"If You Have a Hammer…": Shaping the Armed Forces' Discourse on Information Maneuver

Pijpers, P.B.M.J.; Ducheine, P.A.L.

DOI
10.1080/08850607.2023.2197560

Publication date
2023

Document Version
Final published version

Published in
International Journal of Intelligence and CounterIntelligence

International Journal of Intelligence and CounterIntelligence, 36: 1164–1183, 2023
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2023.2197560

Routledge
Taylor & Francis Group

PETER B.M.J. PIJPERS AND PAUL A.L. DUCHEINE

"If You Have a Hammer …": Shaping the Armed Forces' Discourse on Information Maneuver

Peter B.M.J. Pijpers, Ph.D., is an Associate Professor of Cyber Operations at the Faculty of Military Sciences of the Netherlands Defense Academy and a researcher at the Amsterdam Centre of International Law, University of Amsterdam. He is a Colonel in the Netherlands Army and has been deployed to Iraq and Afghanistan. He was seconded to the European Union (EU) External Action Service and serves as a defense advisor to the EU Delegation for Libya. The author can be contacted at b.m.j.pijpers@uva.nl.

Paul A.L. Ducheine is Professor for Cyber Warfare at the Netherlands Defense Academy and endowed Professor of Law of Military Cyber Operations at the University of Amsterdam. Brigadier-General Ducheine studied Public Administration (Free University, Amsterdam) and Constitutional Law (Utrecht University) and holds a Ph.D. in Law (University of Amsterdam). He served at Headquarters 1 (German/Netherlands) Corps, 1 (Netherlands) Division "7 December" and Multinational Division South-West SFOR (NATO Stabilization Force) in Bosnia-Herzegovina. The author can be contacted at p.a.l.ducheine@uva.nl.

Abstract: The dawn of cyberspace has been conducive to unlocking the potential of the information environment. As a result, armed forces embrace concepts of engagement in the information environment, in cyberspace, and especially in information maneuver—the concept of generating effects in the information environment. Unfortunately, some within the military remit perceive information maneuver as the "2.0 version" of existing intelligence capabilities emphasizing the digitization of the battlefield. While enhanced intelligence, understanding, and decisionmaking are essential, information maneuver is, above all, a means to act and generate effects in the cognitive, virtual, or physical dimension similar to deception, propaganda, or covert actions. The concept of information maneuver must not be seen as an "add on" to existing capabilities within the military instrument of power but instead as a way of exerting power and achieving effects within the remit of information as an instrument, away from the traditional physical military approach to conduct operations.

> Among the logical fallacies formulated by the Ancient Greeks, the causal fallacy is understood to occur when two events that appear together or follow one another are presumed to have a causal relationship, rather than just appear before or next to the other.[1]
>
> Where you sit, depends on where you stand.[2]

On 10 May 2020, Major General Cole, the UK Army's director of information, addressed an audience at the Royal United Services Institute (RUSI) Information Maneuver Conference, arguing that "information maneuver involves the use of information in all its forms to understand the operating environment better than anyone else and subsequently to make the most of that advantage. The aim is simultaneous to shape perceptions to ensure the Army's activities and intentions are appropriately recognized by allies, populations and adversaries."[3]

Maneuvering in the information environment, or information maneuver, is one of the latest topics in doctrinal thinking,[4] and not only in the military realm. In the precyberspace era, however, operations in the information environment, apart from military deception operations, were a secluded remit predestined for intelligence and security services,[5] especially where national interests are concerned. The emergence of cyberspace has unlocked the information environment (e.g., via social media), and, compared to some decades ago, access to and usability of the information environment has expanded exponentially, deluging the traditional domains of (military) engagement (land, air, and sea). Consequently, an abundance of new actors with a global reach has entered the security arena, meaning new opportunities for communication, competition, and conflict.[6]

To be more successful than others (competitors or opponents) implies gaining a superior position to advance one's interests, hence to "outmaneuver" others (even if only temporary and locally), which is a truism valid for the military,[7] as it is for marketing campaigns. As with many new developments, actors seize these cornucopian concepts to advance their position and interests. The military realm is no exception and cynically speaking, the latest generation of jet fighters and submarines, but also the land forces that operate among the people,[8] are sometimes framed as the acme of "maneuvering-in-the-information-environment," especially by the services themselves.

Although armed forces have used information and intelligence since the beginning of humankind to acquire understanding, improve decisionmaking, and execute operations, many (Western) military institutions find it—paradoxically—difficult to get their heads around the concept of information maneuver.[9] Due to their enemy-centric tenure,[10] it appears that Western armed forces focus on enhancing and improving the connectivity of existing information and communication technology (ICT) infrastructure for intelligence collection, understanding, and support of decisionmaking,[11] hence gaining an advantageous position during the preparatory phases of physical military activities.

The concept of information maneuver must, however, not be seen as an "add on" to existing capabilities in the traditional land, sea, and air domain within the military instrument of power.[12] Instead, information maneuver is a way of exerting power and achieving effects within the remit of information as an instrument, away from the traditional physical military approach to conducting operations.

Although improved interoperability, robust ICT systems, and better understanding of the environment and opponents must be applauded, this is only half the story[13]: the center of gravity of information maneuver is to use information not only to "understand" and subsequently to "decide," but also to "act." The latter entails using information in any cognitive, virtual, or physical form to shape the operational environment of other actors (i.e., opponents) advantageously, but moreover to use information as a weapon of influence—concepts that border deception, propaganda, or covert action.[14]

Information maneuver is not an uncontested notion that makes a reflection on the role of the armed forces in the concept of information maneuver appropriate, thereby contributing to the ongoing discourse on what originated information maneuver, what it entails, and how to place the armed forces therein.

