The Hague Centre
for Strategic Studies

The concept of Information Manoeuvre

Winning the Battle of Perceptions

Judith T. van de Kuijt (TNO), Naomi Keja (TNO) and Jacoline C. Slaager (TNO)

May 2023

The Hague Centre
for Strategic Studies

Paper 3

The concept of Information Manoeuvre

Winning the Battle of Perceptions

Authors:
Judith T. van de Kuijt (TNO), Naomi Keja (TNO) and
Jacoline C. Slaager (TNO)

This paper is part of the *Information-based behavioural influencing and Western practice* paper series.

May 2023

This paper is published 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 in the military context. We bring together international experts and practitioners from both military and academic backgrounds to explore the military-strategic, ethical, legal, and societal 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.

Paper series: Information-based behavioural influencing and Western practice

The military application 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. These tactics are placed under the banner of influencing human behaviour. Behavioural influencing is the act of meaningfully trying to affect the behaviour of an individual by targeting people's knowledge, beliefs and emotions. Within the Dutch armed forces these tactics fall under title of Information Manoeuvre. With the ever-larger and more evasive employment of information-based capabilities to target human cognition, the boundaries of the physical and cognitive battlefield have begun to fade.

This paper is published 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 in the military context. We bring together international experts and practitioners from both military and academic backgrounds to explore the military-strategic, ethical, legal, and societal 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.

For this paper series scholars, experts and policymakers submitted their papers on the employment of information-related capabilities to influence human behaviour in the military context. From the perspective of an individual European or NATO country's perspective. The Information-based behavioural influencing and Western practice paper series is edited by Arthur Laudrain, Laura Jasper and Michel Rademaker.

Seven papers will be published in this series. These are the following:

- **Deception as the Way of Warfare. Armed Forces, Influence Operations and the Cyberspace paradox.** By Colonel dr. Peter B.M.J. Pijpers, Netherlands Defence Academy and University if Amsterdam, and Brigadier-General prof. dr. Paul A.L. Ducheine, Netherlands Defence Academy and University of Amsterdam
- **Influencing security professionals: are they biased and by which source?** By Johan de Wit, TU Delft & Siemens Smart Infrastructure
- **A discursive analytical approach to understanding target audiences. How NATO can improve its actor-centric analysis.** By Yannick Smits, Research Master Middle Eastern studies Leiden University
- **The concept of Information Manoeuvre: Winning the Battle of Perceptions.** By Judith T. van de Kuijt (TNO), N. Keja (TNO), J.C. Slaager (TNO)
- **Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare.** By Pontus Winther, LL.D. Swedish Armed Forces, and Per-Erik Nilsson, Ph.D. Swedish Defence Research Agency and Associate Professor at Uppsala University
- **Cognitive Warfare as Part of Society: Never-Ending Battle for Minds.** By Robin Burda, Ph.D. candidate Security and Strategic Studies Masaryk University
- **Behavioural Influence Interventions in the Information Environment: Underlying Mechanisms and Technologies.** By dr. Hans Korteling (TNO), Beatrice Cadet (TNO), Tineke Hof (TNO)

1. Introduction

Information has always been critical to the battlefield. Today, however, developments such as globalization and digitalization have led to increased data volume and velocity. Furthermore, it has led to a growing uncertainty on the credibility of information, as social media enables literally everyone to send his or her message unfiltered to large audiences within seconds by using social media. This uncertainty is aggravated by the disruptive possibilities of new information technology, such as deep-fakes. The result is an ever-growing importance of timely and accurate information gathering and dissemination during conflicts.

With this changing nature of the current (and future) operating environment, the Royal Netherlands Army is now called upon to strengthen its information position and ways of handling information in order to cope with the major changes and challenges in the information environment. A new operational concept is therefore necessary, allowing the Royal Netherlands Army to make better use of information as enabler, means and weapon.

A proper implementation of Information Manoeuvre should ensure a future-proof Royal Netherlands Army that is successful in future conflicts.

Information Manoeuvre is such a concept, and it has become increasingly central to many discussions within the military realm. The concept focuses on the use of military information capabilities to influence the behaviour of audiences through generating effects in the operating environment. According to Dutch policy documents,[1] a proper implementation of Information Manoeuvre should ensure a future-proof Royal Netherlands Army that is successful in future conflicts.

However, as of early 2023, debate is still on-going about what the concept of Information Manoeuvre exactly comprises. What is the essence of the concept and what elements does it consist of? What type of activities deliver Information Manoeuvre? What does it mean when information is used as a military tool? Subsequently, what does Information Manoeuvre exactly entail when the concept is operationalized in a military context? What is the role of intelligence within Information Manoeuvre? In brief, many questions arise about Information Manoeuvre in the operating environment, leaving room for applied research to start investigating its characteristics and its span. In this paper, the authors explore four fundamental elements of Information Manoeuvre and identify three dilemmas concerning its scope and conceptual considerations.

2. An overview of Information Manoeuvre

This paragraph introduces different perspectives and interpretations of Information Manoeuvre that exist in current literature, national doctrines and debates. While acknowledging that legal aspects are important when conceptualizing Information Manoeuvre, it is outside the scope of this paper.

1 Ministry of Defence [MOD] of the Netherlands [NL] (2020). *Defence Vision 2035: Fighting for a safer future* [Translated from: Defensievisie 2035: Vechten voor een veilige toekomst]. The Hague, NL: Ministry of Defence. Accessed on February 23, 2023, via: https://www.defensie.nl/onderwerpen/defensievisie-2035/downloads/publicaties/2020/10/15/defensievisie-2035.

Different doctrinal and conceptual perspectives

Information Manoeuvre is a relatively new addition to the already congested conceptual space of activities that focus on behavioural influencing and performing information activities. The level of maturity and implementation of these concepts differ between militaries from country to country.

