The Hague Centre
for Strategic Studies

# Information-based behavioural influencing in the military context

## Mapping current expert thinking

Lotje Boswinkel, Michel Rademaker and Sofia Romansky

June 2022

The Hague Centre
for Strategic Studies

# Information-based behavioural influencing in the military context
## Mapping current expert thinking

**Authors:**
Lotje Boswinkel, Michel Rademaker and Sofia Romansky

**Contributors:**
Stella Kim and Ricardo Pereira Teixeira

June 2022

This production is being 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 in the military context, dissecting the ethical, legal and military-strategic issues and boundaries involved. Responsibility for the contents rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Royal Netherlands Army.

# Table of contents

# Introduction

In information warfare, information-based capabilities are employed to target human cognition, seeking changes in attitudes, perceptions and behaviour. While physical manoeuvres can do just that, here the military seeks to influence behaviours by manipulating the flow of information. Even if information has always been used to shape adversary thinking and decision-making, major advancements in information and communications technologies but also cognitive psychology have added to their centrality.[1] As a result, state and nonstate actors have ramped up efforts to exploit and manipulate the information environment for tactical, operational and strategic purposes. With influencing efforts becoming increasingly pervasive, Western military organisations are shifting their attention accordingly. Since NATO published its Allied Joint Doctrine for Information Operations in 2009,[2] information has also taken an increasingly prominent place in national military doctrines and operations.[3] For instance, the British Army launched the 77th Brigade, a force specialised in psychological operations and the use of social media; the Royal Netherlands Army formally introduced a 'branch of information manoeuvre; and the French Ministry of Defence developed a special doctrine for its conduct of information operations.[4]

Participants from the Netherlands, Belgium, France, Germany and the UK reflected on the available, relevant and desirable military actions to influence behaviours in the information environment

To further discussions on and advance our understanding of the use of information to influence behaviours in conflict, the Royal Netherlands Army has commissioned the *Platform Influencing Human Behaviour*. As part of this project, The Hague Centre for Strategic Studies brought together a group of international experts and practitioners with both military and non-military backgrounds to explore and discuss the broad variety of information-related capabilities that could potentially be employed by armed forces. Using three scenarios of relevance to European armed forces, twenty-two participants from the Netherlands, Belgium, France, Germany and the UK reflected on the available, relevant and desirable military actions to influence behaviours in the information environment. The scenarios were either fictional or historical, and included six different audiences that were located either on NATO/EU territory or outside of that. In all scenarios, NATO was in the process of generating forces. Crucially, five out of six audiences were civilian, but not necessarily friendly. Participants were instructed to, as much as possible, disregard any potential legal, ethical or moral inhibitors to their choices of what capabilities to implement as the exploration of such limitations fell beyond the scope of the workshop. Instead, participants were asked to brainstorm freely and creatively about the potential use and effects of information-related capabilities to complement military actions and achieve favourable outcomes. The discussions held between the experts during the scenario workshop can be summarised in eight main observations.

[1] Alicia Wanless and Michael Berk, "The Changing Nature of Propaganda," in *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, ed. Timothy Clack and Robert Johnson (Routledge/Taylor & Francis Group, 2021), https://www.taylorfrancis.com/chapters/edit/10.4324/9781003046905-16/information-warfare-robert-johnson.

[2] NATO, "AJP-3.10 Allied Joint Doctrine for Information Operations" (NATO Standardization Office, November 23, 2009), 2, https://info.publicintelligence.net/NATO-IO.pdf.

[3] See for instance Ministry of Defence, "Netherlands Defence Doctrine" (The Hague, June 2019), https://english.defensie.nl/downloads/publications/2019/06/27/netherlands-defence-doctrine; Ministère des Armées, "Strategic Update 2021" (DICoD - Bureau des Éditions, January 2021).

[4] Ewen MacAskill, "British Army Creates Team of Facebook Warriors," *The Guardian*, January 31, 2015, https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade; KAP Arthur van Beveren, "KL creëert wapen van de informatiemanoeuvre," Koninklijke Landmacht, accessed November 16, 2021, https://doi.org/10/02_wapen-van-de-informatiemanoeuvre; Ministère des Armées, "Florence Parly présente la doctrine militaire de lutte informatique d'influence," October 21, 2021, https://www.defense.gouv.fr/actualites/articles/florence-parly-presente-la-doctrine-militaire-de-lutte-informatique-d-influence.

