Information Manoeuvre and the Netherlands Armed Forces: Legal Challenges Ahead

Ducheine, P.A.L.; Pijpers, P.B.M.J.; Pouw, E.H.

DOI
10.2139/ssrn.4113046

Publication date
2022

Document Version
Final published version

UNIVERSITY OF AMSTERDAM

INFORMATION MANOEUVRE AND THE NETHERLANDS ARMED FORCES: LEGAL CHALLENGES AHEAD

Paul A.L. Ducheine

Peter B.M.J. Pijpers

Eric H. Pouw

Amsterdam Law School Legal Studies Research Paper No. 2022-12

Amsterdam Center for International Law No. 2022-07

Information Manoeuvre and the Netherlands Armed Forces: Legal Challenges Ahead

Paul A.L. Ducheine, Peter B.M.J. Pijpers, & Eric H. Pouw *

Keywords: *Information Manoeuvre, Data Protection, Armed Forces, the Netherlands, GDPR.*

Abstract:

With the Defence White Paper "Defence Vision 2035", the Netherlands have articulated that its armed forces need to be capable to execute 'information-driven operations'. This intent reflects the threats and opportunities emerging from the inception of cyberspace, with the Russia-Ukraine war as a case in point. Cyberspace has unlocked the information environment, raising obvious concerns about the use of data and potential infringements of privacy since it simultaneously gives new impetus to use data to improve military intelligence and understanding, enhance decision making, but moreover to use information as a 'weapon' of influence. However, while (nascent) capacity and will to employ the armed forces in the information environment are present, parts of the conceptual component cause friction. The principal cause for this is the current legal framework applicable to information manoeuvre, that seriously hampers training and preparing for operations. The 'lacuna' must be dealt with, for it would be hypocritical to demand security without empowering the agencies with the tools that ensures their readiness for deployment.

'War is ninety percent information'[1]

1. Introduction

The *raison d'existence* of the Netherlands' armed forces is to defend and protect the Kingdom's interests, and to maintain and promote the international legal order.[2] Though these objectives could stand the test of time, the dynamics of the (geopolitical) security context within which the State's interests need to be protected have changed, partially as a result of the dawn of cyberspace.[3]

* Paul A.L. Ducheine Ph.D. is the Netherlands Defence Academy (NLDA) Professor for Cyber Operations and endowed Professor of Law of Military Cyber Operations at the University of Amsterdam. Peter B.M.J. Pijpers Ph.D. is an Associate Professor of Cyber Operations at the NLDA and researcher at the Amsterdam Centre of International Law (ACIL), University of Amsterdam. Eric H. Pouw Ph.D. is a senior military legal advisor within the Dutch armed forces, research fellow at the NLDA and researcher at ACIL, University of Amsterdam. Corresponding author: p.a.l.ducheine@uva.nl.

[1] Attributed to Napoleon Bonaparte.

[2] Art. 97(1) Constitution of the Kingdom of the Netherlands.

[3] Marcus Willett, "Assessing Cyber Power," *Survival* 61, no. 1 (2019): 85–90. pp. 85-87.

Whilst organisational readjustment to the evolving security landscape is required, the domain of engagement – land, sea, air, space or cyberspace – is indifferent to the protection of interests; a view that is echoed in the Netherlands' Defence Vision 2035 (DV35).[4] This Defence White Paper articulates the defence organisation's ambition to be an effective agent in the information environment and to make better use of available data and information in the military realm.[5]

One of the baselines is to be able to execute so-called 'information-driven operations', also (and from here on) called information manoeuvre,[6] in 2035. The defence organisation should not only be capable of obtaining an authoritative information position, which is needed for integrated command and control and 'information-driven operations', it must also use information as a 'weapon', i.e. as a means or instrument of influence.[7]

From a legal point of view, manoeuvring in the information environment affects the armed forces in at least two ways. Firstly, before armed forces are deployed, they need to achieve the appropriate level of readiness. Adopting the concept of information manoeuvre demands the expertise and familiarisation of personnel with new concepts, doctrine, procedures, standards and equipment, by means of education, experimentation, exercises and training (hereinafter referred to as 3ET) with data and information. Requirements that need to be achieved prior to and not whilst deployed. To the extent 3ET involves real world data and information available in the current information-environment, this unavoidably implies the processing of personal data which could infringe privacy.

Secondly, an authoritative information position needs to be obtained prior to a planned or envisioned deployment. The collection, processing and dissemination of data and information must start before the commencement of a mission mandate. If this includes a role for the armed forces, this raises questions regarding (the scope of) the purpose, tasks and legal authorities of the armed forces outside deployments and their relationship with those of others, such as the intelligence and security services.

The aim of this contribution is two-fold. First, it articulates the legal framework applicable to armed forces manoeuvring in the information environment; with a particular focus on the processing of personal data. Second, it aims to raise awareness on the implications of the legal framework for activities of the armed forces for 3ET and obtaining an

[4] Netherlands Ministry of Defence, "Defence Vision 2035: Fighting for a Safer Future," 2020. Accessible here: https://english.defensie.nl/downloads/publications/2020/10/15/defence-vision-2035

[5] Though similar trends are visible in other states, see e.g.: Christine E. Wormuth, "Message from the Secretary of the Army to the Force," *US Army*, 2022., in this article, 'defence organisation' refers to the defence organisation of the Kingdom of the Netherlands. The same principle applies to 'Ministry of Defence', 'armed forces' and 'intelligence and security services'. MoD and defence organisation encompass the armed forces (army, navy, airforce, marechaussee) as well as the Military Intelligence and Security Service (MIVD).

[6] British Army, "Force Troops Command Handbook," 2019.; Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, "Manoeuvring and Generating Effects in the Information Environment," in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017*, ed. Paul A.L. Ducheine and Frans P.B. Osinga, 2017.

[7] Netherlands Ministry of Defence, "Defence Vision 2035: Fighting for a Safer Future." Annex p. XII

authoritative information position in the readiness phase and provides some suggestions to overcome these implications.

