Information and Communication Technology Companies on the Battlefield: Explanations and Implications

E.H. Pouw, P.A.L. Ducheine, B.M.J. Pijpers & K.L. Arnold[1]

Abstract

The war in Ukraine witnessed an influx of non-state actors on the battlefield, including ICT-companies (ICTC), such as Microsoft or Starlink. The war in Ukraine – and most likely all future war – will have a substantial cyberspace dimension. Since the ICTC own and control the largest part of cyberspace state rely on them to generate fighting power – the main source of the military instrument of power. States need their informational infrastructure to collect intelligence, support decision making processes and coordinate activities, especially when executing cyber operations or digital influence operations. In effect states are dependent on ICTC, knowing that the loyalty of the ICTC can alter over time based on financial or reputational considerations. Given the informational power of ICTC, the question that arises is who should be loyal to whom.

Keywords information and communication technology companies (ICT-companies), cyberspace, information environment, informational power, fighting power

1. Introduction

During the early stages of Russia's invasion of Ukraine on 24 February 2024, Russia incapacitated Viasat, a commercial satellite Internet communications provider crucial to Ukraine, with malicious software (malware). The cyberattack resulted in the loss of, *inter alia*, battlefield communications, particularly in the region near the heavily threatened Kyiv, rendering Ukrainian forces virtually blind to Russian troop dispositions and movements.[2] Two days later, aiming to fix this 'black hole', Ukraine's Minister for Digital Transformation, Mykhailo Fedorov, directly approached SpaceX-CEO Elon Musk via Twitter with a request to

[1] Lieutenant-Colonel dr. Eric Pouw is a military legal advisor of the Army Legal Service and currently serves as an Assistant Professor and Researcher Cyber Operations at the Faculty of Military Sciences of the Netherlands Defense Academy.
Brigadier-general professor dr. Paul Ducheine, MSc, LL.M. is the Professor for Cyber Operations and Chair of the War Studies Department at the Faculty of Military Sciences of the Netherlands Defence Academy. Starting in the Engineer Regiment, he joined the Army Legal Service. At the University of Amsterdam, he was endowed professor of Law of Military Cyber Operations (2014-2024).
Colonel dr. Peter B.M.J. Pijpers is Vice-Dean of Education at the Faculty of Military Sciences and an Associate Professor Cyber Operations at the Faculty of Military Sciences of the Netherlands Defence Academy, a researcher at the Amsterdam Centre of International Law, University of Amsterdam and a non-resident fellow at the University of South Florida.
Lieutenant-colonel (retd.) Kraesten Arnold MSc EMSD served as an Assistant Professor and Researcher Cyber Operations at Faculty of Military Sciences of the Netherlands Defense Academy.

[2] Patrick Howell O'Neill, "Russia hacked an American satellite company one hour before the Ukraine invasion," *MIT Technology Review*, May 10, 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

CONCEPT

roll out Starlink satellite Internet services in Ukraine.[3] Musk was quick to reply: "Starlink is now active in Ukraine. More terminals en route".[4] Musk decision to support Ukraine was his own; no contracts were signed, no costs were charged, at least not at that time.

While Starlink was never designed for use in warfare, it's availability to Ukrainian soldiers has bolstered Ukraine's fighting power, as it significantly restored and potentially improved its effectiveness. Described as the "essential backbone of communication on the battlefield",[5] its use has been particularly critical for drone warfare, for example to monitor enemy positions or to direct artillery and for unmanned attacks at sea. Starlink's participation in this war has made visible that the interests of states engaged in an armed conflict and those of information- and communication technology companies (ICTC) may not just differ, but also conflict. When requesting Musk to support Ukraine with Starlink, Ukrainian officials' main concern was to restore communications to prevent defeat.[6]

However, the consequences of Ukraine's dependence on Starlink for its military operations were immediately felt upon Musk's decision in September 2022 to deny Ukraine's use of Starlink for a surprise attack on Russian naval bases in Sevastopol, in Russian occupied Crimea. According to Roulette, Musk's decision to deploy Starlink was initially driven by humanitarian purposes, like restoring communications and supporting civilians, rather than serving as a tool for offensive military operations. He did not want to be blamed to have provoked a larger conflict with unintended consequences, including a potential nuclear escalation. He felt that this, personal and commercial, interest outweighed the interests of Ukraine.[7] Such clash of interests could again be witnessed in October 2022, this time driven by financial imperatives: Musk, feeling increasingly less comfortable with the enormous costs of Starlink – estimated at 400 million USD annually – insisted that the expense of supplying satellite Internet service in Ukraine should now be covered by the Pentagon, or else he would shut down connectivity to the system.[8]

Musk's wavering allegiance not only had a (potentially) negative impact on Ukraine's military efforts on the battlefield for Ukraine, it also raised serious concerns about the possible geopolitical effects. Fears in the Pentagon that Musk "would wake up one morning and just decide, like, he didn't want to do this anymore" eventually led to the signing of a contract between the Pentagon and SpaceX to secure future Ukrainian use of Starlink.[9]

---

[3] Myhailo Fedorov (@FedorovMykhailo): "@elonmusk, while you try to colonize Mars – Russy try to occupy Ukraine! While your rockets successfully land from space – Russian rockets attack Ukrainian civil people! We ask you to provide Urkaine with Starlink stations and to address sane Russians to stand," Twitter (now X), February 26, 2022, https://x.com/FedorovMykhailo/status/1497543633293266944.

[4] Elon Musk (@elonmusk), X, February 26, 2022, https://x.com/elonmusk/status/1497701484003213317.

[5] Ronan Farrow, "Elon Musk's shadow rule," *The New Yorker*, August 21, 2023, https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule, citing an anonymous Ukraine soldier.

[6] Farrow, "Elon Musk's shadow rule.".