Aware of country-specific organizational and legal structures,[15] a division between "armed forces" and "Intelligence Communities" (ICs) is made as a

point of departure.[16] The former is an inherently physical asset for armed conflict, at least in the contemporary Western military tradition, while the latter focus on national security (not only military) issues in the wider spectrum of (and between) war and peace, but predominantly below the use of force. Furthermore, information in this article relates to all cognitive, virtual, and physical forms, such as ideas, images, binary code, words, sounds, or explosions.

To give substance to the reflection on the role of the armed forces in the concept of information maneuver, the origin of information maneuver is revisited, arguing that cyberspace has unlocked the information environment, thereby inundating all other domains, and consequently overwhelming the existing capabilities of ICs and armed forces. After that, it is argued that the concept of information maneuver does not solely encompass intelligence gathering for understanding and to support decisionmaking, but is also a means to act (i.e., use information as a "weapon" to influence and to target the information environment [i.e., cyberspace] itself). Finally, before the conclusions, the role of the armed forces in information maneuver is alluded to.

CYBERSPACE: THE CATALYST TO INFORMATION MANEUVER

The main objective for states is to protect and further their vital interests.[17] To do so, states will cooperate with other states, but they could also employ instruments to exert power trying to persuade, coerce, or manipulate other states to change their position.[18] Depending on the goal to be achieved, instruments of power related to economy, information, diplomacy, or the military can be implemented in one or several traditional domains or via cyberspace; the domain is the area where the actual engagement with the (audiences of the) other states takes place.[19]

While diplomatic means, a cultural exchange, or installing economic sanctions are what Nye would call means of soft power to further and protect national interests,[20] the military instrument of power will be an obvious state's choice when in (armed) conflict, "compelling adversaries through the threat or application of physical power in the form of destructive or disruptive force to achieve victory."[21] For pursuing physical effects, states most likely turn to their armed forces.[22]

Apart from the instruments mentioned above, states can also employ their informational instrument of power, which refers to how states use data and knowledge to understand and shape the complex nature of the information environment to further national interests.[23] Although this may have constructive effects, informational instruments can also aim to disrupt other actors' ability to direct objective content to its target audience, to properly grasp reality, and to establish effective defensive action capability.[24]

ICs, but also armed forces' psychological operations, have traditionally used means of influence, including deception, propaganda, and covert action, to pursue effects in the informational environment. Deception entails "deliberate measures to mislead targeted decision-makers into behaving in an [advantageous] manner."[25] Propaganda can be defined as the "dissemination of information in support of government policy,"[26] which can be applied in an overt ("white") manner that includes forms of strategic communication (StratCom),[27] or more covert and with malign intent ("black") to deceive or mislead opponents,[28] and "manipulate perceptions in support of one's cause or to damage an adversary."[29] Covert action is a "programme to influence a foreign audience to alter its policies or actions in ways that benefit or support the goals of the government that is conducting it and which mask the original sponsorship of that government."[30] At the top of the ladder of covert action, destructive (cyber) campaigns intend to destabilize or punish other states rather than influence political decisions.[31]

While operations in the information environment are nothing new, what is new is that with the inception of cyberspace, new opportunities for human interaction have been introduced. And cyberspace activities,[32] with the Internet and social media as the engagement area (i.e., the "battlefield"), have been far more influential than propaganda was in the past.[33]

The information environment can be (conceptually) divided it into three dimensions (see Figure 1). The physical dimension encompasses geolocations and all tangible objects and persons. The cognitive dimension entails people's individual and collective ideas, values, knowledge, perceptions, and wisdom.

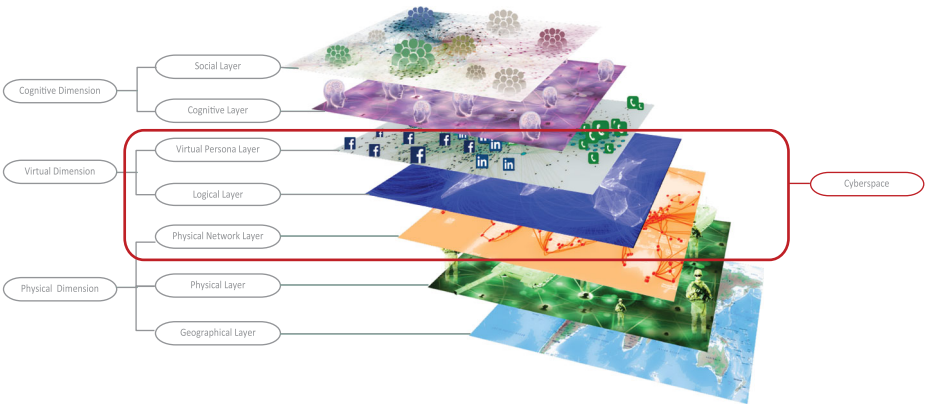

Figure 1. Information environment and cyberspace. See Paul A. L. Ducheine, Jelle van Haaster, and Richard van Harskamp, "Manoeuvring and Generating Effects in the Information Environment," *ACIL Research Paper 2017-25* (2017), p. 6; see also Jelle van Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict" (PhD Thesis, 2018), p. 173, note 898, https://dare.uva.nl/search?identifier=26737c1c-8be3-4147-ad13-1ff63ea972bc

The virtual dimension relates to where and how information is digitally collected, processed, stored, and disseminated.

Cyberspace can be positioned in the information environment. The scope of cyberspace consists of three layers in two dimensions. First, the physical network layer of hardware, the computers, cables, and hubs in the physical dimension.[34] The two components in the virtual dimension are the cyber objects (logical layer of software and data) and the cyber identities (i.e., the virtual persona layer entailing the reflections of persons or groups, enabling them to interact on the Internet and social media).

The new virtual layers provide a gateway to the information environment. In that sense, cyberspace has "unlocked" the information environment, not as an instrument or a weapon as such, but "an enabling environment that allows actors to transmit information to large audiences at low cost, near instantaneously, through multiple distribution points, across borders and with heightened opportunities for anonymity."[35] In addition, many physical objects, such as cars or weapon systems, are somehow connected to cyberspace and thus potentially accessible via cyberspace. Moreover, via cyberspace, insight in perceptions, attitudes, and so on can be quickly established.