Multi-Domain Operations, the Behavioural-centric approach, *Informatiegestuurd Optreden* and Information Manoeuvre are concepts that have been used and explored by the Royal Netherlands Army in recent years. They all refer to the use of information for the purpose of military action. However, the interpretation of what these terms mean varies greatly, and some argue that they overlap. In this paper, the authors focus on elaborating the concept of Information Manoeuvre.

Describing the added value of Information Manoeuvre to the military as an organisation is challenging.

Seen from an international perspective, no standard terminology for the concept of using information as a military tool to create effects has been defined yet or has been widely accepted by NATO member states. Similarly to the Netherlands, the UK refers to this concept as Information Manoeuvre. According to the UK, Information Manoeuvre integrates information capabilities to gain or maintain a position of information advantage to support integrated action.[2] The US military refers to information as a form of manoeuvre, however, it thereby still uses the NATO concept of Information Operations (Info Ops). Their Armed Forces' doctrine refers to information as the seventh joint function of the military.[3] France, on the other hand, has given its own twist to it and talks about *Lutte Informatique d'influence* which roughly translates to an IT fight of influence.[4] Finally, the German Army views the information concept as part of their cyber operations.[5] Within NATO, there is no established doctrine/definition of Information Manoeuvre yet. Therefore, it can be argued that there are still many different doctrinal and conceptual perspectives on Information Manoeuvre.

At the intersection of different fields

Describing the added value of Information Manoeuvre to the military as an organisation is challenging. The doctrinal embedding in both NATO and Dutch doctrine of Information Operations as well as the Manoeuvrist approach already exists,[6] whilst this is not yet the case for the concept of Information Manoeuvre. However, according to some existing literature on the topic, the added value of Information Manoeuvre can be seen from the perspective of cross-synergy. Information Manoeuvre can be interpreted as an overarching concept exploiting synergy existing between different capabilities such as Command, Control, Communications, Computers & Information (C4I), CEMA, Communication and Engagement (including PsyOps, StratCom and Info Ops), Data Science and Artificial Intelligence Robotics (DSAIR), and Intelligence. It is the coordination and synchronization of different ways of transmitting information and countering the adversary's information means that turns military

2 HQ Land Warfare Centre [LWC] of the UK (2023). *Doctrine Note 23/02: Information Manoeuvre.* Warminster, UK: LWC UK.

3 Joint Staff (2017). *Joint publication 1: Doctrine for the Armed Forces of the United States.* Accessed March 6, 2023, via: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

4 Ministère des Armées (2021). *Éléments publics de doctrine militaire de lute informatique d'influence (L21).* Paris, FR: Ministère des Armées. Accessed on March 7, 2023, via: https://www.defense.gouv.fr/sites/default/files/ema/doctrine_de_lutte_informatique_dinfluence_l2i.pdf.

5 Bundeswehr (2019). *Bearbeitung der Lage im Informationsumfeld.* Mayen, DE: Zentrum Operative Kommunikation der Bundeswehr.

6 NATO (2009). AJP-3.10: Allied Doctrine for Joint Information Operations. Brussels, BE: NATO. Accessed on February 22, 2023, via: https://info.publicintelligence.net/NATO-IO.pdf.

action into Information Manoeuvre.[7] Conceptually, Information Manoeuvre is about creating multiple dilemmas for the adversary which requires the combination of different capabilities. The strength of each capability is brought to the fore, so as to expose an adversary's weakness to another armed forces.[8] As an example, during the recent Russo-Ukraine war, Ukraine combines different information tactics. These include intercepting Russian calls to geolocate phones and target key figures, spreading narratives such as the Snake Island heroes and the Ghost of Kyiv,[9] managing tactical intelligence, and using social media.

With regard to the different perspectives that exist on Information Manoeuvre, it can be concluded that it is yet too early to establish a definition that is supported by all NATO members. Additionally, the way how Information Manoeuvre is interpreted is highly determined by a country's cultural and historical context. In this paper, the authors therefore continue to investigate what Information Manoeuvre entails for the Royal Netherlands Army. It starts with presenting four fundamental elements that underly the concept itself. These fundamental elements were identified based on conversations with representatives from the Royal Netherlands Army and represent the common ground that was found in the different visions that are present. By getting to the core of what Information Manoeuvre means in the operational context, this paper hopes to provide direction for necessary doctrine development in the future.

The essence of Information Manoeuvre is generating effects to, for example, shape audiences' attitudes, perceptions, and behaviour, maintain relationships of trust and confidence or mislead and/or persuade the adversary.

3. Information Manoeuvre: four fundamental elements

In order to understand the concept of Information Manoeuvre, it is necessary to operationalize this new manner of exerting power. This chapter examines four elements that characterize Information Manoeuvre according to the authors: its purpose, its actions, its character, and its contribution to a military strategy.

The purpose of Information Manoeuvre is to influence behaviour

Although not specific for Information Manoeuvre but according to the authors a vital element, the purpose of Information Manoeuvre is to achieve a competitive advantage relative to others and to achieve effects in the effects dimensions in order to accomplish the mission at hand.[10,11] When an information advantage is secured, information can be used to influence an audiences' behaviour. From this perspective, the essence of Information Manoeuvre is generating effects to, for example, shape audiences' attitudes, perceptions, and behaviour, maintain relationships of trust and confidence or mislead and/or persuade the adversary. In this way,

7 Elder, R.J., & D. Engr (2021). Information Maneuver in Military Operations. *Strategic Multilayer Assessment.* Accessed on February 24, 2023, via: https://nsiteam.com/social/wp-content/uploads/2021/08/IIJO-Invited-Perspective_Info-Maneuver-in-Mil-Ops_FINAL-2.pdf.