[7] Joey Roulette, "SpaceX curbed Ukraine's use of Starlink internet for drones -company president," *Reuters*, February 9, 2023, https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/.

[8] Alex Marquardt, "Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab," *CNN*, October 14, 2022, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

[9] Ronan Farrow, "Elon Musk's shadow rule,"

Starlink is just one example of numerous ICTC offering support to Ukraine in its war against Russia. Similar backing has been provided by Microsoft, Google, and Amazon, to name a few. Of course, support to a state is not new, nor special; the use of their products (i.a.: Windows) and services (e.g.: cyber security and cyber threat intelligence) by government institutions, including the armed forces, is as common as it is for private individuals. This role of ICTC in the Russian-Ukrainian war, however, adds a dimension to contemporary warfare that merits further research, as they exert (faces of) powers in an geopolitical arena that historically was the domain of states and (their) armed forces.

As the example of Starlink demonstrates, such display of power by ICTC may seriously impact on and conflict with a state's ability to apply its sovereign powers, in particular its military power, to protect is vital, strategic interests in a wartime situation. Moreover, considering informational power as an (increasingly) essential strategic instrument of states,[10] these ICTC display various faces of that instrument: structural power by owning the physical infrastructure (i.a. intercontinental undersea cables), institutional power for being key in the governance of communications, and productive power for enabling the creation and distribution of content.

This contribution firstly aims to explain ICTC ('sudden') appearance at the frontlines of this war and whether this will be the case in future too. As ICTCs are intrinsically linked to informational power, the concepts of the information environment at large and cyberspace in particular, will be used as lenses through which this question will be answered. This allows us to determine the role and position of ICTCs in informational power. The second purpose of this contribution is to further examine the potential implications of ICTC involvement in wars on a state's ability to exercise military power. Because military power finds expression in the actual application of capabilities and resources by armed forces, we will use the concept of fighting power as a framework to assess these implications. Using the Russian-Ukrainian war as a case study, we thus seek to explain the prominent position and role of ICTC in war and what are the potential implications thereof for the development and application of states' (military) power.

To answer this question, (in paragraph 2) this chapter will first set the stage by briefly introducing the concepts and terms central to this contribution: the information environment, cyberspace and informational power. Paragraph 3 will then explain the utility of the information environment and cyberspace for fighting power. Paragraph 4 will take a closer look at ICTC's role in the Russian-Ukrainian War by examining their contributions and motives. In paragraph 5 we will subsequently assess the potential implications of wartime involvement of ICTC for the development and application of fighting power, and hence for their relation to military power and informational power. In paragraph 6 we will arrive at concluding thoughts.

This analysis will not consider legal and ethical issues (i.e., state responsibility) related to the various roles ICTC play in war. Nor is this analysis meant to compare a change in the nature and scale of involvement of non-state actors, i.e. ICTC in war.

2. The Information Environment, Cyberspace and Informational Power

[10] Paul Ducheine and Peter Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework," in *Deterrence in the 21st Century—Insights from Theory and Practice*, ed. Frans. Osinga and Tim Sweijs, , *Netherlands Annual Review of Military Studies* 2020 (Springer, 2021), also available at https://ssrn.com/abstract=3748348.

In this paragraph, we will first introduce the concepts of the information environment and cyberspace as part of it. Subsequently, the concept of informational power will be addressed.

2.1. The Information Environment

The information environment, as a concept, highlights the outlook on today's world, through the lens of the increasing relevance of data and information. It is a reflection of the "information revolution", since the late 20th century, in which information and communication technologies, such as computers, the Internet, smartphones, satellites, artificial intelligence (AI) and quantum computing, are at the core of our economic, social and political decision-making processes worldwide, on all levels of human interaction. This era is commonly referred to as the Information Age.

For the purpose of this chapter, the concept of the information environment particularly focusses on the strategic and operational use, and dynamics, of information by a wide range of actors, including individuals, organizations, leaders and decision-makers, in a particular context, such as the application of military power by a state.[11] Taking the security lens, the information environment is a key concept of NATO doctrine, which describes it as the environment "[…] where humans and automated systems observe, orientate, decide and act upon information, and is therefore the principal environment of decision-making."[12]

In today's world, information is a fundamental characterizing factor of our day-to-day living environment, which can be conceptualized in different ways, denoting different purposes, functions and characters of information.[13] First, it can be viewed as a resource of data available in the environment in all kinds of forms (ranging from objects and events to sounds and smells) which can in turn be used for understanding and decision-making and command. It can also be viewed as a representation of knowledge available in physical, digital and cognitive form, which together with data form the framework of an individual's understanding of a particular situation, which in turn shapes his or her decision making. Thirdly, information can be used as a tool, an instrument or 'weapon', i.e. as a message that is produced and distributed with the intent to influence the perception, attitude and behaviour of another actor, in a direction that is preferred by the sender. A fourth conceptualization of information concerns its function as part of the communication process inherent to every form of human interaction, which itself relies profoundly on human behaviour and sense-making processes.[14]

The manifestation of information takes place in three dimensions that, together, assist in characterizing the information environment. The cognitive dimension concerns collective

[11] Other instruments of national power are diplomatic, informational, and economic measures and activities. Together with the military instrument of national power, these instruments form the widely-used acronym DIME.

[12] NATO, *MC 422/3 NATO Military Policy for Information Operations*. See also NATO *AJP-3.10 Allied Joint Doctrine for Information Operations*, Novembe 2009.

[13] Marije Timmer and Paul Ducheine, "Conceptual Manoeuvring: The Interpretation of Information Manoeuvre within the Netherlands Ministry of Defence", *Militaire Spectator* 192, no. 11 (2023): 545-546.