# Observation 1
## Messages and deeds

Coherence between messages and deeds is typically deemed crucial for the effective and legitimate implementation of information-based capabilities by democratic actors, especially when it comes to civilian audiences. These considerations can be summarised in two main dimensions: consistency and controllability.

First, when influencing civilian populations, democratic actors should avoid using mutually contradicting capabilities. It can be problematic – and even counterproductive – to spread messages about freedom and cooperation while simultaneously using capabilities that obstruct said values. To illustrate, it is debatable whether it is at all possible to align the restrictive message sent by blocking access to communication for an audience while simultaneously using this audience to, for instance, build a common network for open dialogue with hostile forces. Instead, transparency-promoting capabilities can be preferable, such as the creation of a friendly media environment to raise awareness about bilateral defence cooperation through influencer level engagement and population engagement. Individuals that are perceived to be neutral who voluntarily spread positive messages – so-called earned communicators – play a particularly crucial role here. In this way, consistency between messages and deeds could be explicitly conveyed.

Using false information is only an option when engaging enemy forces in tactical operations with short-term goals

Second, truthful messages may be easier to control and hence more useful than disinformation. This is true for civilian audiences but also military ones. The use of false information can easily be disproven, resulting in the interruption of strategic planning and loss of legitimacy.[5] Moreover, in today's information environment, operations are unlikely to remain local. Social media allows for news to instantly go global, increasing the probability that disinformation will eventually be uncovered. As such, it is nearly impossible to continuously maintain false information. Furthermore, even true narratives are likely to change and be questioned as they are interpreted online. With this in mind, saturating an information sphere with more misinformation may make it more difficult for the truth to surface. That said, capabilities involving disinformation need not be entirely abandoned but, instead, tied to very specific conditions. Using false information is effectively only an option when engaging enemy forces in tactical operations with very short-term goals – but indeed only if the information environment is highly restricted.

[5] Still, untruthful information can be effective, as is explained in the first publication of the *Platform Influencing Human Behaviour*: Lotje Boswinkel et al., "Weapons of Mass Influence: Shaping Attitudes, Perceptions and Behaviours in Today's Information Warfare" (The Hague Centre For Strategic Studies, April 20, 2022), https://hcss.nl/report/weapons-of-mass-influence-information-warfare/.

## Observation 2
## **Audience understanding**

The effectiveness of any behavioural influencing campaign is contingent on a thorough understanding of the audience. An analysis of audiences and the complex societal structures they are embedded in must occur prior to the implementation of any informational capability. Unsurprisingly, therefore, accounting for information-gathering capabilities in military planning is crucial. It is debatable what would actually constitute a sufficient level of situational awareness; what is required to obtain adequate audience understanding; and whether complete understanding is possible. As such, behavioural influencing campaigns should always be approached with great caution. Generally, a sufficient level would vary depending on the desired effects of capabilities but should encompass an understanding of the audience's language, culture, and media environment. There are various sophisticated and structured approaches to determine which audience to target, why and how.[6] Finally, it remains debatable how long information-gathering takes. Indicated timelines range from a few weeks to a year and a half. This variation depends on the ease with which an audience could be accessed due to a conflict's stage, intensity, and cultural proximity.

## Observation 3
## **Capability maturity**

Sufficient levels of maturity of both information-gathering and behavioural influencing capabilities are crucial but not always guaranteed. It has been argued that in some approaches to information gathering, there is insufficient focus on culture and in creating intercultural understanding between the conflict and intervening armed forces. What is more, not enough time is dedicated to a thorough analysis of a state's information architecture. However, these criticisms of deficiency do not go unchallenged, and audience analysis capabilities vary across NATO allies.

[6] For an overview of tools, see for instance "Tools voor toepassing gedragsinzichten," Behavioural Insights Netwerk Nederland (BIN NL), accessed June 2, 2022, https://www.binnl.nl/kennisbank/tools/default.aspx.

Yet, a key weakness of both information-gathering and influencing capabilities is measurement. While on a practical level many behavioural influencing capabilities are feasible, the scale at which they can be implemented and their impact is dubious. There are few mechanisms for assessing the effects of informational capabilities, specifically assessments of whether messages were delivered and understood. Often, the tools that could be used for influence-measurement are not sufficiently developed or examined in the military context. Moreover, deciding on operationalisations of effects as well as having access to data has proven to be difficult, even in academic spheres.

