The Hague Centre
for Strategic Studies

Information-based behavioural influencing
and Western practice

Deception as the Way of Warfare

Armed Forces, Influence Operations and the Cyberspace paradox

Colonel dr. Peter B.M.J. Pijpers and Brigadier-General prof. dr. Paul A.L. Ducheine

May 2023

The Hague Centre
for Strategic Studies

Paper 1

Deception as the Way of Warfare

Armed Forces, Influence Operations and the Cyberspace paradox

Authors:
Colonel dr. Peter B.M.J. Pijpers and
Brigadier-General prof. dr. Paul A.L. Ducheine

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)

Maneuver warfare is, to put it simply, a kick in the groin, a poke in the eye, a stab in the back.

It is quick, violent for a moment, and unfair. It is decisive, even preemptive, at the expense of protocol and posturing.

Maneuver warfare puts a premium on being sneaky rather that courageous, and it's not at all glorious, because it typically flees from the enemy's strength.[1]

1. Introduction

Though fake news, alternative facts and manipulation of information and data appear to be the latest hype, instruments to influence and change human behaviour have been around for ages, also during conflict and war. In effect, deception is the way of warfare.[2]

Nowadays states can make use of numerous instruments of power to exert influence to change behaviour of opponents. The military instrument is an obvious one, but – with the emergence of cyberspace – the informational instrument of power is of increasing importance. Cyberspace is a catalyst enabling the full use of the information environment, transforming the conveying of information from the cumbersome employment of pamphlets, news articles or radio to a high-speed and all-encompassing tool prompted by the possibilities of Internet and social media.

Similar to outmanoeuvring opponents in the physical realm, state agents can now also 'manoeuvre in the information environment'. These are actions to gain a position of relative advantage by using information to target and change the perception of opponents and their information environment. Information as an instrument to influence the cognition of targeted audiences can be used in tandem with military and other instruments of power as also witnessed in the Russo-Ukraine War.

For the Netherlands, the inception of cyberspace also provides new opportunities to protect and further its national interests. The Netherlands has the capabilities and expressed the intent to use them.[3] However, while cyberspace has significantly increased the possibilities to deliberately influence the cognitive dimension of target audiences the Netherlands is - paradoxically enough - reticent in utilising them.

The object of this contribution is therefore to explore how states manoeuvre in the information environment, how they exert influence, and how traditional deceptive and manipulative operations differ from cyber-based influence operations, in order to explore where the reticence to

[1] Leonhard, *The Art of the Maneuver: Maneuver-Warfare Theory and AirLand Battle*. p. 61.

[2] Sawyer, *Sun Tzu: Art of War*. p. 168.

[3] Voo, Hemani, and Cassidy, "National Cyber Power Index 2022."; Netherlands Ministry of Defence, "Defence Vision 2035: Fighting for a Safer Future."

use digital influence operations stems from. To substantiate the analysis, the article starts with (§2) the concept of influence as an instrument of power and (§3) how states can exert influence by outmanoeuvring others through pre-emption, dislocating and disrupting. To assess the effect of cyberspace on influence operations, cyberspace will be introduced (§4) as well as the actions that are possible in that domain. (§5) before articulating how to manoeuvre in a digitalised information environment (§6) and how influence operations in cyberspace generate effects (§7). Finally, this assessment queries why the Netherlands is reticent to apply influence operations in cyberspace (§8).

2. The Concept of Influence

States generally co-exist in a peaceful and interdependent way. However, when interests conflict, they can exert influence to protect or further their national interests. States can employ their instruments to persuade, coerce or manipulate other states to change their position.[4] States will resort to diplomatic or military means, but can also make use of the informational instrument of power.

Information as an element of national power refers to the way states use data and knowledge to understand and shape the nature of the information environment in support of their national interests.[5] The informational instrument – when used to exert malign and deceptive influence - aims to disrupt "the opponent's ability to direct objective content to its target audience, to properly grasp reality and to establish effective defensive action capability".[6]

Cyberspace is a catalyst enabling the full use of the information environment.

3. Manoeuvring in the Information Environment

When using information as a tool of influence, it is essential to gain a competitive advantage over other actors and achieve effects in the informational sphere. In other words, one needs to manoeuvre in the information environment to gain effects –- i.e. to cooperate with, persuade, coerce or manipulate the opposing actor resulting in a change of position.

The notion of 'manoeuvring' is – even in a military sense – not a weapon but an approach whereby one targets the vulnerabilities of the opposite actor rather than its strength.[7] Where in attrition warfare two (armed) forces collide head-on destroying the enemy's mass,[8] manoeuvre warfare focusses on the command and control hubs or the logistical supply routes. Better still, it targets the societal support for the endeavour in the home state of the opponent or undermines the cohesion of opposing alliances.

[4] Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World."

[5] Farlin, "Instruments of National Power: How America Earned Independence." p. 5. Or as McDougal and Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War." p. 793.