The main question in this article is whether the current legal framework offers adequate room for the armed forces to manoeuvre in the information environment prior to deployment.

The structure of the article is as follows. In the next section the authors describe the information manoeuvre concept. Section 3 outlines relevant aspects of the general legal framework applicable to activities of the armed forces in this concept. In section 4, based on a fictitious scenario in the near future, the implications of this framework for the armed forces to conduct 3ET with real world data and information, as well as for its role in obtaining an authoritative information-position, will be assessed. Finally, the article will reflect on the main research question, provide suggestions how to deal with the implications and return to the secondary aim of the article – raising awareness of the implications of the current legal lacunae for the conceptual component of military power.

As a point of departure, unless otherwise indicated, the article focusses solely on activities of the armed forces in the information environment[8] in the readiness phase[9] for a (possible or planned) deployment abroad.[10] It is in the readiness-phase that most legal challenges can be found.

2. Information Manoeuvre

The information environment is the environment we live in and from which we gather data via our senses, and after storing, fusing and processing the data to information and knowledge, we can communicate in the information environment. This information environment (see figure 1) entails the physical, the virtual and the cognitive dimension.

The information environment is not new, however, with the emergence of cyberspace new layers were introduced,[11] most prominently the virtual layers of data and software (logical layer) and of virtual personae - our reflections in cyberspace using (inter alia) social media accounts.

Cyberspace has substantially enlarged the information environment. From a security and military perspective, the expanded access to and usability of the information environment

[8] Wherever this (implicitly or explicitly) involves activities of military intelligence entities (such as reconnaissance platoons of infantry battalions, or the units belonging to Joint ISTAR-Command), this concerns units of the armed forces, not of the (defence) intelligence and security service(s). In the Netherlands, the Defence Intelligence and Security Service (MIVD) is an entity within the Ministry of Defence, under the authority of the Secretary-General of the Ministry of Defence. It is not part of the armed forces, acting under the authority of the Chief of Defence (CHoD).

[9] This phase entails activities related to 3ET prior to deployment. In Dutch: "gereedstelling".

[10] A 'deployment' is a military operation sanctioned by the Netherlands' government. In Dutch: "inzet".

[11] Ducheine, Haaster, and Harskamp, "Manoeuvring and Generating Effects in the Information Environment."

has created (re)new(ed) opportunities and threats, including digital espionage, influence operations or subversion via cyberspace,[12] not least due to the low costs of entry, high speed of dissemination and high degree of penetration into societies.

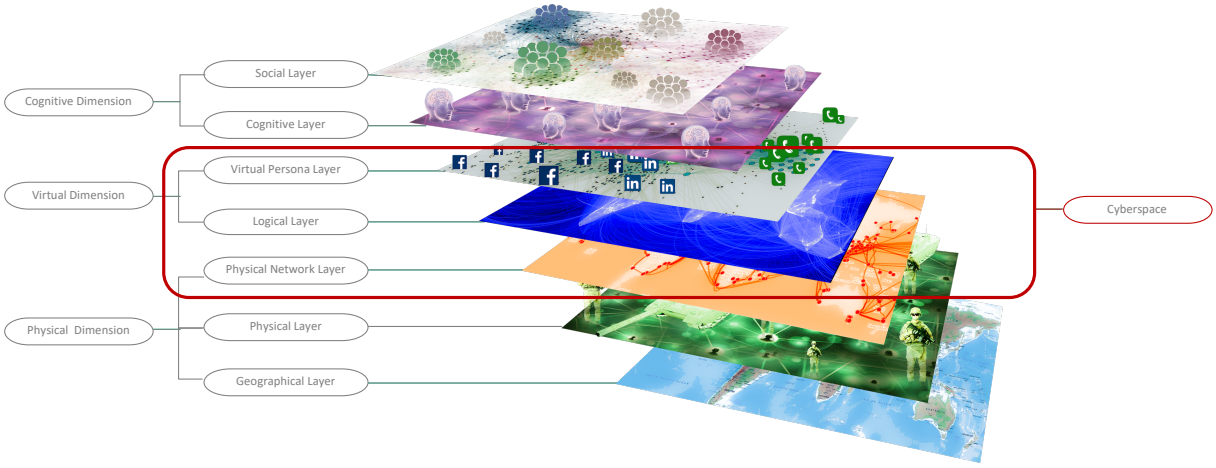

Figure 1: Information Environment and Cyberspace[13]

Previously unheard-of threats, such as a DDoS-attacks,[14] have materialised,[15] and it is therefore not the question *whether* but *how* the Netherlands must respond to malign use of the information environment. The concept of information manoeuvre is (being) developed to facilitate this response.

Information manoeuvre can be defined as the use of information of a cognitive, virtual (digital) or physical nature by armed forces 'in the operational environment [...]to achieve a position of advantage in respect to others […] in order to accomplish the mission'.[16] Information manoeuvre is, therefore, a way of exerting power and achieving effects by using information in any cognitive, virtual of physical form to shape the operational

[12] AIVD, MIVD, and NCTV, "Dreigingsbeeld Statelijke Actoren," 2021. pp. 32-34.
[13] Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, "Manoeuvring and Generating Effects in the Information Environment," *ACIL Research Paper 2017-25*, 2017. p. 6.; see also: Jelle van Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict" (2018). p. 173 (note 898).
[14] DDoS means a distributed denial of service wherein an overwhelming number of computers let a website crash, rendering it (temporarily) unavailable, see e.g.: United Kingdom Government, "UK Assess Russian Involvement in Cyber Attacks on Ukraine," 2022.
[15] For example, the cyber-attacks on the Iranian nuclear facility in 2010 or the attack on the Ukrainian Electricity Grip in 2015. Kim Zetter, *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon*, 2015.; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 2016.
[16] Derived from NATO's (AAP-6) definition of 'to manoeuvre': "The Employment of forces on the battlefield through movement in combination with fire, or fire potential, to achieve a position of advantage in respect to the enemy in order to accomplish the mission."

environment in an advantageous manner,[17] but moreover to use information as a weapon, i.e. a means of influence.

