was not surprising, given that the meeting was prompted by the joint advisory report on cyber warfare of the Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV) of 2011[7] and the government's responses to this report.[8] The AIV/CAVV report focused on two key issues: the legal bases for initiating military (and non-military) cyber operations, and the applicability of international humanitarian law as a legal regime when

---

2 *Parliamentary Papers II 2011-2012*, 33 321, no. 1, Defence Cyber Strategy (hereinafter, DCS), p. 1.

3 DCS, p. 3. This was reiterated in the 'Update of the Defence Cyber Strategy' of 23 February 2015. *Parliamentary Papers II 2014-2015*, 33 321, no. 5; and the Defence Cyber Strategy 2018, *Parliamentary Papers II 2018-2019*, 33 321 no. 9.

4 Including the expansion of the Defence Computer Emergency Response Team (DefCERT) through a joint initiative with the General Intelligence and Security Service (AIVD) and the Joint Sigint Cyber Unit (JSCU).

5 *Parliamentary Papers II 2013-2014*, 33 321, no. 4, Report of a meeting on the Defence Cyber Strategy on 26 March 2014 (hereinafter, DCS meeting report).

6 Legitimacy comprises legality (legal basis and legal regimes) and public support. See: Ducheine & Pouw 2012, p. 33.

7 AIV/CAVV, *Cyber Warfare*, advisory report no. 77/22 (December 2011), available at: <ttp://www.aiv-advice.nl> and *Parliamentary Papers II 2011-2012*, 33 000 X, no. 68 (hereinafter, AIV/CAVV report).

8 *Parliamentary Papers II 2011-2012*, 33 000 X, no. 79 and follow-up letters *Parliamentary Papers II 2011-2012*, 33 000 X, no. 99 and *Parliamentary Papers II 2013-2014*, 33 321, no. 3.

conducting military cyber operations.[9] In its initial response, the government broadly accepted the report's findings and recommendations.[10] More recently, the Netherlands government explicitly acknowledged that a cyber attack could trigger the right to self-defence.[11]

These aspects of legitimacy, that is legality – the legal bases (e.g. self-defence) and legal regimes (e.g. international humanitarian law) for cyber operations – have already been examined in an earlier publication.[12]

Issues that have so far received little attention, but which were discussed at length during the above-mentioned 'cyber warfare' parliamentary meeting, are – political – decision-making, the provision of information to parliament and hence the features of parliamentary control and oversight.[13] In other words, who qualifies that the Netherlands faces a cyber attack crossing the threshold of an armed attack, triggering the right to self-defence?[14] Who informs whom?[15] And, of course, who monitors whom?[16] These pertinent questions have not been discussed in much detail.[17]

1.1.1. Aim

In this chapter, we therefore analyse and describe the procedures for political decision-making on and informing parliament about the commitment or deployment of military cyber capabilities in cross border military operations. Our analysis is based on the assumption that - by now - the government actually has such capabilities at its disposal, in addition to regular military units and special forces.[18] We will focus on expeditionary military operations that fall under responsibility of the Chief of Defence, covering the entire breadth of the armed forces' three core tasks. Hence, military police operations and military assistance to the civil authorities in the domestic arena, as well as operations

---

9 For the full text of the request for advice, see AIV/CAVV report, Annex 1.

10 *Parliamentary Papers II 2011-2012*, 33 000 X, no. 79.

11 *Parliamentary Papers II 2018-2019, 3*3 694, no. 47 (International law in cyberspace), p. 4: "at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force" and pp. 8-9 "There is therefore no reason not to qualify a cyberattack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or non-conventional weapons".

12 Ducheine, Voetelink, Stinissen & Gill 2012, pp. 101-128. Ducheine 2015, pp. 456-175; and Ducheine 2016.

13 DCS meeting report, p. 13.

14 MP Angelien Eijsink: 'What is really interesting is who determines whether a cyber-attack should be regarded as an armed attack.' DCS meeting report, p. 13.

15 DCS meeting report, p. 19.

16 *Parliamentary Papers II 2013-2014*, 33 321, no. 4, pp. 3, 10.

17 For a short description, see DCS meeting report, pp. 12-13.

18 Special forces units: Commando Corps and parts of the Marine Corps. These units can carry out both special and regular operations. In the case of special operations, a specific decision-making procedure applies (see paragraph 1.9).

conducted by the Defence Intelligence and Security Service (MIVD) are beyond the scope of this chapter.[19]

In her letter to parliament on offensive cyber capabilities, the Minister of Defence starts from the premise that 'Cyber capabilities [will] form an integral part of the overall military capability of the Netherlands armed forces. […] In terms of planning and implementation, cyber operations are broadly similar to traditional military operations.'[20] Our own premise is that cyber capabilities are a relatively new addition to the spectrum of military capabilities but that their introduction is highly compatible with accepted procedures, doctrines and concepts regarding command and control.[21]

1.1.2. Structure

For armed forces to fulfil their mission in the digital domain,[22] it is vital to define the military objectives as clearly as possible. With this in mind, we start with a description of the constitutional purpose of the Netherlands' armed forces, which is supposed to guide *all* military efforts. We then briefly consider the core tasks of the armed forces. After this, we describe the key actors in the decision-making process on military deployment – government and parliament – and analyse their individual roles. The reason for this approach is that the constitutional purpose of the armed forces also guides the decision-making procedures for and control/oversights mechanisms over military operations.[23]

Next, we analyse the decision-making procedures themselves. We introduce each procedure with a fictitious scenario concerning an expeditionary military cyber operation.