[6] Cohen and Bar'el, "The Use of Cyberwarfare in Influence Operations." p. 8, Cohen and Bar'el refer to perception warfare in this sense.

[7] Strange, *Centers of Gravity & Critical Vulnerabilities : Building on the Clausewitzian Foundation So That We Can All Speak the Same Language*.

[8] Leonhard, *The Art of the Maneuver: Maneuver-Warfare Theory and AirLand Battle*. pp. 18-24.

The core elements of manoeuvre warfare are pre-emption, dislocation and disruption.[9] Pre-emption means to seize an opportunity before the enemy does. This is often at odds with elaborate rational decision-making processes, since the opportunity must be seized with a certain boldness and resolve thereby 'emphasizing speed rather than caution'.[10] While seizing opportunities is a core principle of warfare it can conflict with military principles meaning that the decision to seize an opportunity will increase the risks during the confrontation and will have consequences in the aftermath of act.[11] Dislocation means to lead the enemy forces away from the decisive battle by using feint capacities or misleading manoeuvres (e.g. 1943 Operation Mincemeat) or by changing the 'location' of the decisive battle, both in position and function. A nuclear power can be dislocated when the 'decisive battle' is transferred to submarine warfare or even the courtroom. In essence dislocation renders the enemy's strength irrelevant. Disruption emphasizes the practice of defeating the enemy's centre of gravity (or critical vulnerability) rather than its mass. By targeting the vulnerabilities, the enemy is incapable of deploying its force according to a predestined plan. In May 1940 the Netherland defence plan was built around fortifications and inundations. A plan that was completely disrupted when Nazi-Germany's Luftwaffe circumvented the deluges and destroyed Rotterdam, the economic heart of the country.

In May 1940 the Netherland defence plan was built around fortifications and inundations. A plan that was completely disrupted when Nazi-Germany's *Luftwaffe* circumvented the deluges and destroyed Rotterdam, the economic heart of the country.

4. The Inception of Cyberspace

Influence operations, to dislocate or disrupt an opponent (whether coined as Active Measures or Political Warfare) are nothing new.[12] What is new, is that the inception of cyberspace has changed the dynamics and characteristics of influence operations, not least by adding new digital layers to the information environment to exert influence.[13]

Cyberspace is a man-made domain encompassing the virtual dimension (the logical and the virtual persona layer) and part of the physical dimension (the physical network layer) (Figure 1).[14] Though cyberspace is a neutral domain, similar to the land or air domain, it can also be used to target (or be targeted by) other actors.

[9] Leonhard. pp. 62-76

[10] Leonhard. p. 63.

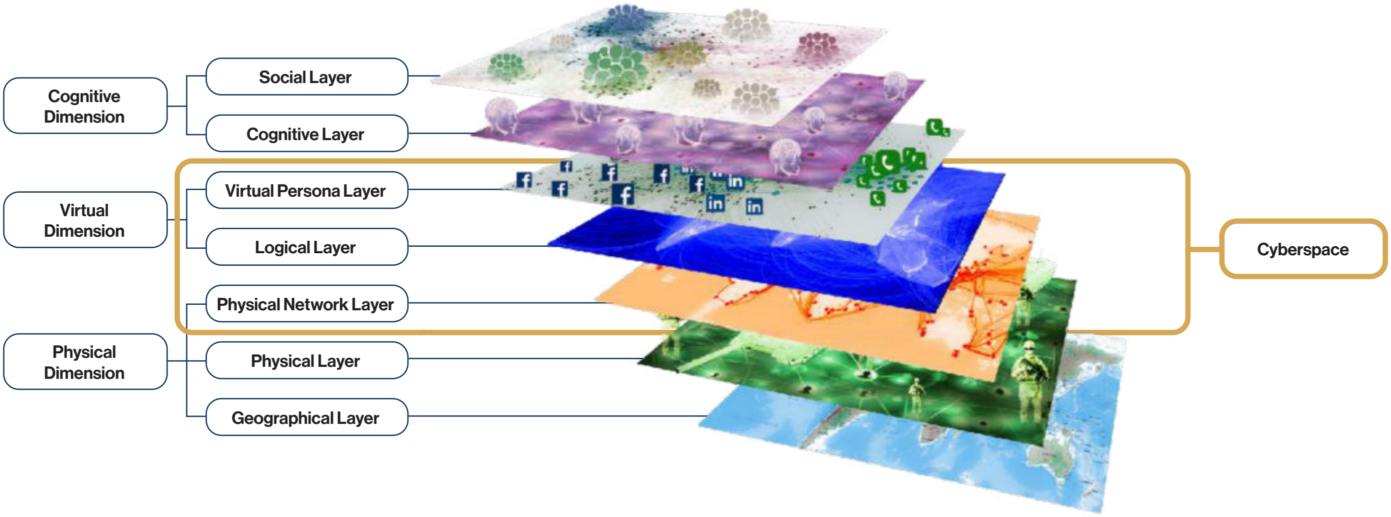
[11] E.g. Guderian's Pantzer advance in Northern France in 1940, or the 2003 US Marine Expeditionary Force's advance in Iraq leaving open their flanks and outpacing their logistic resupply.