To apply this concept, obtaining an authoritative information position is crucial. This position is to be acquired through various mechanisms and sensors ('observe' in Figure 2), which enables adequate understanding (or sensemaking) of situations (insight) and attain foresight for future development.[18] Based on understanding, effective decisions can be made, and action in any of the dimensions of the information environment can be taken.[19]

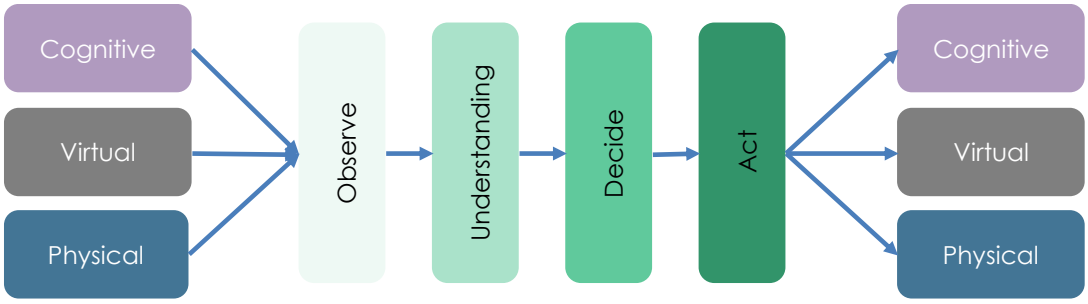

Figure 2: Information Manoeuvre Conceptualised[20]

The purpose is to be faster and better in decision making and act more effective than others. This process can result into several activities. One, is kinetic action with effects in the physical dimension to influence audiences in an indirect manner. The acme of information manoeuvre, however, is to ultimately use information (of any nature) as a means to achieve (offensive or defensive) effects.[21] The DV35 envisions 'armed forces that also use information as a weapon in its own right and that are permitted to use this weapon at an early stage and offensively where necessary.'[22] This may take place in three forms (or a combination thereof). First, the use of military and kinetic force generating effects in the physical dimension. Second, as so-called hard-cyber operations, i.e. the targeting in cyberspace itself through digital subversion or sabotage operations to achieve effects in the virtual dimension (virtual objects such as data and personae including social media accounts) and the physical network layer (computers, routers). And finally, via so-called soft-cyber operations (digital influence operations), meaning that information can be used as a weapon to influence the cognitive dimension of targeted audiences using cyberspace

[17] Army, "Force Troops Command Handbook."
[18] UK JDP-04 Understanding and Decision-making (2nd Ed.).
[19] See e.g. Henk Warnar, "Warships as Tools for International Diplomacy," *Atlantisch Perspectief*, no. 2 (2022): 9–13.
[20] Peter B.M.J. Pijpers and Paul A.L. Ducheine, "'In You Have A Hammer': Reshaping the Armed Forces' Discourse on Information Maneuver," *ACIL Research Paper 2021-34*, 2021. p. 8, accessible here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3954218
[21] Pijpers and Ducheine. pp. 11-13.
[22] Netherlands Ministry of Defence, "Defence Vision 2035: Fighting for a Safer Future." Annex p. XII

as a vector.[23] These influence operations aim to change the attitude of (opposing) actors by persuading them in a constructive manner or 'the deliberate use of information […] to confuse, mislead and ultimately influence the actions that the targeted population makes.'.

3. The Legal Framework for Activities in the Information Environment

This paragraph outlines the general legal framework for activities of the Netherlands' armed forces in the information environment.[24] The legal framework comprises the legal bases for action and the legal regimes that apply to the action itself.

Task, Order and Legal Authority

The armed forces are one of the so-called 'sword powers' of the government.[25] Based on the principle of legality - one of the principles of the Netherlands' constitutional law - activities of the armed forces require a legal basis if and when their actions impair the rights and privileges of citizens and organisations. This implies that such armed forces' actions typically may only take place (1) if they can be based on, and are carried out within the boundaries of, a formally assigned task, (2) an (implied or explicit) order by the government to execute this task and, (3) a legal authority to carry out the activity in the execution of the task. The notion 'legal authority' refers to the requirement to have of a national or international legal basis for the execution of a legitimate task which may constitute an infringement upon the (human) rights and freedoms of citizens - both in the Netherlands and abroad.[26]

The next sections explain where tasks, orders and legal authorities derive from in the context of an international deployment, and how they relate to the readiness phase.

International deployment

Article 97 of the Netherlands' constitution is the principal provision setting out the position of the armed forces in the constitutional order:

[23] For the difference between these cyberoperations see also: Peter B.M.J. Pijpers and Kraesten L. Arnold, "Conquering the Invisible Battleground," *Atlantisch Perspectief* 44, no. 4 (2020). pp. 12-14; Sean Cordey, "Cyber Influence Operations: An Overview and Comparative Analysis," *Center for Security Studies (CSS), ETH Zurich*, 2019. pp. 15-19.

[24] The framework for the intelligence & security services, MIVD and the General Intelligence and Security Service (AIVD), is quite distinct and set out in the Intelligence and Security Act 2017 (WIV 2017).

[25] The two 'sword powers' are the armed forces and the police.

[26] For international deployment, these three steps are combined in the so-called Article 100 procedure referring to Article 100 of the Dutch Constitution. See also: *Parliamentary Papers II 2013-2014*, 29 521, no. 226; Paul A.L. Ducheine, Kraesten L. Arnold, and Peter B.M.J. Pijpers, "Decision-Making and Parliamentary Control for International Military Cyber Operations by The Netherlands Armed Forces," in *Liber Amicorum*, ed. Rogier Bartels et al., 2020, 59–81.