Trial and error is one effective way to conduct behavioural influencing operations. By testing a tactic on a small scale first, its effects can be closely observed and evaluated, without the risk of causing large-scale harm. This way, campaigns can be carefully finetuned and, when proven successful, incrementally expanded.

Behavioural influencing can be questionable when implementation timelines do not match military ones

## Observation 4
## **Deciding who does what, and when**

When it comes to behavioural influencing in the military context, inevitably questions arise as to *who* gets involved *when*. Therefore, additional discussions should take place as to who should conduct audience analysis and carry out behavioural influencing campaigns, and when such operations are to take place.

Whether behavioural influencing, including audience analysis, should be conducted by the armed forces or other branches of government continues to be the subject of intense debate. These discussions closely relate to questions about when to get involved in information operations as a foreign military at all. If the resolution of a conflict could be reasonably expected to be the responsibility of a domestic government, then the involvement of a foreign military would not be legitimate. Especially when it comes to NATO allies or fellow EU member states, behavioural influencing may be considered the responsibility of the host country. Second, the suitability of some behavioural influencing capabilities can be questionable when implementation timelines do not match military ones. Indeed, psychological research has shown that for information to take hold, long exposure is necessary, but not all military missions are of sufficient duration. Finally, both legal and doctrinal restrains may hinder action in the informational environment and the implementation of behavioural influencing capabilities.

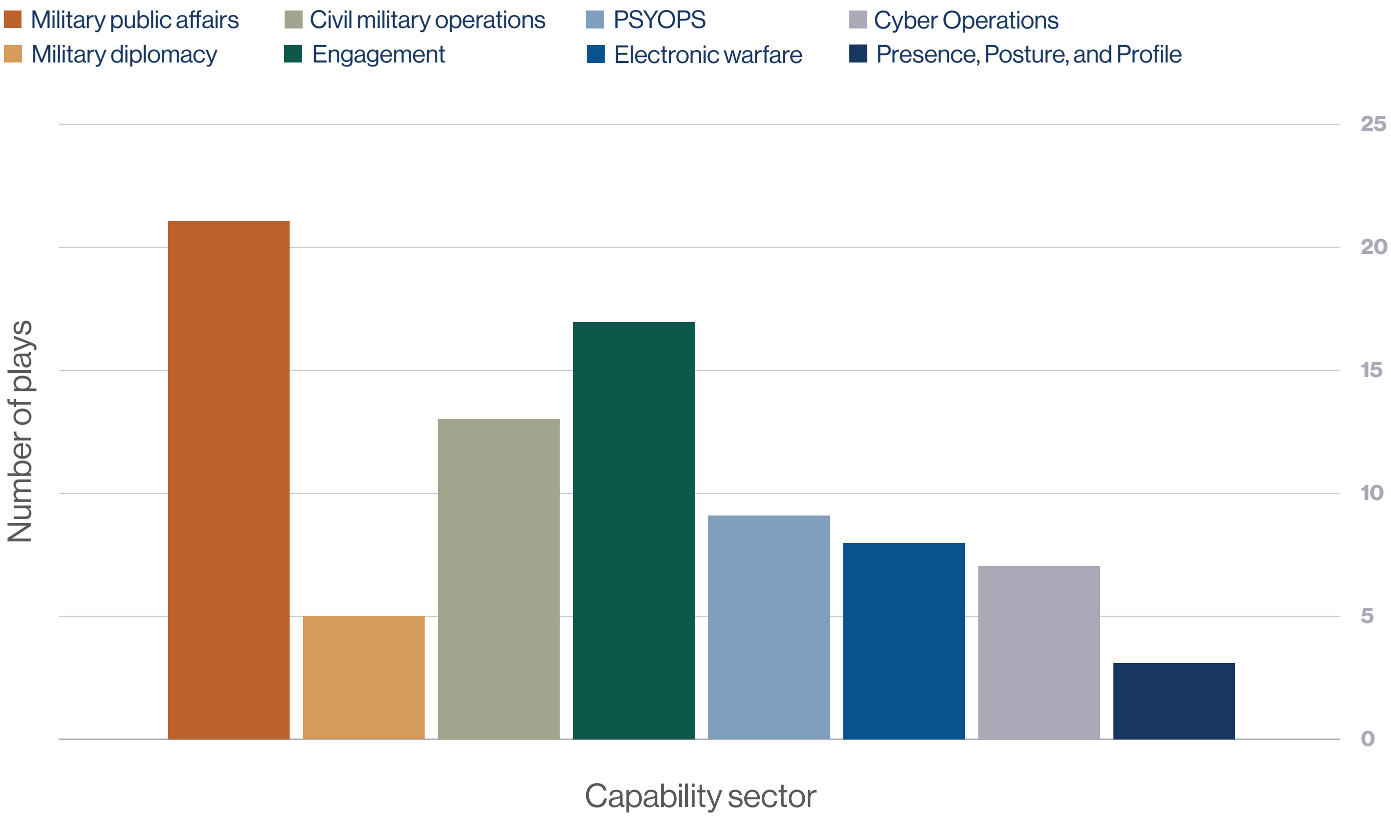
# Observation 5
## Better safe than sorry