Therefore, when states (maliciously) employ power, they often avoid the traditional domains of engagement but instead seek to address, interact with, or confront other actors (including opponents) in the elusiveness of cyberspace.[36] Apart from espionage via cyberspace, activities in cyberspace can be divided into actions that affect the three layers of cyberspace itself—the so-called hard-cyber operations or digital sabotage[37]—and actions that use cyberspace as a vector to affect the cognitive dimension—the soft-cyber or digital influence operations.[38]

Cyberspace has been the catalyst to transform traditional activities in the informational environment into information maneuver. And because cyberspace inundated the traditional domains of (military) engagement (land, sea, air), information maneuver is no longer confined to the undercover world of the IC, but defensive and offensive activities related to information maneuver via cyberspace are a concern for all, including the armed forces that have the monopoly of state violence.

The essence of maneuvering in the information environment is to gain a competitive advantage over (opposing) audiences by using information as a source to assess and understand actors (i.e., opponents) and their environment, to decide and to engage their information environment (especially cyberspace), and to use information as an instrument (a "weapon") to influence the cognition of those audiences, to affect (i.e., to undermine) the deliberate understanding and autonomous decisionmaking process of targeted audiences.

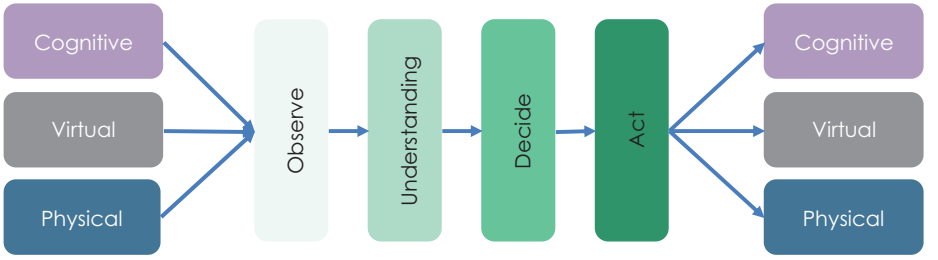

Figure 2. Information maneuver.

In order to gain effects—that is, to cooperate with, persuade, coerce or manipulate (opposing) actors resulting in a change of position—information maneuver activities gain data and information from observing the environment. The intelligence produced, combined with knowledge and experiences, generates understanding of the situation offering insight and foresight that is used to decide what to do and subsequently how to act (Figure 2).[39] Acting entails employing diplomatic, economic, informational, or military means to achieve effects in the cognitive, virtual, or physical dimension.

INFORMATION MANEUVER AS A CONCEPT

Information maneuver as a concept, but also cyberspace as the fifth domain of (military) operations,[40] has been embraced by armed forces that—in the Western military culture—predominantly operate in, and are organized to conform to, the traditional physical domains of engagement: land, sea, and air.

Armed forces have tried to amalgamate these novel concepts in the military instrument of power, their traditional base of statecraft. Because military effects in Western contemporary culture are traditionally realized by using physical force as a weapon, it stands to reason that armed forces employ information maneuver as an upgraded collection process of military intelligence, what we will refer to as "intelligence 2.0." The aim of military intelligence is to "provide situational awareness, develop understanding,"[41] and "feed information into resilient and responsive C2 [Command and Control] structures, better informing the force and enabling faster decision-making."[42] Hence, armed forces want to have an "information edge"[43] in the preparatory phase of the operation,[44] to create kinetic effects in the physical dimension (see Figure 3).

But information maneuver entails more than "intelligence 2.0" or enhanced military intelligence. During the 2016 U.S. presidential election, cyberspace-enabled activities were executed by agents of the Russian Federation (RF). The RF agents hacked the ICT infrastructure of the

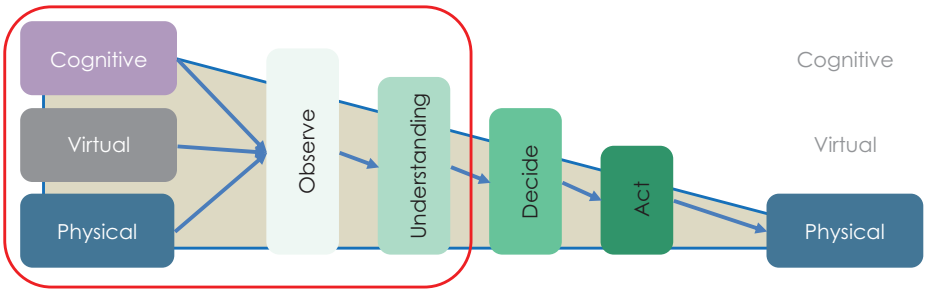

Figure 3. Intelligence 2.0.

Democratic National Congress and Hillary Clinton's campaign team, retrieving valuable and compromising data, especially about Clinton.[45] The data were later used—as a "weapon" of influence—to undermine the integrity of candidate Clinton, thereby affecting the cognitive dimension of U.S. voters.

Information maneuver should not be seen as an "add on" to existing military doctrine within the employment of the military instrument of power that focuses on action and effects in the physical dimension but as an exponent of the informational instrument of power with the purpose to affect the deliberate understanding and autonomous decisionmaking process of targeted audiences. In the concept of information maneuver, information will not only be used as a source to gain intelligence and understanding and to support decisionmaking but moreover as a means to alter the opposing information environment by weaponizing information to influence target audiences in the cognitive dimension, or to engage with the virtual and physical dimensions of the information environment (i.e., via cyberspace), itself.

Information as a Source to Understand and Decide

The first and foundational element of information maneuver is the use of information to gain understanding and subsequently insight and foresight to support decisionmaking. Gaining information about other actors, including opponents, but also about the environment in which one operates is a crucial precondition for success.