[14] Maureen McCreadie and Ronald Rice, "Trends in Analyzing Access to Information. Part I: Cross-Disciplinary Conceptualizations of Access," *Information Processing and Management* 35 (1999): 46-48.

and individual and beliefs, thoughts, opinions, norms, values, emotions, *et cetera*. The virtual dimension embodies intangible digital identities that facilitate access to digital objects (software, applications and data). The physical dimension consists of physical entities, such as objects or persons, and their geographical locations. From these physical entities, all kinds of information can be retrieved, combined and subsequently used.

2.2.Cyberspace

Cyberspace is a specific part of the information environment (see also Figure 1), defined by NATO as "[t]he global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data"[15] is a – in terms of historical origins – a relatively new concept that has added a virtual and entirely man-made dimension to the existing physical and cognitive dimensions.[16]

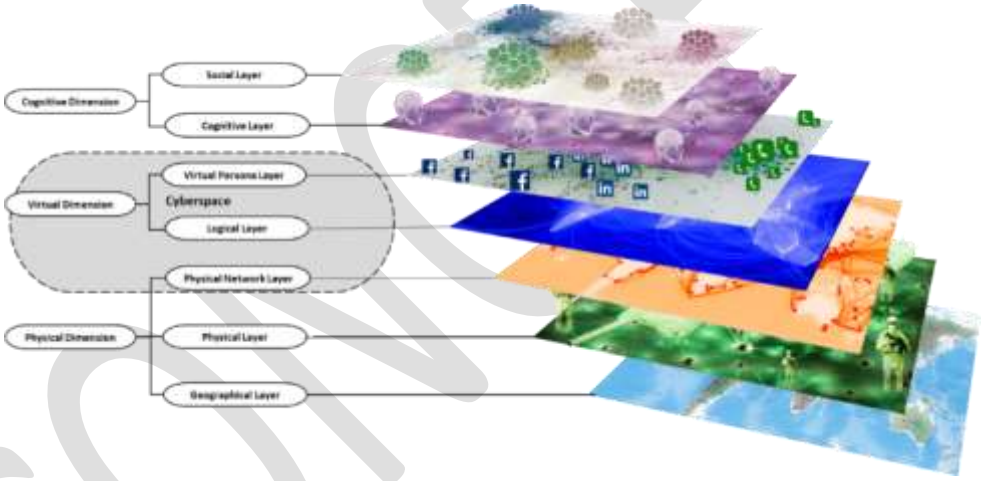


Figure 1: The information environment including cyberspace

A significant part of cyberspace is made up of virtual identities and objects that together form the virtual dimension of the information environment. The virtual persona-layer, reflecting human's collective or individual cognition, contains virtual identities, such as e-mail addresses, social media profiles, computer usernames or websites, by which individuals or organizations gain access to virtual objects (software and data). The virtual object-layer is essential for the digital creation, processing and storage of data, information, intelligence and knowledge made possible by computer programs (software), protocols, operating systems, IP-addresses or other digital data.

Another part of cyberspace is the tangible, physical network-layer of cyberspace, which overlaps with and forms part of the physical dimension of the information environment. This

[15] NATO, *AJP-3.20 Allied Joint Doctrine for Cyber Operations*, Edition A, Version 1, January 2020.
[16] Paul 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*, ed. Paul Ducheine and Frans Osinga, 2017.

layer enables digital communication and connectivity. This includes all hardware, such as the network of computers, smartphones, servers, and date carriers, crucial to data creation, processing and storage,[17] as well as the objects, such as routers, modems, cables, WiFi-routers, and satellites with their ground stations, required for communication and connectivity.

Cyberspace furthered the accessibility of the information environment and will continue to do so due to fast-paced innovations, such as AI and quantum-computing.[18] Without cyberspace, gaining understanding of the cognitive dimension (e.g. sentiments) or physical dimension (e.g. troop locations) required physical contact or a physical vector, which required many resources and was time-consuming. Cyberspace has enabled this to be achieved remotely and near instantly via the virtual dimension, by anyone. Moreover, the amount of information contained within the information environment has been amplified with the availability and information wealth of cyberspace.[19]

Together, the information environment and cyberspace function as a space that enable actors to collect, to disseminate and to release information for communication, decision-making and exchange of knowledge. As such, it provides a basis for social interaction in a digital and interconnected world. As we will see later, this function is of great significance for the development and use of fighting power (paragraph 3 and 4). The next subparagraph, however, will first briefly set out the concept of utilizing information as a form of power.

2.3.Informational power

Addressing informational power requires to recognize its part in a larger strategic context in which all states' strategic power instruments, often briefly summarized as DIME (diplomacy, information, military and economy).[20]

Next to this classic DIME typology, other instruments, such as financial, intelligence, legal,[21] or culture and knowledge, might be added,[22] to fully grasp the instruments used to exert power in today's geopolitical arena, as witnessed in the war in Ukraine. Examples of these instruments are culture as a (soft) power element,[23] (Radio Free Europe, China's Confucius

[17] Also called 'physical network layer', see NATO AJP-3.20, 3.

[18] Roy van Keulen, "Digital Force: Disrupting Life, Liberty and Livelihood in the Information Age," (PhD diss., Leiden University, 2018).

[19] Paul Ducheine, Peter Pijpers, and Marten Zwanenburg, "Rapport Tanden voor de leeuw – een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving," (*War Studies Research Centre*, Faculteit Militaire Wetenschappen, Nederlandse Defensie Academie, 2024), 23, available via https://www.rijksoverheid.nl/documenten/kamerstukken/2024/12/19/aanbieding-rapport-tanden-voor-de-leeuw. See also Jelle van Haaster, "*On Cyber: The Utility of Military Cyber Operations during Armed Conflict*" (PhD diss., University of Amsterdam, 2019), pp. 70-84; Keulen, van, "*Digital Force*," 19-38.