First, we examine the procedure under Article 100 of the Constitution for missions 'to maintain or promote the international legal order' (hereinafter: the Article 100 procedure), followed by the procedure for national or collective defence. Next, we briefly consider the expeditionary protection of vital 'interests of the Kingdom' and missions with overlapping constitutional purposes. Finally, we examine the specific procedure for expeditionary 'special operations'.

1.2. Constitutional purpose

According to Article 97 of the Constitution, the Netherlands armed forces are an instrument of – and in support of – the Netherlands' status as a democracy governed by

---

19 These operations are based on domestic legislation such as the 2012 Police Act and the 2017 Intelligence and Security Services Act. Moreover, these operations are not conducted as military operations under responsibility of the CHoD.

20 *Parliamentary Papers II 2013-2014,* 33 321, no. 3, p. 3. Reiterated in Defence Cyber Strategy 2018, *Parliamentary Papers II 2018-2019*, 33 321 no. 9, p. 13.

21 As can be seen in the Netherlands Armed Forces Doctrine for Military Cyberspace Operations 2019.

22 Taken from the title of a speech by the Minister of Defence, Hans Hillen, in Breda on 27 June 2012 to mark the launch of the DCS.

23 Ducheine 2012, pp. 15-32.

the rule of law. This is apparent from their threefold purpose (first paragraph) and their subordination to the civil authorities (second paragraph):

1. There shall be armed forces for the defence and protection of the interests of the Kingdom, and in order to maintain and promote the international legal order.
2. The Government shall have supreme authority over the armed forces.

The constitutional purpose of the armed forces is threefold. In view of how that purpose is linked to their core tasks we have classified its three elements in the following order:[24]

- defending the Kingdom, including collective defence;[25]
- maintaining and promoting the international legal order;
- protecting other interests of the Kingdom. [26]

These elements can overlap.[27] As a matter of fact, the first two – defending the Kingdom and promoting the international legal order – coincide with several vital interests of the Kingdom.[28] This interpretation is in keeping with the definition of the term 'national security' in the 2007 Strategy National Security,[29] the 2013 International Security Strategy[30] and the 2019 National Security Strategy.[31]

Although their purposes are broadly defined, the armed forces cannot be deployed to protect *all* the interests of the Kingdom.[32] In fact they will only be deployed if one of the state's *vital* interests is threatened or actually harmed.[33] These six vital interests – physical security, economic security, ecological security, territorial integrity, the international legal order, and social and political stability – are part of the Netherlands' national and international security strategies.[34]

---

24 Bovend'eert e.a. 2004, p. 145, where one of the authors (J.W.A. Fleuren) uses the phrase: 'this is a threefold task [sic]'. He relies on the list used by the government in its Explanatory Memorandum, see *Parliamentary Papers II 1996-1997*, 25 367, (R 1593), no. 3, p. 3.

25 *Inter alia* based on Article V NATO-Treaty or Article 42.7 EU Treaty.

26 *Parliamentary Papers II 1996-1997*, 25 367, (R 1593), no. 3 (Explanatory Memorandum), p. 3.

27 See AIV 2004. Also: *Parliamentary Papers II 2013-2014*, 29 521, no. 226.

28 Soetendaal 1997, p. 288. Also: Ducheine 2012, p. 20.

29 *Parliamentary Papers II 2006-2007*, 30 821, no. 1, Strategy National Security.

30 *Parliamentary Papers II 2012-2013*, 33 694, no. 1, International Security Strategy: A Secure Netherlands in a Secure World.

31 *Parliamentary Papers II 2018-2019,* 30 821, no. 81, National Security Strategy 2019

32 Ducheine 2008, p. 55 and *Proceedings of the Senate 1997-1998*, 22, 3 March 1998, pp. 1064-1080; *Parliamentary Papers I 1999-2000*, 26 243 (R 1622), no. 165a (Memorandum of Reply), pp. 4-5.

33 Ducheine 2008, p. 20. Also: Soetendaal 1997, p. 288. See also Strategy National Security and International Security Strategy, *supra* nn. 29 and 30.

34 Interestingly, the 2019 National Security Strategy (p. 12) asserts that "cybersecurity is interwoven into all interests as well. In addition, the integrity of cyberspace has been added as an aspect of territorial security, which includes the availability, confidentiality and integrity of essential information services."

1.3. Core tasks

In consecutive Defence White Papers (2000, 2018), the Ministry of Defence converted and affirms the three constitutional purposes of the armed forces into the following three core tasks:[35]

- protecting the integrity of national and allied territory, including the Caribbean parts of the Kingdom;
- promoting the international legal order and international stability; and
- supporting civil authorities in the fields of law enforcement, disaster relief and humanitarian aid, both nationally and internationally.

The differences between the constitutional purposes and the core tasks laid down in the Defence White Papers reveal that the third core task is formulated more restrictively than the third constitutional purpose: 'protecting other interests of the Kingdom'.[36] Since the White Paper is a policy document, it should be clear that the constitutional definition would prevail if the scope of the third core task were to become the subject of debate. Such a debate would be conducted mainly in parliament, and its outcome would ultimately be determined by the views of the bodies responsible for the substance of the Constitution, namely the government and parliament.

Decision-making procedures for the deployment of the armed forces, with or without cyber capabilities, are regulated by constitutional law. The government and parliament are the main actors in this respect. Although the Prime Minister and the Ministers of Defence and Foreign Affairs are key players when it comes to agenda-setting and decision-making, the Constitution does not recognise their authority in this area. The same applies to the Minister of Defence's chief military adviser, the Chief of Defence (CHOD), who is also responsible for executing most missions.[37] In light of the unity of government policy and the constitutional framework, we regard the government as a collective entity. We also examine its relations with the supervisory branch, as represented by parliament, from this perspective.