> "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."[27]

Paragraph 1 sets out the triple purposes for the Kingdom's armed forces: (1) to defend the Kingdom and allies, (2) to maintain and promote the international legal order, and (3) to protect the (other vital) interests of the Kingdom.[28]

The decision to make use of the armed forces for these purposes, i.e. to deploy them abroad, lies solely with the Government of the Netherlands and is, besides political and military strategic considerations, based on the legal framework (legal bases and legal regimes) applicable to a mission or operation.[29] Such a decision forms the mandate, and thus constitutes the basis for the task and legal authorities, for deployment.[30]

In the event of an international deployment, legal authority for activities required to execute the mandate follows from the legal basis in international law for the mission or operation and the applicable legal regime(s).[31] The following legal bases in international law are internationally recognised:

1. The consent of a host State, which in the first place governs the presence of foreign armed forces on its territory, territorial sea and airspace above it,[32] and secondly may set out which specific activities may be executed, and under which conditions they may be carried out.[33] In so far activities in the information environment affect the sovereignty of the host State, it must be ensured that the consent of host State governs such activities.

---

[27] Official English translation of the Constitution of the Kingdom of the Netherlands, available at https://www.denederlandsegrondwet.nl/id/vkwrf6d92rnm/de_tekst_van_de_grondwet_met_toelichting.

[28] Ducheine, Arnold, and Pijpers, "Decision-Making and Parliamentary Control for International Miiltary Cyber Operations by The Netherlands Armed Forces." Available at SSRN: https://ssrn.com/abstract=3540732.

[29] See e.g. P.A.L. Ducheine & E.H. Pouw, 'Legitimizing the Use of Force´, Chapter 3, pp. 33-46; respectively 'Controlling the Use of Force: Legal Regimes´, Chapter 5, pp. 67-80, in: J. van der Meulen, A. Vogelaar, R. Beeres and J. Soeters (eds.) Mission Uruzgan : Collaborating in multiple coalitions for Afghanistan, Amsterdam: AUP (2012).

[30] In the execution of his responsibility to direct the execution of all military operations, the CHOD, by means of an order of his Director of Operations, will 'translate' the mandate in specific orders for units assigned for deployment.

[31] Such as International Human Rights Law or – if appropriate – International Humanitarian Law.

[32] North Sea Continental Shelf Cases, ICJ Reports (1969). Para 59, p. 37; Gleider Hernandez, *International Law* (Oxford, United Kingdom: Oxford University Press, 2019). pp. 474-475.

[33] It must be noted, however, that the consent of the host State does not serve as an independent source for authorities. This may require an international agreement or arrangement to ensure mutual understanding on the terms and conditions. This is to prevent that armed forces carry out executive powers abroad that, while allowed under the laws of the host State, are not allowed or would violate the law of the Sending nation, including obligations under international law, for example those following from international human rights treaties to which the Sending nation is a party, such as the European Convention on Human Rights (ECHR).

2. A UN Security Council Resolution (UNSCR) adopted under Chapter VII of the UN Charter, in which case the (interpretation of the) text of the resolution determines the nature and scope of the measures that may be taken.[34]

3. (Collective) self-defence in case of an armed attack, as recognised under Article 51 of the UN Charter.[35]

Deployment of the armed forces in an international context, however, may also take place without a specific legal basis in case of (ad hoc or standing) cooperation, for example in the case of the Dutch contribution to the Standing NATO Maritime Group (SNMG).[36]

In sum, when deployed abroad,[37] activities in the information environment may only take place within the confines of a mandate, which reflects the legal basis for the deployment, and takes into account the legal regimes applicable in the context of the deployment.

Readiness

In order to effectively execute military power in fulfilment of a mandate during deployment abroad, appropriate levels of readiness of the armed forces must be achieved, *inter alia* by means of 3ET. In the Netherlands, a distinction is made between, on the one hand, 'general readiness' (OG),[38] and, on the other hand, deployment-specific readiness (IG)[39] following a governmental decision to deploy.[40]

Deployment and readiness constitute the core elements of the Ministry of Defence's business process. A ministerial decree – the General Organisation Decree for Defence (AOD) - sets out the responsibilities for the chief authorities within the ministry, such as the Chief of Defence (CHOD) and his subordinate commanders.[41] Article 3 AOD, for example, stipulates that the CHOD is responsible for the direction of the preparation, execution and evaluation of all military operations, subject to the instructions of the Minister of Defence.[42] It is important to emphasize that while the AOD tasks the CHOD

[34] An international deployment of Dutch armed forces on the basis of a UNSCR may take place in the context a UN-led mission (as was the case in for example MINUSMA, or UNMISS), or a UN-mandated mission (e.g. SFOR, or ISAF). In addition to the legal basis of the UNSCR and depending on the context (armed conflict or peace), the legal regimes of IHL and/or IHRL determine the legal room for manoeuvre.

[35] In which case the right to self-defence and most notably International Humanitarian Law (IHL or the Law of Armed Conflict LOAC) and – when applicable - International Human Rights Law (IHRL) determine the authority to act.

[36] See: JFR Boddens Hosang, Force Protection, Unit Self-Defence and extended Self-Defence, in: Gill & Fleck, Hb ILMO (2nd Ed), chapter 24, pp. 476-501.

[37] The decisions to deploy armed forces domestically, rests with the authorities designated by the legislator in formal law, such as the Minister of Justice and Security in case of military support to the Police. See e.g. Articles 57-59 of the Police Act 2012.

[38] In Dutch: 'Operationele Gereedstelling' or OG.

[39] In Dutch: 'Inzetspecifieke Gereedstelling' or IG.

[40] Based on Article 97 Constitution for deployment abroad (or on specific formal acts for domestic deployment).

[41] In Dutch: Algemeen Organisatiebesluit Defensie 2021, or AOD 2021.

[42] Article 3(c) AOD 2021.

and his subordinate commanders (of the army, navy etc.) with responsibilities concerning the readiness of their forces, it is not a document providing legal authority.