8 Elder, R.J., & D. Engr (2021).

9 Romansky, S., L. Boswinkel & M. Rademaker (2022). *The parallel front: An analysis of the military use of information in the first seven months of war in Ukraine*. The Hague, NL: The Hague Centre for Strategic Studies [HCSS].

10 CLAS (2020). *Vision Information-Driven Operations for Land Forces: Maneuvering in the Information Environment* [Translated from: Visie Informatiegestuurd Optreden voor de Landmacht: Manoeuvreren in de Informatieomgeving]. Utrecht, NL: CLAS.

11 Pijpers, P.B.M.J., & P.A.L. Ducheine (2021). "If You Have a Hammer...": Reshaping the Armed Forces' Discourse on Information Maneuver. *Amsterdam Law School Legal Studies Research Paper No. 2021-34 / Amsterdam Center for International Law No. 2021-12.* Accessed February 24, 2023, via: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3954218.

information can be seen as a distinct instrument of power which can affect the understanding and decision-making process of an audience rather than being an underpinning element only.[12,13] In order to explain the concept of Information Manoeuvre, it is important to acknowledge that information is not merely used to understand the operational environment alike intelligence – whereby information functions as enabler - but also as a means to act (information as weapon). Thus, Information Manoeuvre is the use of information as a weapon to influence audiences' attitudes and perceptions and change or maintain their behaviours.

Based on a good understanding (i.e. insight and foresight) of the situation, decisions can be made on how to act in the information environment. The information environment is, besides the physical and human environment, a sub-environment of the operating environment. By matching these actions with information capabilities that generate effects in the operating environment, the audiences' behaviour can be influenced.

The action should take place in the information environment

Many different interpretations exist internationally (including NATO doctrine) concerning the concept of environments, dimensions and domains. For the purpose of this paper the authors used their own interpretation of how Information Manoeuvre relates to the environments and dimensions.

To classify an action as a contribution to Information Manoeuvre, the action must take place in the information environment. The information environment "encompasses all forms of storage and transmission of analogue and digital data and information. It includes information security, and all supporting communication and information systems and processes".[14]

The information environment is part of the operating environment and consists of three interrelated dimensions where effects are sorted: physical, virtual and cognitive. In the case of Information Manoeuvre physical and virtual activities are conducted in the information environment. According to the authors, it is not (yet) possible to perform direct cognitive activities. Pijpers and Ducheine agree with this statement and argue that direct engagement via the cognitive dimension, such as telepathy, does not make sense in the military context.[15] Thus, Information Manoeuvre entails physical and virtual activities in the information environment, to influence audiences' attitudes and perceptions and change or maintain their behaviours in the operating environment. This is illustrated in Figure 1.

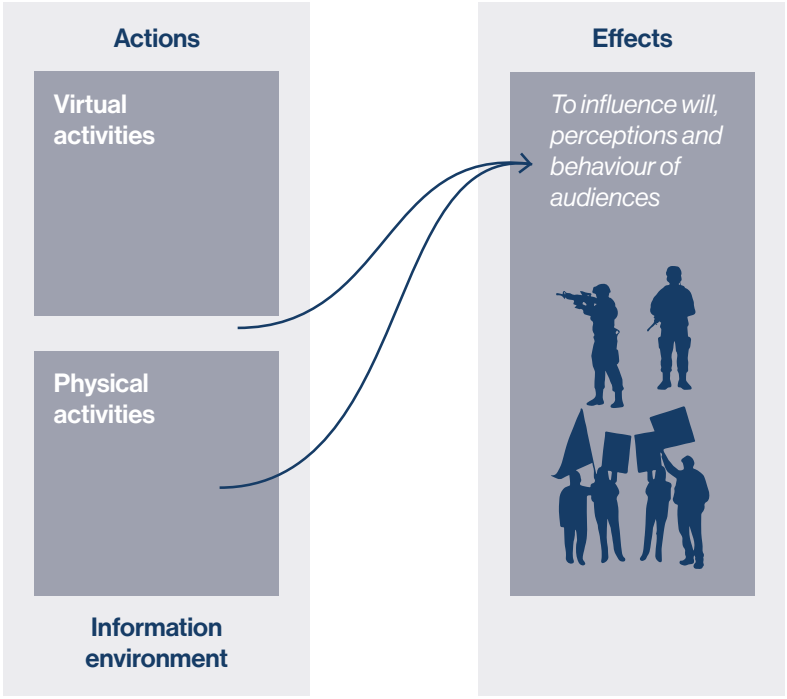
12 Reynolds, N. (2020). Performing Information Manoeuvre Through Persistent Engagement. *Occasional Paper.* London, UK: Royal United Services Institute [RUSI].

13 Pijpers, P.B.M.J., & P.A.L. Ducheine (2021). "If You Have a Hammer…": Reshaping the Armed Forces' Discourse on Information Maneuver. *Amsterdam Law School Legal Studies Research Paper No. 2021-34 / Amsterdam Center for International Law No. 2021-12.* Accessed February 24, 2023, via: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3954218.

14 CLAS (2020). *Doctrinebulletin 2020-03: Environments, dimensions, domains.*

15 Pijpers, P.B.M.J., & P.A.L. Ducheine (2021).

Figure 1. Relation between activities in the information environment and the intended effect to influence will, perceptions and behaviour of the target audience.



To explain and understand the information manoeuvre activities in the information environment, the effects dimensions can be used as a framework. The effects dimensions entail different entities that can be engaged by means of the information manoeuvre activities. For this purpose, the virtual and physical dimension are described below to explain how different information manoeuvre activities could look like.