1.4. Key actors: the government and parliament

Relations between government and parliament are governed by written and unwritten constitutional law. Under normal political circumstances, the government 'governs' and parliament 'scrutinises'. This axiom has two aspects. First, it is the government, not parliament, that governs. In its capacity as the executive branch, moreover, the

---

35 *Parliamentary Papers II 1999-2000*, 26 800 X, no. 46, p. 41; *Parliamentary Papers II 2017-2018*, 34 919 no 1, p. 9.

36 On this, see *Parliamentary Papers II 1996-1997*, 25 367, (R 1593), no. 3 (Explanatory Memorandum), p. 3: 'Protection of the other interests of the Kingdom includes, for example, military support (pursuant to [Article 58, 2012 Police Act 2012], military assistance to civilians in emergency situations, support for disaster relief efforts, for example in the event of floods or forest fires, and other forms of assistance.'

37 See footnote 19 for mission that fall outside his responsibility.

government has various operational services at its disposal, including the armed forces. Second, the government accepts the oversight role of parliament, which, as a last resort, can invoke the most important constitutional rule of all: the rule of parliamentary confidence. In principle, if a minister or government loses the confidence of parliament, in particular the House of Representatives, the incumbent must resign.

Article 97, paragraph 2 of the Constitution contains a provision regarding control over the armed forces: 'The Government shall have supreme authority over the armed forces.' The government, or in practice the cabinet,[38] thus has the prerogative to deploy the armed forces (or make them available).[39]

In the constitutional framework, parliament provides a fitting counterweight to this prerogative. The Netherlands parliament has several means at its disposal to directly and indirectly scrutinise the government and the armed forces. First of all, it shares responsibility for the substance of the Constitution with the government, which means that they jointly formulate the constitutional provisions on defence.[40] Second, parliament is a co-legislator in the realm of statutory law. Examples relevant to the armed forces, are the 2012 Police Act, which lays down the duties of the Royal Military and Border Police (Marechaussee) and regulates military assistance to the police, or the 2017 Act on Intelligence and Security Services. Third, parliament is responsible for approving the government's budget acts. By withholding approval, it can influence government policy. Fourth, under Article 68 of the Constitution, the government is obliged under normal circumstances to respond to requests for information from parliament.[41] Fifth, under Article 70 of the Constitution, parliament has a right of inquiry. Finally, parliament can influence the government by adopting motions. By means of a motion of non-confidence, for example, it can force the resignation of the government or individual ministers. On the other hand, the freedom of political parties in parliament to execute these powers is sometimes limited by coalition agreements.

Written and unwritten[42] constitutional law also contains instructions on informing parliament and adopting government decisions to deploy the armed forces (or make them available). In practice, this means that the government informs and formally or informally consults parliament about military deployments – either voluntarily or mandatory. The notion that the expeditionary deployment of the armed forces requires the support of parliament and society plays an important role in this regard as it provides one of the elements of legitimacy.[43]

---

38 Officially, the government consists of the King and the ministers. Because of ministerial responsibility for sovereign immunity, decisions concerning the armed forces are made by the cabinet or a delegation thereof.

39 In accordance with the text of Article 100 of the Constitution, a distinction is made between deploying the armed forces and making them available.

40 See, e.g. articles 97 and 100 of the Constitution.

41 Article 68 of the Constitution states: '[…] provided that the provision of such information does not conflict with the interests of the State.'

42 Unwritten constitutional law consists of non-codified rules, such as the principle of parliamentary confidence.

43 Kristic 2012.

However, the procedure for informing parliament about expeditionary operations differs for each constitutional purpose and core task. Given its prominence and the level of detail involved, we start with an explanation of the Article 100 procedure for missions falling under the second purpose/core task. After that, we discuss the other deployment options. In each case, we introduce our analysis of the decision-making and information procedures with a fictitious scenario that gives rise to the deployment in question and the decision whether or not to deploy military cyber capabilities.

1.5. Second purpose/core task: Article 100 procedure

1.5.1. Scenario: UN Security Council mandate

We will illustrate the reasons for using the Article 100 decision-making procedure with two short fictitious scenarios concerning cyber activities against international terrorist group 'Z@'.

The UN Security Council has previously concluded in a resolution that this group, Z@, poses a threat to international peace and security within the meaning of Article 39 of the UN Charter. This serves as a prelude to a follow-up resolution in which the Security Council authorises the use of 'all necessary means' to combat Z@ within a defined area or for a certain cause. This resolution provides the legal basis for military deployment. A coalition of states asks the Netherlands to contribute a cyber task force in 2020, in light of its new 'niche capability' in this area. The task force possesses several cyber instruments generating tactical effects and the knowledge to develop and deploy a high-quality cyber instrument producing strategic effects.

1.5.2. Substance

Since 2000, Article 100 of the Constitution provides that the government - after having decided on the issue - shall inform parliament of its decision to deploy the armed forces (or make them available) for the purpose of certain expeditionary operations (e.g. international crisis management operations) in a timely manner, i.e. before deployment.[44] The following criteria play a role in this regard:

- military units are deployed (or made available) to maintain or promote the international legal order or to provide humanitarian aid in the event of armed conflict;
- the military personnel are deployed as a unit;
- the performance of the military task also involves using or risking exposure to armed force.[45]

---

44 Article 100, paragraph 1 of the Constitution states: 'The Government shall inform the States General in advance if the armed forces are to be deployed or made available to maintain or promote the international legal order. This shall include the provision of humanitarian aid in the event of armed conflict.'

45 *Parliamentary Papers II 2013-2014*, 29 521, no. 226, p. 1.

In certain situations, the government is – temporarily – relieved of its duty to inform parliament, for example in the case of special operations (see below paragraph 1.9).