[12] Rid, *Active Measures: The Secret History of Disinformation and Political Warfare.; Robinson et al., Modern Political Warfare: Current Practices and Possible Responses*.

[13] Paterson and Hanley, "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes.'"

[14] The physical network layer contains ICT infrastructure (computers, router or glass-fibre cables. The logical layer are the data and software, and the virtual persona layer are the digital reflections of persons or groups on social media and the Internet (What's app, Instagram, Facebook accounts, email addresses).

Figure 1. Information Environment and Cyberspace[15]



What is new, is that the inception of cyberspace has changed the dynamics and characteristics of influence operations, not least by adding new digital layers to the information environment to exert influence.

5. Operations in Cyberspace

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 (e.g. intelligence services, law enforcement agencies, armed forces) have embraced possibilities to engage in the information environment - via cyberspace - in order to generate effects.

Activities that are made possible via cyberspace include[16] (i) digital espionage, or Computer Network Exploitation (CNE),[17] extracting data confined in virtual repositories; (ii) operations that undermine or subvert the three layers of cyberspace itself (Computer Network Attacks (CNA)) with binary code, in order to modify or manipulate data, and to degrade or destroy the ICT infrastructure, resulting in (virtual and physical) effects in cyberspace.[18] The final set of activities are, (iii) influence operations that use cyberspace (more specifically Internet and social media) as a vector to target the cognitive dimension, using content, words, memes and footage as 'weapon'.[19]

Cyberspace has not only widened the engagement area allowing numerous actors (including non-state actors) to enter at low costs, but also makes communication go faster and more diffusional.[20] Furthermore, it enables (state and non-state) actors to surgically target specific audiences with bespoke (computationally enhanced) messages based on algorithms and big

[15] Ducheine, van Haaster, and van Harskamp, "Manoeuvring and Generating Effects in the Information Environment." p. 6.; Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict." p. 173 (footnote 898).

[16] Whyte and Mazanec, *Understanding Cyber Warfare : Politics, Policy and Strategy*. pp. 100-101.

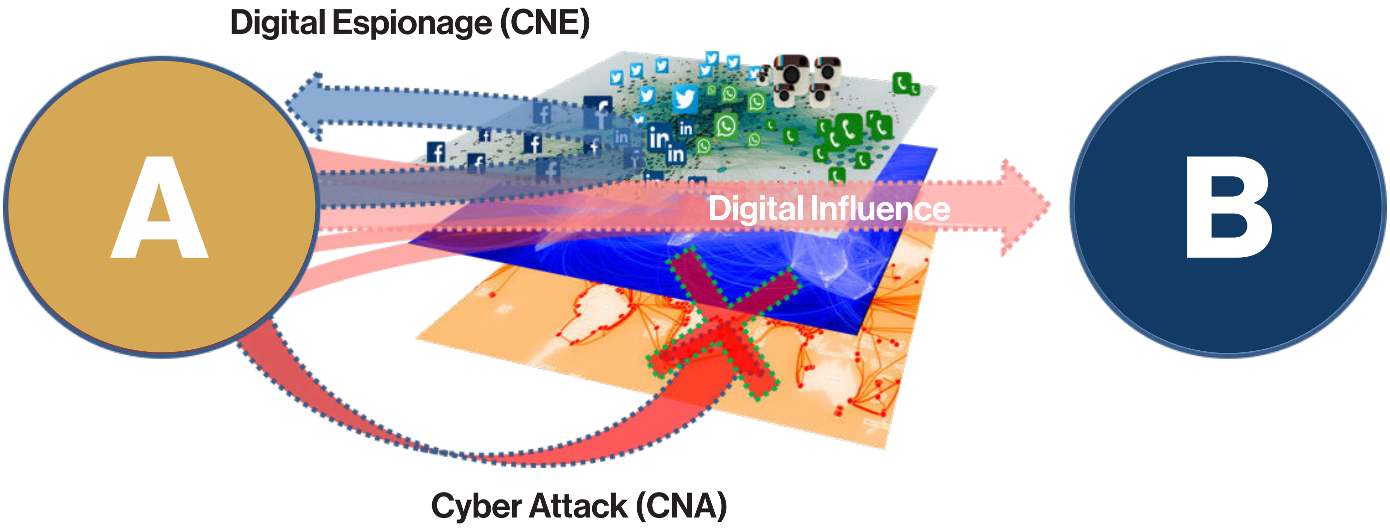
[17] Owens, Dam, and Lin, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities." pp. 1-2.

[18] Pijpers and Arnold, "Conquering the Invisible Battleground."