General readiness activities must comply with national legislation without exemption. For the purposes of achieving general readiness, there is no specific Dutch law and therefore no explicit legal basis permitting the armed forces to carry out activities that infringe upon the rights and freedoms of citizens. Neither is there an international legal basis to fall back on since OG takes place prior to actual deployment and therefore outside the context of the international legal bases and regimes set out above.[43]

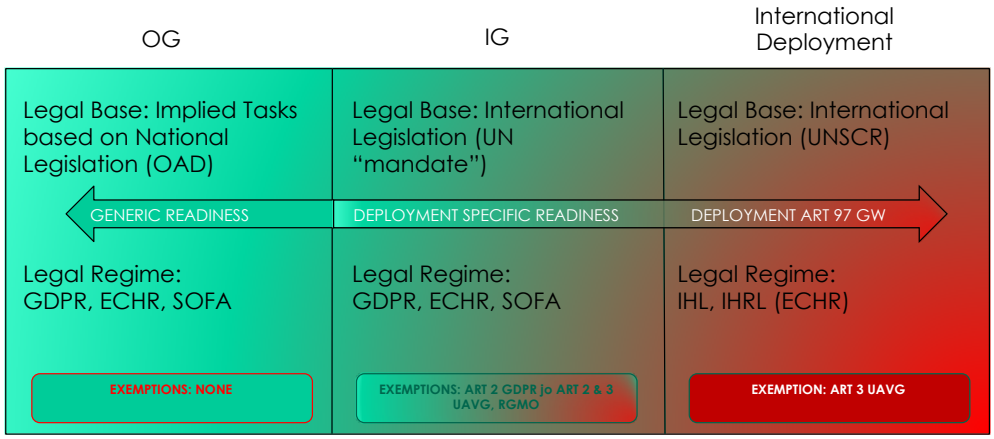

Table 1: Readiness & Deployment matrix for International Deployment

As for IG, the situation is different (see Table 1). In this case, legal authority derived from the Government's decision to deploy and the international legal basis for that deployment can also be used for activities to prepare for the specific deployment, including activities carried out prior to actual deployment. The IG period is understandably limited in time and subject to specific guidance by the CHOD who directs all military operations. However, in the event of a deployment without a specific legal basis, as explained above, no legal authorities will become available for the armed forces for deployment-specific readiness activities. In that case, the activity requires a basis somewhere in Dutch law.

To sum up:

[43] The exception being readiness-activities taking place abroad with the consent of the host State through e.g. a Status of Forces Agreement determining what is permitted and what not. Such activities will be governed by International Human Rights Law, implying that activities amounting to any infringement of human rights requires a basis in law, in this case meaning that both the law of the host State as well as the Sending state's (e.g. Dutch) national law must provide such basis.

- activities may only be carried out based on an order that falls within the scope of an assigned task and require a legal authority to the extent it constitutes an infringement upon (human) rights, *regardless of* deployment or readiness;

- readiness activities may only be carried out within the scope of the readiness-tasks assigned to the CHOD and his subordinate commanders. To the extent that these activities infringe with (human) rights, a legal authority must follow from Dutch law (OG and IG) or international law (IG).

The following section will make clear that the legal latitude for activities that amount to the processing of personal data or otherwise infringe with the right to privacy differs significantly between deployment and IG on the one hand, and OG on the other hand.

Some Aspects Concerning the Processing of Personal Data

Activities of the armed forces in the information environment may infringe upon the right to privacy, irrespective of location. This is for example the case when collecting, processing and sharing personal data from open sources such as the internet or social media for purposes of Open Source Intelligence (OSINT), and when using Intelligence, Surveillance and Reconnaissance (ISR) sensors that process personal data.

The right to privacy is a constitutional right protected in Article 10 of the Netherlands' constitution:

> "1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.
>
> 2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.
>
> 3. […]."

The Netherlands is also party to human rights treaties that protect the privacy of persons, such as the International Convention on the Protection of Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR).[44] Article 8 of the ECHR stipulates:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.

[44] See also Protocol 223 to the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of the Council of Europe, to which the Netherlands is a signatory. The Protocol will enter into force as of 11 October 2023.

> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety (…)."

Being a member of the European Union (EU), the Netherlands is also bound by the EU's General Data Protection Regulation (GDPR),[45] which has direct effect in Dutch law. The GDPR contains rules on a specific element of privacy, namely the (automated) processing[46] of personal data.[47] In order to further regulate certain aspects of the GDPR, the Dutch legislator adopted the GDPR Implementing Law (UAVG).[48]

The GDPR does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Union law',[49] nor to activities which fall 'within the scope of Chapter 2 of Title V of the TEU' which relates to the Common Foreign and Security Policy, including defence-related matters.[50]

The processing of personal data in the interests of national security, for example those carried out by a Member State's intelligence and security services,[51] but also the processing of personal data by its armed forces,[52] falls outside the scope of the GDPR.[53]

This inapplicability of the GDPR, however, does not mean that the processing of personal data by the armed forces is left unregulated. After all, both the Dutch constitution and international legal obligations such as those emanating from the ECHR demand that State interference with the right to privacy requires a basis in law.[54]

---

[45] In Dutch: Algemene Verordening Gegevensbescherming (AVG). The GDPR is accessible here: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[46] 'Processing' is defined in Article 4(2) of the GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[47] 'Personal data' is defined in Article 4(1) of the GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

[48] In Dutch: Uitvoeringswet AVG, or UAVG.

[49] Article 2(2)(a) GDPR.

[50] Article 2(2)(b) GDPR; Articles 23-46 of the Consolidated Version of the Treaty on European Union, C–326 Official Journal of the European Union (2012). This includes Article 42(7), the mutual assistance clause.

[51] With respect to the Dutch intelligence and security services AIVD and MIVD, the Intelligence and security services Act 2017 (WIV 2017) provides such basis. For that reason, the GDPR jo UAVG Article 3(3)(b) is not applicable to the processing of personal data by the AIVD and MIVD to the extent authorized by WIV 2017. This means that the processing of personal data by both AIVD and MIVD that does not find a legal basis in the WIV 2017 is still governed by the GDPR and UAVG.