When cyber capabilities are deployed as part of a Task Force characterised by the above criteria, Article 100 applies to the whole of that Task Force. This appears to be the most likely deployment setting.[46] In some cases, however, where the element of "using or risking exposure to armed force" is less evident, or where the cyber capabilities are operating from within the Netherlands' territory, it is less clear whether Article 100 formally applies. In those circumstances, one would have to fall back on the analogous procedure described in paragraph 1.6 below.

In addition to the government's specific duty to inform parliament of its decisions prior to deployment, parliament has a general right to information under Article 68 of the Constitution.[47] This means that members of parliament can request additional information from the government at any time, even prior to or during military missions about which they have already been informed pursuant to Article 100 of the Constitution or otherwise. Article 68 thus has a broader scope than Article 100, but requires parliament to take the initiative.

1.5.3. Right of consent?

Opinions on the meaning of Article 100 of the Constitution are divided. According to one view, parliament has a substantive right of consent. This appears to be the case because, after informing parliament of its decision to deploy the armed forces, the government tries to secure support for this decision taking in mind that the government is mandated by a coalition of political parties. As a result, parliament has a certain amount of leeway to influence government decisions. The government increases this leeway by sounding out the opinions of coalition and opposition parties in advance and responding accordingly, for example by changing the force composition, ruling out high-risk areas or tasks, and so forth. Motions (e.g. requesting changes in the conditions of the deployment) are part of the same picture. On this issue, the government notes:

> This means that both houses of parliament receive information concerning the decision in question in a timely manner, which can result in a debate in which motions are adopted. The government will give serious consideration to such motions and will not dismiss them lightly. In these circumstances, it cannot be ruled out that the government will reconsider its decision and the implementation of that decision in whole or in part.[48]

---

46 See *infra* notes 59 and 60.

47 Article 68 of the Constitution states: 'Ministers and State Secretaries shall provide, orally or in writing, the Houses either separately or in joint session with any information requested by one or more members, provided that the provision of such information does not conflict with the interests of the State.'

48 *Parliamentary Papers I 1999-2000*, 26 243 (R 1622), no. 165a (Memorandum of Reply), p. 6.

Another view emphasises the fact parliament has no formal or substantive right of consent, since it only has a formal right of information.[49] Bovend'eert points out, for example, that the government can and should decide on its own, that it is not obliged to implement parliamentary motions and that even a motion of no-confidence cannot curtail its authority to deploy the armed forces.[50]

1.5.4. Procedure

Regardless of whether or not parliament has a right of consent, there is consensus on the various steps of the information and decision-making procedure, which unfolds as follows.

- Letter of notification: The government informs parliament that, in response to a request from an international organisation or on its own initiative, the civil service is examining the 'desirability and feasibility' of contributing to a crisis management operation.
- Government decision: The civil service's examination, which includes the CHOD's military advice and the MIVD's assessment, considers all potential military capabilities, including cyber capabilities, and results in a government decision. In the case of a negative decision, parliament is notified. In the case of a positive decision, the government informs parliament in accordance with Article 100 of the Constitution.
- Article 100 letter: Prior to deploying the armed forces (or making them available), the government explains its decision with reference to the criteria of the Assessment Framework.[51] In the case of extension or premature conclusion of a deployment, a change in the relevant mandate or tasks or a change in the area of responsibility (AOR) that has implications for the mandate or tasks, the government issues a new Article 100 letter.
- Parliamentary debate: As a rule, the House of Representatives places the Article 100 letter on its agenda, after which a debate takes place. In principle, all options are available during this debate. In response to motions, questions or a lack of sufficient backing, the government can reconsider, amend or nevertheless persist in its decision. The government usually secures parliament's backing by the end of the debate. According to popular opinion, parliament is then said to have 'consented' [sic] to the mission.
- After the parliamentary debate, the government informs the organisation or coalition that is directing the operation of its decision. It then informs parliament of the response to its offer.
- Progress reports: While the deployment is being prepared and the operation is being carried out, the government regularly informs parliament about progress and developments by meeting with the relevant parliamentary committees or otherwise.

---

49 *Parliamentary Papers II 2005-2006*, 30 162, no. 3 (Report of the committee chaired by MP Hans van Baalen), p. 18.

50 Bovend'eert 1998, p. 1596.

51 Except for special operations, see below.

- Interim evaluation: Every year, on the third Wednesday in May, parliament receives an interim evaluation from the Ministers of Defence and Foreign Affairs concerning all current operations in which Dutch military units are participating.
- Final evaluation: After the Netherlands' deployment has ended, the government presents parliament with a final evaluation of the operation, which touches on its military and political aspects. This evaluation is discussed in parliament.
- Post-mission assessment: In addition, in certain cases,[52] the government has recently started issuing post-mission assessments that evaluate the impact of the Netherlands' participation in Article 100 missions five years after the end of the mission. This assessment focuses on developments in the mission area after the conclusion of the Dutch deployment and on the effects of the deployment that are still discernible.[53]

1.5.5. Assessment Framework

The preparation of the government's decision by the civil service, the Article 100 letter and, where relevant, the ensuing parliamentary debate follow the criteria of the Frame of Reference for Decision-Making for the Deployment of Military Units Abroad (also known as the Assessment Framework).[54] This Assessment Framework, which has been enshrined in policy, serves two aims: to guarantee the quality of the decision-making process and to facilitate oversight and the assessment of government decisions by parliament:

> It is specifically intended for decision-making by the government and its consultations with parliament concerning the deployment of military units that, in the performance of their tasks, may be required to use or risk exposure to armed force.[55]

The Assessment Framework contains a list of criteria that are used to reach a well-reasoned military and political decision on Dutch participation in crisis management operations on a case-by-case basis.[56] Depending on the nature of the mission, the criteria on the list carry different weight. Moreover, they are not absolute values: their weight is relative and they are often measured in qualitative terms. The Assessment Framework is thus not a list of binding conditions that need to be met one after the other before a decision can be made.[57]

Key criteria include, for example, the grounds for the mission, including its legal basis and mandate, feasibility and effectiveness, influence and risks. Feasibility relates to the

---

52 The final evaluations of Dutch contributions to Article 100 missions indicate whether a post-mission assessment will be carried out.