1. The virtual dimension "entails where and how information is collected, processed, stored, disseminated, and protected digitally".[16] An example of Information Manoeuvre in this dimension is the use of Telegram and WhatsApp by Russian soldiers to breach the morality of Ukrainian soldiers, by threatening them with murdering their families and sending bursts of harrowing SMS text messages to cell phones to intimidate the military adversary into deserting or fleeing their positions.
2. With regard to the physical dimension, the authors argue that the definition of the virtual dimension can also be applied for coherency. Although there is a large prevalence of definitions, most of them are not consistent with each other or mix up different terms like environments, dimensions and domains.[17] So, the authors argue that the physical dimension entails where and how information is collected, processed, stored, disseminated, and protected physically. Examples of Information Manoeuvre in this dimension are using a newspaper to spread narratives among an audience to influence their attitudes about a specific topic, or dropping devices that create fake geolocation data by interfering with radio frequency signals.

16 Pijpers, P.B.M.J., & P.A.L. Ducheine (2020). Influence Operations in Cyberspace – How They Really Work. *Amsterdam Law School Research Paper No. 2020-61, Amsterdam Center for International Law No. 2020-31,* p. 5. Accessed February 24, 2023, via: https://ssrn.com/abstract=3698642 or http://dx.doi.org/10.2139/ssrn.3698642

17 Lin, H. & J. Kerr (2017). *On Cyber-Enabled Information/Influence Warfare and Manipulation. Social Science Research Network*. New York, USA: Social Science Research Network [SSRN], p. 5. Accessed February 24, 2023, via: https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/cyber-enabled_influence_warfare-ssrn-v1.pdf

Bayraktar: cross-synergy between the different environments and dimensions

An example of the synergy between actions the information and the physical environment and synchronization of effects in the different dimensions can be found in the Bayraktar TB2 drone strikes. The Turkish-made Bayraktar drone has been a key instrument used by the Ukrainian military to repel Russian forces after they invaded the country in 2022. The drones destroyed and severely damaged Russian military equipment. Along with the physical damage, aerial videos showing how the drone targeted and engaged Russian assets circulated widely on various social media platforms which boosted Ukraine's propaganda efforts. The virtual dimension was even further exploited by the Ukrainian patriotic propaganda song "Bayraktar" that went viral. This song had morale effects on both sides, boosting the morale of the armed forces of Ukraine and degrading the morale of the Russian army.[18]

Information Manoeuvre can be both offensive and defensive

As stated in the first two elements, Information Manoeuvre uses information to influence an audience's behaviour, will and/or perceptions. In order to manoeuvre effectively in the information environment, both offensive and defensive actions must be coordinated for these cognitive effects to be achieved. For the Royal Netherlands Army, the focus on using information as a weapon and offensively in its operations is relatively new.[19]

In military terms, an offensive often refers to a more or less aggressive projection of combat power in order to (re)gain initiative and thereby achieve strategic, operational or tactical goals. With regard to Information Manoeuvre, offensive information activities are carefully planned in the information environment with the intention to create positively constructive or negatively degrading effects concerning the will, behaviour and perception of the audience.[20] Examples are cyberattacks on information infrastructure, manipulation of the operating environment with CEMA means or the use influencers and troll armies to affect online audiences.

Kharkiv or Kherson? Ukraine's plan to deceive Russia

An example of an offensive action in the information environment is the deliberate disinformation campaign of Ukrainian forces at the tactical level that distracted Russia's attention from the Kharkiv region to the southern region of Kherson. As a result of extensive social media coverage of Ukraine's alleged offensive near Kherson, the Russian forces had moved a significant part of their materiel and personnel to the south – including units that were formerly stationed near Kharkiv. Due to the role of social media and the involvements of informants in Ukrainian-controlled parts of the operations area, the Russian forces were wrong-footed by Ukraine's coordinated military offensive and its successes near Kharkiv.[21]

18 Carlin, M. (2022). How the Turkish-made TB2 drone gave Ukraine an edge against Russia. *Business Insider [online]*. Accessed on February 24, 2023, via: https://www.businessinsider.com/how-turkish-baykar-tb2-drone-gave-ukraine-edge-against-russia-2022-9?international=true&r=US&IR=T

19 Ministry of Defence [MOD] of the Netherlands [NL] (2020). *Defence Vision 2035: Fighting for a safer future* [Translated from: Defensievisie 2035: Vechten voor een veilige toekomst]. The Hague, NL: Ministry of Defence. Accessed on February 23, 2023, via: https://www.defensie.nl/onderwerpen/defensievisie-2035/downloads/publicaties/2020/10/15/defensievisie-2035.

20 CLAS (2020). *Vision Information-Driven Operations for Land Forces: Maneuvering in the Information Environment* [Translated from: Visie Informatiegestuurd Optreden voor de Landmacht: Manoeuvreren in de Informatieomgeving]. Utrecht, NL: CLAS.

21 Koshiw, I., L. Tondo & A. Mazhulin (September 10, 2022). Ukraine's southern offensive 'was designed to trick Russia'. *The Guardian [online]*. Accessed on February 24, 2023, via: https://www.theguardian.com/world/2022/sep/10/ukraines-publicised-southern-offensive-was-disinformation-campaign.

Defensive actions are aimed at protecting the military's sustainment of its combat power and freedom of action. The effects resulting from these defensive actions in the information environment can be achieved by taking passive and active measures. An example of passive measure is the denial of information by using encryption. Examples of active measure are often reactive to information activities by the adversary, such as blocking CEMA attacks on platforms and communications. Also, they can be targeted at disrupting the adversary's decision-making cycle by, for instance, overflooding their ISR capabilities with information and thereby limiting their situational awareness.[22]

How to prepare your population for war

An example of a defensive information activity is the distribution of a defence leaflet to the Swedish population by its government in 2018. Due to raised tensions after the annexation of Crimea by Russia and an intensified internal security discussion, this 20-page leaflet contained information on how to prepare in event of a conflict. The focus is on advising Swedish households how to secure basic requirements such as shelter, food, heat and water, where to find shelter during bombings and what an individual's contribution to Sweden's *total defence* looks like. Another section of the pamphlet focused on how fake news could be identified by checking the sources of the information.[23]

Information Manoeuvre should be part of a military strategy

It should be incorporated into planning from strategic to tactical level, both offensively and defensively.

