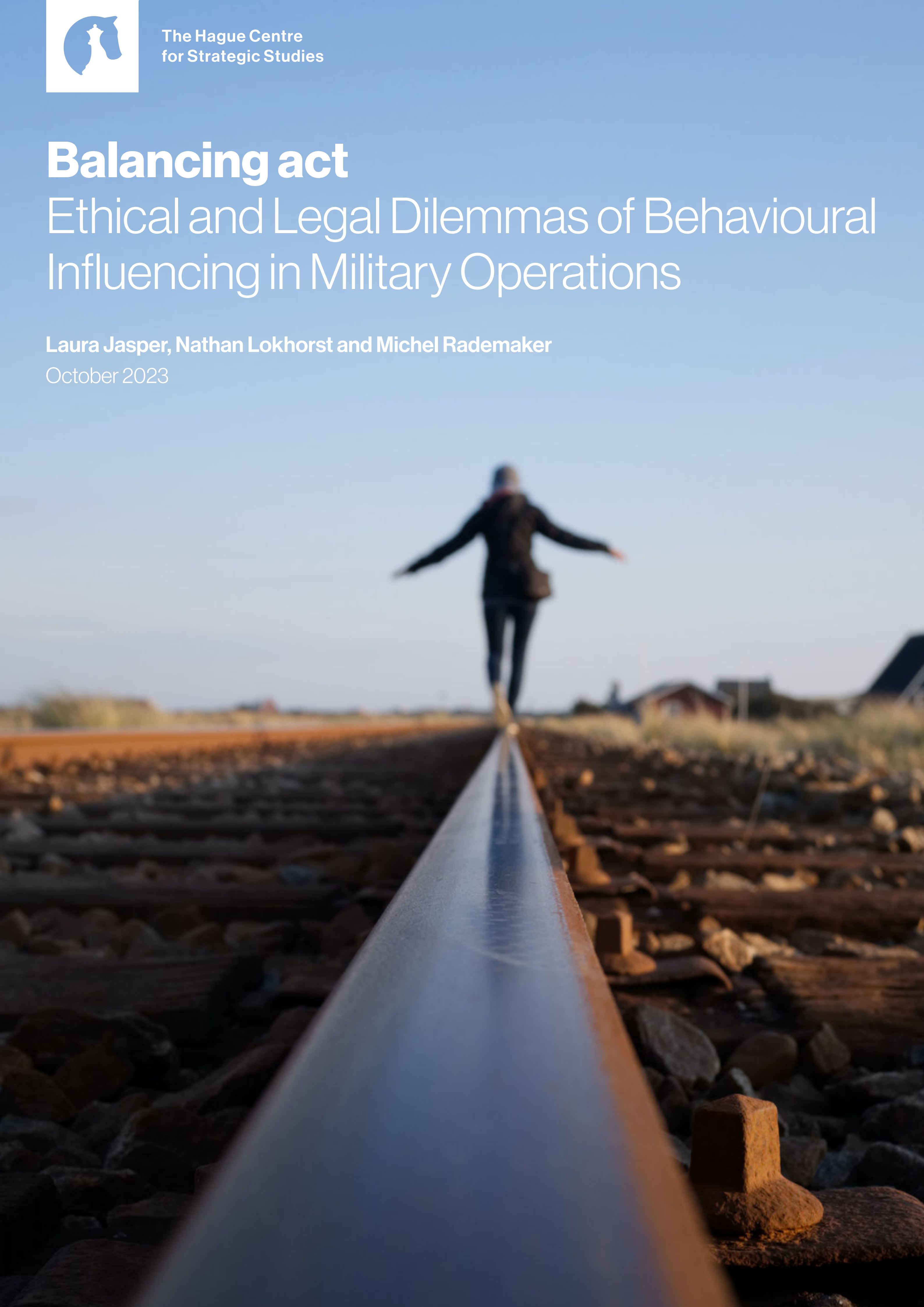
The Hague Centre
for Strategic Studies

# Balancing act
## Ethical and Legal Dilemmas of Behavioural Influencing in Military Operations

Laura Jasper, Nathan Lokhorst and Michel Rademaker

October 2023



The Hague Centre
for Strategic Studies

# Balancing act
## Ethical and Legal Dilemmas of Behavioural Influencing in Military Operations

**Authors:**
Laura Jasper, Nathan Lokhorst and Michel Rademaker

**Cover image credit:**
Niklas Ohlrogge, Unsplash

October 2023

This paper has been written as part of the project Platform Influencing Human Behaviour, commissioned by the Royal Netherlands Army. The aim of this platform is to build and share knowledge on information-based Behavioural Influencing (BI) in the military context, dissecting the ethical, legal and military-strategic issues and boundaries involved. Responsibility for the content rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Royal Netherlands Army.

The authors would like to thank the following individuals and organizations for sharing their expertise and experience which have significantly contributed to the overall content and quality of this research paper. Evidently, the content of this paper is the sole responsibility of the authors.

- Lieutenant-Colonel Björn de Heer, seconded at HCSS
- Professor mr. dr. Lonneke Peperkamp, Netherlands Defence Academy
- Colonel mr. dr. Peter Pijpers, Netherlands Defence Academy

All interviewees and participants of the expert workshop held April 13th, 2023

# Table of Contents

# Executive Summary

## Context

The military employment of information has a long history in influencing the outcome of war and conflict on, and off, the battlefield. The act of meaningfully trying to influence the behaviour of an individual or group, by targeting people's knowledge, beliefs and emotions using information tactics is coined behavioural influencing (BI). Recent technological developments have been a driving force in enhancing the possibilities and scope for military operations in the information environment. With that comes a renewed discussion on the applicable ethical and legal frameworks. But even more so, where the ethical and legal boundaries lie, and which possible dilemmas arise on these boundaries. The intent of this research was not to provide answers or solutions to existing ethical or legal dilemmas when it comes to BI, but rather to facilitate the discussion on this topic and to highlight when, where, and why these dilemmas may occur.

## Methodology

This paper is the result of an accumulation of desk research, individual interviews,[1] and an elaborate expert session.[2] In first instance the desk research served as input for a previously written position paper which was used as the basis for the expert session. This session brought together a variety of international military and non-military experts and practitioners. During the session different vignettes were presented with the intent to discuss possible dilemmas arising when employing BI capabilities. The input from this desk research, the position paper and expert session was then supplemented by individual interviews conducted with international military practitioners from the Netherlands, Belgium, Germany, France and the United Kingdom.

## Legal obstacles and options

The paper introduces the relevant legal framework, in order to pinpoint whether there is friction between the existing bodies of law and the notion of behavioural influencing in the military context. The main area of difficulty in the existing legal framework is found to be the binary aspect of law which demarcates between either 'peace' or 'war'. This creates uncertainty for cases that fall short of both notions, the so-called 'grey zones'. Limiting analytical thinking to the dichotomic notions of either war- or peacetime obstructs making legal considerations regarding these (grey-zone) operations, which in turn increases the risk of ethical dilemmas that arise within this uncharted grey zone.

[1] Interviews took place online via MS Teams over the course of December 2022 and January 2023.

[2] The expert session was held in person on Thursday April 13th at the Oranjekazerne in Schaarsbergen, The Netherlands.

## Ethical ends and means

Regarding the ethical dimension, the paper builds upon the *jus in bello* branch of Just War theory, which consists of 1) distinction, 2) necessity, and 3) proportionality[3]. This framework provides a useful analytical starting point for information operations in the context of armed conflict, with which arising dilemmas can be discussed. For example, how to measure proportionality if BI operations are not kinetic? Can the existing Just War framework translate in such a way that it becomes applicable to BI operations, or is this not impossible? These questions can be answered by a renewed dialogue on the meaning of the criteria of just war theory which sheds light on the ethical boundaries of BI operations. This dialogue should move away from the binary approach and adopting an analytical lens that allows for operations taking place somewhere in between the two ends of peace and war.

## International Benchmark

The terminology addressing capabilities associated with BI is not universal. Therefore, the paper introduced an international comparison of five countries to function as a way to benchmark to the international discussion that followed from the vignettes. This benchmark culminated in three main takeaways.

First, there is no common nor shared definition to frame information-driven practices that aim to influence behaviour in the military context. This disconnect occurs between countries on the international stage, as well as within countries, between their respective levels of government and military operations. This disconnect between common definitions and shared understanding complicates planning, training, and execution of BI capacities. Furthermore, it culminates in differences at the structural organisation level between countries. This in turn might complicate international cooperation, for example within NATO.

The second takeaway is that the main restrictions, as well as differences between countries, when it comes to inter-operability and deployment of BI capabilities lie with the usage of data and adherence to privacy regulations such as the GDPR.

The last finding regards current developments in terms of their key promises and pitfalls. Principle frictions in the employment of such capabilities seem to lie in the often described ‘paradoxical’ discovery that influencing appears to be viewed with more scrutiny and constringent controls compared to traditional or kinetic capabilities. Frictions appear to not necessarily lie with the action, used tactic or intended goal of an influencing operation as such, but rather with the imagined or conceived potential effect that was caused but not intended.

## Dilemmas in practice

Using four different vignettes, which were first discussed in the expert session, six different dilemmas are introduced to highlight several instances where the balance between operational utility of BI and the existing legal and/or ethical framework is lost or found. These

[3] As discussed by Prof. mr. dr. Lonneke Peperkamp in a key note speech during the expert session.

dilemmas function as examples to make that friction tangible. They thus not present every possible dilemma imaginable but are rather based on the examples of the vignettes. This is in line with the intent of the expert session and this research, being the identification of possible disconnect between these capabilities and the framework in which the interventions take place.