53 See *Parliamentary Papers II 2011-2012*, 29 251, no. 191 and *Parliamentary Papers II 2012-2013*, 29 251, no. 195.

54 *Parliamentary Papers II 1994-1995*, 23 591, no. 5, with updates in 2001, 2005, 2009 and 2014.

55 *Parliamentary Papers II 2000-2001*, 26 454, no. 7-8 (Final report of the Temporary Committee on Decision-Making on Deployment (TCBU)), p. 3.

56 *Parliamentary Papers II 2000-2001*, 23 591 and 26 454, no. 7, p. 3.

57 *Parliamentary Papers II 2005-2006*, 30 162, no. 3 (Report of the Van Baalen Commitee), p. 28.

required military capability, including the 'size and composition of the military units and the equipment and weapons issued to them'.[58] It appears that composition, equipment and weapons also cover potential cyber capabilities:

> This means that cyber capabilities supplement existing military capabilities and that the two should be deployed in an integrated manner. It also means that issues relating to the digital domain should be included in the planning and preparation of operations. In cases where Article 100 applies to a military deployment, the same applies to the relevant cyber units.[59]

The Assessment Framework also covers the Concept of Operations for and the Rules of Engagement of the military operation.[60]

Although it officially only applies to Article 100 missions, the Assessment Framework and the criteria it introduces can also play a role in decision-making, oversight and assessment regarding other missions (see below).[61]

1.6. First purpose/core task: defence

1.6.1. Scenario: Armed cyber attack

A NATO ally suffers a cyber attack on its already vulnerable power grid. Despite preventive government measures and campaigns, public life comes to a standstill following an unexpected cascading failure.[62] Trains, public lighting, traffic controls, households and utilities are all without power for a prolonged period. Although opening hours and transport options are limited, a run on stores and banks quickly develops, and the lack of money and food leads to mass riots in which looting and destruction are commonplace. The emergency services and public order agencies are hindered in their work. As a result, public order and physical safety are no longer guaranteed. Political and social unrest takes on unacceptable forms.

With the conclusions of the NATO summits in Wales and Brussels in mind,[63] the North Atlantic Council states that if it can be demonstrated that the attack was directed from

---

58 *Parliamentary Papers I 2013-2014*, 29 521, D, p. 17.

59 *Parliamentary Papers I 2013-2014*, 29 521, D, pp. 5-6.

60 *Parliamentary Papers I 2013-2014*, 29 521, D, p. 17: 'The description of the concept of operations specifies the military objectives, the end situation to be achieved, and the tasks and modus operandi of the military unit.'

61 *Parliamentary Papers II 2005-2006*, 30 162, no. 3 (Report of the Van Baalen Commitee), p. 28. See also the government's position in *Parliamentary Papers I 2013-2014*, 29 521, D, p. 3.

62 Shakarian, Lei and Lindelauf 2014.

63 NATO Wales Summit Declaration (2014): 'Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.' See <www.nato.int/cps/en/natohq/official_texts_112964.htm>. In Brussels NATO (2018) stated that

abroad, it should be qualified as an 'armed attack' within the meaning of Article V of the NATO Treaty and Article 51 of the UN Charter, in light of its scale and effects.

In line with its response to the AIV/CAVV's advisory report on cyber warfare, which examined this issue, the government instructs the Kingdom of the Netherlands' Permanent Representative to NATO as follows:

> A serious, organised cyber attack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of Article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state. In such cases, there must be a 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 for it to be qualified as an armed attack.[64]

When it becomes clear from digital forensic analysis and other intelligence sources that the cyber attack was launched from the Middle East by the state-affiliated armed group 'EXIT' operating transnationally, the North Atlantic Council reconvenes and determines that it was indeed an 'armed attack' within the meaning of Article V of the NATO Treaty. Knowing that the Netherlands also has troops stationed in the Middle East, the ally subsequently requests military assistance for a response in self-defence.

1.6.2. Procedure

Operations conducted in the framework of alliance obligations, such as NATO and EU operations, fall outside the scope of the Article 100 procedure (see above). The same applies to several other deployment options that do not fall under Article 100 of the Constitution.[65] In other words, the government is not under a formal constitutional *obligation* to inform parliament in such cases. Nevertheless, it does so voluntarily by analogy with the Article 100 procedure:[66]

> [T]he government [strives] to keep the House fully informed, where possible in advance and where necessary in retrospect. […] The main objective is to inform the House in a manner that is as similar as possible to the Article 100 procedure.[67]

The government is thus honouring its undertaking to also 'seek to inform parliament as swiftly and comprehensively as possible' in cases falling outside the scope of Article 100.[68] The procedure in such cases is as follows:

---

the cyber threats to the security of the Alliance are becoming more frequent, complex, destructive, and coercive.' See <www.nato.int/cps/en/natophqofficial_texts_156624.htm>.

64 AIV/CAVV report, p. 20.

65 However, the parliamentary right of information enshrined in Article 68 of the Constitution applies without restriction to these kinds of operations, including individual deployments, civil missions, humanitarian aid missions, etc.

66 *Parliamentary Papers II 2005-2006*, 30 162, no. 3 (Report of the Van Baalen Committee/NRF report), p. 26.