The fourth and last element that characterizes Information Manoeuvre is that it should be part of a military strategy. In other words, the effect that follows from performing Information Manoeuvre activities must be linked to a military strategy. An important condition is that the action cannot be performed at random without any premeditation but must deliberately and consciously fit within the current military strategy that is adhered. This means that the actions must be planned as part of the overall intent and cannot be treated as being outside the central planning and execution cycle.[24] Even more so, to have an appropriate overall effect, Information Manoeuvre cannot be an afterthought to a ground manoeuvre plan or "be sprinkled on" at the end of planning.[25] It should be incorporated into planning from strategic to tactical level, both offensively and defensively.

An important remark in this respect is that the actor that executes the action does not have to be military in nature. Proxies or third parties can also perform Information Manoeuvre, provided that the effect contributes to a military strategy. The military can, in one way or another, consciously stimulate proxies or third parties to perform an action in the information environment. The effect of the action contributes to the strategy that the military currently adheres. This implies that the actor does not consciously need to know that it is performing an act of Information Manoeuvre. For example, a Russian tank deliberately drives close to the Ukrainian border with the purpose that Ukrainian civilians post tweets about the tank

22 Land Warfare Centre (2020). *Doctrinebulletin 2020-03: Environments, dimensions, domains.* Amersfoort: CLAS.

23 Henley, J. (May 21, 2018). Sweden distributes 'be prepared for war' leaflet to all 4.8m homes. *The Guardian [online].* Accessed on February 24, 2023, via: https://www.theguardian.com/world/2018/may/21/sweden-distributes-be-prepared-for-war-cyber-terror-attack-leaflet-to-every-home.

24 Ministry of Defence [MOD] of the UK (2019). *Doctrine Note 19/04: Information Manoeuvre.* London, UK: MOD UK.

25 Elder, R.J., & D. Engr (2021). Information Maneuver in Military Operations. *Strategic Multilayer Assessment.* Accessed on February 24, 2023, via: https://nsiteam.com/social/wp-content/uploads/2021/08/IIJO-Invited-Perspective_Info-Maneuver-in-Mil-Ops_FINAL-2.pdf.

that 'Russia is preparing for battle'. This action, executed by Ukrainian civilians in the virtual dimension of the information environment, will likely affect the perception and behaviour of the audience that read the tweets. For example, it might increase fear among Ukrainian civilians of a kinetic conflict in the near future. It may however also be the case that proxies, and third parties are aware of the fact that they are performing an action that contributes to a military strategy – as is the case with the troll factories, spreading online propaganda about the war in favour of Russia.[26]

To conclude, Information Manoeuvre is characterized by its purpose to influence the will, perceptions and behaviour of the audiences, its actions in the information environment, its offensive or defensive character and its central contribution to a military strategy. In the next section, the authors illustrate how Information Manoeuvre can be operationalized by using existing military decision-making processes.

4. Information Manoeuvre in Military Operations

What does this 'new manner' of exerting power mean for the Royal Netherlands Army? Making use of the information environment to influence perceptions and behaviour does not happen overnight and requires a profound understanding of the military decision-making process. Military action at tactical level (from platoon to Army Corps level) has mainly focused on action in the physical environment. However, in a dynamic and integrated operating environment, the Observe, Orient, Decide and Act (OODA) loop must be considered in the context of the human and information environment as well. In the following paragraph the concept of Information Manoeuvre is integrated in the OODA loop to illustrate its contribution to integrated operations.

How Information Manoeuvre fits within the OODA loop

First and foremost, the OODA loop can be used as a step-by-step guide in which to conduct Information Manoeuvre. It consists of four steps, Observe, Orient, Decide and Act, and is illustrated in Figure 2. During the Observation phase, those involved in Information Manoeuvre collect information about different audiences, including the adversary, and significant events in the operating environment. As these observations take place in the physical and information environment, information activities are best targeted here to have full effect. Observations to support our own decision-making processes can be done by using the human senses or it can be supported with technology by using ISR sensors. The continuing digitization of the information environment facilitates the collection of data and its analysis,[27] enhancing the next step of the OODA loop. The next step, Orientation, is centred around reflection on what kind of information has been collected during the first step. Adequate situational awareness and understanding of audiences is needed in order to make a solid and accurate decision. During the Decision step,

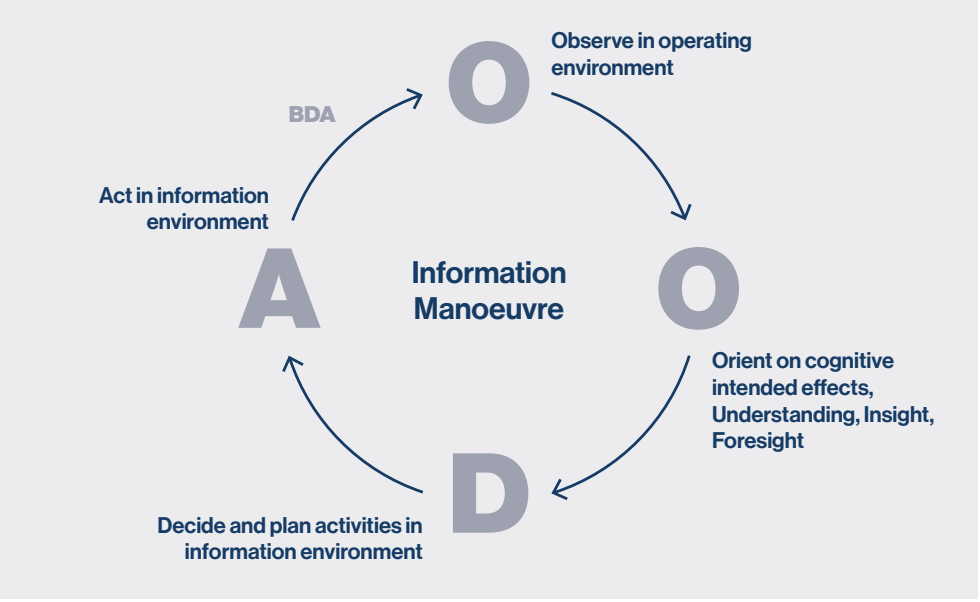
26 The Guardian (May 1, 2022). 'Troll factory' spreading Russian pro-war lies online, says UK. *The Guardian [online]*. Accessed on February 23, 2023, via: https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk.