The first vignette looks at two possible dilemmas; those relating to norms and values and the occurrence of spill-over effects. Friction between norms and values is an inevitable part of military operations. In this context possible dilemmas arise between the personal and professional level of carrying out BI operations. Here, the cultural and societal norms and values of the target audience in the area of operation also take part in the balancing process. Additionally, the dilemmas that can arise regarding norms and values are derived from the previously mentioned three core principles of distinction, necessity and proportionality. The second dilemma that was introduced in this vignette is that of potential spill-over effects amongst and beyond the target audience on the short, middle, and long term. Here the following questions are posed. To what extent is it possible to map out spill overs? Furthermore, does the (in)ability to make this assessment alter the proportionality consideration?

The second vignette deals with privacy as a possible dilemma. Based on this vignette the following questions were discussed. Can one collect, store and analyse data prior to a mission on a large scale in order to properly prepare for actual deployment? Furthermore, can one apply this collected, stored and used data through specific BI activities as a 'weapon'? The dilemmatic nature of privacy and operability appears to be partly determined by which one of these two purposes, information as 'weapon' or as 'source', is adopted.

Dilemmas regarding target audience selection and dehumanisation are discussed in the third vignette. Reaching the right audience means shaping the narrative in such a way, that the intended audience is most susceptible to the message. If this is not the case, and the audience is thus not susceptible, the campaign cannot be successful. Audience's specific heuristics and vulnerabilities determine the framing of the narrative. The actor deliberately adopts a narrative in which two or more topics appear to be connected. Because this narrative appears to be true and is appealing to the audience (due to the exploitation of vulnerabilities), the audience perceives this message as true. The decision to deliberately exploit vulnerabilities of the target audience can be at friction with moral standards, as manipulative measures limit the audience's ability to have meaningful options. Dehumanisation being the failure of recognizing an individual's or group's humanity, can lead to individuals adopting their own personal moral identity, which helps them deal with moral dilemmas also referred to as desensitization. However, one's actions are not always in line with one's moral identity, which creates friction.

The fourth and last vignette looks at dilemmas brought about by operating in the so-called grey zone. It builds on the absence of a legal framework regarding grey zone operations, linked to the binary approach to peace and war. New technological developments in the virtual dimension have increased this grey-zone, by enhanced accessibility of BI activities and complicating attribution. Furthermore, this dilemma discusses where the threshold of war is or should be located with BI operations. It is proposed that one should step away from the traditional binary notion of peacetime or warfare, and rather develop a framework of 'different types of warfare', in which BI is included too.

# Main findings

As the intent of this research was not to provide answers or solutions to existing ethical or legal dilemmas when it comes to behavioural influencing but rather to facilitate the discussion on this topic and to highlight when, where, and why these dilemmas may occur the paper ends with two main findings, rather than conclusions.

1. The lack of legal framework, more specifically the fact that the grey zone is insufficiently governed by international law, increases the occurrence of ethical dilemmas. Accordingly, when operating outside of the legal grey zone, fewer ethical dilemmas appear to occur when operating in accordance to the three core principles. The ethical dilemmas that do occur appear to not be fundamentally new ones compared to cases in existing international and non-formal frameworks.

2. The question of data collection and governance appears to be the main reoccurring dilemma. This relates to the legal feasibility of carrying out data collection, analysis, and governance in preparation of an intervention. Which comes down to the General Data Protection Regulation (GDPR) and the Implementation Act GDPR.[4] The GDPR provides exemptions in its material scope related to security, foreign affairs and defence, the area of the Common Foreign and Security Policy [articles 23-26 TEU]. Via the Implementation Act the Netherlands revokes the provisions for exceptions for the operational context. In doing so one colours oneself into a difficult corner when it comes to the applicability and utility of information-based BI operations. The very specifically chosen Dutch implementation Act of the AVG thus creates an operational obstacle. This is seen as a broader issue within the Netherlands and is not solely limited to the Armed Forces.[5]

[4] The Algemene Verordening Gegevensbescherming (AVG) is the translation of the GDPR into Dutch law. The Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) is the implementation law. See: Autoriteit Persoonsgegevens, 'Algemene Verordening Gegevensbescherming (AVG)', 17 April 2016, https://autoriteitpersoonsgegevens.nl/uploads/imported/verordening_2016_-_679_definitief.pdf; Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Uitvoeringswet Algemene verordening gegevensbescherming', wet, 2021, https://wetten.overheid.nl/BWBR0040940/2021-07-01.

[5] Algemene Rekenkamer, 'Omgang Met de AVG in Relatie Tot Uitvoering Overheidstaken', 30 March 2023, https://www.rekenkamer.nl/publicaties/kamerstukken/2023/03/30/omgang-met-de-avg-in-relatie-tot-uitvoering-overheidstaken.

# 1. Introduction

The military employment of information has a long history in influencing the outcome of war and conflict on the battlefield, be it by deceiving the opponent, maintaining troop confidence, or shaping public opinion. We place these tactics under the banner of influencing human behaviour. Information-based behavioural influencing (BI) is the act of meaningfully trying to affect the behaviour of an individual, or a group of individuals, by targeting people's knowledge, beliefs and emotions. Recent technological advances have been a driving force in enhancing the possibilities and scope for military operations in the information environment. With that comes a renewed discussion on applicable ethical and legal frameworks in the information environment, but even more so, where the ethical and legal boundaries of those frameworks lie and the dilemmas that arise across those boundaries.

This paper attempts to highlight a number of instances where the balance between operational utility of BI and the existing legal and ethical framework is lost and found.

This paper attempts to highlight a number of instances where the balance between operational utility of BI and the existing legal and ethical framework is lost and found, through a theoretical and practical approach, which is reflected in the methodology section. This is done by first introducing the relevant ethical and legal framework, in order to pinpoint whether there is friction between the existing framework and the notion of BI. The terminology addressing capabilities associated with BI is not universal across countries. Therefore, an international comparison of five countries, The Netherlands and it's four main strategic partners[6], is provided. In doing so the aim is to take stock of the current practices in BI to help guide the discussion on arising dilemmas. The resulting comparative analysis of current and emerging developments regarding the ethical and legal boundaries, allows to map the direction of where BI practices are headed, and how this influences international discussions on the topic.

The international benchmark provides the basis for an international discussion on ethical and legal dilemmas of BI practices. To make this topic more tangible, four dilemmas in the context of operationalising BI are identified, pointing towards the legal or ethical framework, or the interplay between both. These dilemmas function as the basis for four corresponding tactical vignettes created in order to reflect on the issues and boundaries that come with operationalizing BI. The final part reflects on the implications and potential recommendations on how to address the identified issues underlying the dilemmas.

[6] Belgium, Germany, France, and the United Kingdom

# 2. Methodology

This paper is the result of an accumulation of desk research, individual interviews,[7] and an elaborate expert session.[8] Thereby it adopts both a theoretical and practical approach. The desk research aimed at collecting existing knowledge in the current academic and political playing field. This literature approach also forms the starting point for the ethical and legal dilemmas discussed in this paper.

The individual interviews were conducted with international military practitioners from the Netherlands, Belgium, Germany, France and the United Kingdom. The interviews took a general approach to the concept of BI. During the interviews, questions were asked regarding four main topics that touch upon these military practices. The topics discussed were: developments in the field, the ethical and legal boundaries of BI, current practices and capabilities regarding information-based BI, internal, and external cooperation. For this paper, the gathered material is used to construct the relevant scope of ethical and legal dilemmas in an international setting. The interviews served to combine and reveal a combination of theoretical and practical in country specific cases that is set apart in the international comparison section.

In preparation of the expert session, a position paper was written based on the desk research done prior. This position paper outlined four possible dilemmas that could occur due to friction between operational utility of BI and the existing ethical and/or legal framework. The contents of the position paper are further developed here. For the expert session, these dilemmas were operationalised using four practical vignettes. The expert session brought together a variety of international military and non-military experts and practitioners, ranging from academia, and military personnel to policymakers. The countries represented where the Netherlands, Belgium, and Germany. During this session, the participants discussed the four dilemmas on the basis of the vignettes. These practical vignettes were used to guide the discussion during the expert session. Both the ethical and legal aspects and considerations of these four dilemmas were explored and discussed. The aim of the workshop was not to find concrete solutions to these dilemmas, but rather to sketch the various playing fields and conceptions. These discussions also provide practical evidence to the aforementioned described theory, and thus also contributed to ethical and legal framework presented here. During the expert session two keynote speeches were given.

Prof. mr. dr. Lonneke Peperkamp of Military Ethics and Leadership at The Netherlands Defence Academy gave a keynote on the ethics of cognitive warfare and usage of information as a weapon. This keynote speech provided an ethical framework based on just war theory, which was taken as a starting point for the ideas developed in this paper. At the end of expert session, Colonel mr. dr. Peter B.M.J. Pijpers, Associate Professor of Cyber Operations at the Netherlands Defence Academy, gave a keynote on capacities and constraints of BI operations. This keynote served as the starting point for the legal framework further developed in this paper.

Before publication of this paper, further input and feedback was provided by the interviewees and participants of the workshop, contributing to the first draft of this paper. This was done to ensure a final quality assurance on the content. Responsibility for the content rests solely with the authors.

[7] These interviews take place online via Teams over the course of December 2022 and January 2023.

[8] This expert session was held in person on Thursday April 13th at the Oranjekazerne in Schaarsbergen.

# 3. Legal and ethical framework

Given recent technological advances that have influenced military operations in the information environment and thus information-based BI, the existing ethical and legal framework comes under renewed discussion.