[19] Lupion, "The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News." pp. 329-330; Walton, "What's Old Is New Again: Cold War Lessons for Countering Disinformation."

[20] Tansino, "Analysing Strategic Communications through Early Modern Theatre." p. 57.

Figure 2. Activities in Cyberspace



data analysis in order to gain an insight into the correlation between activity and effect rather than on its causality. Cyberspace is therefore a catalyst for influence operation.[21]

Cyberspace is therefore a catalyst for influence operations.

6. Information Manoeuvre and Cyberspace

The core elements of manoeuvre are pre-emption, dislocation and disruption. In the physical realm, these deceptive and misleading techniques are executed by physical tools. The manoeuvrist approach is, in the traditional sense, a psychological contest using physical means. Applying the manoeuvrist approach to achieve effects in the wider information environment, means to be faster and better in decision making and act more effective than others using informational means, hence achieving effect in the physical, virtual and cognitive dimensions.

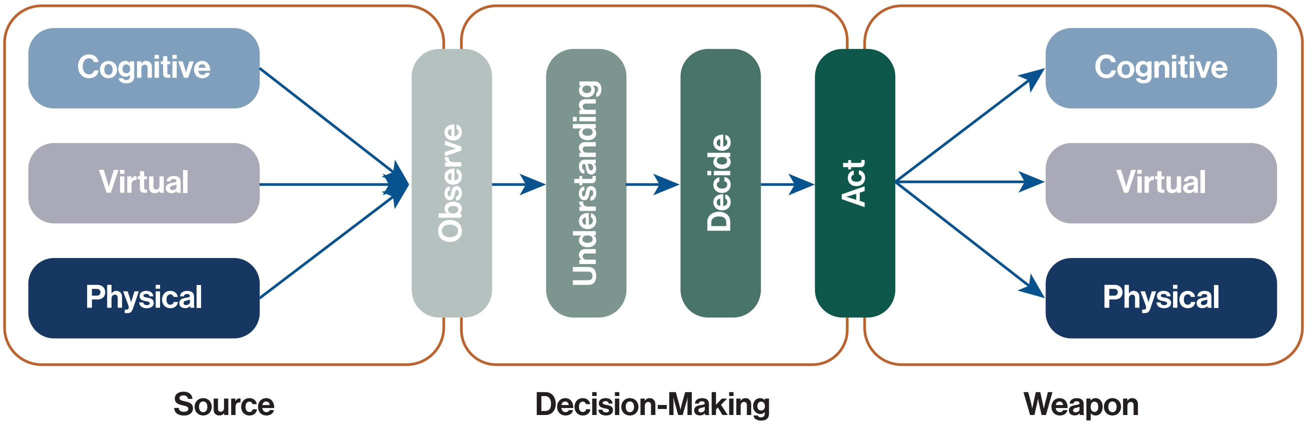
While traditional kinetic action (with effects in the physical dimension to influence audiences in an indirect manner) are far from obsolete,[22] information manoeuvre – in a contemporary cyberspace setting – strives to outmanoeuvre the opponent also, or predominantly, via the virtual dimension of Internet and social media. Operations enabling this target the virtual dimension (virtual objects such as data and personae including social media accounts) and the physical network layer (computers or routers) through digital subversion or sabotage operations. These operations are unique to the cyberspace domain. Moreover, influence operations use information as a weapon to influence the cognitive dimension of targeted audiences.[23]

[21] The Russian doctrine, contrary to most Western concepts, distinguishes between information-technology warfare and information-psychological warfare irrespective of the domain of operations (Land, Sea, Air, Cyberspace and Space). Degrading, undermining of sabotaging the ICT infrastructure could be labelled information-technology warfare, while operations affecting the cognitive dimension are information-psychological warfare, of influence operations. Giles, "Handbook of Russian Information Warfare." pp. 7-11.

[22] Johnson, "The First Phase of the Russian Invasion of Ukraine 2022."

[23] Pijpers and Ducheine, "'If You Have A Hammer': Reshaping the Armed Forces' Discourse on Information Maneuver."

Figure 3. The elements of Information Manoeuvre



Using information as a weapon of influence is the acme of information manoeuvre and aims to undermine the deliberate understanding and autonomous decision-making process of the targeted audiences by means of pre-emption, dislocation and disruption.

7. Influence Operations in Cyberspace

Influence operations can be executed using cyberspace as vector.[24] Influence operations can therefore be defined as malign activities whereby one party deliberately uses information on the population of an opponent to confuse, mislead and ultimately influence the actions the targeted population takes.[25] The main characteristics of influence operations (in cyberspace) are the absence of a threat or use of force, the focus on the cognitive dimension and the objective to change the behaviour of other actors directly or indirectly via a change in attitude. To achieve this, influence operations will utilise persuasive, coercive or manipulative techniques (see figure 4).[26]

Not all influence operations are malign per se. During persuasive influence operations, State A aims to change the weighing and number of options available to the targeted audience, in order for State B to make a voluntary (or willing) choice that is beneficial to State A. Coercive influence operations, conversely, cut short or circumvent the deliberate understanding and autonomous decision-making process of the targeted audiences of State B forcing them to consciously make an ‘unwilling’ choice.