67 *Proceedings of the House of Representatives 2001-2002,* 24, p. 1767.

- letter of notification (outlining the 'desirability and feasibility' of participation);[69]
- government decision following the civil service's examination (including the CHOD's military advice and the MIVD's assessment);
- letter of information to parliament;[70]
- parliamentary debate;
- provision of information to the alliance or international coalition that is directing the operation;
- progress reports during the preparation and implementation of the operation;
- interim evaluation of current operations (third Wednesday in May);
- final evaluation.[71]

In practice, missions carried out under the first core task will follow a decision-making and information procedure analogous to that of Article 100 operations. The difference is in the formal aspects, namely the voluntary nature of the provision of information, the lack of specific references to Article 100 of the Constitution and the fact that the criteria of the Assessment Framework are not a compulsory part of the decision-making process.[72].

1.7. Third purpose: protecting vital interests

1.7.1. Scenario: Cyber hijacking

For some time now, the Netherlands has been providing protection for vulnerable Dutch merchant ships passing the Horn of Africa, off the Somali coast. The UN Security Council has not issued a mandate for this activity. In addition to combating piracy, the government sees the purpose of this military operation as protecting the Kingdom's economic interests.[73] It now appears that large and vulnerable special transport ships and dredgers from the Dutch company Dockwise are being 'digitally hijacked' by ransomware in Asia. The chair of the Royal Association of Netherlands Shipowners (KVNR) urges the government to investigate – and if necessary, help counter – this new threat. Because of a lack of capacity in the civil domain, the government asks the Ministry of Defence whether the DCC can step in.

---

68 *Parliamentary Papers II 2000-2001*, 23 591, no. 8, p. 5. Also: *Proceedings of the House of Representatives 2004-2005*, 56, p. 3661.

69 See, e.g., *Parliamentary Papers II 2004-2005*, 27 925, no. 170.

70 See, e.g., *Parliamentary Papers II 2001-2002*, 27 925, no. 24 and *Parliamentary Papers II 2004-2005*, 27 925, no. 159. This is different in the case of a special operation (see below).

71 See, e.g., *Parliamentary Papers II 2006-2007*, 29 521, no. 33, annexe. For the time being, it appears that post-mission evaluations are not being used in this category of missions.

72 *Parliamentary Papers I 2013-2014*, 29 521, D, p. 3.

73 *Parliamentary Papers II 2010-2011*, 30 706, no. 1, in which the government classifies protecting the interests of the Kingdom as falling under the first core task.

1.7.2. Objective

Besides the Defence organisation's primary responsibility for protecting territorial security and the international legal order, the armed forces are also on hand to protect other vital interests, including social and political stability and economic, ecological and physical security. The civil authorities are generally responsible for protecting these interests. It is clear from the Defence Cyber Strategy and the Defence organisation's ambitions that cyber capabilities should also be made available for the third purpose/core task. In other words, at the request of the civil authorities, cyber capabilities can also be deployed abroad to protect the Netherlands' vital interests. The deployment of Vessel Protection Detachments (VPDs) to combat piracy and protect merchant shipping has served as a model for our analysis.

1.7.3. Procedure

In our view, the procedure operates as follows:

- Request: The National Cyber Security Centre (NCSC) receives or formulates a request for assistance involving military cyber capabilities.
- Government decision: After receiving the CHOD's military advice and the MIVD's assessment, the government can deploy the armed forces abroad to protect other vital interests of the Kingdom. The nature of the deployment will differ from case to case and may encompass regular, special-forces or cyber units.
- Information: In the case of regular operations, including those with cyber capabilities, the government will inform parliament of its decision and the relevant considerations. In the case of long-term deployments, moreover, it will provide regular updates.[74]

1.8. Overlapping objectives

If the armed forces are deployed (or made available) in pursuit of overlapping objectives, that is, for self-defence (first purpose) or the protection of vital interests (third purpose) as well as to maintain and promote the international legal order (second purpose), the government will follow the Article 100 procedure.[75] This might apply, for example, in the case of action taken in self-defence following an armed attack, eliminating the attacker's offensive military cyber or non-cyber capabilities, as this promotes the international legal order by reducing this threat to international peace and security.

1.9. Special operations

Besides regular operations, including those with cyber capabilities, the government can also decide to commission special military operations characterised by 'substantial

---

74 Cf. *Parliamentary Papers II 2010-2011*, 32 706, nos. 1 and 9.
75 *Parliamentary Papers II 2013-2014*, 29 521, no. 226.

political and military risks and the need for strict secrecy'.[76] Such operations are usually carried out by special forces that have been 'designated, trained and equipped to carry out missions under exceptional circumstances (secrecy, substantial security threats and extreme physical exertion)'.[77] Examples of such operations include special intelligence gathering, special arrests, assaults on selected targets (direct action), military assistance for allies, evacuation of Dutch nationals from life-threatening situations and operations to combat international terrorism.[78]

1.9.1. Scenarios: MH-17, ransom payments and the MIVD

Scenario 1: Cyber protection of the MH-17 investigation. The investigation into (and on-site collection of evidence concerning) the crash/downing of flight MH-17 is being seriously hampered by a foreign party using cyber capabilities. To ensure that the investigation can continue unimpeded, the Netherlands decides to deploy additional security measures, including the DCC's cyber capabilities. To increase the chances of success and in light of political sensitivities, the government decides to keep this decision secret.

Scenario 2: Digital recovery of ransom payments in Somalia. In resolution 2020, the UN Security Council extended its authorisation of the use of 'all necessary means' to combat piracy in Somalia's territorial waters and on Somali territory. After a ship-owner has paid a ransom to secure the release of one of its ships and its international crew, the international military force in the region asks the Netherlands if it is willing to use its cyber capabilities to track the ransom payment and, if the money in question is located within Somalia's jurisdiction, to secure and recover the funds by digital means.