[20] Michael Mann, "The Sources of My Sources," *Contemporary Sociology*, 42 no. 4, 499-502; Ralph Schroeder," Introduction: the IEMP model and its critics," in *An Anatomy of Power: The Social Theory of Michael Mann*, ed. J.A. Hall and Ralph Schroeder (Cambridge University Press ,2015), 1-16; UK Ministry of Defence, *Joint Doctrine Publication 0-01: British Defence Doctrine* (2011), 1-6; US Joint Chiefs of Staff, *Joint Publication 1: Doctrine for the Armed Forces of the United States* (2013), I-12.

[21] Haaster, van, "*On Cyber*, 64; C.A. Rodriguez, T.C. Walton, C. Hyong, "Putting the "Fil" into "Dime": Growing Joint Understanding of the Instruments of Power", *Joint Force Quarterly*, 97 no.2 (2020): 121-128

[22] Nye Jr, Joseph, "Hard, Soft, and Smart Power," in *The Oxford Handbook of Modern Diplomacy*, ed. Andrew Cooper, Jorge Heine, and Ramesh Thakur (Oxford University Press, 2013), 1-17

[23] Nye Jr, Joseph, "Hard, Soft, and Smart Power," 10-14.

institutes,[24] Soros' Open Society Foundation)[25] and lawfare, i.e., legal action or litigation[26] used strategically as an alternative for the military instrument[27] in conflict situations;[28] e.g. the US' indictments of foreign cyber operators.[29]

Diplomacy is linked to foreign relations and generally about communicating and advocating national or international interests and values. Diplomats, international (governmental) organisations, alliances, international agreements, resolutions, cooperation, coordination, or norm development are the face of diplomacy.[30] Economic power as an instrument ranging from consensual (i.a. loans) to compulsory (i.a. sanctions) activities to gain a comparative advantage,[31] and can be enlarged with the financial instrument of power. It covers passive elements (e.g. macro-economic characteristics) as well as active measures (assets freeze, investments, etc.).

Fighting power is used to exert the military instrument - as will be further elaborated below in paragraph 3. It may be used in various ways, from (treaty-based or ad hoc) peaceful cooperation based on shared values and norms, to armed conflict. The modalities, means and

CONCEPT

[24] N. Young, "The Cultural Crusades," *New Internationalist* 423, :8–10, https://newint.org/features/2009/06/01/culture; R. Łoś, "U.S. and China: Hard and Soft Power Potential," *International Studies. Interdisciplinary Political and Cultural Journal*, 22, no. 1 (2018): 39-50, <https://doi.org/10.18778/1641-4233.22.03>.

[25] See <https://www.opensocietyfoundations.org/who-we-are>.

[26] See for example Russia's false accusations on Ukraine's acts of genocide in the UN SC. Radio Free Europe, "Ukraine Tells UN's Top Court Russia Using 'False' Genocide Allegations As Pretext For War," https://www.rferl.org/a/ukraine-tells-un-russia-false-genocide-war-pretext/32599619.html, September 19, 2023.

[27] Aurel Sari, "Hybrid threats and the law: Concepts, trends and implications," *Hybrid Centre of Excellence Trend Report* 3 (April 2020), https://www.hybridcoe.fi/wp-content/uploads/2020/05/Hybrid-CoE-Trend-Report-3.pdf.

[28] Joop Voetelink, "Reframing Lawfare" in *Winning without Killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, ed. Paul Ducheine and Frans Osinga, Netherlands Annual Review of Military Studies 2017 (TMC Asser Press, 2017).

[29] See, *inter alia*, US Department of Justice, "Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government," https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government, September 6, 2024; US Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and, October 19, 2020; Jason Horowitz, "Italy Orders Seizure of Migrant Rescue Ship*," New York Times*, 20 November 2018 https://www.nytimes.com/2018/11/20/world/europe/italy-aquarius-seizure-order.html; Eilleen Sullivan and Benjamin Weiser, "U.S. Seizes North Korean Ship for Violating Sanctions," *New York Times*, 9 May 2019 https://www.nytimes.com/2019/05/09/us/politics/wise-honest-north-korea-ship-seized.html; John Bellinger III, "Suing China over the coronavirus won't help. Here's what can work," *The Washington Post*, April 23, 2020, https://www.washingtonpost.com/opinions/2020/04/23/suing-china-over-coronavirus-wont-help-heres-what-can-work/.

[30] See e.g. the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (UNGGE) at <https://www.un.org/disarmament/group-of-governmental-experts/>; and the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), at <https://www.un.org/disarmament/open-ended-working-group/>.

[31] Francesco Giumelli, "Winning Without Killing: The Case for Targeted Sanctions," in *Winning without Killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, ed. Paul Ducheine and Frans Osinga, Netherlands Annual Review of Military Studies 2017 (TMC Asser Press, 2017), pp 91-106.

methods used, may vary from physical weaponry to non-kinetic[32] and information related capabilities, including hard (hacking) and (soft) cyber enable influence operations.[33]

Information as a power instrument, is at the core in the present chapter. It can be understood in several ways. First, it involves the relative value of physical, cognitive or virtual information sources itself.[34] These sources may be observed by men and/or machine, enabling 'understanding' and decision-making.[35] Large data sets containing personal information related to (large) groups, or traffic data, are also examples of power resources. This substantive facet may ultimately be used to affect other actors, which can be viewed as compulsory power.[36] Secondly, it entails structures to communicate in terms of capabilities, procedures and as a medium or vector. One could think of mainstream (physical) communication channels (i.a. papers), social media platforms (i.a. Telegram), the (intercontinental) glass fibre cable network and 4/5G networks and satellites for mobile Internet connectivity (i.a. Starlink). Ownership or (partial) control over these structures, may be used to exert power. Thirdly, institutions overseeing, designing, contributing to the flow of information may offer a powerbase as well, e.g. the Internet Corporation for Assigned Names and Numbers (ICANN), or Regional Internet Registries (i.a. RIPE).[37] Fourthly, information has a productive aspect, i.e., to generate debate, to reproduce and reinforce discourse or messaging, to construct and disseminate new information, whether malevolent or benevolent. Consider the (alleged) role of TikTok, X (Twitter) and Facebook in marketing or elections.