27 Pijpers, P.B.M.J., & P.A.L. Ducheine (2021). "If You Have a Hammer...": Reshaping the Armed Forces' Discourse on Information Maneuver. *Amsterdam Law School Legal Studies Research Paper No. 2021-34 / Amsterdam Center for International Law No. 2021-12.* Accessed February 24, 2023, via: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3954218.

all considerations with regard to the outcome are discussed. This can be an internal process happening in the mind of a commander or externalized as part of a meeting at staff level. Both Orient and Decide are cognitive processes as they entail considerations, compromises, argumentation, and decision-making. These processes thus result in decisions about own information activities and how to target the Orient and Decide steps of the adversary. Also, these processes can be indirectly influenced by information activities of the adversary. The last step, Act, is about the decision and its immediate observable action in the physical and information environment. With regard to Information Manoeuvre, the input for the OODA-loop is information via observations and the outcome are information activities.[28] Between Act and Observation – thus the start of a new OODA loop – lies the feedback loop. This is often the Battle Damage Assessment (BDA). However, as stated before, there is not yet a possibility to directly observe the effect of information activities. Assessment, however, is possible by observing actions and (changed) behaviour of people in the physical and information environment.

The OODA-loop can also be used to describe the decision-making process behind audiences' (e.g. adversaries) behaviour. In this sense, Information Manoeuvre can be used to intervene and disrupt the OODA loop of adversary actors and influence their behaviour. This is the case for both offensive and defensive information activities. With regard to the former, influencing the will, perception and behaviour of the audience can take place in all four steps of the decision-making cycle of the adversary's decision-making cycle. However, it is most effective to influence the adversary's Observe or Orient steps with planned information activities, as this informs the Decide and subsequently the Act phase. With regard to the defensive information activities, protection or encryption of own information or other barriers to prevent intervention in the information environment will have a limiting effect on the Observe and Act possibilities of the adversary.

Figure 2. Integration of Information Manoeuvre in the OODA-loop to illustrate its contribution to integrated operations.



28 Duistermaat, M., A.J. van Vliet, R.A.E. van der Boor & A.F. van Daalen (2017). Behavioural change as the core of warfighting. *Militaire Spectator* 186(10), pp. 424-438. Accessed on January 11, 2023, via: https://militairespectator.nl/artikelen/behavioural-change-core-warfighting.

Integration and operational tempo

Instead of arguing that Information Manoeuvre is a separate silo, it is more effective to integrate Information Manoeuvre into the existing military planning processes. The OODA loop remains a key concept for those who fight, including in the field of information. In the end, collecting relevant information more rapidly than the adversary and being able to integrate it more quickly in military plans is key. Thus, tempo is where the OODA-loop and Information Manoeuvre meet.[29] In order to gain an information advantage over the adversary, it is important to "get 'inside' the [adversary] loop by transitioning from one mode of action to another, before the other party can react".[30] The credibility and timeliness of deterrence is also radiated by increasing the speed of decision-making relative to the adversary.[31] This is also addressed by the US Army, when Lieutenant General Stephen G Fogarty argued that:

> The emergence of the so-called information revolution in military affairs in the 1990s led the services to use information to strike targets faster and more accurately through concepts such as net-centric warfare and effects-based operations through networking, sensors, computers, and satellites.[32]

Tempo is where the OODA-loop and Information Manoeuvre meet.

Cyber operations, information operations, particularly social media and influence operations, are fast and sometimes deliver effects that are either virtually instantaneous or occur within a matter of minutes.[33] Russia masters the concept of informational tempo. Recent attempts to block NATO accession by Montenegro and North Macedonia by amplifying internal crises is such an example of Russia being able to shift its lines of operations rapidly, before Western nations can respond.[34] In sum, using information as a form of manoeuvre offers a useful and understandable template for the planning and integration of information activities into joint military operations.

5. Information Manoeuvre: so, what?

As mentioned in the introduction of this paper, much debate focuses on what the concept of Information Manoeuvre defines. The authors therefore also have, next to the four fundamental elements, identified three overarching dilemmas concerning the concept of Information Manoeuvre that need further consideration.

29 Reynolds, N. (2020). Performing Information Manoeuvre Through Persistent Engagement. *Occasional Paper.* London, UK: Royal United Services Institute [RUSI].

30 Creveld, van, M., K.S. Brower & S.L. Canby (1994). *Air Power and Maneuver Warfare*. Montgomery, AL/US: Air University Press.

31 Reynolds, N. (2020). Performing Information Manoeuvre Through Persistent Engagement. *Occasional Paper.* London, UK: Royal United Services Institute [RUSI].