[52] See e.g. Marten C. Zwanenburg, "Het Gebruik van Biometrie in Militaire Missies: Aanzet Voor Een Studie van Het Juridisch Kader," *Militair Rechtelijk Tijdschrift*, 2021, 1–18. pp. 11-15.

[53] Military deployments outside of EU missions are exempt based on Article 2(2)(a) GDPR, deployments within the EU scope based on Article 2(2)(b) GDPR. See Zwanenburg. p. 13.

[54] Article 6 sub 3 TEU considers the Fundamental right as guaranteed in the ECHR are part of Union Law. Consolidated Version of the Treaty on European Union, C–326 Official Journal of the European Union (2012).

As it would be unconstitutional and contrary to international legal obligations to leave the processing of personal data by the armed forces unregulated, the legislator used the UAVG to declare the GDPR applicable to any processing of personal data by the armed forces in the execution of its own tasks.[55] This means that the GDPR and UAVG are also applicable during deployments abroad. However, realizing that circumstances during deployments do not always allow for the full compliance with all provisions of the GDPR, the UAVG and a ministerial regulation – the Regulation on Data Protection Military Operations (RGMO)[56] - indicates that under certain conditions (parts of) the GDPR and the UAVG are nonetheless *not* applicable to the processing of personal data. These conditions are that:

> (1) the government decides to deploy or make available[57] armed forces for the purposes set forth in Article 97 of the Netherlands' Constitution;[58] and
>
> (2) the international legal basis for the operation for the benefit of which personal data is processed authorizes such processing;[59] and
>
> (3) the processing of personal data is necessary for the execution of the mandate or the protection of the forces;[60] and
>
> (4) the Minister of Defence subsequently decides to make use of the authority granted under Article 3(3)(a) UAVG to decide to exempt the armed forces from applicability of parts of the GDPR and UAVG for this particular operation or mission.[61]

While the RGMO is not explicit on this, the processing of personal data may also take place in the IG-phase, under the same conditions set out above

Two important conclusions can be drawn from the above. First, in the IG-phase and during military deployments for the purposes of Article 97 of the Dutch Constitution, the processing of personal data is *permitted* only when the Minister of Defence decides so, based

---

[55] *Parliamentary Papers II 2017-2018*, 34851 no 3 (2018), footnote 4 on page 9 & p 14. The Explanatory Memorandum to the law is accessible here: https://zoek.officielebekendmakingen.nl/kst-34851-3.html. See also: Article 3(1) and (2) UAVG. See also the commentary to the UAVG, available at https://zoek.officielebekendmakingen.nl/kst-34851-3.html.

[56] In Dutch: Regeling Gegevensbescherming Militaire Operaties, or RGMO.

[57] In Dutch: beschikbaar stellen. 'Making available' refers to the making available of units to EU or NATO, for example to NATO's VJTF.

[58] This includes national deployment in support of national authorities. This type of deployment falls outside the scope of the RGMO, because in these instances any processing of personal data by the armed forces takes place in the execution of tasks and legal authorities of the national authorities. This explains why the focus in the RGMO lies on international operations only, as illustrated by the second condition ("to the extent this is authorized by the international legal basis for the operation for the benefit of which personal data is processed").

[59] Article 1(1) and (2) RGMO.

[60] Article 1(1) RGMO. This includes foreign coalition forces, for example NATO partners.

[61] In other words: without an explicit decision by the Minister of Defence, the processing of personal data during the military operation is governed by the GDPR (with the exception of UN-led missions, such as MINUSMA. In those missions, the processing of personal data is governed by the rules of the UN). In the event of such decision, the Dutch Data Protection Authority (in Dutch: Autoriteit Persoonsgegevens, or AP) must be informed as soon as possible, Article 3(4) UAVG.

on an assessment of the necessity for the execution of the mandate or the protection of the forces. Second, without a legal basis elsewhere in national law (such as WIV 2017),[62] the processing of personal data by the armed forces is governed by the GDPR.

In view of the latter, the question then is: away from a deployment and IG period, when is the processing of personal data by the armed forces lawful under the GDPR?

Processing of personal data under GDPR for achieving readiness

It follows from both definitions of 'processing' and 'personal data'[63] that the threshold for processing personal data by the armed forces is easily crossed, particularly when using the Internet or employing means and methods of ISR.

If so, the processing of personal data must comply with the principles set forth in Article 5 GDPR,[64] *provided that* one of the six bases that authorize the processing of personal data is applicable.[65] While some of these bases are not relevant for achieving the levels of readiness of the armed forces, others appear better suited, but are still troublesome.

This concerns, to begin with, 'consent', but the processing of personal data on the basis of consent is subject to very strict conditions.[66] In the context of 3ET it can therefore only take place in a controlled setting, which makes that 'consent' fits 3ET in very limited

[62] In Dutch: Wet op de inlichtingen- en veiligheidsdiensten 2017, or WIV 2017.

[63] See footnotes 46 and 47.

[64] Article 5 GDPR: "1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. (…)

[65] Article 6 GDPR, paragraph 1: "Processing shall be lawful only if and to the extent that at least one of the following applies:(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[66] Article 7 GDPR.

circumstances.[67] In the context of activities carried out to obtain an authoritative information position, this basis appears not suitable at all.

A second processing base, 'processing [that is] is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' requires a legal base for the processing of personal data in the law of the EU or national law, setting out, *inter alia*, who is the public authority tasked to do so, a sufficient description of the task and the purpose for the processing.[68] There is no such legal basis for the armed forces for 3ET, nor for activities in support of obtaining an authoritative information position.

The third basis – processing that is necessary for the purposes of the legitimate interests pursued by the controller or a third party[69] – whilst applicable for deployment, is not available for public authorities that process personal data in the execution of their task.[70] The reason is that it is up to the legislator to create the legal basis for the processing of personal data by public authorities. As noted, no legal bases for the processing of personal data by the armed forces for the purposes of its (general or mission-specific) preparation for deployment are in place at this moment in either EU or Dutch law.