As demonstrated, the information environment including cyberspace is used to gather, transfer, handle and produce information, enabling understanding and decision making, whilst virtual information (i.e. data, software, protocols) is also used as a tool an instrument, as a vector and as a target to generate effects in this 'arena'. In this environment, informational power is perceived through various lenses: in a structural form related to e.g. ownership or position, institutional for one' role in the logical layer, and in a compulsory or productive form.

---

[32] Paul Ducheine, "Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting," in *Targeting: Challenges of Modern Warfare*, ed. Paul Ducheine, Michael Schmitt, and Frans Osinga (TMC Asser Press, 2015), 201-220; Ivor Wiltenburg, "Security Force Assistance: Practised but not Substantiated," *Militaire Spectator* 188, no. 2, 88-99, available at https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire Spectator 2-2019 Wiltenburg.pdf.

[33] Ducheine, van Haaster, and van Harskamp, "Manoeuvring and Generating Effects in the Information Environment"; Peter Schrijver and Paul Ducheine, "Cyber-enabled Influence Operations: the Case of the Belarusian Cyber-Partisans," *Militaire Spectator* 192, no.11, 284-295. https://militairespectator.nl/artikelen/cyber-enabled-influence-operations.

[34] UK Ministry of Defence, *Joint Doctrine Publication 04 (JDP 04): Understanding and Decision-Making* (2nd edition, December 2016), 2-5, https://www.google.com/search?q=uk+joint+doctrine+publication+4&rlz=1C1GCEB_enNL1000NL1000&oq=uk+joint+doctrine+publication+4&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDg5MDNqMGo0qAIAsAIA&sourceid=chrome&ie=UTF-8.

[35] Ducheine, van Haaster, and van Harskamp, "Manoeuvring and Generating Effects in the Information Environment."

[36] In the terminology used by Bets and Stevens: compulsory power. See David Betz, David, and Tim Stevens, "Chapter One: Power and Cyberspace." *Adelphi Series* 51, No. 424 (2011): 35-54. doi: 10.1080/19445571.2011.636954. See also the four categories by Barnett and Duvall: compulsory, structural, institutional and productive power. See Michael Barnett, and Raymond Duvall, "Power in International Politics," *International Organisation* 59, no..1 (2005): 43.

[37] ICANN is responsible for the Domain Name System (DNS); Regional Internet Registry for Europe, Middle East and Central Asia (RIPE) registers Internet Protocol (IP) addresses and Autonomous System Numbers (ASN.

As promised, the next paragraph will elaborate on the military instrument and fighting power and will address the utility of the information environment and cyberspace for the military instrument in some details.

3. The Utility of the Information Environment and Cyberspace for Fighting Power

As mentioned above, fighting power is the main component of the military instrument of power. This concept will be explained first. Subsequently, the functionality or utility of the information environment and cyberspace for fighting power with be explained.

3.1.Fighting Power

Fighting power is intrinsically linked with (the exercise of) military power as an instrument of national power, i.e. a state's (or coalition of state's) use of credible force in order to persuade another actor to choose a particular course of action or to refrain from one. In short, fighting power is a military doctrinal concept used by states[38] that expresses the efficiency and effectiveness with which armed forces are capable of carrying out military operations in the execution of the tasks bestowed upon it.

According to military doctrine, fighting power consists of three components: the physical component, the conceptual component and the mental component.[39] Effective fighting power as a capability requires that components are not void and together generate a synergetic coherency.[40]

The physical component - capacities - concerns manpower, equipment, training, sustainability in order to train and - ultimately - operate and fight. Despite its "tangible and physical" typecasting the component also encompasses non-lethal, non-kinetic and cyber capacities, e.g. cyber operators or 'hackers'.

The conceptual component contains the knowledge and plan (how) to effectively train, deploy and operate with the capacities aforementioned and is defined as the "coherent, intellectual basis and theoretical foundation for the deployment of military forces".[41] Sources are, i.a., education and research on conflict and combat and the wider strategic environment, strategic visions on the use of power and the pursuance of national interest, historical experiences and lessons learned from conflicts and exercises, conceptual innovation to adapt to new circumstances, as well as ethical and legal frameworks. These sources function as a framework to provide commanders a wider understanding of the context in which they will operate and thus how to apply fighting power.

The moral component applies to the willingness of people – in the military context: the willingness of soldiers to engage in combat. This willingness is determined by four factors:

[38] See for example NATO, *AJP-01 Allied Joint Doctrine*, Edition F Version 1, December 2022.

[39] Although this is a Western view of fighting power, it also reflects how other, non-Western, actors consider military capabilities. And while these components relate to military fighting power, the present authors regard them as equally relevant to the 'fighting power' of any other instrument of power.

[40] Ducheine, Zwanenburg and Pijpers, "Rapport Tanden voor de leeuw – een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving," 30.

[41] See Ministry of Defence of the Kingdom of the Netherlands, *Netherlands Defence Doctrine*, June 2019, 72.

CONCEPT

motivation, leadership, responsible organization of the deployment of available personnel and materiel, and perception.

3.2. Utility of the information environment and cyberspace

The question that follows is: what is the utility of the information environment and cyberspace for fighting power? Or alternatively, how can the information environment (and the aspects of information power deriving from it) augment fighting power in its understanding, decision making and activities.