Whilst persuasive and coercive influence operations make use of rational and conscious techniques, manipulative influence operations use subconscious and covert techniques that subvert or usurp the autonomous decision-making process. Manipulative influence operations are inherently deceptive and make use of heuristics and biases luring the victim

[24] See also: Pijpers and Arnold, “Conquering the Invisible Battleground.” pp. 12-14; Cordey, “Cyber Influence Operations: An Overview and Comparative Analysis.” pp. 15-19.

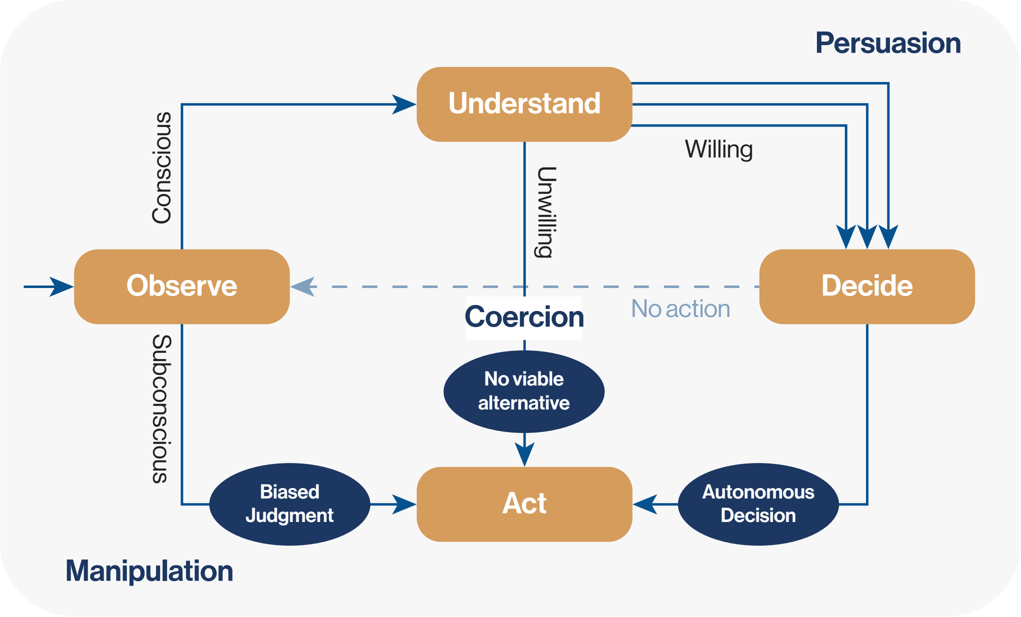
[25] Lin and Kerr, “On Cyber-Enabled Information Warfare and Information Operations.” p. 3.

[26] Susser, Roessler, and Nissenbaum, “Online Manipulation: Hidden Influences in a Digital World.”; Pijpers, *Influence Operations in Cyberspace: On the Applicability of Public International Law during Influence Operations in a Situation Below the Threshold of the Use of Force*. Chapter 2.

audience away from rational decision-making processes in favour of – what Petty and Cacioppo call - the peripheral route.[27] The peripheral route is invoked by means of two mechanisms. First the targeted audience needs to be triggered by a socially divisive topic, forcing groups in society to communicate.[28] To generate a trigger, information will be framed and adjusted to the targeted audience.[29] Second, the ability to process the data must be impaired. The peripheral – or subconscious - route can be invoked once groups or peoples are faced with an overload of data, a shortage of time or are otherwise incapable to verify or make sense of incoming data.[30] If the ability to process is impaired, the targeted audiences are deflected into making reflexive and biased judgements based on cognitive and social heuristics, such as the confirmation or availability bias;[31] rendering the targeted audience unable to validate the authority of the data provided which in turn prevents them from making a deliberate verification of the information.[32]

To invoke heuristics, and executing the strategic narratives, digital influence operations make a range of techniques including disinformation,[33] trolling, or the leaking of sensitive data. The techniques are effective once they are able to connect large quantities of data sets, which contain personal data provided by individuals and groups via social media platforms such as Facebook, Instagram, Telegram or Vkontakte.

Figure 4. Avenues of Influence



[27] Petty and Cacioppo, “The Elaboration Likelihood Model of Persuasion.” p. 126.

[28] Such as the Netherlands’ Black Pete discourse or the Covid-vaccination policy. See also: Tansino, “Analysing Strategic Communications through Early Modern Theatre.” p. 53.