In sum, with the exception of (the highly cumbersome) 'consent' as mentioned in the GDPR, the armed forces appear to have *no* legal basis to process personal data when carrying out activities for the purposes of OG.

There would be a legal basis once the Government has decided to deploy or make available Dutch armed forces and:

- the CHOD has ordered the mission or operation specific preparation (IG), and;
- there is an international legal basis, and;
- a legal authority to process personal data can be derived from the international legal basis, and;
- the processing of personal data is necessary for the execution of the mandate or the protection of the forces.

[67] An example in case is the education, training, exercise and experimentation with biometrical data, in which it is possible to gain consent of role players, however, thereby taking notice of the fact that consent must be given entirely freely. This means, for example, that it is not possible to use role players from the same unit that conducts the exercise.

[68] In addition, there must be publicly available law that informs the citizen with sufficient accuracy which personal data will be collected and processed for the purposes of a certain public task, and under which conditions these data will be adapted, kept and used.

[69] E.g. for reasons of fraud prevention or network and information security.

[70] Article 6(1) AVG.

Based on that, the Minister of Defence may subsequently decide to make use of the authority granted under Article 3(3)(a) UAVG to decide to exempt the armed forces from applicability of parts of the GDPR and UAVG for this particular operation or mission.

In the next paragraph, we will apply these conclusions set out above information manoeuvring activities as envisioned by the DV2035.

4. Implications for information manoeuvring activities

We will use a hypothetical scenario in the near future in which in the concept of information manoeuvre as outlined in the DV35 has been implemented, while the legal framework as set out above (in paragraph 3) has not changed. Would that legal framework permit the armed forces to (1) educate, exercise and experiment and train (3ET) to achieve an acceptable level of readiness and (2) to collect, process and disseminate information to contribute to the authoritative information position?

Setting the Stage

In the fictitious scenario one State has invaded another State outside the EU and NATO-alliance – similar to the Russia-Ukraine war. The Netherlands is not a belligerent party, but the vicinity of the war impedes our national interests. As part of NATO's strengthening of deterrence strategy and the defence of the eastern flank of NATO's European territory,[71] it can be imagined that the Netherlands will deployed troops to front-line States including Lithuania, Romania or Slovakia.[72] In addition, the Netherlands, together with other States, have supported the invaded victim State with weapons and other military equipment.[73]

The Dutch armed forces have the capacity to roam the information environment with a wide variety of sensors to collect, process, analyse, interpret and disseminate data and information needed to provide the CHOD and his subordinate commanders with insight and foresight required to understand the situation and to make decisions based thereon.

At this stage in the conflict an international legal basis from which a legal authority to process personal data by Dutch armed forces can be derived, is still lacking. The conflict does not amount to a case of collective self-defence involving the Netherlands,[74] a UNSCR is not at hand, and – in absence of additional enabling SOFA's - the consent of the host

[71] NATO, "SACEUR Statement on the Activation of the NATO Response Force," *Shape Newsroom*, 2022.
[72] Letter of Minister of Defence and Minister of Foreign Affairs to the Chair of Parliament, 18 March 2022, BS 2022006331.
[73] Sebastien Roblin, "The Dutch Are Sending Huge German Armored Howitzers To Ukraine," *Forbes*, 2022.
[74] There has been no armed attack by Russia or by non-State agents under authority and control of Russia on a NATO-member that would trigger the right to self-defence of that member, based on Article 5 of the NATO-treaty.

States Lithuania, Romania and Slovakia is insufficient to serve as a legal basis to process personal data.

The following example will be examined to illustrate if today's legal framework fits the concept of information manoeuvre. While receiving strategic intelligence from the MIVD, the CHOD orders the – then established - joint information manoeuvre unit of the armed forces (JIMU) to provide a daily update of the tactical situation on the ground, to complete the intelligence picture needed to obtain an authoritative information position in support of Article 3 AOD.[75] In addition, their products can be disseminated to the army, navy and air force commands, as well as to the commanders of the units stationed in Lithuania, Romania and Slovakia. In the execution of this order, the JIMU makes extensive use of Internet-based open sources.

The question is: in view of the legal aspects discussed in the previous paragraph(s), would the abovementioned activity be permissible in terms of task, legal basis, and legal authorities?

Task, Order and Legal Authority

In this scenario, the JIMU is not deployed yet, nor is there a solid international legal basis to prepare for a specific deployment. Does the current legal framework offer a basis to task the armed forces, in this case the JIMU, to roam the information environment for data and information to enhance the information position of the CHOD *cum suis*? A search for an explicit task in law stipulating such a responsibility for the armed forces will be without result, for there is none. It can nonetheless be argued that the task is implied in so far it falls within the scope of the responsibilities of the CHOD and the armed forces' subordinate commanders as set forth in the AOD.

This can be problematic once the implied tasks of the armed forces infringe upon human rights of citizens. Notwithstanding the threat described in the scenario, the legal situation for the Netherlands and its armed forces is one of peace, and any State action is governed by the international law, IHRL in particular. As noted, when using real world data and information, it is rather impossible to avoid that personal data will be processed.

Unless the Government decides to deploy forces or make them available and the Minister of Defence makes use of the Article 3(3)(a) UAVG authority, in light of the fact that the international legal basis provides the legal authority to process personal data, the GDPR and UAVG apply in full; hence personal data cannot be processed in the course of information manoeuvring activities by the armed forces. Applying the above, JIMU is not

[75] Besides the responsibility to direct the preparation, execution and evaluation of all military operations and the responsibility to direct the readiness of the armed forces, his responsibilities also include the task of primary military advisor to the Minister of Defence, as well as directing the operational commands of the navy, air force, army and Royal Marechaussee (the latter to the extent their activities are a responsibility of the Minister of Defence; most activities of the Royal Marechaussee are carried out under authority of the Minister of Justice and Security.

permitted to process personal data since JIMU is not deployed or preparing to be deployed (IG) nor did the Minister of Defence invoke Article 3(3)(a) UAVG.[76]

The legal challenge

It is precisely here that a major vulnerability with respect to the role of the armed forces manoeuvring in the information environment surfaces. While the DV35 articulates that de Defence organisation must be able to manoeuvre in the information environment, the armed forces lack the legal framework to do so. At current only the MIVD has an explicit task and legal authority to roam the information environment, including the processing of personal data, outside the context of a deployment. However, the MIVD is tasked for other purposes, and therefor deliberately restricted in tasks and authority by the legislator.