Behavioural influencing (BI) capabilities have been used in military campaigns throughout history. A famous example is Operation Mincemeat, where British intelligence placed an in uniform dressed-up corps of a homeless man on the Spanish coast. The set-up contained (misleading) information on an upcoming allied invasion of Sardinia and Greece, which successfully resulted in German troops moving away from Sicily, which was the actual location of the invasion.[9] This case of strategic deception is just one of the many examples of the historical application of BI. However, given recent technological advances that have influenced military operations in the information environment and thus information-based BI, the existing ethical and legal framework comes under renewed discussion. More specifically, questions arise on where the ethical and legal boundaries of those frameworks lie and what dilemmas present themselves across those boundaries. This section aims to introduce the relevant ethical and legal framework, in order to pinpoint whether there is friction between the existing framework and the notion of BI. It will serve as a basis for the discussion based on dilemmas that might arise on the ethical and legal boundaries.

## Options and obstacles in the current legal framework

Currently, international law is not tailored to optimally fit to accommodate BI activities in the current technological and ICT context. International law guides the states' behaviour addressing what is in accordance with international legal norms and what is not. The problem states face is that the new (technological) context gives rise to diverging interpretations of international law. Most prominently is the discourse on how to apply the legal standard of sovereignty to cyberspace. This ambiguity on how to apply international law creates uncertainty for states in how to behave and how to respond to activities of other states. This ambiguity in international law fall within what we call the 'grey zone'. Therefore, the term 'grey zones' is not a legal term, but aims to describe those cases in which ambiguity exists due to the variances in interpretations of international law (most often related to activities in the ICT or cyberspace-context). Projected on military action, the demarcation between war and peace follows clear legal binary approach which is 'out of sync' with the fluidity of actions that take place in the grey zone. Activities in the grey zone can be defined as actions that go beyond the threshold of normal state competition but are below the threshold of conventional war.[10] NATO's model of 'the continuum of competition' lays out a spectrum of interstate interaction

[9] See: Klaus Gottlieb, 'The Mincemeat Postmortem: Forensic Aspects of World War II's Boldest Counterintelligence Operation', *Military Medicine* 174, no. 1 (2009): 93–99, https://doi.org/10.7205/MILMED-D-02-4007.

[10] Peter B.M.J. Pijpers, 'Sovereignty and Non-Intervention - The Legal Framework', in *Influence Operations in Cyberspace* (Repro FBD, 2021), 113–62; Agata Kleczkowska, 'Explaining the Meaning of "Grey Zones" in Public International Law Based on the Example of the Conflict in Ukraine', *Contemporary Central & East European Law*, no. 1 (133) (2019): 75–93, https://doi.org/10.37232/cceel.2019.07.

ranging from cooperation to armed conflict.[11] A previous HCSS report argued that "the confrontation space below the threshold of armed conflict is generally the space to which concepts like hybrid warfare and grey-zone conflict are applied."[12] Although the demarcation as to where peace ends and the grey zone starts, or where the grey zone ends and war begins is not clearly outlined, the notion 'grey zone' serves as a useful analytical term, especially for the context of BI, to which the existing legal framework cannot be applied properly.[13]

As the existing legal framework does not clearly fit either peacetime or wartime terminology, uncertainty on the applicability of a different legal framework for BI operations arises, be it laws that governs peace-time or, law that refers to wartime.

The use of terms 'peace' and 'war' as binaries, as is done in most legal approaches, falls short when it comes to BI operations in the spectrum of possibilities. Limiting analytical thinking to either war- or peacetime obstructs making legal considerations regarding these operations, which in turn leads to ethical dilemmas that arise within this uncharted grey zone. This ambiguity is witnessed more broadly in the information environment, in which BI operations take place. This paper adheres to the NATO definition of that term, which states that the information environment refers to "the virtual and physical space in which information is received, processed and conveyed".[14]

Wanless and Berk argue that using "information to influence audiences tends to fall somewhere in between the strategic and tactical, political, and military, in a grey area without boundaries, rules or inherent clarity, which hinders countering information threats."[15] Vagueness on the boundaries between war and peace is increased by the rise of concepts such as hybrid threats (in which both military and non-military instruments are adopted, often below the conventional threshold of war),[16] digital propaganda and cyber capabilities, al lot of which take place in the Information environment.[17] The ambiguity of such terms is at the basis of the legal dilemma's revolving around BI. Existing legal frameworks use clearly demarcated terminology, with different laws applying to different ends of the spectrum. As such these frameworks only cover these two ends and not cover the 'confrontation' phase of the NATO continuum. The conduct of military operations in peacetime is governed by different laws than military conduct in wartime. In general, some military actions that are not specifically covered by laws might be considered desirable from a political or operational point of view. As the existing legal framework does not clearly fit either peacetime or wartime terminology, uncertainty on the applicability of a different legal framework for BI operations arises, be it laws that governs peace-time or, law that refers to wartime. This ambiguity creates a spill over from the legal into the ethical domain, since a lack of legal grounds or terminology can cause ethical dilemmas to arise. This is further discussed in the next section.

[11] NATO, 'NATO AJP-10.1 Allied Joint Doctrine for Information Operations', January 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133515/AJP-10.1-Info_Ops_web_accessible.pdf.

[12] Markus Iven, Laura Jasper, and Michel Rademaker, 'Cognitive Effects in Combined Arms: A Case Study of Division 2025' (The Hague Centre For Strategic Studies, February 2023), p.5, https://hcss.nl/wp-content/uploads/2023/02/Cognitive-Effects-in-Combined-Arms-A-Case-Study-of-the-Division-2025-Final-2-1.pdf.

[13] Nicholas Wright, 'From Control to Influence: Cognition in the Grey Zone', July 2017, https://nsiteam.com/from-control-to-influence-cognition-in-the-grey-zone/.

[14] NATO, 'AJP-10, Allied Joint Doctrine for Strategic Communications, [Edition A Version 1]', 2022,https://www.nato.int/docu/review/articles/2018/11/16/trident-juncture-and-the-information-environment/index.html.

[15] Alice Wanless and Michael Berk, 'The Changing Nature of Propoganda', in *The World Information War*, 1st ed. (Routledge, 2021), 63–80.

[16] For more information, see: Mattia Bertolini, Raffaele Minicozzi, and Tim Sweijs, 'Ten Guidelines for Dealing with Hybrid Threats' (The Hague Centre For Strategic Studies, April 2023), https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf.

[17] Jan Almäng, 'War, Vagueness and Hybrid War', *Defence Studies* 19, no. 2 (3 April 2019): 189–204, https://doi.org/10.1080/14702436.2019.1597631; Elie Perot, 'The Blurring of War and Peace', *Survival* 61, no. 2 (4 March 2019): 101–10, https://doi.org/10.1080/00396338.2019.1589089.

One novel aspect of the existing legal grey zone around BI operations is the issue of attributing and countering operations that take place in the virtual dimension. As technological developments (e.g. social media, cyber and AI) have catalysed an adversary's ability to conduct BI operations with increased scale and reach. Additionally, operations in cyberspace generally fail to meet the threshold of armed conflict: "though cyber operations may have violent intent, most cyber activities do not reach the level of the use of force, let alone armed conflict."[18] Furthermore, non-state actors can possess similar BI capabilities which complicates the asses whether non-state actors are proxies to a state. Being unable to attribute actions to a state or link a non-state actor to a government is a practical complication feeding into the debate on where the threshold of armed conflict is located in the context of BI operations.[19] One of these technological developments can be found in the field of cyberspace, which has broadened both the actors and potential of BI operations, according to Ducheine and Pijpers. They state that "the inception of cyberspace has served as a catalyst to unlock the potential of the information environment. As a result, non-state actors, firms but also agents of the state have embraced possibilities to engage in the information environment - via cyberspace - in order to generate effects".[20]

Being unable to attribute actions to a state or link a non-state actor to a government is a practical complication feeding into the debate on where the threshold of armed conflict is located in the context of BI operations.

## Ends and means of the ethics of behavioural influencing

Information-based behavioural influencing (BI) operations can have a defensive or offensive character, and the offensive use of information as weapon is ethically most challenging suggest, as Prof. dr. mr. Lonneke Peperkamp during the expert session held in April 2023.[21] In this session, she discussed just war theory as an ethical framework to apply to BI. The following section adopts this framework, and complements it with input from the expert session, interviews and desk research.

Just war theory is a widely accepted ethical framework that governs armed conflicts. It is a tradition of thought that is rooted in Greek and Roman philosophy, has developed throughout history, and today it constitutes the moral foundation of the laws of armed conflict. This theory describes the rights and wrong of warfare. It consists of three branches, and provides norms when to go to war (Jus ad Bellum), how to conduct warfare (Jus in Bello), and how to deal with the period after the war (Jus post Bellum).[22] Taking into account the aforementioned ambiguity of the normative application for BI operations, the norms of Jus in Bello should be adhered to in the conduct of influencing operations, when BI is conducted during wartime. Regarding Jus in Bello, Just War Theory states that for ethical conduct of warfare, three core principles should be applied. First, a clear demarcation between non-combatants and combatants is made, i.e. the principle of discrimination (or distinction).[23] This principle is also

[18] Peter B.M.J. Pijpers, 'Introduction', in *Influence Operations in Cyberspace* (Repro FBD, 2021), 17–49.

[19] Eugeniusz Cieślak and Audrone Petrauskaite, 'Ethical Dimension of Military Information Operations', *Security Forum*, no. 3 (2019): 105–12, https://doi.org/10.26410/SF_1/19/8.