[29] Lakoff, *The Political Mind: A Cognitive Scientist’s Guide to Your Brain and Its Politics*. An example of which are the pro-life and pro-choice frames.

[30] Korteling, Duistermaat, and Toet, “Subconscious Manipulation in Psychological Warfare.”; Benson, “Cognitive Bias Cheat Sheet.”

[31] See e.g. Korteling, Duistermaat, and Toet, “Subconscious Manipulation in Psychological Warfare.”. For social heuristics see: Cialdini, *Influence: The Psychology of Persuasion*.

[32] Nye Jr., “Protecting Democracy in an Era of Cyber Information War.” p. 4.

[33] Lanoszka, “Disinformation in International Politics.” p. 229

The manipulative mechanism of influence operations is the basis for the Russian Active Measures-doctrine, relying on reflexive control,[34] i.e. "conveying to a partner or an opponent specially-prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[35] During the 2016 UK referendum on whether or not to leave the EU (Brexit), the Leave camp[36] coined frames such as 'Let's take back control' or made the suggestion that the EU would cost £350 million per week.[37] 'Let's take back control' provides an example of the functioning of the peripheral route. The socially divisive topic is the EU membership of the UK, a stone of contention since the UK joined in 1973.[38] It was further invoked ingrained sentiments suggesting that the EU controls UK policies and UK remittances exceed the benefits.[39]

Russian influence operation supported the 'Leave-camp' in the UK EU referendum with manipulative activities included the running of 419 Twitter accounts, pretending to be domestic actors. Similarly, in the 2016 US presidential election the integrity of Hilary Clinton was the main object of the influence campaign of both Russian and domestic antagonist urging to 'Lock her up'.[40] The 2022 Russo-Ukraine war also saw (manipulative) Russian influence operations to target opposing, Western or domestic audiences.[41]

8. The Utility of Influence Operations - the Cyberspace-paradox

In the Cold War-era the world was under constant threat of large quantities of nuclear warheads. Oddly enough, in that bipolar world the sheer number of nuclear weapons in the arsenal of the United States and the Soviet Union kept them from using them. In other words, the greater the number of nuclear weapons the greater the stability, while non-nuclear conflicts created instability.[42]

This paradox cannot be transfigured to the cyberspace-era one-on-one, but that does not mean that there are no contrarieties in cyberspace. While access to the information environment has grown exponentially - due to the inception of cyberspace - and thereby the potential to influence other actors in a non-kinetic manner, states appear to be ever more reticent to use this potential due to ethical and legal concerns.

The latest Netherlands White Paper envisions 'armed forces that also use information as a weapon in its own right and that are permitted to use this weapon at an early stage and

[34] Thomas, "Russia's Reflexive Control Theory and the Military." pp. 238-243.

[35] Thomas. p. 237. See also: Ajir and Vailliant, "Russian Information Warfare : Implications for Deterrence Theory." pp. 72-73.

[36] The UK referendum did not follow party affiliations since each party had segments wanting to Leave the EU or to Remain in the EU. The Electoral Commission, "Electoral Commission Designates 'Vote Leave Ltd' and 'The In Campaign Ltd' as Lead Campaigners at EU Referendum."

[37] Cummings, "How the Brexit Referendum Was Won."

[38] Atikcan, Nadeau, and Belnager, *Framing Risky Choices: Brexit and the Dynamics of High-Stakes Referendums*.

[39] Cummings, "How the Brexit Referendum Was Won."

[40] Gentry, "Trump-Era Politicization: A Code of Civil–Intelligence Behavior Is Needed." p. 763.

[41] Boswinkel, Rademaker, and Romansky, "Information-Based Behavioural Influencing in the Military Context Mapping Current Expert Thinking."

[42] Snyder, "The Balance of Power and the Balance of Terror."; Lieber, "The Illogic of American Nuclear Strategy."

offensively where necessary.[43] While these words are in line with the main purpose of armed forces i.e. to defend and protect the state's interests, including to maintain and promote the international legal order,[44] irrespective of the domain of operation, the context and dynamics of operating in the virtual and cognitive dimension of the information environment appear to be at odds with the employment of Netherlands armed forces in the cyberspace-enabled information environment.

According to Belfer Centre reports, the Netherlands is a top-notch actor in cyberspace taking the 5th or 6th place in the cyber-power index.[45] This might be true in terms of what the Netherlands security agents (law enforcement, intelligence and armed forces) are capable and willing to do, but is hampered when assessing what these agents are allowed to do. Related to the employment of influence operations via cyberspace by the armed forces, two elements are of relevance in this context: the institutional conceptualisation of cyberspace operations and the legal framework.

While access to the information environment has grown exponentially and thereby the potential to influence other actors in a non-kinetic manner, states appear to be reticent to use this potential due to ethical and legal concerns.