Scenario 3: The CHOD is asked to deploy military cyber capabilities in support of an MIVD operation in a foreign country.

The first and third scenarios can be classified under the third purpose/core task, which is to protect the vital interests of the Kingdom. The second scenario is also related to efforts to promote the international legal order and combat piracy.

1.9.2. Objective

Special operations can be carried out for several reasons, including defence, maintaining and promoting the international legal order or protecting other vital interests of the Kingdom. In other words, special operations can be commissioned under the first, second and third purpose/core task.

---

76 *Parliamentary Papers II 1999-2000*, 26 800 X, no. 46, p. 1.
77 *Parliamentary Papers II 1999-2000*, 26 800 X, no. 46, p. 1.
78 *Parliamentary Papers II 2000-2001,* 27 400 X, no. 29, p. 2.

1.9.3. Procedure

The government has stated that, 'in accordance with Article 100, paragraphs 1 and 2 of the Constitution, it will inform parliament about special military operations in a manner that respects the States General's involvement in deployment of the armed forces in exceptional circumstances, the existing constitutional framework and the need for secrecy that surrounds such operations.'[79] In the case of the second purpose/core task, Article 100 provides the government with the option of informing parliament only later or to a limited extent. This exception is enshrined in the second paragraph.[80] It applies to:

> emergencies and other situations in which military personnel must be deployed at very short notice, or military interventions which can only be meaningful if they take place unannounced and in the strictest secrecy, for instance if there is imminent danger in life-threatening situations and action must be taken promptly or in strict secrecy. In such acute emergencies, it may be impossible to supply information in advance.[81]

If it decides to invoke this exception, or if there are other reasons to favour a special operation, the government follows a procedure that has been described and explained in other letters to parliament.[82] This procedure operates as follows:

- Establishment of a Ministerial Core Group on Special Operations (MKSO): At its first (constitutive) meeting following a change of government, the cabinet establishes an MKSO, which includes at least one minister from each coalition party in order to guarantee sufficient support. In 2020 the MKSO consisted of the Prime Minister, the (three) Deputy Prime Ministers and the Ministers of Defence and Foreign Affairs.
- In each case, after receiving a recommendation from the civil service (including the CHOD's military advice and the MIVD's assessment), the MKSO decides whether or not to commission a special operation.
- The MKSO also decides whether and, if so, when to include other members of the cabinet in the decision-making process.
- Finally, the MKSO decides how and when to inform parliament (in accordance with Article 100 of the Constitution or otherwise). Options include submitting a concise report to the leaders of the parliamentary parties in advance or issuing a brief description of the operation afterwards.[83]

Since the entry into force of Article 100 of the Constitution in 2000, the government has not made use of the 'exceptional circumstances' clause enshrined in the article's second

---

79 *Parliamentary Papers II 2000-2001,* 27 400 X, no. 29, p. 3.

80 Article 100, paragraph 2 of the Constitution states: 'The provisions of paragraph 1 shall not apply if compelling reasons exist to prevent the provision of information in advance. In this event, information shall be supplied as soon as possible.'

81 *Parliamentary Papers I 2013-2014*, 29 521, D, pp. 2-3, which states that Article 100, paragraph 2 of the Constitution has yet to be invoked.

82 *Parliamentary Papers II 1999-2000*, 26 800 X, no. 46, *Parliamentary Papers II 2000-2001*, 27 400 X, no. 29, *Parliamentary Papers II 2017-2018*, 34 775 X, no. 88 (Speciale Operaties en Geheime operaties).

83 *Parliamentary Papers II 1999-2000*, 26 800 X, no. 46, p. 2.

paragraph.[84] Before that, the Minister of Defence presented a brief description of a special operation to parliament on at least one occasion.[85]

When committing capabilities under the first and third core purpose/task only, the government will apply the procedure set out above as well. The only exception concerns the formal reference to Article 100 and the fact that the Article 100 and its second paragraph itself are not applicable.

Given their characteristics, we suspect that a certain proportion of cyber capabilities will be deployed under the heading of 'substantial political and military risks and the need for strict secrecy'. In other words, the decision to deploy these capabilities will often be made by the MKSO and will be followed by the provision of limited information.

1.10. Conclusion

This chapter focuses on the highly pertinent issues of political decision-making and the provision of information to parliament in the context of the deployment of military cyber capabilities. In all cases, the decision to deploy cyber capabilities (or make them available) rests with the government.

The government always takes note of the CHOD's military advice and the MIVD's assessment. It also informs parliament, although the way in which it does so differs according to the purpose/core task concerned. Under the constitutional framework, parliament can actually influence the government's decision. We conclude that the decision-making and information procedure, also for operations in cyberspace, usually adheres to the standard model when overt deployments are at stake, which in turn facilitates a normal accountability process.

Decisions regarding deployments of cyber capabilities that have been classified as special operations are in the hands of a small part of the government, namely the Ministerial Core Group on Special Operations (MKSO). The information procedure is different in such cases which must not be attributed to the cyber domain environment but to the sensitive circumstances of the mission.

After examining the constitutional purpose of the armed forces, we have identified the Article 100 procedure for 'maintaining and promoting the international legal order' as the basic modus operandi. The civil service's examination of the aim and necessity of deploying the armed forces, which is preceded by a letter of notification from the government to parliament, results in a positive or negative government decision. In the case of a positive decision, the government sends parliament an Article 100 letter. The criteria of the Assessment Framework serve as a guideline for the civil service's examination, the government's decision and the Article 100 letter. Parliament is

---

84 *Parliamentary Papers I 2013-2014*, 29 521, D, p. 3.