[20] Peter B.M.J. Pijpers and Paul A.L. Ducheine, 'Deception as the Way of Warfare' (HCSS, May 2023), https://hcss.nl/wp-content/uploads/2023/05/01-Ducheine_Pijpers_Deception-as-the-way-of-warfare.pdf.

[21] Prof. dr. mr. Lonneke Peperkamp, *Information as Weapon? The Ethics of Cognitive Warfare.*, keynote speech, 2023.

[22] Robert Williams and Dan Caldwell, 'Jus Post Bellum: Just War Theory and the Principles of Just Peace on JSTOR', *Inetrational Studies Perspectives* 7, no. 4 (November 2006): 309–20.

[23] Nils Melzer, 'Chapter 12 The Principle of Distinction Between Civilians and Combatants', in *The Oxford Handbook of International Law in Armed Conflict* (Oxford University Press, 2014), 296–331.

clearly laid out in the Geneva Convention, which states that the application of force against civilians is prohibited.[24] Secondly, Jus in Bello entails the concept of proportionality, based on a consequentialist ethical reasoning. The principle of proportionality states that the military attack cannot be excessive in relation to expected military advantage. Article 51(5) of Additional Protocol I of the 1977 Geneva Conventions indicates that proportionality prohibits any "attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".[25] The notion of proportionality bears the question whether the actions taken are in proportion to their intended goal, and if the intended positive consequences of the taken action (the military advantage) are proportional to the potential negative ones. The third principle is that of military necessity, meaning that the minimum amount of force required should be used. In other words: "The principle [of necessity] does not say that whatever is necessary is permissible, but that everything permissible must be necessary".[26] Necessity thus asks the question whether the military advantage can be achieved in any other, potentially less far-reaching manner, presuming a legitimate target.

These three core principles form the basis of an ethical approach to warfare. Using this framework, the conduct of BI operations seems justifiable at first glance. For example, in the notion of proportionality, BI operations are less lethal than conventional weapons, as they aim to influence with as result changing behaviour. However, simultaneously, difficulties in measuring BI effects make the proportionality consideration vis à vis conventional operations harder. The objectives of BI operations might not be lethal in first instance, however their spill overs as a consequence of altered behaviour might result in disproportionate effects. Furthermore, BI operations are often aimed at a broader target than kinetic operations. For example, when targeting an individual, a kinetic operation is solely aimed at that individual, whereas a BI operation might attempt to create opposition against that individual and is thus aimed at an entire group or population. Which is makes the distinction principle harder to adhere to.

Due to its specific characteristics, it is difficult to see what the application of just in bello principles means for BI. There might be a misfit between BI and the existing norms due to its unconventional nature, BI is not about the use of military kinetic force, and often involves psychological influencing of a wider group of people, not only enemy combatants. The issue of how to solve this disconnect arises. In attempting to morally assess BI operations in the context by using the existing framework, the following questions arise. Can the Just War framework translate in such a way that it can be used to shed light on the ethical boundaries of BI operations, or is this not possible? In order to answer these questions, a renewed dialogue on the ethical boundaries of BI operations is required. Because of the unconventional nature of BI, the focus on violence and the physical dimension makes the application of just war theory complicated. More subtle and longer term effects should be taken into consideration. Additionally, the binary character of just war theory is a problem here as well, its norms are applicable and specific to the extreme situation of war, not to peacetime operations. Lastly, in conducting such a dialogue, the principles of just war theory must be complemented by other norms that are important when thinking about the ethics of BI, such as existing democratic norms and values, human autonomy, and freedom of thought.

[24] UN, 'IV Geneva Convention Relative to the Protection of Civilian Persons in Time of War of 12 August 1949', 12 August 1949, https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf.

[25] ICRC, 'Protocols Additional to the Geneva Conventions of 12 August 1949', n.d., https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf.

[26] Alexander Blanchard and Mariarosaria Taddeo, 'Jus in Bello Necessity, The Requirement of Minimal Force, and Autonomous Weapons Systems', *Journal of Military Ethics* 21, no. 3–4 (2 October 2022): 286–303, https://doi.org/10.1080/15027570.2022.2157952.

# 4. International benchmark

The terminology used in addressing capabilities associated with information-based behavioural influencing (BI) is not universal across countries. Therefore, an international benchmark encompassing five countries, the Netherlands, Belgium, Germany, France, and the United Kingdom, is provided. This benchmark serves as way to ensure that the discussion regarding ethical and legal dilemmas takes place with a common understanding of the topic at hand. The international benchmark is based upon four different aspects of BI practices. Namely - developments in the field, the ethical and legal component of BI, specific methods and techniques of BI, internal, and external cooperation. Whereas the focus of this paper is the ethical and legal realm, the interviews were set up such that it provides an encompassing view of the practices associated with what we define as BI. Rather than providing a detailed overview per country on the basis of all the different aspects listed above, this benchmark puts forward three main findings that are of relevance to the discussion of ethical and legal dilemmas.

There is no common nor shared definition to frame information-driven practices that aim to influence behaviour in the military context.

The interviews that lead to this international comparison culminated in three main findings. First and foremost, that there is no common nor shared definition to frame information-driven practices that aim to influence behaviour in the military context. Influencing in a military context is not a new phenomenon, as there are examples ranging from the Gulf War, the Bosnian war, WOI, WOII, as far back as ancient Greece.[27] These capabilities are now subject to the rapid emergence of new communication and information technologies. This is creating new dimensions in both reach and depth of what is possible on the front of the information environment. These recently accelerated changes incite the emergence of new terms to describe practices that have been around for centuries. This is causing a fragmented framework of different terminology between countries on the international stage, as well as within countries between their respective levels of government and military organisation. Common definitions ought to be provided by over-arching NATO doctrines, as the shared notion within NATO is that the country-specific terminology must be compatible to those of NATO. However, every country wields their own interpretation, causing a difference between common definitions and shared understanding. There appears to be no shared understanding in the operational context, as the understanding remains limited to few subject matter experts which complicates the transferring of information within and between countries. This disconnect between common definitions and shared understanding complicates planning, training, and execution of BI capabilities. Furthermore, it culminates in differences at the structural, organisational level between countries, which in turn might complicate international cooperation, for example on the NATO-level. The lack of a shared lexicon is the main problem across and between countries when it comes to information-based influencing. An example of this is the difference between adhering to an audience-centric or a

[27] See for example: Jeffrey B. Jones and Jack N. Summe, 'Psychological Operations in Desert Shield, Desert Storm and Urban Freedom', Landpower Essay Series (The Institute of Land Warfare, August 1997), https://www.ausa.org/sites/default/files/LPE-97-3-Psychological-Operations-in-Desert-Shield-Desert-Storm-and-Urban-Freedom.pdf; Steven Collins, 'Army PSYOP in Bosnia: Capabilities and Constraints', *The US Army War College Quarterly: Parameters* 29, no. 2 (1999): 57–73, https://doi.org/10.55540/0031-1723.1928; Gottlieb, 'The Mincemeat Postmortem'; W. den Boer, 'Political Propaganda in Greek Chronology', *Historia: Zeitschrift Für Alte Geschichte* 5, no. 2 (1956): 162–77.

behaviour-centric approach. The behaviour-centric approach that was recently introduced as the fourth key tenet of NATO doctrine.[28] This corresponds with the notion that behaviour stands equal to decision-making in the military context. While on the other hand the UK-army decided to take an audience-centric approach.[29] Corresponding to the notion that one needs to understand the audience and not just their behaviour as that is only a manifestation. Differences between these two approaches can manifest in the way capabilities to influence are constructed and measure of effectiveness determined.

Main frictions in the employment of BI capabilities seem to lie in the often described 'paradoxical' discovery that influencing appears to be viewed with more scrutiny and constringent controls compared to traditional or kinetic capabilities.

The second takeaway is that the main restrictions when it comes to inter-operability and deployment of BI capabilities lies with restrictive legislature regarding data protection. More specifically, the usage of data and adherence to privacy regulations such as the GDPR (in Dutch the AVG). Similarly, this is also were there is a noticeable difference between the countries. This was again observed during the international expert session, and comes back under the second vignette dealing with privacy. An example here is the difference in how cyber capabilities are understood in relation to information-based influencing. The main difference is viewing cyber capabilities as one possible tool, or means for carrying out information-based BI, and regarding cyberspace as the only vector for causing influencing effects. This difference in how cyber and influencing capabilities relate to each other also corresponds to differences in the organisational structure of BI within the military structures. For example, whether influence capabilities solely falls under a cyber command, like in the French case, or whether the administrative structures fall solely under one command, such as with the 77th Brigade of the UK Army. This is related to the question of who owns the effects of influencing. Coming back to the main restrictions in regarding to data and privacy regulations. As the issues for most countries seem to fall under this topic, there is a difference as to what causes the problem, being either privacy or data governance concerns. While in France the restrictions are more related to the privacy regulation, the UK experiences most restrictions with the monitoring and usage of data gathered for example through social media.[30] An issue Belgium, for example, does not experience to the same extent.

The last main finding regards current main developments in terms of their promises and pitfalls. Main frictions in the employment of BI capabilities seem to lie in the often described 'paradoxical' discovery that influencing appears to be viewed with more scrutiny and constringent controls compared to traditional or kinetic capabilities. The question of defamation versus killing remains at the centre of this. Military organisations are traditionally regarded as having the mandate and duty to carry out operations associated with traditional forms of 'fighting' and disabling the enemy. This role is understood and excepted on a societal level. Once moving outside this traditional or kinetic area, such as with influencing or hybrid warfare, their actions are viewed with more scrutiny. Frictions appear to not necessarily lie with the action, used tactic, or the intended goal of an influencing operation as such, but rather the perceived control over the effect that was caused. As the impact of information-based influencing is often observed over longer stretches of time, thus creating an impact that is often more strategic rather than tactical in nature. Additionally, handling information carries the notion of having a more strategic component due to the reach to target audiences. The strategic level, however, is more broadly interpreted as being the political level.