The digitization of the information environment has changed the collection of intelligence. Cyberspace has affected our societies through an exponential increase in processing power,[46] storage capacity for data, and transmission speed facilitated by the dematerialization of data,[47] making cyberspace a repository of data, and thereby a trove for digital espionage.[48] However, because large parts of data are publicly available (via open source social media platforms), the data are available to all interested parties. Intelligence

and understanding can be generated using network-based ICT systems and algorithms and big data analysis.[49] Tech companies (Facebook, Alphabet) already use these techniques, as well as political consultancy firms (Cambridge Analytica), without relying on espionage.

Digitization will also make large quantities of data available for the armed forces, enabling them to gain enhanced intelligence, understanding, and ultimately insight and foresight regarding the operational environment (i.e., the battlefield) as a whole and the opponent's intent and positions in particular. It will also support and accelerate decisionmaking on who, when, and what to engage or target and will, in turn, result in more precise or bespoke activities and a more efficient use of assets.

Because military intelligence collection concentrates on opponents and their operational environment, their focus is generally type-casted as "enemy-centric" and related to the preparatory phase of military action. During this phase, intelligence activities include human intelligence but also computer network exploitation activities (gaining nonconsensual access to ICT infrastructure of opposing forces and retrieving data)[50] that can take place without damaging cyberspace (i.e., without degrading or deleting cyber objects [software or data] and cyber identities [accounts]).

Using information as a source to gain intelligence and understanding can—if decided so—result in an act affecting the cognitive, virtual, or physical dimension. Enhanced military intelligence can still lead to a traditional physical act aiming for effects in the physical dimension (as depicted in Figure 2). Although such action will be executed more surgically due to increased intelligence, effects could also be achieved using information—ranging from software to words, sounds, pictures, or footage—as a means to act affecting other dimensions (i.e., virtual or cognitive).

Information as a Means to Act

The second and core element of information maneuver is the use of information in any form to affect the information environment of other or opposing audiences (i.e., engaging with informational [nonkinetic] effects in the physical, virtual, and cognitive dimension of actors whose attitude and behavior require change). The pinnacle of all employments of instruments of power is a change in the cognitive dimension of other actors. However, because this dimension cannot be addressed directly, signaling is required using the virtual or physical dimension as a vector.[51]

Ultimately, to achieve such cognitive effects, the information environment, more prominently cyberspace, is used as a vector. Activities can target the other state's cyberspace, and can even weaponize information to influence specific groups, audiences, or individuals within (or related to) other states. Information maneuver uses information as a weapon of influence to achieve

ultimately effects in the cognitive dimension, and as a target obtaining effects in the virtual or physical dimension—the hard-cyber operations.

On Influence Operations

Influence operations, which use information as an instrument (weapon), aim to change the attitude (and subsequent behavior) of opposing actors by "the deliberate use of information by one party on an adversary population to confuse, mislead and ultimately influence the actions that the targeted population makes."[52]

Digital influence activities use cyberspace as a vector with the aim of targeting the cognitive dimension.[53] Although these digital influence operations can be exerted in every domain, cyberspace is particularly apt for influencing other states or audiences within that state.

Present-day digital influence operations, which are not exclusively executed by intelligence services,[54] use coercive, persuasive, or manipulative techniques.[55] Coercion and persuasion are rational, conscious activities. Until now, apart from deception operations, most informational activities the armed forces use are persuasive in nature (e.g., public affairs activities or StratCom to, referring to Cole's earlier quote, shape perceptions to ensure the activities and intentions are appropriately recognized)[56]; in effect, to form "white" propaganda. Coercive activities (whether executed by armed forces or ICs) are traditionally executed using physical, not informational, means. Manipulative influence operations aim to circumvent subconsciously the rational processing of incoming data. When deceiving, confusing, and misleading are the intent, manipulative influence operations will be the instrument or weapon of choice.

The core principle of manipulative influence operations is to lure target audiences into making judgments based on heuristics or mental rules of thumb—what Petty and Cacioppo call the peripheral route.[57] Cyberspace is inducive to deflect persons and groups to make biased judgments, because

> (a)lthough the volume and velocity of information has increased by orders of magnitude in the past few decades, the architecture of the human mind has not changed appreciably in the last few thousand years, and human beings have the same cognitive and perceptual limitations that they have always had.[58]

The heuristics cannot be addressed directly because these are neural processes of persons or groups. Heuristics can, however, be invoked by techniques including an overload or shortage of data,[59] scarcity in time, but moreover, in altering the content of a message or the source of the message,[60] which is the essence of "weaponizing" information. Information is

weaponized if specific narratives or frames are applied.[61] Other techniques entail disinformation,[62] misleading news outlets (e.g., Russia Today or Sputnik)[63] or false social media accounts, impersonating the target state's nationals.[64] All these elements will impair the ability of target audiences to value the incoming information or give significance to the data, deflecting them toward heuristics.

On Hard-Cyber Operations

The digitization of the information environment has generated new opportunities to target: the physical network layer (hardware), cyber objects (software, data), and cyber identities (i.e., user accounts, websites).[65] Apart from using the information environment (including cyberspace) as a vector to use information as an instrument, a weapon, during influence operations, the three layers of cyberspace can also be targeted.[66]

Hard-cyber operations use information and data to target these three layers of cyberspace and have an effect *in* cyberspace by altering, disabling, disrupting, hijacking, or destroying hardware, software,[67] or virtual persona.[68] The attacks change the attributes of the cyber identities, cyber objects, or—indirectly—the physical network (the hardware) by emplacing malware (malicious software), manipulating data, or through a distributed digital denial of service attack,[69] as was the case in Estonia (2007), Georgia (2008), and Ukraine (2022).[70] The result will be that the virtual dimension and/or the physical network layer of cyberspace are/is impaired or that data are disclosed,[71] as occurred during the 2016 U.S. presidential election. Targeting the virtual dimension of the information environment can even have effects in the physical dimension,[72] as was the case during the Stuxnet attack (2010),[73] or the hacking of the power grid during the 2015 Ukrainian power outage,[74] and the ViaSat satellite at the onset of the 2022 Russian invasion in Ukraine.[75]