First of all, the utility of information as an instrument to understand, decide or act (use as a 'weapon') can - in the military terms - be labelled as manoeuvring in the information environment. Information manoeuvring "comprises the direction and execution of activities in the cognitive, virtual, and physical dimensions of the information environment, to achieve a position of advantage in respect to an audience in order to accomplish a mission".[42] Like manoeuvre or hybrid warfare, information manoeuvre offers a framework for reflection on the purpose and consequences of the application of fighting power in this particular context (information manoeuvring).[43] This, in turn, impacts the development of the physical component, (including the cyber capabilities) for example because of equipment or technology purchased as a result of insights gained from the thinking about the use of fighting power in the information environment and cyberspace, or of the moral component, for example as a result of social or political reluctance to permit the military the use of cyberspace as a training area for digital military operations,[44] which may negatively impacts their motivation.

Secondly, the information environment and cyberspace offer cognitive, virtual or physical information sources that can be observed in order to gain an understanding of the cause and context of a situation or conflict, the capabilities of opposing, favourable and neutral audiences, as well as of the "interrelated networks of political, military, economic, social, infrastructure and information systems, each exerting pressure and influence on the others."[45]

Thirdly, cyberspace and the information environment serve as a backbone for communication and information sharing and also facilitate faster and more effective decision-making and coordination and synchronization through command and control (orchestration), which is specially made possible by the virtual dimension and cyberspace.

Finally, the information environment functions as the arena that allows for the manoeuvring with fighting power, for the deployment of capacities (act) in accordance with the decision taken. This requires instruments or tools (a.k.a. information as a weapon) taken from the very information environment, e.g. in the form of malware or content. This instrument is then transmitted through one of the dimensions (e.g., land, air, cyberspace) serving as a vector, targeting an element in one of the layers of the information environment, e.g. a virtual object.[46]

---

[42] Timmer and Ducheine, "Conceptual Manoeuvring," 545-546.

[43] Peter Pijpers and Paul Ducheine, "'If You Have A Hammer': Shaping the Armed Forces' Discourse on Information Maneuver," *International Journal of Intelligence and Counter-Intelligence* 36, no. 3 (2023).

[44] Ducheine, Zwanenburg and Pijpers, "Rapport Tanden voor de leeuw – een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving, 22.

[45] Commonly referred to as 'operations environment. See NATO, *AJP-01*, 94.

[46] Pijpers, Peter B.M.J., and Kraesten L. Arnold, 'Conquering the Invisible Battleground,' *Atlantisch Perspectief*, 44, no. 4 (2020), 10-14.

CONCEPT

Action thus takes shape via activities in or via the three dimensions: cognitively, such as an influence campaign; virtually, for example via a computer hack; or physically, for example by aerial bombardment. That being said, the cognitive dimensions is perhaps the most relevant dimension for fighting power, as it is here that fighting power must be directed at the vulnerabilities of a particular audience (foe, friend, or neutral) and eventually result in influencing its thinking process, decision-making and behaviour in order to obtain an advantage that contributes to the accomplishment of a mission.[47]

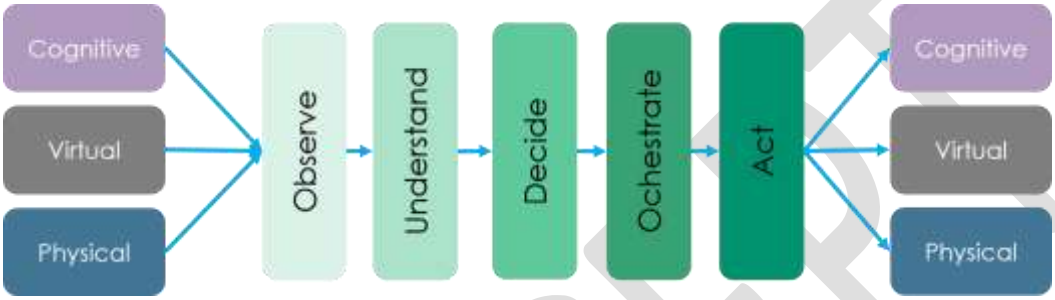


Figure 2: Backbone and activities in the information environment.

In sum, relying on the backbone structure, this process of observe, understand, decide, orchestrate and act is continuous: the effects of the application of fighting power form the impetus for (another) cycle of observation, understanding, decision-making, *et cetera* (by the actor itself, or by others, such as the opponent). This backbone and process is reflected in **Figure 2**. As will be explained in the next paragraph, nearly all of this can be attributed to the role and position of ICTC in cyberspace.

4. ICTC in the Russian-Ukrainian War: Contributions and Motives

As has been the case for many other states engaged in armed conflict, it has become clear that Ukraine's survival heavily depended and still depends on external support. On the one hand, Ukraine has received support – diplomatic/political, intelligence, economic/financial and military - from other states, predominantly coming from members of NATO and the EU.[48] On the other hand, Ukraine's survival also relied on the backing of ICTC, in a wide range of cyberspace-related sectors.[49]

The role of ICTC during armed conflict, in contrast to those of states, is built on a numerous – sometimes changing or contradicting – interests. This paragraph explores their contributions and motivations. Not all behaviour of ICTC is based on an ideological impetus. Sanctions, imposed after the 2022 invasion, heavily impacted services offered by ICTC to Russian clients.[50] The access of state-owned Russia Today (RT) and Sputnik news in Europe

[47] Timmer and Ducheine, "Conceptual Manoeuvring," 550.
[48] https://www.nato.int/cps/en/natohq/topics_192648.htm; https://european-union.europa.eu/priorities-and-actions/eu-support-ukraine_en.
[49] The overview below is not intended to display a complete picture, but merely offers examples available in open sources.
[50] Andrew Sanger, "Piercing the State's Corporate Veil: Using Private Actors to Enforce International Norms," *EJIL: Talk!* (17 March 2022), https://www.ejiltalk.org/piercing-the-states-corporate-veil-using-private-actors-to-enforce-international-norms/.

and in some cases globally was restricted. Conversely, as a consequence of Russian legislation, services of Twitter, YouTube, and Google were banned in the Russian Federation.[51] Moreover, many companies (e.g broadband providers such as Lumen and Cogent)[52] service provides (PayPal) and vendors (Apple, Microsoft)[53] decided to stall services beyond the level required by the sanction regime.[54] Shortly after the Russian invasion, the Vodafone telecommunication company cut off communication in large parts of the Russian-occupied Donbas region, rendering pro-Russian separatists digitally incapacitated.[55] Stalling and reducing services beyond the sanctions and legal requirements, can arguably be explained on moral grounds and on (long term) marketing and public relations considerations.