32 Ibid.

33 Ibid.

34 Elder, R.J., & D. Engr (2021). Information Maneuver in Military Operations. *Strategic Multilayer Assessment.* Accessed on February 24, 2023, via: https://nsiteam.com/social/wp-content/uploads/2021/08/IIJO-Invited-Perspective_Info-Maneuver-in-Mil-Ops_FINAL-2.pdf.

Information Manoeuvre cannot be performed in the physical environment... or can it?

Although there seems to be general agreement that the purpose of Information Manoeuvre should be to influence the will, perception and behaviour of the audience, an ongoing debate exists concerning where the action itself should take place. This is especially the case for the more physical activities. On the one hand, it is argued that as long as it concerns an activity in the physical and virtual dimension of the information environment, it can be classified as Information Manoeuvre. On the other hand, however, it is argued that some activities in the physical environment can be classified as Information Manoeuvre as well, depending on the effect it creates. For example, a Russian tank deliberately driving close to the Ukrainian border to signal a threat might influence the perceptions and behaviour of Ukrainian civilians and could be seen as communication strategy. However, the action itself takes place in the physical environment and not in the information environment. The question remains how strict the dividing line between activities in different environments should be made.

Force protection is not Information Manoeuvre... or is it?

Earlier in this paper the authors argued that Information Manoeuvre can be both offensive and defensive. Defensive effects are aimed at protecting the military's sustainment of its combat power and freedom of action. Effects in the information environment (e.g. defend, deny, reconnect, repair) can be achieved by taking passive (passive information denial with encryption) and active (camouflage or contra-intelligence) measures. When taken into consideration the description of passive measures of Information Manoeuvre, one can argue that this closely relates to force protection. Force protection can be defined as "preventive measures taken to mitigate hostile actions against Department of Defence personnel (to include family members), resources, facilities, and critical information".[35] Specifically, digital force protection is to increase awareness of the vulnerabilities, threats, and impact of the digital environment. Activities in this context, such as training own staff to use social media safely and responsibly or setting in place protection mechanisms for information systems, might be appreciated as defensive Information Manoeuvre activities. However, it must not be mistaken for the same. Force Protection refers to the functional concept of protecting military personnel, family members, facilities etc. Activities are primarily aimed at building resilience, defined as the ability of the armed forces as well as the concerned populations to withstand the effects of the adversary's actions.[36] To the contrary, defensive measures of Information Manoeuvre are still aimed at generating effects in the operating environment. Defensive measures, such as information denial, influence the adversary's understanding and decision-making process because observation capabilities are being limited or affected. However, where force protection ends, and Information Manoeuvre starts is a question that requires more attention.

35 DOD US (2021). *DOD Dictionary of Military and Associated Terms*. Accessed on February 24, 2023, via: https://irp.fas.org/doddir/dod/dictionary.pdf.

36 Ministry of Defence [MOD] of the UK (2019). *Doctrine Note 19/04: Information Manoeuvre*. London, UK: MOD UK.

Intelligence is not a part of Information Manoeuvre... or is it?

The central question for this dilemma is how Information Manoeuvre fits within the existing Information Life Cycle (e.g. collect, organise, store, exploit). On the one hand, Information Manoeuvre is considered a niche concept: only the final stage, where information is used to influence the audience, is appreciated as Information Manoeuvre. In this specific case, intelligence is a precondition for this final stage, and therefore not part of Information Manoeuvre itself. From this perspective Information Manoeuvre only entails the performed activities in the information environment. On the other hand, Information Manoeuvre can be interpreted as an overarching concept that also include Intelligence. According to this perspective, Intelligence is not just a precondition for Information Manoeuvre but part of the concept itself. The question arises how broad the scope of Information Manoeuvre should be: is it limited to the use of information as a means to act, thus the use of information to affect the operating environment? Or does it also entail the use of information to gain Intelligence (i.e. information an enabler)?

6. Reflections and conclusions

Information Manoeuvre is a concept that is critical to today's battlefield as it uses information as a means to act. In this paper, the authors have investigated what Information Manoeuvre entails for the Royal Netherlands Army. Generally seen, Information Manoeuvre is the use of information as a weapon to influence audiences' attitudes and perceptions and change or maintain their behaviours. Although a standardized definition cannot yet be given, an exploration of the underpinning elements has shed light on the span of the operational concept in the military domain. These elements of Information Manoeuvre are its purpose, its actions, its character, and its contribution to a military strategy.

Furthermore, the examples in this paper illustrated that Information Manoeuvre is visible in current military conflicts, such as the war in Ukraine and the wider tensions in the region. Given the prominence of information activities in the military strategy of both Ukraine and Russia, it is plausible to have effects on changing behaviour in favour of the mission and tasks at hand, contributing to a military advantage. Getting a grip on assessing these (indirect) effects in the cognitive dimension is a research path that is worth exploring. As such, the added value of Information Manoeuvre as an operational concept is rooted in the cross-synergy it creates and the effects that it sorts. By incorporating Information Manoeuvre into the OODA-loop as part of integrated operations, which is a key model itself, it can fulfil its promise to collect relevant information more rapidly than the adversary and subsequently exploit this position with targeted information activities.

Nevertheless, the concept is not unambiguous. Three dilemmas were identified, namely whether or not Information Manoeuvre can be performed in the physical environment, its relation to Force Protection, and the role of intelligence. These dilemmas provide interesting sub-topics for further research such as more in-depth research on incorporating Information Manoeuvre into existing military processes, exploratory research on how Information Manoeuvre could facilitate cross-synergy between relevant disciplines, measuring effects in the cognitive dimension, and synchronization of activities in the information and physical environment for optimal effects. This work will improve the concept and make it more mature in its substance and scope.

References

Bundeswehr (2019). *Bearbeitung der Lage im Informationsumfeld.* Mayen, DE: Zentrum Operative Kommunikation der Bundeswehr.