8.1. On the concept

There is a mismatch between the organisation of security agents in the Netherlands and the actual influence activities via cyberspace. The security agents are structured and organised in a manner that makes perfect sense for the traditional threats arising from the physical dimension. The dominant operational concept for armed forces is to protect the national borders after an armed attack (red square in Figure 5), or else in an international setting during United Nations (UN) or NATO military missions. The national police can use force to maintain public order or to enforce the law, but solely in a national context, while agencies including the National Cyber Security Centre operate nationally without using force. Intelligence services can operate in the entire arena but only to execute a specific task under strict conditions.[46] The security actors cover the threat landscape but are largely mutually exclusive by design based in legal frames, thematic focus and governmental responsibilities.

Conversely, operations in cyberspace, especially digital influence operations (when used as a manipulative and deceptive instrument of power) are predominantly below the threshold of the use of force and have effects in an international setting – the grey area in figure 5.[47] This excludes activities of the armed forces which traditionally operate above the threshold of the use of force, or law enforcement agents which are governed by and limited to national jurisdiction. As a result, solely intelligence agents can, and have the authority to, act. Problematic is that intelligence agencies – while a capable and effective asset - are not designed for influence operations. Moreover, the intelligence agencies have capacities that are adjusted (hence limited) to their task and are unable to cope with all malign, foreign influence operations threatening the Netherlands.

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

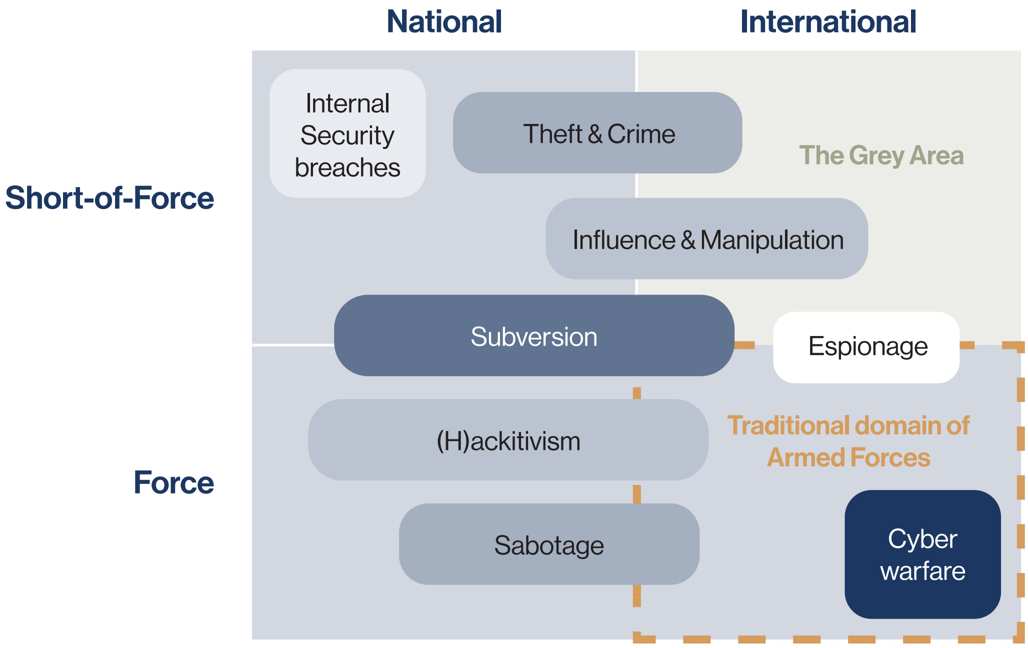
[44] Art. 97(1) Constitution of the Kingdom of the Netherlands.

[45] Voo et al., "National Cyber Power Index 2020."; Voo, Hemani, and Cassidy, "National Cyber Power Index 2022."

[46] See articles 8 and 10 for the tasks of the General resp. Military Intelligence and Security Service, General Intelligence and Security Service, "The Intelligence and Security Services Act 2017."

[47] Bos and Pijpers, "Cyberoperaties in de Gray Zone - Juridische Overwegingen Omtrent de Rol Voor de Krijgsmacht."

Figure 5. The information environment landscape



8.2. On the legal frame

During deployment the Netherlands armed forces have a clear task, authority and legal mandate to operate also in the wider information environment. However, during mission-preparation or when acquiring a level of readiness these the armed forces cannot rely on this mandate and will have to find a legal base in national legislation.[48]

To be able to defend, and execute offensive operations, against an opponent it is necessary to train and maintain a level of readiness. In military terms this would entail learning how to handle a riffle and conduct military exercises in fictional nations such as Skolkan, Occasus or 'Redland'.[49] Apart from a level of readiness, security agents, when earmarked for a specific deployment, need to prepare for that mission – switching from Skolkan to the actual security landscape in Mali, Iraq or Afghanistan, the powerbroker and the ecosystem of friendly, neutral, and opposing actors on site. This mission-related preparation occurs in the Netherlands (i.e. outside the mission area) during peacetime before the actual mandate (national or via the UN) starts.