While the broader technology industry has generally demonstrated strong support for Ukraine (or followed sanctions and legislation), some companies have continued their operations or upheld relationships with the Russian government. Notable examples include Yandex, a Russian-based company comparable to Google; Kaspersky Lab, a Russian cybersecurity firm; and Rostec, a Russian state corporation involved in technological development for defence purposes.

Although outside the scope of ICTC, perhaps to be regarded as a waiver for incompleteness, it should be noted that institutions that are considered to form the core of the Internet, e.g. ICANN and RIPE, notwithstanding the pressure that was exerted upon them, have remained their neutral stance in this conflict.[56] Others organizations responsible such as SWIFT, responsible for virtual financial massaging between banks, were forced to stall service as a result of international (i.a. EU) sanctions.[57]

Notwithstanding moral and PR considerations, ICTC are ultimately driven by economics, even when services are (temporarily) offered for free. One area in which ICTC support has proved to be vital is cybersecurity. Prior to the actual invasion and in anticipation of predictable Russian cyberattacks,[58] Ukraine - based on cyber threat intelligence (CTI) - increased its resilience in cooperation with the US and the UK (initially on-site and later

[51] Shannon Bond and Bobby Allyn, "Russia is restricting social media. Here's what we know," *NPR*, March 21, 2022. https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban.

[52] Doug Madory, "Updated: Cogent and Lumen curtail operations in Russia," *Kentik*, March 7, 2022, https://www.kentik.com/blog/cogent-disconnects-from-russia/.

[53] Microsoft, "Microsoft suspends new sales in Russia," *Microsoft Official Blog*, 4 March 2022, https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/

[54] Chris Isidore, "Why many businesses are getting tougher on Russia than sanctions require," *CNN*, 3 March 2022, via https://edition.cnn.com/2022/03/03/business/business-go-beyond-russian-sanctions/index.html.

[55] Cathal McDaid and Rowland Corr, "The Mobile Network Battlefield in Ukraine – Part 3," *Adaptive Mobile Security*, April 25, 2022, https://www.enea.com/insights/the-mobile-network-battlefield-in-ukraine-part-3/.

[56] ICANN, Letter from Göran Marby to Mykhailo Fedorov,(2 March 2022, https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[57] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a messaging service that substantially facilitates information exchange between banks and other financial institutions. SWIFT connects more than 11 000 entities worldwide. See European Council, "EU sanctions against Russia explained ", via: https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/.

[58] Lally Weymouth, "Volodymyr Zelensky: 'Everyone Will Lose' If Russia Invades Ukraine," *The Washington Post*, January 20, 2022, https://www.washingtonpost.com/outlook/2022/01/20/ukraine-russia-zelensky-interview/.; Paul Sonne, Missy Ryan, and Hudson. John, "Russia Planning Potential Sabotage Operations in Ukraine , U . S . Says," *The Washington Post*, January 14, 2022, https://www.washingtonpost.com/national-security/russia-ukraine-invasion-sabotage-operations/2022/01/14/769314a2-754f-11ec-8ec6-9d61f7afbe17_story.html.

remotely)[59] and a variety of ICTC: e.g. Microsoft, Mandiant, ESET, Amazon Cloud Services.[60] They have provided Ukraine with advice and fixes for Russian cyber-attacks and technical and security services.[61] Google expanded the availability of Project Shield, free software designed to protect vulnerable and under-resourced news-websites with "media, elections, and human rights related content"[62] against DDOS-attacks, thus ensuring the continuation of critical services provided by the Ukrainian government. Microsoft, Amazon Web Services, and Google also assisted Ukraine by virtually relocating vital government data to cyber infrastructure outside its territory.[63] Thus, active incident response and information sharing between Ukraine, cybersecurity firms and allied defenders likely disrupted Russia's destructive cyberattacks.[64]

Other companies have supported Ukraine by making available intelligence through their commercial satellite services. Google's satellite service Google Maps has been used by Ukrainian forces in the early days of the war to locate and subsequently attack Russian troops. When discovering that the Russian's used this tool in a similar fashion, Google disabled certain features to shield Ukrainian forces from attacks. Additionally, the company developed an air raid alert application to safeguard Ukraine's citizens from Russian bombardment.[65] Companies such as Palentir Technologies, Planet Labs and Blacksky Technology provided geospatial imagery for intelligence, surveillance and reconnaissance purposes, often in combination with AI and open-source information.

Ukraine has also received cyber-tech support in the field of decision support systems such as Artificial Intelligence. Clearview AI, a U.S.-based company, has provided AI-based facial recognition software. The company's search engine matches individuals' faces to a database of more than twenty billion images collected from the Internet's social media platforms, including the Russian social media service VKontakte.[66] Ukraine utilized the technology, which it received free of charge, to "identify the faces of the Russian military who

[59] Alexander Martin, "US Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command," Sky News, 2022. https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139.

[60] Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications", *Carnegie Endowment for International Peace*, December 16, 2022, 14, https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en.

[61] Google Threat Analysis Group and Mandiant, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," February 2023. Retrieved from https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

[62] Russell Brandom, "Google launches new anti-DDoS service called 'Project Shield'", *The Verge*, 21 October 2013, https://www.theverge.com/2013/10/21/4862724/google-launches-new-anti-ddos-service-called-project-shield

[63] The rationale behind this relocation of government data was (and is) the assumption that Russian attacks on data centres in Western states (and under the protection of these (mostly U.S.) companies were deemed less likely to occur, as the states involved would consider such attacks as armed attacks by Russia, which would result in escalation of the conflict to a degree not desired by Russia.