Carlin, M. (2022). How the Turkish-made TB2 drone gave Ukraine an edge against Russia. *Business Insider [online].* Accessed on February 24, 2023, via: https://www.businessinsider.com/how-turkish-baykar-tb2-drone-gave-ukraine-edge-against-russia-2022-9?international=true&r=US&IR=T

CLAS (2020). *Vision Information-Driven Operations for Land Forces: Maneuvering in the Information Environment* [Translated from: Visie Informatiegestuurd Optreden voor de Landmacht: Manoeuvreren in de Informatieomgeving]. Utrecht, NL: CLAS.

Creveld, van, M., K.S. Brower & S.L. Canby (1994). *Air Power and Maneuver Warfare*. Montgomery, AL/US: Air University Press.

DOD US (2021). *DOD Dictionary of Military and Associated Terms*. Accessed on February 24, 2023, via: https://irp.fas.org/doddir/dod/dictionary.pdf.

Duistermaat, M., A.J. van Vliet, R.A.E. van der Boor & A.F. van Daalen (2017). Behavioural change as the core of warfighting. *Militaire Spectator* 186(10), pp. 424-438. Accessed on January 11, 2023, via: https://militairespectator.nl/artikelen/behavioural-change-core-warfighting.

Elder, R.J., & D. Engr (2021). Information Maneuver in Military Operations. *Strategic Multilayer Assessment.* Accessed on February 24, 2023, via: https://nsiteam.com/social/wp-content/uploads/2021/08/IIJO-Invited-Perspective_Info-Maneuver-in-Mil-Ops_FINAL-2.pdf.

Henley, J. (May 21, 2018). Sweden distributes 'be prepared for war' leaflet to all 4.8m homes. *The Guardian [online].* Accessed on February 24, 2023, via: https://www.theguardian.com/world/2018/may/21/sweden-distributes-be-prepared-for-war-cyber-terror-attack-leaflet-to-every-home.

Joint Staff (2017). *Joint publication 1: Doctrine for the Armed Forces of the United States.* Accessed March 6, 2023, via: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

Koshiw, I., L. Tondo & A. Mazhulin (September 10, 2022). Ukraine's southern offensive 'was designed to trick Russia'. *The Guardian [online].* Accessed on February 24, 2023, via: https://www.theguardian.com/world/2022/sep/10/ukraines-publicised-southern-offensive-was-disinformation-campaign.

Lin, H. & J. Kerr (2017). *On Cyber-Enabled Information/Influence Warfare and Manipulation. Social Science Research Network*. New York, USA: Social Science Research Network [SSRN]. Accessed February 24, 2023, via: https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/cyber-enabled_influence_warfare-ssrn-v1.pdf.

Land Warfare Centre (2020). *Doctrinebulletin 2020-03: Environments, dimensions, domains.* Amersfoort: CLAS.

Ministère des Armées (2021). *Éléments publics de doctrine militaire de lute informatique d'influence (L2I).* Paris, FR: Ministère des Armées. Accessed on March 7, 2023, via: https://www.defense.gouv.fr/sites/default/files/ema/doctrine_de_lutte_informatique_dinfluence_l2i.pdf.

Ministry of Defence [MOD] of the Netherlands [NL] (2020). *Defence Vision 2035: Fighting for a safer future* [Translated from: Defensievisie 2035: Vechten voor een veilige toekomst]. The Hague, NL: Ministry of Defence. Accessed on February 23, 2023, via: https://www.defensie.nl/onderwerpen/defensievisie-2035/downloads/publicaties/2020/10/15/defensievisie-2035.

Ministry of Defence [MOD] of the UK (2019). *Doctrine Note 19/04: Information Manoeuvre.* London, UK: MOD UK.

NATO (2009). AJP-3.10: Allied Doctrine for Joint Information Operations. Brussels, BE: NATO. Accessed on February 22, 2023, via: https://info.publicintelligence.net/NATO-IO.pdf.

Pijpers, P.B.M.J., & P.A.L. Ducheine (2020). Influence Operations in Cyberspace – How They Really Work. *Amsterdam Law School Research Paper No. 2020-61, Amsterdam Center for International Law No. 2020-31.* Accessed February 24, 2023, via: https://ssrn.com/abstract=3698642 or http://dx.doi.org/10.2139/ssrn.3698642

Pijpers, P.B.M.J., & P.A.L. Ducheine (2021). "If You Have a Hammer...": Reshaping the Armed Forces' Discourse on Information Maneuver. *Amsterdam Law School Legal Studies Research Paper No. 2021-34 / Amsterdam Center for International Law No. 2021-12.* Accessed February 24, 2023, via: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3954218.

Reynolds, N. (2020). Performing Information Manoeuvre Through Persistent Engagement. *Occasional Paper.* London, UK: Royal United Services Institute [RUSI].

Romansky, S., L. Boswinkel & M. Rademaker (2022). *The parallel front: An analysis of the military use of information in the first seven months of war in Ukraine*. The Hague, NL: The Hague Centre for Strategic Studies [HCSS].

The Guardian (May 1, 2022). 'Troll factory' spreading Russian pro-war lies online, says UK. *The Guardian [online].* Accessed on February 23, 2023, via: https://www.theguardian.com/world/2022/may/01/troll-factory-spreading-russian-pro-war-lies-online-says-uk.

Judith van de Kuijt received a M.Sc. degree in Human Geography (Conflicts, Territories and Identities) at the University of Nijmegen and a MA degree in Military Strategic Studies at the Dutch Defense Academy (NLDA) in Breda. At present, Judith is working as senior researcher and consultant at the Military Operations department at TNO where she works on projects in the field of Hybrid Threats, Information Operations, Behavioral Influencing, and Disinformation. She is also a reserve officer in the Dutch army.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA Hague

Follow us on social media:
@hcssnl

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