[28] Iven, Jasper, and Rademaker, 'Cognitive Effects in Combined Arms: A Case Study of Division 2025'.

[29] Ministry of Defence, 'Joint Doctrine Note 2/19 Defence Strategic Communication: An Approach to Formulating and Executing Strategy', 3 May 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Stratrategic_Communication_jdn_2_19.pdf; Ministry of Defence, 'The Orchestration of Military Strategic Effects', January 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/970529/20210316-OMSE_new_web-O.pdf.

[30] Forces Network, 'Army "monitoring of UK Citizens" Social Media Posts' to Be Investigated, Ben Wallace Says', Forces Network, 31 January 2023, https://www.forces.net/politics/army-monitoring-uk-citizens-social-media-posts-be-investigated-ben-wallace-says.

# 5. Dilemmas in practice

The following vignettes are a snapshot of possible actions that might be taken in military operations, focussed on BI tactics. They were used in the expert session to help guide the discussions and are purely fictional and stand-alone cases. For the participants of the expert session, there were no right or wrong answers, as the goal of the vignettes was to challenge the position of the participants. The aim of the expert session was to learn from the discussions that arise regarding these dilemmas.

## Vignette 1: Norms and values & Spill-over effects

Brigade X is on a mission at the border of an eastern European country. There is a mix of state, opposition and freedom fighters. Its mission is to deter local freedom fighters that aim to destabilize the diaspora in the country, hoping to mobilize the population to stand up against the current government. Brigade X plans are being made to use behavioural influencing, to spread the rumour that interventions are planned to capture key leaders of the freedom fighters, using children distributing flyers and to encourage local population to be brave and take a stance.

The case of Brigade X provides an example of a military operation in which a consideration between existing norms and values has to be made. For example, dilemmas arise on whether it is ethical to spread rumours or to use children to convey a message. This example is indicative for a renewed discussion on norms and values in light of BI operations. The spill-over effects in the case of this vignette lie in the potential distance between the intended and the reached effect of spreading rumours amongst a population on the short, middle and long term.

Friction between norms and values is an inevitable part of all military operations. Military servicemen and women are both legally allowed to use violence and required to respond to violence, which results in far-reaching consequences of military decision making.[31] Furthermore, outcomes of dilemmatic decision-making in military operations are hardly generalisable in terms of morally right or -wrong, as every situation is unique in context,

[31] Miriam C. de Graaff, Ellen Giebels, and Desiree E. M. Verweij, 'On Moral Grounds: Moral Identity and Moral Disengagement in Relation to Military Deployment', *Military Psychology* 32, no. 4 (3 July 2020): 363–75, https://doi.org/10.1080/08995605.2020.1774321.

trade-offs and stakes. Given the dynamic and expanding nature of BI, considerations on the norms and values that are at the basis of such operations are constantly evolving and subject to change. Furthermore, the ethical considerations of more 'traditional' operations are often operation-specific and thus remain embedded in an ungeneralisable area.

The increasing complexity of contemporary military operations, combined with rapid technological developments in the information environment, enhances the need for consistency between individual and professional values on all levels of decision making. Furthermore, a renewed discussion on what actions to take when these values clash is needed. One of the aspects in which these moral considerations experience friction can be found in the hierarchical, multi-level nature of military organisations. Friction between personal and military ethics can be experienced by those that engage in operations. On the other hand, the hierarchical structure of military organisations creates the notion of 'an order is an order'. Simultaneously, there are boundaries to where this principle applies, and where personal ethics become more dominant.

The increasing complexity of contemporary military operations, combined with rapid technological developments in the information environment, enhances the need for consistency between individual and professional values on all levels of decision making.

Demarcating these boundaries is essential in eliminating ethical friction between the personal and professional level. Different parameters can be applied in making such ethical considerations. Whereas the utilitarian approach aims to create the greatest good for the greatest number of people, a deontological approach reasons that some actions are intrinsically wrong, regardless of the consequences.[32] Furthermore, the cultural and societal norms and values of the population in the area in which the operation takes place are part of this balancing process.

The dilemma that arises stems from the difficulty in applying existing norms and values, in the ways in which they can be applied to 'traditional' operations, to this specific scenario. These existing norms and values are derived from the aforementioned three core principles of Jus in Bello, the discrimination, proportionality and necessity principle.

## Distinction principle

In the vignette, the question whether a demarcation between combatants and non-combatants can be made when engaging in BI in the eastern European country is posed. After all, when performing such an operation in a military context, the target audience should in some form be labelled as 'combatants', for the operation to be legally feasible. Simultaneously however, if engaging in a 'traditional' operation, that same audience is likely considered as 'non-combatants'. This audience, i.e. the diaspora, is unarmed and not part of any of the Armed Forces participating in a conflict, ergo legally they appear to be considered non-combatants.

In general, in BI, the distinction between combatants and non-combatants cannot be made, nor is this necessary. Because BI operations are, in principle, not kinetic, they appear to fall outside of the scope of (non-)combatants' considerations of 'traditional' operations.

In the case of Brigade X, the usage of children for the distribution is a clear dilemma of where military and personal ethics can clash. From the military point of view, the usage of children in BI is not new. Children specifically were used during operations in Iraq, Afghanistan and Bosnia, to reach their parents as part of a BI operation. For example, by organizing football matches, children were befriended, so that they created a direct line of influence to their parents. Another example is Bosnia, where parents were influenced by showing that their children were able to play together, regardless of their ethnic or religious origin (be it Muslim, Bosniak or Christian).

[32] John Mizzoni, *Ethics: The Basics*, 2nd ed. (John Wiley & Sons, Incorporated, 2017).

## Proportionality

A similar dilemma deals with the proportionality of the proposed operation. At first glance, engaging in BI seems more proportional than engaging in a 'traditional', kinetic operation, as it is less lethal. However, in making the proportionality consideration for this BI operation, the possible spill overs should be taken into account too. Two main questions arise. To what extent is it possible to map out possible spill overs? Furthermore, does the (in)ability to make this assessment alter the proportionality consideration?

Measuring impact and effects is important within the process of deploying BI. Here, a distinction should be made between short and long term effects. The term spill over does not effectively reflect reality, as it implies an unforeseen and uncalculated manifestation of an operation. Rather, some operations can have effects on both the short and long term, be it intended or not. From a military point of view, the focus is on creating short term, tactical effects whereas the long term effects can be assessed but are not prioritised or desired. As the sought-after effects are often short term, and the responsibility of the Armed Forces is to create a tactical effect, making the consideration of the impact of long term effects should be a political, strategic, responsibility.

Here the comparison with economic sanctions can be made. With economic sanctions, one also tries to elicit changes in human behaviour with a certain target audience. Most of the time the target audience is not the audience that is directly affected by economic sanctions. For example, when implementing economic restrictions, usually the population of a state is affected the hardest. The specific aim however is exactly those spill over effects towards the political elite, e.g. through reinforcing domestic opposition. Here too, the long term impacts are more strategic or political in nature, and thus these considerations usually cannot be made at the tactical level.

This is particularly the case when using BI to engage in a defensive operation against adversaries attempting to influence one's own population. Whereas the Armed Forces can conduct BI to manifest short term effects, the long term impact on the domestic population should be considered by the political leadership. Therefore, for the military, the question should not be on the feasibility of making spill over considerations, but rather on when the military responsibility ends, and the political responsibility starts.

## Necessity

The notion of necessity requires a military operation to use the minimum amount of force needed to obtain the military goal. In other words, using BI is necessary when it is the only way of achieving the military objective. Here it can be argued that there are cases in which BI operations are not considered the only available option, as a kinetic operation can achieve the desired goal as well. However, one could argue that given the non-lethal effect of BI operations compared to a kinetic action, a BI operation can be considered as using the required 'minimum amount of force', and therefore meets the requirement of necessity.

In light of this consideration, the 18th century philosopher Immanuel Kant can offer some insights. Kant argues that it is never ethically justified to use a human being purely as a means to an end. He states: "So act that you use humanity, whether in your own person or in the person of any other, always at the same time as an end, never merely as a mean".[33]

[33] Immanuel Kant, 'Groundwork of the Metaphysics of Morals 4:429'.

Following Kant, deliberately using a human being as a means to achieve a military end fails to meet the necessity requirement. This is further developed by Kleingeld, who argues that in order to meet Kant's requirement, *actual consent* of the used human being is needed.[34] This is something that is lacking in BI operations, were the TA usually is unaware of them being influenced.

## Vignette 2: Privacy

Brigade X is ordered to prepare for a short mission to a western Balkan country to help stabilize the situation. The local government has agreed with the deployment. It is foreseen that national parliament of Brigade X's national Parliament decide on the matter in one month, after which deployment starts immediately. Brigade X assesses BI is required to be effective, and is collecting target audience data to make appraisals and prepare for interventions. Plans are made to start preliminary BI-interventions two weeks before deployment in the western Balkan country.

The case of Brigade X refers to the legal issues that arise when it comes to the trade-of between being able to effectively prepare a mission in advance vis à vis the harbouring of data collection rights in light of privacy.