Undermining and sabotaging the virtual dimension and the physical network layer can also benefit armed forces during conflict. The result of this is the malfunctioning of the Global Positioning System–supported fire support systems for artillery,[76] or undermining and impairing the enemy's command and control systems,[77] to deteriorate the virtual dimension (virtual persona, logical layer) and physical network layer (hardware) of opponents to hamper them to exploit vulnerabilities.[78]

THE ROLE OF ARMED FORCES IN INFORMATION MANEUVER

Even though states are regularly affected, even "attacked" by other states trying to achieve informational effects via cyberspace, or apply cyber

operations during an armed conflict, information maneuver is not necessarily restricted to war(fare). The interactions (or infringements) in the informational remit or via cyberspace seldom reach the force threshold. They are, despite the current use of cyber operations in Ukraine, predominantly engagements outside armed conflicts.

Furthermore, the "targeted" actors or actors engaged are not always "enemies" in a military sense. These could be allies or agitators,[79] ranging from white hackers, whiz kids, disgruntled employees, (cyber)criminals to advanced persistent threats or intelligence agencies and state-sponsored cyber groups. Moreover, foreign acts of information maneuver, especially the hard-cyber and influence operations, predominantly affect the economic, diplomatic, or informational realm instead of the military.

This renders the question of whether armed forces—outside conflict and war—have a role to play in the wider concept of information maneuver. To make an assessment, several issues need to be taken into account. First of all, information maneuver, when solely used as enhanced military intelligence ("intelligence 2.0"), can still result in achieving effects in the physical dimension, which in general remains the prerogative of the armed forces. Second, because cyberspace has unlocked the information environment, the traditional domains (land, sea, and air) of engagement are deluged by a virtual dimension.

This assessment results in a dilemma. Armed forces are, on the one hand, not the most prominent agents to act in case of a peacetime nonkinetic cyberspace-related interference with an effect within a state. While, on the other, because cyberspace has made the information environment widely accessible, activities in the informational realm—including cyberspace-related influence and (hard) cyber operations—are no longer the exclusive realm of the IC alone.

To defy this conundrum, the employability of armed forces in the information environment needs to be revisited. In armed conflict, the armed forces can first be used as a stand-alone entity when an information maneuver results in a physical operation affecting the physical dimension. Second, armed forces can be employed to achieve (defensive or offensive) effects with (hard) cyber operations, in the virtual dimension, either alone or in tandem with intelligence agencies, cognizant that the latter have different objectives and authorities. Cooperation and synchronization of efforts would be beneficial, not least due to the vastness and the number of ongoing (hard) cyberattacks.

Close collaboration would also be favorable when activities take place in a domestic setting during peacetime. One could even argue that by generating effects in the cognitive dimension via digital influence operations or executing digital espionage, the armed forces could be supportive.

Due to the focus of armed forces on traditional domains (land, sea, air) and on the generation of military (physical) effects, the pitfall is when armed forces execute digital influence operations or activities in the broader concept of information maneuver during peacetime, a physical mindset or "hammer" is applied to achieve a goal, as they would be during armed conflict.

Therefore, when employing the concept of information maneuver, armed forces will need to shift focus from a predominantly physical stance to an informational approach, especially because the informational instrument of power is often employed in a situation short of force and outside war (armed conflict). The military instrument is the embodiment of the threat or use of force in physical operations—the hard power of the state.[80] As such, it can be used for offensive or defensive physical deployment of power, but also deterrence by the show of force or showing a clear sign of resolve. Conversely, information as an element of power refers to the way a state uses information—data and knowledge—to shape the environment in an enduring effort to support national interests. The latter implies a different set of norms, ethics, and rules. The armed forces will need to change their attitude and enlarge their toolbox and be able to adjust their mindset and manner of operating to the changing paradigms in which to operate.[81] Activities supporting law enforcement agencies in a national setting follow domestic legislation instead of the laws of armed conflict during war.

In sum, when using the concept of information maneuver, the intelligence and knowledge required should not only be enemy-focused. Furthermore, for successful cyber and especially influence operations, data, information, and intelligence of targeted audiences is required related to all dimensions of the environment and all audiences, including domestic and supporting audiences. Finally, information should not solely be used as a prerequisite to plan operations and to reduce uncertainty on the one hand, but information should also be used to exploit the opponents' quest to reduce uncertainty on the other side.[82]

In the concept of information maneuver, different information is required during planning, decisionmaking, and executing the operation. Apart from military intelligence, information is needed as a means to act and shape the information environment to impose one's will on other actors; hence, information used as a weapon as an alternative to kinetic means.

CONCLUSION

All in all, information maneuver is a concept that can be utilized to generate effects in cognitive, virtual, and physical dimensions. Using information as a source for enhanced (military) intelligence (including via digital espionage), understanding and decisionmaking can result in a kinetic and military operation with an effect in the physical dimension. However, the acme of

information maneuver is to use information also as a means to act to generate effects, for example, through the employment of hard-cyber operations to affect the virtual (and physical) dimension by targeting the three layers of cyberspace or through the use of information as a weapon to influence the cognitive dimension of the targeted audience via digital influence operations.

Activities in the information environment have been around for ages, including deception, espionage, propaganda, and covert actions (i.e., sabotage).[83] The emergence of cyberspace has changed these activities fundamentally as it has deluged the traditional domains of engagements with a virtual layer, thereby unlocking the information environment as an area open to all—state and nonstate actors that have access to and partake in cyberspace.