During the scenario workshop, the capabilities that were implemented the most were those related to military public affairs and engagement (see Figure 1).[7] Meanwhile, electronic warfare and cyber capabilities were implemented less frequently.[8] Though considered effective, such capabilities were deemed controversial when used to influence civilian populations, whether friendly, neutral or enemy (but less so when used against enemy forces). When trying to align deeds and messages, electronic warfare and cyber capabilities would be difficult to effectively combine with other capabilities for a desired effect. What is more, especially in pre-conflict settings, these capabilities were seen as most likely to escalate a situation as 'technical' capabilities could be more easily interpreted as attacks. Instead, safer approaches based on soft power that also target root causes of conflict were preferred, for instance capabilities in the military public affairs and engagement sectors that make use of networks of cooperation and the reach of social media. Within these sectors, narrative persuasion and influencer level engagement capabilities were implemented the most (see Figure 2). Across scenarios, narrative persuasion often served as the cornerstone of behavioural influencing operations, with other capabilities supporting the central message. Meanwhile, influencer level engagement was perceived as most directly linked to social media, and therefore the fastest way to reach an audience. The parallel implementation of both military public affairs and engagement capabilities was especially relevant when participants considered whole-of-government approaches. Here, involvement could create ground for reconciliation and sustainable peace.

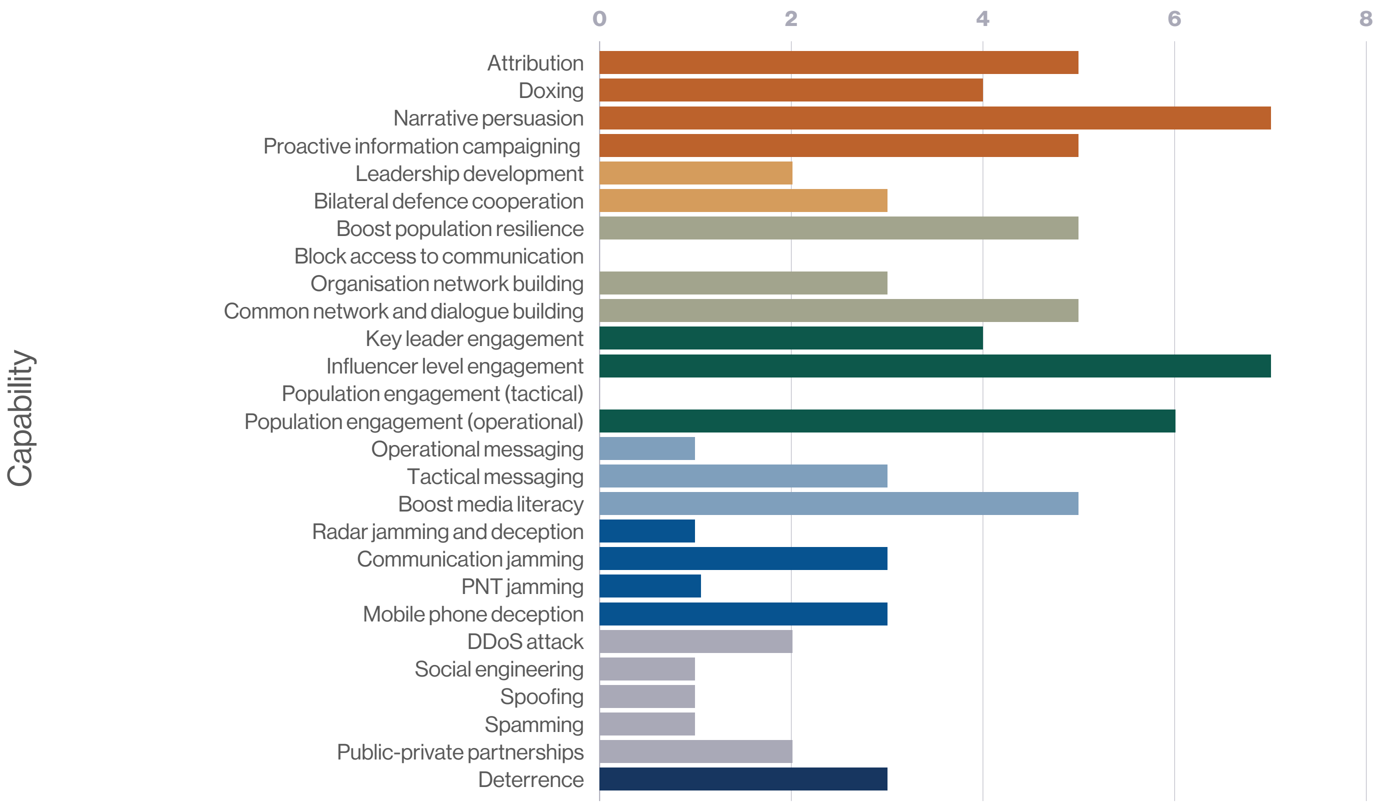
[7] For an overview of behavioural influencing capabilities, see Annex A.