Hempson-Jones describes the renewed demand for an ethical framework when it comes to privacy and military information campaigns.[35] Regarding the collection of information, he argue that the 'traditional' concepts of necessity and proportionality can only be applied clearly in extreme cases like terrorism or insurgencies. It is harder, however, to apply these concepts to more moderate cases. Furthermore, the demarcation between 'public' and 'private' information is not always clear, especially on social media platforms like Facebook or Twitter. They argue that the intent of the data source should be taken into account, when making the ethical consideration. Additionally, proportionality in privacy is determined by the method of data access, i.e., whether this method is intrusive or not. Lastly, they raise the question of collateral intrusion, describing the extent to which it is acceptable to infringe on the privacy of non-directly related third parties to gather data.

The concept of data-protection, being one of the aspects of privacy, can be seen as a bundle of related norms and values dealing with the prevention of harm and economic exploitation, of non-discrimination and respect for moral autonomy.[36] These are demarcated by legal concepts such as the General Data Protection Regulation (GDPR) and the European Convention on Human Rights (ECHR). As mentioned, military decision-making can involve

[34] Pauline Kleingeld, 'How to Use Someone "Merely as a Means"', *Kantian Review* 25, no. 3 (September 2020): 389–414, https://doi.org/10.1017/S1369415420000229.

[35] Justin S. Hempson-Jones, 'The Ethics of Online Military Information Activities', *Journal of Military Ethics* 17, no. 4 (2 October 2018): 211–23, https://doi.org/10.1080/15027570.2019.1586357.

[36] J. van den Hoven et al., 'FuturICT — The Road towards Ethical ICT', *The European Physical Journal Special Topics* 214, no. 1 (1 November 2012): 153–81, https://doi.org/10.1140/epjst/e2012-01691-2.

life and death scenarios in which the line between fixed norms and values on the one hand, and measures required for an effective operation on the other hand, can become blurry. Furthermore, the balance between these two concepts depends on the legal framework in which one operates, be it peace or war-time operations. This raises important questions. Can one collect, store and analyse data on a large scale in order to properly prepare for a mission deployment? Furthermore, can one apply this collected, stored and used data through specific BI activities as a 'weapon'? The dilemmatic nature of privacy and operability is partly determined by which one of these two purposes, information as 'weapon' or as 'source', is adopted. Information as a 'source' means gathering information from a source, where the source is not affected. Information as 'weapon' means the dissemination of information, with the aim to directly affect the receiver's behaviour. Note that these purposes are mutually exclusive, as information can first be used as a 'source' in preparation for an influence operation, in which information is used as a 'weapon'.

Although the ethical dilemma's regarding privacy appear to exist in the above-mentioned theories, in practice these dilemmas are considered non-existent. Participants of the expert session agree that starting preliminary BI-interventions two weeks before deployment is operationally desirable. Differences however arise when comparing the legal feasibility in different countries of such an early engagement in terms of data collection, usage, and governance. Whereas in Belgium, the military unit concerned with BI is allowed to engage in such operations without its respective intelligence agency, in the Netherlands the Dutch Implementation Act of the GDPR creates an operational obstacle. This is seen as a broader issue within the Netherlands and is not solely limited to the Armed Forces.[37]

Reaching the right audience means shaping the narrative in such a way, that the intended audience is most susceptible to the message.

## Vignette 3: Targeting audiences & Dehumanisation

> Brigade X in on a mission. An analysis shows that some target audiences and key leaders show serious vulnerabilities. They have been related to abuse and corruption as well as human trafficking. The plan is to use BI to portray the key leaders as unreliable spirits, corrupt and undermining religious beliefs of the diaspora as well as the local population.

In the case of Brigade X, one of the dilemmas that occur revolves around the Target Audience Selection (TAS). In order to make this selection, the specific characteristics and suspected effects on that audience should be properly assessed in a Target Audience Analysis (TAA).[38] Reaching the right audience means shaping the narrative in such a way, that the intended audience is most susceptible to the message. If this is not the case, and the audience is thus not susceptible, the campaign cannot be successful. Audience's specific heuristics and

[37] Algemene Rekenkamer, 'Omgang Met de AVG in Relatie Tot Uitvoering Overheidstaken', 30 March 2023, https://www.rekenkamer.nl/publicaties/kamerstukken/2023/03/30/omgang-met-de-avg-in-relatie-tot-uitvoering-overheidstaken.

[38] Steve Tatham, 'Target Audience Analysis', *The Three Swords Magazine* 28 (2015).

vulnerabilities determine the framing of the narrative. The actor deliberately adopts a narrative in which two or more topics appear to be connected. Because it appears to be true and is appealing to the audience (due to the exploitation of vulnerabilities), the audience perceives this message as true. For example, in the case of Brigade X, tapping into existing religious beliefs of the diaspora and connecting these with the frame of unreliable spirits lets the audience perceive this message as true.

Susser et al. describe two ways in which decision-making can be influenced.[39] First, one can alter the way a person understands their options, changing their perception of them. This impacts their internal decision-making process. Second, one can change the options available altogether. This impacts an audiences external decision-making space. Complementary to this, Pijpers describes three types of measures through which audiences can be influenced.[40] Persuasive measures are often overt and focus on the conscious liberation in order to influence the audience. This is similar to the Susser et al. method of changing the internal decision-making process. The targeted audience remains able to make a conscious and willing choice, but their perception of the choices is altered. Similar to Susser et al. their method of changing the decision-space, Pijpers' compelling measures often attempt to alter the audience's decision-making by limiting its options while still focussing on conscious liberation. Thus, the targeted audience remains in control, however, their options are limited unknowingly. In contrast, manipulative measures exploit the audience's cognitive shortcomings, be it biases and heuristics or lack of rationale. Pijpers describes them as follows:

> *"These subconscious techniques circumvent, subvert or even usurp the understanding and decision-making process in a way that can be harmful, confusing, or disadvantageous to the receiver, and ultimately influence targeted audiences in making quick judgements instead of deliberate appreciations and decisions"*[41]

The decision to deliberately exploit vulnerabilities of the target audience can be at friction with moral standards, as manipulative measures can limit the audience's ability to have meaningful options. In this case the manipulative operation becomes compelling.

In practice, the TAS is performed as follows. An array of preselected targets is sent up the decision-making chain, where there is a selection process at every link. Closely related to selecting the audience is the selection of the method that will be used. For BI operations to be effective, the *modus operandi* should be specifically tailored to the target audience, according to Pijpers.[42] Various influence tactics and methods are identified, each of which can be more effective depending on the selected target audience.[43]

[39] Daniel Susser, Beate Roessler, and Helen F. Nissenbaum, 'Online Manipulation: Hidden Influences in a Digital World', *SSRN Electronic Journal*, 2018, https://doi.org/10.2139/ssrn.3306006.

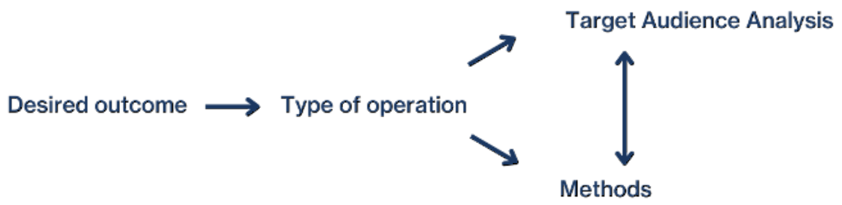
[40] Peter B.M.J. Pijpers, 'Influence Operations - The Concept', in *Influence Operations in Cyberspace* (Repro FBD, 2021), 51–112.

[41] Pijpers. p. 82

[42] Peter B.M.J. Pijpers, 'Influence Operations - The Concept', in *Influence Operations in Cyberspace* (Repro FBD, 2021), 51–112.

[43] For an overview of behavioural influencing capabilities please consult: Lotje Boswinkel et al., 'Weapons of Mass Influence: Shaping Attitudes, Perceptions and Behaviours in Today's Information Warfare' (The Hague: The Hague Centre for Strategic Studies, April 2022), https://hcss.nl/wp-content/uploads/2022/04/Weapons-of-Mass-Influence-Information-Warfare-HCSS-2022-V2.pdf.

## Figure 1. BI operations decision cycle



The following decision cycle can be identified for BI operations. Ethically, any operation should follow this cycle, where an ethical consideration is made per node.

An ethically justified TAA should start with a clear demarcation of the desired outcome. If the desired outcome is unclear or not defined, any BI operation is considered unethical. A clearly defined desired effect functions as a guideline for the ethical considerations performed in the rest of the cycle. In the case of Brigade X, the desired outcome can be described as the elimination of the key leaders. Deciding on the means necessary to achieve this outcome is part of the next part of the cycle.

In choosing the type of operation, one can decide on engaging in BI, in contrast to 'traditional', kinetic operations. For both, and other options an ethical trade-off should be made, including an assessment of potentials spill over effects.

An interplay exists between TAS, and deciding on the method that will be used. As mentioned, Pijpers describes how the success rating of a method is audience specific, thus the selection analysis is two-folded.[44] Operationally, choosing the smallest possible audience is preferred, as this limits spill over as much as possible. Simultaneously, choosing a broader target audience leaves more options and flexibility. In general, the ethical consideration takes place most predominantly when selecting the method. After all, every target audience can be considered an ethically justified target as long as the used method falls within an ethical framework. However, as the two are intertwined, both the TAS and method selection is subject to ethical considerations.

## Dehumanisation

Within this whole cycle, the notion of dehumanisation plays a role as well. Dehumanisation entails the concept of individuals adopting their own personal moral identity, which helps them deal with moral dilemmas. However, one's actions are not always in line with one's moral identity, which creates friction. In order to deal with this friction, individuals engage in moral disengagement, to help them justify their actions:

> "*This implies a psychological mechanism that permits an individual to selectively, either deliberately or unconsciously, reframe one's own actions and to dissociate from them in order to isolate those actions from one's personal standards of what is morally acceptable" (p. 365).*[45]

[44] Pijpers.