The cyberspace-enabled information environment is difficult to align with traditional demarcations (of national or international jurisdictions, and between armed conflict and peace) the existing legal framework is a poor fit for operations in the grey area, where the main commodity is (personal) data. Armed forces are able to observe, acquire and analyse data to obtain intelligence and understanding, they are not allowed to gather personal data, a difference that is not always easy to make online. Personal data is and should be protected safe

[48] This includes elements of EU legislation, such as the GDPR, which have a direct application in the Netherlands. One of the national legal regimes is the Intelligence and Security Services Act 2017.

[49] Derksen, "360° Scope Scenario Design and Development in JWC."

for issues of national security for which exemptions exist in privacy legislation, including the GDPR. Baltic states use these exemptions while Germany and the Netherlands revoked them.

There is a flaw in the legal frame related to the cyberspace-enable information environment.[50] While the Netherlands armed forces have an obligation to deploy in all domains and dimension in order to protect national interests, they lack the mandate to learn the skills for the deployment. How can one acquire hacking skills or a level of readiness to influence target audiences if peacetime (privacy) legislation applies in full? How can one gain intelligence, situational awareness if one is not allowed to use (personal) data from Internet and social media – the information repositories of our times?

9. **Reflection**

Influence operations, as an element of information manoeuvre, apply non-kinetic means to gain an advantage over the opposing audiences by outmanoeuvring them using information. Information manoeuvre could be defined as: "means using information as a source for understanding and decision-making but also as a means to act, thereby generating informational effects in the cognitive, virtual or physical dimension (directly or indirectly), using information as a target, vector or weapon to ultimately affect the cognitive dimension of audiences, friend or foe."[51]

Manipulative influence operations lure audiences away from rational decision-making processes towards biased judgements with the aim to change the attitude and behaviour of the targeted state. Cyberspace-induced manipulative influence operations are similar to traditional deceptive operations, but characteristics such as pre-emption, dislocation and disruption are now transfigured to cyberspace, using (personal) data and information as the main tool of influence. In that sense, deception still is the way of warfare. Or rather; the inception of cyberspace has made it even more manipulative and deceptive.

Paradoxically enough, the larger the opportunities in the information environment, enabled by cyberspace, the less the Netherland utilises its armed forces to create (defensive or offensive) effects. Reason for this is that the bulk of malign and deceptive operations in the information environment take place in the grey area below the use of force with transnational effects. An area where not only states but also proxies, non-state actors, private firms and individuals act.

To defend the Netherlands against manipulative influence operations via cyberspace, two actors emerge each with sufficient handicaps. The armed forces have a constitutional task and substantial manpower to defend the vital interests of the Netherlands but, despite the wording in the Defence Vision 2035, have – due to national limitations – no legal mandate or authority to act in the information environment. The Intelligence services have a mandate but are limit in tasks and capacity. Hands-on practical solutions have arisen; in the so-called Cyber Mission Teams capacity of the armed forces work with the Intelligence service under the latter's legal mandate. While these initiatives must be applauded, they remain suboptimal as they reflect the deficiencies in the Netherlands' conceptual and legal setting.

[50] Ducheine, Pijpers, and Pouw, "Information Manoeuvre and the Netherlands Armed Forces: Legal Challenges Ahead."

[51] Pijpers and Ducheine, "'If You Have A Hammer': Reshaping the Armed Forces' Discourse on Information Maneuver."

Legislation protecting the users of social media and the internet will only grow in number, also by the EU. These legislations, including the GDPR, however, always offer exemptions for purposes of national security and defence, which must be considered based on national vital interests. Dismissing these exemptions all together is certainly an idealistic legislative prerogative but blind to realistic geopolitical consequences. After all, '*кто контролирует сферу ИКТ, тот контролирует мир*'.[52]

Paradoxically enough, the larger the opportunities in the information environment, enabled by cyberspace, the less the Netherland utilises its armed forces to create (defensive or offensive) effects.

[52] Meaning: "who controls the ICT sphere controls the world", a modernized version of Rothschild's "who controls money controls the empire", in Melnikova, "International Telecommunication Union: Technical Regulator or Arena for New Confrontation?"

Peter B.M.J. Pijpers Ph.D. is an Associate Professor Cyber Operations at the Faculty of Military Sciences of the Netherlands Defence Academy in Breda, and PhD researcher at the University of Amsterdam. Dr Pijpers is a Colonel (GS) in the Netherlands Army and has been deployed four times including to Iraq and Afghanistan.

Brigadier-General **dr. Paul A.L. Ducheine** is the Professor for Cyber Operations and Cyber Security at the Netherlands Defence Academy, and a Legal Advisor (Netherlands Army Legal Service). At the University of Amsterdam, he was named professor by special appointment of Law of Military Cyber Operations.

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