Owing to the overwhelming vastness of cyber-enabled activities employed in the information environment, primarily due to cyberspace, the existing capacities in this remit—the intelligence services and psychological teams within armed forces—are insufficient to counter foreign activities in the information environment, let alone employ assertive activities. Neglecting activities in the information environment, enabled by cyberspace, is not an option because influence operations via cyberspace and the hacking of ICT systems by state or nonstate actors are not hypothetical but happen on a daily basis.

Armed forces and intelligence agencies can—and will have to—join efforts to effectively execute information-enabled activities in cyberspace in a comprehensive manner within their respective mandates. But a precondition is that armed forces will need to revisit their perception on understanding the environment, the language, culture, and values applicable to achieve informational effects, especially during digital influence operations.

If the armed forces want to use the full breadth of information maneuver, they will need to adopt a different stance and frame of thinking and need to realize that other protocols, norms, ethics, and rules apply—similarly to when military service personnel would operate in the diplomatic realm. When operating in peacetime, the context of activities within the informational instrument of power will most likely be under the authority of the civil authorities (i.e., national police, law enforcement, or intelligence agencies); or will be mandated based on a national justification (legal basis) to protect vital interests abroad within a given legal regime.[84]

Using the military "hammer"—the physical approach used in armed conflict—will prove ineffective, especially in achieving effects in the virtual and cognitive dimension outside conflict.

REFERENCES

[1] Raphael Sassower, "Causality and Correlation," *The Wiley-Blackwell Encyclopedia of Social Theory* (2017), https://doi.org/10.1002/9781118430873.est0585.

[2] Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971).

[3] Jonathan Cole, "Manoeuvring into the Future of Information Manoeuvre," The UK Army, 2020, https://www.army.mod.uk/news-and-events/news/2020/03/manoeuvring-into-the-future-of-information-manoeuvre/

[4] The term *information maneuver* was coined in UK Army doctrine (e.g., British Army, *Force Troops Command Handbook*, 2019, pp. 3–4; UK Army Doctrine Note 19/04, "Information Manoeuvre," 2019). See also: Paul A. L. Ducheine, Jelle van Haaster, and Richard van Harskamp, "Manoeuvring and Generating Effects in the Information Environment," in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis—NL ARMS 2017*, edited by Paul A. L. Ducheine and Frans P. B. Osinga (The Hague: Springer T.M.C. Asser Press, 2017).

[5] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020).

[6] Paul A. L. Ducheine and Peter B. M. J. Pijpers, "The Notion of Cyber Operations," in *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar, 2021), pp. 271–272; David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War," *New York Times*, 28 February 2022, https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

[7] Marinus, "Marine Corps Maneuver Warfare: The Historical Context," *Marine Corps Gazette* (August 2020).

[8] Rupert Smith, *The Utility of Force: The Art of War in the Modern World*, 2nd ed. (New York: Alfred A. Knopf, 2007), pp. 374 ff.

[9] There are numerous instruments of power, often concisely captured with the acronym DIME. Reynolds approaches information maneuver dominantly from the military instrument of power. Our argument is that it should dominantly be viewed from the Informational instrument of power. Nick Reynolds, "Performing Information Manoeuvre Through Persistent Engagement," *RUSI Occasional Paper* (2020).

[10] Craig A. Dudley, "Information-Centric Intelligence: The Struggle in Defining National Security Issues," *International Journal of Intelligence and CounterIntelligence*, Vol. 31, No. 4 (2018), pp. 758–768.

[11] IBM, "Informatie Gestuurd Optreden: Van Overzicht Naar Overwicht" (IBM, 2020), https://www.ibm.com/downloads/cas/NWLGBZMY

[12] John Arquilla, *Bitskrieg: The New Challenge of Cyberwarfare* (Polity, 2021), pp. 74–75.

[13] Mick Ryan, Tammy Smith, and Patrick Donahoe, "Why We Tweet: General Officer Use of Social Media to Engage, Influence, and Lead," *Strategic Bridge*

(2020), https://thestrategybridge.org/the-bridge/2020/9/7/why-we-tweet-general-officer-use-of-social-media-to-engage-influence-and-lead.

[14] Alexander Nicholas Shaw, "Propaganda Intelligence and Covert Action: The Regional Information Office and British Intelligence in South-East Asia, 1949–1961," *Journal of Intelligence History*, Vol. 19, No. 1 (2020), pp. 51–76.

[15] Ducheine and Pijpers, "The Notion of Cyber Operations," p. 288.

[16] Ilkka Salmi, "Why Europe Needs Intelligence and Why Intelligence Needs Europe: 'Intelligence Provides Analytical Insight into an Unpredictable and Complex Environment,'" *International Journal of Intelligence and CounterIntelligence*, Vol. 33, No. 3 (2020), pp. 464–470, at p. 466.

[17] Netherlands Ministry of Foreign Affairs, "Working Worldwide for the Security of the Netherlands—An Integrated International Security Strategy 2018–2022." Netherlands Ministry of Foreign Affairs Policy Document, published in Dutch in 2018. UK version: https://www.government.nl/documents/reports/2018/05/14/integrated-international-security-strategy-2018-2022

[18] Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," *Georgetown Law Technology Review*, Vol. 4, No. 1 (2019), pp. 1–52.

[19] See also: Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *U.S. Naval War College International Law Studies*, Vol. 89 (2013), pp. 123–156, at p. 123. See also: Joseph S. Nye, Jr., "Cyber Power" (2010), p. 7; François Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?," *Israel Law Review*, Vol. 52, No. 3 (2019), pp. 295–326, at pp. 304–305.

[20] Joseph S. Nye, Jr., "Soft Power," *Foreign Policy*, No. 80 (1990), pp. 153–171.

[21] U.S. Department of Defense, "Joint Concept for Operating in the Information Environment (JCOIE)," 2018, p. 1.