[45] Miriam C. de Graaff, Ellen Giebels, and Desiree E. M. Verweij, 'On Moral Grounds: Moral Identity and Moral Disengagement in Relation to Military Deployment', *Military Psychology* 32, no. 4 (3 July 2020): 363–75, https://doi.org/10.1080/08995605.2020.1774321.

Bandura identifies four ways in which an actor performs moral disengagement, generally applicable to military operations.[46] One could alter the reconstruction of one's own behaviour, role, or the consequences that result from them. Furthermore, one could dehumanize the victims, as a method to downplay the consequences of one's actions. Stripping a victim of human attributions makes it easier to justify immoral or inhumane behaviour towards that victim. Especially in the second node of the cycle, when deciding on the type of operation, this plays a role.

In general, there appears to be more public resistance against 'character assassination' than against a kinetic assassination. In making this consideration, the (expected) public opinion can be used as a guideline. Furthermore, character assassination or another form of dehumanisation can lead to more, uncontrollable spill overs. For example, negatively displaying individuals might result in unforeseen aggression against that person. All this (potential) spill overs should be taken into account as much as possible.

Next to being audience- and method specific, the ethical boundaries of BI are also operation specific. As every operation is unique in its context, generalising ethical frameworks is considered a difficult endeavour. One of the guidelines of setting a more general ethical framework can be found in the notion of 'domestic public support'. In general, if an operation (in a foreign country) is accepted by the domestic public, it can be considered ethical. If, after internal ethical consideration, an operation is performed but faces heavy domestic criticism, the ethical justifiability should be questioned.

In general, there appears to be more public resistance against 'character assassination' than against a kinetic assassination.

## Vignette 4: Grey zone

Kosovo Force (KFOR) Unit X are deployed to Kosovo, on invitation, for stabilising the situation and training of local troops. Tensions are on the rise because the opposition and 'little green men' (supposedly from Russia) are spotted spreading rumours actively hampering Unit X's effective operations and creating unstable, unsecure and unsafe situations. Plans are made to actively influence the opposition troops and the neighbouring country population to counter the influencing. The question is: how far could KFOR go?

The case of KFOR is a clear example of the dilemma sketched in the beginning of this paper regarding the binary approach to war- and peacetime. 'Little green men' that operate somewhere below the conventional threshold of war have to be countered, but ambiguity arises on the extent to which KFOR engages. Whereas in the physical domain, the demarcation between peace and war is rather clear, this distinction is harder to apply in the (often more virtual) information and cyber domain. This brings along a plethora of legal and ethical considerations,

[46] Albert Bandura, 'Moral Disengagement in the Perpetration of Inhumanities', *Personality and Social Psychology Review* 3, no. 3 (1 August 1999): 193–209, https://doi.org/10.1207/s15327957pspr03033.

complicated by the novel nature of the virtual dimension. With cyber and BI operations increasing in intensity over the last decades due to technological developments and subsequently enhanced capabilities, the demand to adjust legal and ethical frameworks is intensifying. Calls to renew this ethical and legal framework are amplified by the fact that technological developments have become drivers for BI operations. Currently, one of the issues of countering BI operations that take place in the virtual dimension lies in their attribution, as technological development (e.g. social media) has enabled adversaries to overtly conduct these BI operations with increased scale and reach. Furthermore, non-state actors can possess similar BI capabilities or be operating under the gaze of states. Being unable to link the actions of non-state groups with states complicates the debate on what constitutes an act of war in BI operations.[47]

One of the dilemmas associated with the case of Brigade X revolves around the threshold of war in BI. Can the spreading of rumours by 'little green man' be considered an act of war? If so, what kind of response does this warrant? After all, acts below the threshold of war require a different response than those that constitute acts of war. Currently, the law does not apply to this grey area, complicating the friction between legality and effectiveness. Although strictly operating within existing legal frameworks enhances transparency and legitimacy, it can obstruct the effectiveness of operations. Thus, the legal framework should be adapted, to limit the 'grey zone' and provide legal clarity, a notion shared by Ducheine et al.[48] They argue that the existing legal framework insufficiently supports the armed forces and should be altered, to provide the armed forces with the legal foundation to effectively perform BI operations.

One of the aspects of existing conceptions on warfare revolve around the use of 'weapons'. In 'traditional' notions of warfare, weapons could solely be considered kinetic. Nowadays however, the notion of weapons does no longer apply to novel aspects of warfare, be it BI or cyber. Furthermore, the binary notion of either wartime or peacetime can also no longer be applied to the context of BI, given its below-the-threshold options. Thus, one should step away from the traditional binary notion of warfare by weapons, and rather develop a framework of different types of warfare, in which BI is included as well. Different types of warfare require and warrant different, tailored, types of reactions.

Drafting new guidelines on how international law, including the threshold for warfare, can be applied to the context of BI is not impossible. For the domain of cyberspace, this has been done in the form of the Tallinn manual,[49] which lays out the applicability of existing international law on cyber warfare. In practice however, such a manual for BI is currently not developed.

It can also be argued that a new manual is redundant, as the existing core principles of international law offer enough guidance in finding an answer to the question of where the threshold of war is positioned in BI. These core principles are the notion of sovereignty and non-intervention, consisting of two, equally important, aspects. Sovereignty refers to both territorial integrity and political independence. Whereas the first aspect is harder to apply to the context of BI, given e.g. the virtual aspects of it, the latter principle is still very much applicable. Thus,

[47] Eugeniusz Cieślak and Audrone Petrauskaite, 'Ethical Dimension of Military Information Operations', *Security Forum*, no. 3 (2019): 105–12, https://doi.org/10.26410/SF_1/19/8.

[48] P.A.L. Ducheine, Peter Pijpers, and Eric Pouw, 'Information Manoeuvre and the Netherlands Armed Forces: Legal Challenges Ahead', *SSRN Electronic Journal*, 2022, https://doi.org/10.2139/ssrn.4113046.

[49] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017). The Tallinn Manual process is an initiative by an Independent Group of Experts on the discourse of how international law governs cyberspace. The manual is not the legal opinion of states and is therefore not a legal document. See e.g. https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

following this reasoning, interference or infringement of the political affairs through BI can constitute an act of war.

Simultaneously, the question on the necessity of charting this existing grey zone is raised. It can be argued that the proposed dilemma is non-existent, as instead of viewing this grey zone as a liability, its simple existence is actually a necessity for BI operations. These operations take place between on the one hand a need for maximum operational effectiveness, and on the other hand a rigid legal framework. After all, operating within the law is part of the norms and values Western countries hold dear. It also ensures legitimacy and accountability towards a domestic population. The core tenet behind this approach is the interpretation of legislation. Countries that maintain a 'positive' interpretation (i.e. if it something is not in the law, it is not prohibited) can use this approach. The fact that legislation is missing, i.e. why the grey zone exists, helps in justifying operations while maintaining legality. Belgium is a country in which such an approach is adopted. On the contrary, in countries that maintain a 'negative' interpretation (i.e. if something is not in the law, it is not allowed) cannot adopt such an approach, as operating within the grey zone is considered illegal. The Netherlands is a country with a proclivity towards the 'negative' approach to legislation around BI.

# Main findings

The intent of this research was not to provide answers or solutions to existing ethical or legal dilemmas when it comes to BI but rather to facilitate the discussion on this topic and to highlight when, where, and why these dilemmas may occur. Therefore, the paper ends with two main findings, rather than conclusions.

1. The lack of legal framework, more specifically the fact that the grey zone is insufficiently governed by international law, causes the occurrence of ethical dilemmas. Accordingly, when operating outside of the 'legal' grey zone, few ethical dilemmas occur when operating in accordance to the three core principles – distinction, proportionality, and necessity. The ethical dilemmas that do occur appear to not be fundamentally new ones compared to cases in existing international and non-formal frameworks.

2. The question of data collection and governance appears to be the main recurring dilemma. This related to the legal feasibility of carrying out data collection, analysis, and governance in preparation of an intervention. Coming back to the aforementioned questions; Can one collect, store and analyse data on a large scale in order to prepare for mission deployment, i.e. using information as a 'source'? Can one apply this collected, stored and used data through specific BI activities as a 'weapon'? In the specific context of the Netherlands this comes down to the AVG and UAVG. The finding here is that by revoking certain exemptions in the AVG specifically made for the operational (defence and security) context, thus opting not to apply provisions for exceptions, one paints oneself into a difficult corner when it comes to the applicability and utility of information-based BI operations. The Dutch Implementation Act of the AVG thus creates an operational obstacle. This is seen as a broader issue within the Netherlands and is not solely limited to the Armed Forces.

# References

Algemene Rekenkamer. 'Omgang Met de AVG in Relatie Tot Uitvoering Overheidstaken', 30 March 2023. https://www.rekenkamer.nl/publicaties/kamerstukken/2023/03/30/omgang-met-de-avg-in-relatie-tot-uitvoering-overheidstaken.

Almäng, Jan. 'War, Vagueness and Hybrid War'. *Defence Studies* 19, no. 2 (3 April 2019): 189–204. https://doi.org/10.1080/14702436.2019.1597631.

Autoriteit Persoonsgegevens. 'Algemene Verordening Gegevensbescherming (AVG)', 17 April 2016. https://autoriteitpersoonsgegevens.nl/uploads/imported/verordening_2016_-_679_definitief.pdf.