[8] This bias may also be a result of participants' backgrounds.

## Figure 1. Frequency of sector implementation



## Figure 2. Frequency of capability implementation



## Observation 6
## Combining capabilities

Information-based influencing capabilities should not be implemented in isolation but in conjunction with other such capabilities. For instance, when engaging the networks of a particular audience, key leaders are typically engaged too as they are important nodes in a network. The rationale behind this is two-fold. First, the implementation of one capability would almost inevitably lead to the implementation of another capability, as the processes of the capabilities are either intertwined or closely connected. Second, and crucially, often the effectiveness of one capability can be bolstered when it is underpinned by other capabilities. This is true for broad capabilities like narrative persuasion, proactive information campaigning, and boosting media literacy. To get the messages of the capabilities across, multiple channels and networks would have to be engaged.

## Observation 7
## Integrating domains

Behavioural influencing takes place in multiple domains and includes physical manoeuvres. For instance, when it comes to deterrence missions, physical manoeuvres in presence, posture and profile can be effectively complemented with information capabilities such as communication jamming or narrative persuasion. The integration of domains not only increases the effectiveness of deterrence, but also allows for a framework for the implementation of information capabilities. Effectively, implementing a behavioural influencing campaign to support deterrence as the cornerstone of a mission remains easier in current thinking.

The current shift to high-intensity warfare inevitably carries with it a shift in the information warfare paradigm

## Observation 8
## From low-intensity to high-intensity warfare

Over the last few decades, Western militaries have mostly prepared for and been involved in low-intensity conflict. Behavioural influencing experts within military organisations are therefore predominantly trained in the implementation of information-based capabilities during expeditionary missions or so-called wars of choice, such as the missions in Iraq and Afghanistan. The focus here lies with influencing audiences' hearts and minds. Therefore, assumptions about how information capabilities work are shaped by a specific subset of operations. The current shift to high-intensity warfare inevitably carries with it a shift in the information warfare paradigm, with practical but also potential ethical and legal implications. Indeed, capabilities targeting civilian audiences that were generally eschewed in expeditionary missions such as in Bosnia, Iraq and Afghanistan, could be less controversial when facing existential threats.

# Conclusion

Even if not a new concept, the scale at which information and communication technologies advance changes the way in which militaries perceive and conduct behavioural influencing. In addition to the new centrality of information in societies, other developments, such as rising casualty aversion and the shift to high-intensity warfare shed new light on information-based behavioural influencing in military contexts.