[22] When the U.S. Central Intelligence Agency uses drones to neutralize insurgents abroad this overseas intelligence agency generates a kinetic effect. See: Eric Schmitt and Matthew Rosenberg, "C.I.A. Want Authority to Conduct Drone Strikes in Afghanistan for the First Time," *New York Times*, 15 September 2017.

[23] Jeff Farlin, "Instruments of National Power: How America Earned Independence" (U.S. Army War College, 2014), p. 5, https://publications.armywarcollege.edu/publication/instruments-of-national-power-how-america-earned-independence/. Or, as Myres S. McDougal and Florentino P. Feliciano, "International Coercion and World Public Order: The General Principles of the Law of War," *The Yale Law Journal*, Vol. 67, No. 5 (1958), pp. 771–845, at p. 793 put it: when speaking about the "ideological instrument" as it was referred to then: "The use of the ideological instrument commonly involves the selective manipulation and circulation [of] symbols, verbal or non-verbal, calculated to alter the patterns of identification, demands and expectations of mass audiences in the target-state and thereby to induce or stimulate politically significant attitudes and behavior favourable to the initiator-state."

[24] Daniel Cohen and Ofir Bar'el, "The Use of Cyberwarfare in Influence Operations," Blavatnik Interdisciplinary Cyber Research Center (2017), p. 8.
[25] NATO, *Glossary of Terms and Definitions* (AAP-06 Edition 2021).
[26] Shaw, "Propaganda Intelligence and Covert Action," pp. 3–4.
[27] Joris Van Esch and Simon Hirst, "How to Operate in the Information Environment," *Militaire Spectator*, Vol. 189, No. 9 (2020), pp. 456–465, at pp. 459–460.
[28] Han A. J. H. Bouwmeester, *Krym Nash: An Analysis of Modern Russian Deception Warfare* (Dissertation, University of Utrecht, 2020) https://dspace.library.uu.nl/handle/1874/400504; Edwards L. Bernays, *Propaganda*, 2nd ed. (New York: Horace Liveright, 1928).
[29] Shaw, "Propaganda Intelligence and Covert Action," p. 18.
[30] Ibid., pp. 17–18.
[31] Loch K. Johnson, "On Drawing a Bright Line for Covert Operations," *American Journal of International Law*, Vol. 86, No. 2 (1992), pp. 284–309, at p. 286; Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, DC: Georgetown University Press, 2020), pp. 109–110.
[32] Gary Brown, "Spying and Fighting in Cyberspace: What Is Which?," *Journal of National Security Law and Policy*, Vol. 8, No. 3 (2016), pp. 621–636, at pp. 627–630.
[33] Holger Möldera and Vladimir Sazonovb, "Information Warfare as the Hobbesian Concept of Modern Times—The Principles, Techniques, and Tools of Russian Information Operations in the Donbass," *Journal of Slavic Military Studies*, Vol. 31, No. 3 (2018), pp. 308–328, pp. 308–309.
[34] Others argue that cyberspace includes the geographical layer (Jelle van Haaster, "On Cyber: The Utility of Military Cyber Operations During Armed Conflict" [2018], p. 128), or even all seven layers. See an exposé in Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), p. 46.
[35] Herbert S. Lin and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," in *Oxford Handbook of Cybersecurity* (Oxford University Press, 2019), pp. 1–29, at pp. 11–14; Eric Jensen, "Cyber Sovereignty: The Way Ahead," *Texas International Law Journal*, Vol. 50, No. 2 (2015), pp. 275–304, at p. 279.
[36] For instance, the U.S. doctrine of Persistent Engagement. See: United States Cyber Command, "Achieve and Maintain Cyberspace Superiority" (2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf
[37] Peter B. M. J. Pijpers and Kraesten L. Arnold, "Conquering the Invisible Battleground," *Atlantisch Perspectief*, Vol. 44, No. 4 (2020), pp. 12–14.
[38] Dale Stephens, "Influence Operations & International Law," *Journal of Information Warfare*, Vol. 19, No. 4 (2020), pp. 1–16, at p. 2.
[39] See also UK's JDP-04 Understanding and Decision-Making, https://www.gov.uk/government/publications/jdp-04-understanding

[40] North Atlantic Treaty Organisation (NATO), "Warsaw Summit Communiqué," No. July (2016), Bullet 70.
[41] NATO, "Allied Joint Doctrine or the Conduct of Operations–AJP 3" (2019), pp. 1-23 to 1-24.
[42] Reynolds, "Performing Information Manoeuvre Through Persistent Engagement," p. 35.
[43] Arquilla, *Bitskrieg*, pp. 17–24.
[44] DCDC, "JDP 04 2nd Edition—Understanding and Decision-Making" (2016), Section 3, pp. 18–25.
[45] Robert S. Mueller, "Report On the Investigation Into Russian Interference in the 2016 Presidential Election," vol. I and II, pp. 24–26 (Washington D.C.: U.S. Department of Justice, March 2019), https://www.justice.gov/archives/sco/file/1373816/download
[46] Salmi, "Why Europe Needs Intelligence and Why Intelligence Needs Europe," p. 465.
[47] Roy van Keulen, "Digital Force: Disrupting Life, Liberty and Livelihood in the Information Age," Disseration, Universiteit Leiden, 2018.
[48] Russell Buchan and Inaki Navarrete, "Cyber Espionage and International Law," in *Research Handbook on International Law and Cyberspace* (2nd ed.), edited by Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2021), pp. 231–52, at p. 233.
[49] Keith Dear, "Artificial Intelligence and Decision-Making," *RUSI Journal*, Vol. 164, No. 5/6 (2019), pp. 18–25; Erik van de Sandt, Arthur van Bunningen, Jarmo van Lenthe, and John Fokker, "Towards Data Scientific Investigations," *Rephrain* (2021), https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2021/03/White-Paper-Towards-Data-Scientific-Investigations.pdf
[50] Alexander Klimburg (ed.), *National Cyber Security: Framework Manual*, *NATO CCD COE Publication*, vol. 6 (Tallinn: NATO CCD COE Publication, 2012), pp. 157–158.
[51] Francois du Cluzel, "Cognitive Warfare" (Innovation Hub, 2021), pp. 6–7.
[52] Lin and Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," p. 4.
[53] Bradley Boyd and Herbert S. Lin, "Affecting the Cognitive Dimension of the Information Environment through Cyber-Enabled Information Operations," *Journal of Information Warfare*, Vol. 18, No. 3 (2019), pp. 49–66, at p. 50.
[54] Aristedes Mahairas and Mikhail Dvilyanski, "Disinformation—(Dezinformatsiya)," *The Cyber Defense Review*, Vol. 3, No. 3 (2018), pp. 21–27, at pp. 23–26, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/CDR_V3N3_Full.pdf; Jakub Janda, "The Lisa Case: STRATCOM Lessons for European States," *Federal Academy for Security Policy*, No. 11 (2016), pp. 1–4.
[55] Susser, Roessler, and Nissenbaum, "Online Manipulation."
[56] See reference 4.