85 This was in the case of Operation Amber Star, in which the Netherlands helped arrest war crimes suspects in the former Yugoslavia. See *Parliamentary Papers II 1997-1998*, 22 181, no. 193.

responsible for placing the debate with the government concerning the decision on its agenda. Before, during and after each deployment, the government, acting in response to a request or on its own initiative, provides information through interim evaluations, final evaluations and/or post-mission assessments.

The procedure for defence-related deployments formally differs from the Article 100 procedure but in terms of substance displays many similarities with it. The same applies to the expeditionary protection of other vital interests of the Kingdom.

The procedure is different for specific cyber operations that are classified as special operations owing to their 'substantial political and military risks and the need for strict secrecy'. The decision to deploy is made by the MKSO, which determines when and to what extent to involve or inform the rest of the government. It also decides how and when parliament should be informed.

In all cases, parliament can make use of the normal oversight mechanisms that it has at its disposal, including questions, debates, motions and, if necessary, motions of no-confidence and its right of inquiry. In short, although the government ultimately decides whether or not to deploy cyber capabilities abroad, its decision is subject to regular parliamentary oversight. This is how it should be in a democracy governed by the rule of law, where the armed forces must carry out their military tasks to the fullest extent of their constitutional purpose, including in the digital domain.

1.11. References

AIV Advisory Council on International Affairs (2004) *The Netherlands and Crisis Management: Three Issues of Current Interest*, advisory report no. 34 (March 2004)

AIV/CAVV, Advisory Council on International Affairs/Advisory Committee on Issues of Public International Law (2011) *Cyber Warfare*, Advisory report no. 77/22 (December 2011), available at: <www.aiv-advice.nl> < www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare>.

Bovend'eert, P.P.T (1998) 'De inzet van strijdkrachten zonder toestemming van de Staten-Generaal' [Deployment of the armed forces without the consent of the States General], in *Nederlands Juristenblad*, 2 October 1998, 35, pp. 1594-2024.

Bovend'eert, P.T., et al. (2004) *Grondwet voor het Koninkrijk der Nederland, Tekst & Commentaar* [Constitution of the Kingdom of the Netherlands: text and commentary], Deventer: Kluwer, p. 145

Ducheine, P.A.L. (2008) *Krijgsmacht, geweldgebruik & terreurbestrijding: een onderzoek naar juridische aspecten van de rol van strijdkrachten*, Nijmegen: Wolf Legal Publishers (diss. University of Amsterdam).

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

Ducheine, P.A.L. (2015) 'Military Cyber Operations', in Gill, T.D. & D. Fleck (reds.), *The Handbook of International Law of Military Operations* (2nd ed.), Oxford: OUP, pp. 456-475.

Ducheine, P.A.L. (2016) '*Je hoeft geen zwaard en schild te dragen om ridder te zijn' - Mythen over digitale oorlogsvoering en recht* (Oratie UvA), Amsterdam: AUP <www.oratiereeks.nl/upload/pdf/PDF-6825weboratie_Ducheine_-_DEF.pdf>. Also in: Militaire Spectator, 185-2 (2016), pp. 123-135, via <www.militairespectator.nl/thema/recht-cyberoperations/artikel/%E2%80%98je-hoeft-geen-zwaard-en-schild-te-dragen-om-ridder-te-zijn%E2%80%99>.

Ducheine, P.A.L. & E.H. Pouw, 'Legitimizing the use of force: legal bases for Operations Enduring Freedom and ISAF, in: Beeres, R. e.a. (reds.), Mission Uruzgan – Collaborating in Multiple Coalitions for Afghanistan, Amsterdam: Pallas Publications/Amsterdam University Press, pp. 33-46, 67-80.

Ducheine, P., J. Voetelink, J. Stinissen & T. Gill (2012) 'Towards a Legal Framework for Military Cyber Operations', in: P. Ducheine, F. Osinga and J. Soeters (eds.), Cyber Warfare: Critical Perspectives – NL ARMS 2012, The Hague: TMC Asser Press, pp. 101-128.

Ducheine, P.A.L., J. van Haaster & R. van Harskamp (2017), 'Manoeuvring and Generating Effects in the Information Environment', in: Ducheine, F. Osinga (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 & Springer – Berlin, pp. 155-180. Via SSRN: <papers.ssrn.com/sol3/papers.cfm?abstract_id=2979287>.

Kristic, A. (2012) *De Staten-Generaal en de inzet van de Nederlandse Krijgsmacht* [The States General and the deployment of the Dutch Armed Forces], Deventer: Kluwer (diss., Tilburg University)

Netherlands Armed Forces Doctrine for Military Cyberspace Operations 2019, The Hague, June 2019 (on file with the authors)

Shakarian, P. H. Lei and R. Lindelauf (2014) 'Power Grid Defense Against Malicious Cascading Failure', 13th International Conference of Autonomous Agents and Multiagent Systems (AAMAS-14), May 2014, available at: <www.usma.edu/nsc/SiteAssets/SitePages/Publications/POWER_GRID_DEF.pdf>.

Soetendaal, E. (1997) 'Boeiend en geboeid, enige beschouwingen over de wijziging van de defensiebepalingen in de Grondwet' [Captivating and captive: some observations on the amendment of the defence provisions in the Constitution], in *Militair Rechtelijk Tijdschrift*, vol. XC, no. 9, pp. 285-297.

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. Kraesten Arnold was the Deputy Commander of the MoD's Task Force Cyber (then in process of establishment). Peter Pijpers is Associate Professor for Cyber Warfare (NLDA).