Moving into this new era, some degree of humility is in order, for three reasons. First, behavioural influencing is relatively immature and understood relatively poorly, especially in comparison with military manoeuvres in the physical environment. Even when understanding and capabilities improve, information gathering, and situational awareness will always be bounded as financial resources are tight, cultural knowhow restrained and access limited. What is more, there will always be limits to what influencing can achieve. Second, democratic societies are at a disadvantage. Western military organisations are tasked to defend and therefore also embody the values of the societies that employ them, and therefore their room for manoeuvre in the information environment is inherently restricted. Even when fighting a high-intensity war, some capabilities may still be off the table. Third, information supremacy or even superiority is unattainable. Contrary to for instance the air domain, in information warfare there will always be contesters, also from within, and no single actor can fully control the information flow. This is the case everywhere but especially in open societies. Compatibility of messaging and deeds is therefore preferred, and every behavioural influencing capability carries the risk of backfiring. Safe choices may therefore prevail but not always be the most effective.

There will always be limits to what behavioural influencing can achieve

Finally, advancing behavioural influencing in the military context is not just contingent on capability development. Somewhat paradoxically perhaps, for campaign designers to think freely and creatively, clearer boundaries need to be established and communicated. These can be legal, doctrinal, and ethical. If this is not the case, opportunities will be missed out of fear for societal condemnation. To achieve increased clarity, societal awareness and acceptance also need to be bolstered. What is more, discussions need to take place with regard to the task division between the various governmental agencies and departments. Establishing who is responsible under which circumstances for which parts of behavioural influencing campaigns is clearly a precondition for any such operation to take place.

# Annex

| Sector | Capability | Symbol | Channel | Capability description & effect | Example activities |
|---|---|---|---|---|---|
| **Military Public Affairs** | Attribution | 🔍 | Official channels, media | Attribute hostile (cyber) activities to impose costs, shape public opinion, deny the hostile actor's ability to manipulate facts, bolster a society's resilience, and unlock (multilateral) action. | Publishing intelligence service assessments, disclosing intelligence information to selected high-profile media outlets. |
| | Doxing | 📢 | Official channels, media | Expose a hostile actor's information network, activities, or capabilities by releasing credible intelligence in order to deny the hostile actor the opportunity to use these capabilities in a covert way. | Declassifying evidence about an adversary's military plans. |
| | Narrative persuasion | ♡ | Official channels, media | Develop and promulgate compelling narratives (in line with the higher level narrative) to support the military operational objectives. | Raising societal awareness, gathering support for responses to hostile actor, communicating external threats, signalling military preparedness. |
| | Proactive information campaigning | ? | Official channels, media | Provide accurate information in a timely manner to maintain credibility with the public, internal audiences, and media, as well as deter adversary propaganda. | Maintain an open information channel where the local population can refer to for fact-checking and updates to foster trust in their government. |
| **Military Diplomacy** | Leadership development | 👥 | Military interaction | Engage proactively in the training and development of knowledge to bring friendly actors in an advantageous position. | Combined training exercises with foreign military organisations, official visits, officer exchange programmes, military contacts with foreign officials. |
| | Bilateral defence cooperation | 🤝 | Military interaction | Military-to-military cooperation to deter and reassure. | Bilateral and multilateral contacts between senior military and civilian defence officials; appointment defence attachés; bilateral defence cooperation agreements; providing military support and aid with material and equipment. |

| Sector | Capability | Symbol | Channel | Capability description & effect | Example activities |
|---|---|---|---|---|---|
| Civil Military Operations | Boost population resilience | | | Identify and engage with susceptible groups to prevent the hostile actor from working with them. | Empowering NGOs and the local media to engage with minorities to keep them aligned with the country's values and policies. |
| | Block access to communication | | Social media, radio, TV, internet, newspapers. | Request to legally block access to communication and information infrastructure to decrease a target actor's possibility to communicate with one's society. | Block the use of mobile phones, landline, email servers, websites, data servers, radio, or TV. |
| | Organisation network building | | | Build relationships with civil actors (NGOs, media, businesses) to gain support and shape the target actor's agenda. | Liaising, coordination and funding of political movement or NGOs; recruitment of journalists. |
| | Common network and dialogue building | | | Build a network of dialogue to inform both civilians and governments about the state of affairs, potential threats, and protective measures to foster resilience and status of the government. | Buttress the local or national authorities by providing information about potental threats and protective meassures. |
| Engagement | Key Leader Engagement | | Face-to-face | Engage key military and political leaders to achieve strategic effect. | Military Force Commander conducts a meeting with influential military and political leaders |
| | Influencer Level Engagement | | Face-to-face | Engage with key communicators/influencers to achieve tactical effects with relatively little effort. The key communicators are well known and seen as trustworthy by their audience. | Tactical PSYOPS Team conducts a meeting with influential religious/military/ethnic/political/cultural leaders or social media influencers. |
| | Population Engagement (tactical) | | Face-to-face | Engage with the local population to achieve limited tactical effects within a small audience. Soldiers can be seen as more approachable by the local population. | Infantry soldiers talk to local population in the streets. |
| | Population Engagement (operational) | | Social media platforms | Participate actively in online conversations with populations in social media platforms using layperson's terms for effective engagement. | Employ listening, educational, and awareness-raising tools in social media. |