[57] See among others: Richard E. Petty and John T. Cacioppo, "The Elaboration Likelihood Model of Persuasion," *Advances in Experimental Social Psychology*, Vol. 19 (1986), p. 126.
[58] Herbert S. Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," *Lawfare* (2018), https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations
[59] Möldera and Sazonovb, "Information Warfare as the Hobbesian Concept of Modern Times," p. 323.
[60] Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, Vol. 185, No. 4157 (1974), pp. 1124–1131.
[61] Filippo Tansini and Yakov Ben-Haim, "Strategies for Communicating Information and Disinformation in War," in *The Conduct of War in the 21st Century*, edited by Robert Johnson, Martijn Kitzen, and Tim Sweijs (Routledge, 2021), pp. 58–71.
[62] Michela Del Vicario et al., "The Spreading of Misinformation Online," *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 113, No. 3 (2016), pp. 554–559, at p. 558.
[63] Ilya Yablokov, "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)," *Politics*, Vol. 35, No. 3–4 (2015), pp. 301–315, at pp. 303–304.
[64] James Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf," *Journal of Cyber Policy*, Vol. 4, No. 2 (2019), pp. 235–256, at p. 240; Nye, Jr., "Cyber Power," pp. 2 and 5.
[65] Although any medium can be used to convey messages, communicating information or data is currently mainly sent via digital channels at the expense of oral or paper means.
[66] M. A. Thomas, "Distinguishing Cyberattacks by Difficulty," *International Journal of Intelligence and CounterIntelligence*, Vol. 35, No. 4 (2022), pp. 784–805.
[67] Sergio Castro, "Towards the Development of a Rationalist Cyber Conflict Theory," *The Cyber Defense Review*, Vol. 6, No. 1 (2021), pp. 35–62, at p. 38.
[68] Ducheine, Haaster, and Harskamp, "Manoeuvring and Generating Effects in the Information Environment," pp. 2 and 15; Kello, *The Virtual Weapon and International Order*, pp. 51–53; Nye, Jr., "Cyber Power." p. 6.
[69] Castro, "Towards the Development of a Rationalist Cyber Conflict Theory," p. 38.
[70] Aaron F. Brantly, "The Cyber Deterrence Problem," *International Conference on Cyber Conflict, CYCON* (Tallinn: NATO CCD COE Publications, May 2018), pp. 31–53, pp. 42–43, https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf; Laurens Cerulus, "Kyiv 's Hackers Seize Their Wartime Moment," *Politico* (2022), https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/
[71] Pijpers and Arnold, "Conquering the Invisible Battleground," pp. 12–13.

[72] Paulo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal* (2011), pp. 1–11, https://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf

[73] See, for example, the 2010 Stuxnet attack on the Natanz nuclear installation. Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*. Vol. 22, No. 3 (2013), pp. 365–404.

[74] Robert Lee, Michael Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *SANS Industrial Control Systems Security Blog*, 2016.

[75] Erica D. Lonergan, "The Cyber-Escalation Fallacy: What the War in Ukraine Reveals About State-Backed Hacking," *Foreign Affairs* (On-Line Snapshot, 15 April 2022), https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy; Paul A. L. Ducheine, Peter B. M. J. Pijpers, and Kraesten L. Arnold, "Bits- or Blitzkrieg? Cyber Operations in the Russia-Ukraine War," *Atlantisch Perspectief*, Vol. 46, No. 3 (2022), pp. 42–47.

[76] Dustin Volz, "Russian Hackers Tracked Ukrainian Artillery Units Using Android Implant: Report | Reuters," *Reuters*, 22 December 2016.

[77] Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," *Wired*, 2022.

[78] United States Cyber Command, "Achieve and Maintain Cyberspace Superiority," pp. 4–6.

[79] Ryan Gallagher, "The Inside Story of How British Spiers Hacked Belgium's Largest Telco," *The Intercept* (2014), https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

[80] McDougal and Feliciano, "International Coercion and World Public Order," p. 795.

[81] Ducheine and Pijpers, "The Notion of Cyber Operations," para, 4, "Applicable Cyber Paradigms for States."

[82] Thomas Waldman, "Shadows of Uncertainty: Clausewitz's Timeless Analysis of Chance in War," *Defence Studies*, Vol. 10, No. 3 (2010), pp. 336–368, at p. 350.

[83] Rory Cormac, "Techniques of Covert Propaganda: The British Approach in the Mid-1960s," *Journal of Intelligence and National Security*, Vol. 1, No. July (2019), pp. 105–112; William J. Daugherty, "Covert Action: Strengths and Weaknesses," in *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson (Oxford University Press, 2010), pp. 609–610.

[84] Paul A. L. Ducheine and Peter B. M. J. Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework," in *Deterrence in the 21st Century—Insights from Theory and Practice*, edited by Frans P. B. Osinga and Tim Sweijs (Springer, 2021), pp. 475–500.