Bandura, Albert. 'Moral Disengagement in the Perpetration of Inhumanities'. *Personality and Social Psychology Review* 3, no. 3 (1 August 1999): 193–209. https://doi.org/10.1207/s15327957pspr0303_3.

Bertolini, Mattia, Raffaele Minicozzi, and Tim Sweijs. 'Ten Guidelines for Dealing with Hybrid Threats'. The Hague Centre For Strategic Studies, April 2023. https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf.

Blanchard, Alexander, and Mariarosaria Taddeo. 'Jus in Bello Necessity, The Requirement of Minimal Force, and Autonomous Weapons Systems'. *Journal of Military Ethics* 21, no. 3–4 (2 October 2022): 286–303. https://doi.org/10.1080/15027570.2022.2157952.

Boer, W. den. 'Political Propaganda in Greek Chronology'. *Historia: Zeitschrift Für Alte Geschichte* 5, no. 2 (1956): 162–77.

Boswinkel, Lotje, Neill Bo Finlayson, John Michaelis, and Michel Rademaker. 'Weapons of Mass Influence: Shaping Attitudes, Perceptions and Behaviours in Today's Information Warfare'. The Hague: The Hague Centre for Strategic Studies, April 2022. https://hcss.nl/wp-content/uploads/2022/04/Weapons-of-Mass-Influence-Information-Warfare-HCSS-2022-V2.pdf.

Cieślak, Eugeniusz, and Audrone Petrauskaite. 'Ethical Dimension of Military Information Operations'. *Security Forum*, no. 3 (2019): 105–12. https://doi.org/10.26410/SF_1/19/8.

Collins, Steven. 'Army PSYOP in Bosnia: Capabilities and Constraints'. *The US Army War College Quarterly: Parameters* 29, no. 2 (1999): 57–73. https://doi.org/10.55540/0031-1723.1928.

Ducheine, P.A.L., Peter Pijpers, and Eric Pouw. 'Information Manoeuvre and the Netherlands Armed Forces: Legal Challenges Ahead'. *SSRN Electronic Journal*, 2022. https://doi.org/10.2139/ssrn.4113046.

Forces Network. 'Army "monitoring of UK Citizens" Social Media Posts' to Be Investigated, Ben Wallace Says'. Forces Network, 31 January 2023. https://www.forces.net/politics/army-monitoring-uk-citizens-social-media-posts-be-investigated-ben-wallace-says.

Gottlieb, Klaus. 'The Mincemeat Postmortem: Forensic Aspects of World War II's Boldest Counterintelligence Operation'. *Military Medicine* 174, no. 1 (2009): 93–99. https://doi.org/10.7205/MILMED-D-02-4007.

Graaff, Miriam C. de, Ellen Giebels, and Desiree E. M. Verweij. 'On Moral Grounds: Moral Identity and Moral Disengagement in Relation to Military Deployment'. *Military Psychology* 32, no. 4 (3 July 2020): 363–75. https://doi.org/10.1080/08995605.2020.1774321.

Hempson-Jones, Justin S. 'The Ethics of Online Military Information Activities'. *Journal of Military Ethics* 17, no. 4 (2 October 2018): 211–23. https://doi.org/10.1080/15027570.2019.1586357.

Hoven, J. van den, D. Helbing, D. Pedreschi, J. Domingo-Ferrer, F. Gianotti, and M. Christen. 'FuturICT — The Road towards Ethical ICT'. *The European Physical Journal Special Topics* 214, no. 1 (1 November 2012): 153–81. https://doi.org/10.1140/epjst/e2012-01691-2.

ICRC. 'Protocols Additional to the Geneva Conventions of 12 August 1949', n.d. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf.

International Committee of the Red Cross. 'Definition of Combatants - IHL'. Accessed 3 May 2023. https://ihl-databases.icrc.org/en/customary-ihl/v1/rule3.

Iven, Markus, Laura Jasper, and Michel Rademaker. 'Cognitive Effects in Combined Arms: A Case Study of Division 2025'. The Hague Centre For Strategic Studies, February 2023. https://hcss.nl/wp-content/uploads/2023/02/Cognitive-Effects-in-Combined-Arms-A-Case-Study-of-the-Division-2025-Final-2-1.pdf.

Jones, Jeffrey B., and Jack N. Summe. 'Psychological Operations in Desert Shield, Desert Storm and Urban Freedom'. Landpower Essay Series. The Institute of Land Warfare, August 1997. https://www.ausa.org/sites/default/files/LPE-97-3-Psychological-Operations-in-Desert-Shield-Desert-Storm-and-Urban-Freedom.pdf.

Kant, Immanuel. 'Groundwork of the Metaphysics of Morals 4:429', n.d.

Kleczkowska, Agata. 'Explaining the Meaning of "Grey Zones" in Public International Law Based on the Example of the Conflict in Ukraine'. *Contemporary Central & East European Law*, no. 1 (133) (2019): 75–93. https://doi.org/10.37232/cceel.2019.07.

Kleingeld, Pauline. 'How to Use Someone "Merely as a Means"'. *Kantian Review* 25, no. 3 (September 2020): 389–414. https://doi.org/10.1017/S1369415420000229.

Koninklijke Landmacht. 'Doctrine Publicatie 3.2 - Landoperaties', 11 February 2014. https://www.defensie.nl/binaries/defensie/documenten/publicaties/2014/02/11/militaire-doctrine-voor-het-landoptreden/DP+3.2.pdf.

Kooman, Ingmar. 'Geen daden maar woorden - 08 - Landmacht'. Webpagina, January 2015. https://magazines.defensie.nl/landmacht/2015/01/psyops-geen-daden-maar-woorden.

Melzer, Nils. 'Chapter 12 The Principle of Distinction Between Civilians and Combatants'. In *The Oxford Handbook of International Law in Armed Conflict*, 296–331. Oxford University Press, 2014.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 'Uitvoeringswet Algemene verordening gegevensbescherming'. Wet, 2021. https://wetten.overheid.nl/BWBR0040940/2021-07-01.

Ministry of Defence. 'Defence Vision 2035 Fighting for a Safer Future', 5 October 2020. https://english.defensie.nl/downloads/publications/2020/10/15/defence-vision-2035.

———. 'Joint Doctrine Note 2/19 Defence Strategic Communication: An Approach to Formulating and Executing Strategy', 3 May 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804319/20190523-dcdc_doctrine_uk_Defence_Stratrategic_Communication_jdn_2_19.pdf.

———. 'The Orchestration of Military Strategic Effects', January 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/970529/20210316-OMSE_new_web-O.pdf.

Mizzoni, John. *Ethics: The Basics*. 2nd ed. John Wiley & Sons, Incorporated, 2017.

NATO. 'NATO AJP-10.1 Allied Joint Doctrine for Information Operations', January 2023. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133515/AJP-10.1-Info_Ops_web_accessible.pdf.

———. 'AJP-10, NATO Allied Joint Doctrine for Strategic Communications [Edition A Version 1]', 2022

Peperkamp, Prof. dr. mr. Lonneke. *Information as Weapon? The Ethics of Cognitive Warfare.* Key note speech, 2023.

Perot, Elie. 'The Blurring of War and Peace'. *Survival* 61, no. 2 (4 March 2019): 101–10. https://doi.org/10.1080/00396338.2019.1589089.

Pijpers, Peter B.M.J. 'Influence Operations - The Concept'. In *Influence Operations in Cyberspace*, 51–112. Repro FBD, 2021.

———. 'Introduction'. In *Influence Operations in Cyberspace*, 17–49. Repro FBD, 2021.

———. 'Sovereignty and Non-Intervention - The Legal Framework'. In *Influence Operations in Cyberspace*, 113–62. Repro FBD, 2021.

Pijpers, Peter B.M.J., and Paul A.L. Ducheine. 'Deception as the Way of Warfare'. HCSS, May 2023. https://hcss.nl/wp-content/uploads/2023/05/01-Ducheine_Pijpers_Deception-as-the-way-of-warfare.pdf.

Rosenberg, Esther, and Karel Berkhout. 'Een Soft Maar Gevaarlijk Wapen: Moderne Oorlogsvoering Richt Zich Op Beïnvloeding van de Bevolking'. *NRC*, 26 June 2020.

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

Susser, Daniel, Beate Roessler, and Helen F. Nissenbaum. 'Online Manipulation: Hidden Influences in a Digital World'. *SSRN Electronic Journal*, 2018. https://doi.org/10.2139/ssrn.3306006.

Tatham, Steve. 'Target Audience Analysis'. *The Three Swords Magazine* 28 (2015).

UK Army. 'Force Troops Command Handbook', n.d. https://www.army.mod.uk/umbraco/Surface/Download/Get/10550.

UN. 'IV Geneva Convention Relative to the Protection of Civilian Persons in Time of War of 12 August 1949', 12 August 1949. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf.

Wanless, Alice, and Michael Berk. 'The Changing Nature of Propoganda'. In *The World Information War*, 1st ed., 63–80. Routledge, 2021.

Williams, Robert, and Dan Caldwell. 'Jus Post Bellum: Just War Theory and the Principles of Just Peace on JSTOR'. *Inetrational Studies Perspectives* 7, no. 4 (November 2006): 309–20.

Wright, Nicholas. 'From Control to Influence: Cognition in the Grey Zone', July 2017. https://nsiteam.com/from-control-to-influence-cognition-in-the-grey-zone/.

The Hague Centre
for Strategic Studies

**HCSS**
Lange Voorhout 1
2514 EA The Hague

**Follow us on social media:**
@hcssnl

**The Hague Centre for Strategic Studies**
Email: info@hcss.nl
Website: www.hcss.nl