4. Conclusion and reflection

The inception of the GDPR has provided the EU with a solid legal regime for the protection of personal data. The GDPR provides several exemptions. First, the GDPR is not applicable in cases that fall outside the scope of Union law (EU jurisdiction). Second, the GDPR does not apply to the processing of personal data in the exercise of activities that fall within the scope of the Common Foreign and Security Policy. These exemptions in the GDPR have been revoked by the Netherland via the UAVG, meaning that that the GDPR and the UAVG apply to the Netherlands' armed forces *in full*. Based on national legislation, the Minister of Defence can decide to lift application of (parts of) the GDPR and the UAVG ex art 3(3)(a) if the armed forces are deployed or made available for deployment under the auspices of Article 97 of the Constitution, subject to certain conditions.

Conclusion

The Netherlands and its citizens rely on its armed forces to protect the vital interests in all domains of the information environment. But, does the current legal framework offer adequate room for the armed forces to manoeuvre in the information environment? The answer is no. As illustrated, if the current legal framework would still apply in the hypothetical case in the near future, the role for the armed forces as envisioned in the DV35 would be seriously hampered.

It can be assessed that for deployments, there is a sufficient - or rather a 'workable' - legal framework for executing information manoeuvre operations by the armed forces provided

[76] Deployment, though, is not inconceivable, as the JIMU could, for example, function as reach back-capacity for the units deployed in Lithuania, Romania and Slovakia. But, as noted, the mere fact of deployment does not generate legal authority to process personal data; this must follow from the international legal basis underlying the deployment which in this scenario is missing.

that the international legal basis and the political mandate provide the required legal authorities and tasks.

However, if the conditions related to task and authority are not in place, or if the activity is not an actual deployment, the GDPR applies in full and the armed forces are in effect disabled to roam the information environment as they are not authorized to process personal data. It can furthermore be concluded that the current legal framework affects the day-to-day activities of the armed forces related to generic readiness tasks, but also to activities that might include the processing of personal data, related to the preparation of an actual deployment.

In general terms, the capability to educate, exercise and experiment and train (3ET) to achieve an acceptable level of readiness in order to manoeuvre effectively in the information environment would be flawed as a result of the failing legal part of the conceptual framework to support the existing and desired capacities. The same flaw hampers the ambition to be have the capability to collect, process and disseminate information in order to contribute to the authoritative information position that is necessary for deployment.

Reflection

Safeguarding privacy and the prior legal authority for infringements of privacy is not the stone of contention in this contribution. However, cognisant of the fact that the GDPR existed before the concept of information manoeuvre came in vogue, it is questionable whether the legislator could have foreseen that the decision to apply the GDPR in full to the armed forces would have caused a near-unworkable situation for the armed forces' information manoeuvre.

This predicament endangers the ambition of the DV35. However, we're not there yet. Aside from the deployment of armed forces for information manoeuvre activities, it is required – to achieve the DV35 ambition – that military personnel should be able to adequately train and exercise (3ET) in order to achieve desired levels of readiness (OG and IG).

The question is how to do so? Three takes are offered.

First, take the given legal framework, comply with it and accept the restrictions. In this context armed forces could work with fictitious data sets for training and exercise purposes or use virtual training 'grounds' that offer virtual and synthetic realistic environments, such as the existing 'second life' society. Though basic skills can be trained, the Internet evolves to fast to make these virtual ranges realistic.

Secondly, one can also find legitimate loopholes or workarounds. Efforts can be made to optimise the legal possibilities offered via the national police or the MIVD. Though the Police Act or the WIV 2017 are not meant to facilitate information manoeuvre activities of the armed forces, organisational constructions including secondments or placing units

under command of the Police and MIVD during specific activities might make the gaps smaller for the readiness phase.

Or – thirdly - pursue a path advocating a change in legislation. The challenge then is to strike the right balance between the protection of privacy and the provision of security, a challenge not solely for the government but society as a whole. Citizens and companies are entitled to enjoy their rights and privileges, for which a certain level of security is required. It is understandable that striking this balance can be difficult since these attempts are likely to be met with opposition, as was witnessed with the adoption of COVID related regulations, the WIV 2017 referendum and the attempts by other public authorities to be granted with similar legal authorities.[77] But security comes at a price and given the conflict in Ukraine security proves to be a poor fit with complacency.

Ultimately, the question is whether the society is willing to accept that the armed forces are expected to master the ins and outs of information manoeuvre whilst being deployed for one of its constitutional aims, while acceptable readiness levels prior to deployment cannot be achieved because the necessary preconditions are absent. The same applies to a role for the armed forces as a contributor to obtaining an authoritative information position. Perhaps a more confronting way of putting this is: is society ready to accept casualties that clearly could have been prevented had the armed forces been fully equipped to do what is necessary and expected of them in the information environment? If the armed forces are to fulfil their task as first responder and the last line of defence in protecting the security interests of the Kingdom, the legal predicaments need to be dealt with. For it would be hypocritical to demand security without providing the armed forces with the appropriate tools and powers to do so.

[77] An example is a recent proposal for a law permitting the NCTV, the national coordinator for combatting terrorism and security, to process personal data, including special data such as religion or political preference, in the exercise of its analyses of trends and phenomena. See: an interview with Frederik Zuiderveen Borgesius, "'Wetsvoorstel Beloont NCTV Voor Iets Wat Niet Mag,'" *Radboud Recharge*, 2022. (The title reads: "Proposal for Law rewards the NCTV for something it is not allowed to do")