| Sector | Capability | Symbol | Channel | Capability description & effect | Example activities |
|---|---|---|---|---|---|
| **PSYOPS** | Operational messaging | 🎙 | Radio, TV, social media, mass media print campaign, leaflet drops | Shape the information environment (long-term) to achievie operational effects by changing attitudes and beliefs of the audience. | Spread rumours about military or political leaders; display (potentially false) information on a government website; broadcast (potentially false) information on an own radio station, TV, YouTube channel and other social media channels; spread (potentially false) information about banks and enterprises. |
| | Tactical messaging | 📣 | Radio, TV, social media, mass media print campaign, loudspeaker, leaflet drops | Shape the information environment to achieve an immediate tactical effect on enemy troops or local population without having to get into direct contact or firing range. | Disseminate leaflets; display (potentially false) information on a government website; broadcast (false) information on enemy radio messages (using EW); provide information about food products in shops; provide soldiers (potentially false) information about their friends and family. |
| | Boost media literacy | 📰 | Social media, radio, TV, newspapers | Reduce vulnerability to disinformation by ensuring availability and accessibility of accurate information. | Make media available in minority languages. |
| **Electronic Warfare** | Radar jamming and deception | 📡 | Electro-magnetic spectrum | Saturate radar receivers with noise or false information in order to complicate the reading of real target signals. | Transmit additional electro-magnetic signals; employ decoys to deceive a radar operator. |
| | Communication jamming | 📶 | Communication systems | Interrupt communications between combat-net radio's as well as mobile phones and base towers to interfere with adversary decision-making. | Disturb the mobile phone or combat-net radio signals in an area where a hostile actor operates. |
| | PNT jamming | 🛰 | Positioning, Navigation, and Timing (PNT) systems | Prevent someone from determining their current and desired position, applying corrections to course, orientation, and speed. | Send a competing signal that obstructs Global Nativagtion Satellite System receiver from decoding satellite input. |
| | Mobile phone deception | 📱 | Mobile phone | Deceive mobile phone users to disrupt information flow. | Provide mobile phones in a particular area with wrong information by using an own base station. |

| Sector | Capability | Symbol | Channel | Capability description & effect | Example activities |
|---|---|---|---|---|---|
| Cyber Operations | DDoS attack | 💻 | | Render various websites and systems unusable for some time to disturb a society | Conduct DDoS attacks on websites of the Ministry of Interior and the Ministry of Culture; put botnets (malware) in the military supply system and in the cargo handling system of a major harbour. |
| | Social Engineering | 😈 | Interactive communication systems | Exploit a target audience's cognitive biases by tricking their confidence to willingly disclose sensitive information. | Vishing, Phishing, Spear Phishing, Pretexting, Smshing, Water holing, Baiting, Tailgating. |
| | Spoofing | 🤡 | Interactive communication systems | Falsify one's identity or authentication credential to gain (illegitimate) access to information or financial resources. | |
| | Spamming | ✉ | Interactive communication systems | Send unsolicited messages in bulk and indiscriminately to cause disruption or interruption of activites. | |
| | Public-Private Partnerships | 🏢 | | Establish information exchange channels with tech-companies to track down cyber- and informational operations more efficiently and disrupt threats. | Cooperate with social media providers (Facebook, Instagram, Twitter, TikTok) to track information. Cooperate with Internet Service Providers (ISPs). |
| Presence, Posture and Profile | Deterrence | 💪 | | Deploy force to send message. | Deploy combat troops or capabilies, conduct military exercises. |

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