[64] Microsoft Threat Intelligence Centre, "A Year of Russian Hybrid Warfare in Ukraine," March 15, 2023, 5, https://nsarchive.gwu.edu/sites/default/files/documents/s9zfme-rssdn/2023-03-15-Microsoft-A-year-of-Russian-hybrid-warfare-in-Ukraine-MS-Threat-Intelligence.pdf..

[65] Aisha Malik, "Google adds Air Raids Alerts to Android Phones in Ukraine," *TechCrunch*, 10 March 2022, retrieved from: https://techcrunch.com/2022/03/10/google-adds-air-raid-alerts-to-android-phones-in-ukraine/?guccounter=2.

[66] Dave Paresh and Jeffrey Dastin, "Ukraine has started using Clearview AI's facial recognition during war," *Reuters*, 14 March 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

were killed or captured, check people at checkpoints, and search for missing persons".[67] AI-based support can further be found with respect to qualification of objects on the battlefield,[68] electronic warfare, encryption, cybersecurity, drone warfare, autonomous ships, undersea drones and uncrewed ground vehicles, to name a few areas.[69] In the same vein, communication systems have been provided: Elon Musk's Starlink, mentioned in the introduction, is one example.

Social media platforms and their parent companies – such as Facebook (Meta), X (Twitter), YouTube, TikTok, and Telegram – have not only become primary sources of real-time data that can inform strategic decisions both domestically and internationally but have also emerged as critical battlegrounds for disseminating narratives aimed at influencing public opinion and troop morale. Meta, for example, took extensive steps to monitor and curb disinformation spread by Russia-controlled media outlets.[70] At the same time, Ukrainian state organs and officials heavily rely on these same platforms offered by the ICTC. President Zelensky, the two Ukrainian intelligence services (HUR and SBU),[71] are just some of the frequent users of the platforms and its handles for so-called (soft) cyber-enabled influence operations.[72] Moving beyond that purpose, these platforms have also been used to prepare for and conduct hard cyber operations. Ukraine's Twitter handle @ITarmyUKR,[73] for example, is used to muster personnel, including hackers and hacktivists, to collect vulnerabilities (in software and protocol), to coordinate and conduct cyberattacks.[74]

The motivations of the companies providing support are not always clear since the ICTC need to strike a balance between commercial, reputational, ideological and compelling (dis)incentives. Understanding the true interests of these ICTC is, however, crucial, as it sheds light on the involvement of non-state actors in geopolitical conflicts and war, their potential to influence international affairs, and will have an impact on the fighting powers of states.

5. Implications of ICTC (Wartime) Involvement

The cases taken from the war in Ukraine, illustrate that the utility of the information environment (and cyberspace) for fighting power of the state, lies in its capability to enable actors to collect and disseminate information for communication, understanding, decision making and action. Given the roles and subsequent position of ICTC in cyberspace and the position of cyberspace within the information environment, it does not come as a surprise that

[67] Quote from Yevgeny Yenin, Deputy Minister of Foreign Affairs of Ukraine, retrieved from the Clearview AI website at https://www.clearview.ai/ukraine.
[68] See e.g. MilitaryNewsUA, 25 January 2024, Tweet ("Ukrainian Saker Scout drone with artificial intelligence"), via: https://twitter.com/i/status/1750444954298577263.
[69] See e.g. Peter Schrijver, "'The Wise Man Will Be Master of the Stars'. The Use of Twitter by a Military Intelligence Service in Wartime: The Case of the GUR 77," in *Reflections on the Russia-Ukraine War*, ed. Maarten Rothman, Lonneke Peperkamp, and Bas Rietjens. Leiden University Press.
[70] Meta, "Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine," February 26, 2022, https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/.
[71] HUR is Ukraine's military intelligence service, SBU the internal security agency.
[72] Schrijver, "The Wise Man Will be Masters of the Stars", 77-96.
[73] See: https://x.com/ITArmyUKR
[74] Stefan Soesanto, "The IT Army of Ukraine Structure, Tasking, and Ecosystem," *CSS Cyberdefense Report*, June (2022).

ICTC are of great significance for the utility of the information environment. This can be expressed in both a positive and negative sense.

5.1.Implications for Informational Power

ICTC can be seen as creator, custodian and as regulator in cyberspace. Not states but ICTC are in a dominant position in cyberspace. This dominant position is reflected in the various expressions of informational power: compulsory, structural, institutional and productive.

As the principal creators of cyberspace, ICTC are responsible for the development and production of (nearly)[75] all infrastructure, technology and services of the three layers of cyberspace. This applies to the physical infrastructure and technology required for data production, data storage, data transmission, and connectivity as well as the plethora of digital products and closed-off digital ecosystems offered and controlled by ICTC.[76] As the custodians of data and information, ICTC wield influence by offering services for data storage and protection of the cyber infrastructure and data.[77] As such, the ICTC wield structural power. Structural power also can be recognized as ICTC also own and operate the principal social media platforms and networks.[78]

The social media platforms, alongside the virtualisation of mainstream media, are central to the notion of productive power as they are used to signal, accelerate, transmit issues and initiate public debate: whether benevolent or malicious. Ownership, e.g., of the social media platforms, also entails compulsory power. This is evident if consumers don't comply with a service or platform agreement and – when in violation – are ousted of expelled from the services.

Moreover, ICTC play a key role in the regulation and governance of cyberspace, hence they wield institutional power as well. Examples are content moderation vis-à-vis the freedom of expression, privacy and data protection, cybersecurity standards, AI, cryptocurrencies and block chain, and property rights on digital content. Ownership and structural positioning offers an opportunity to set rules and standards, and to determine how cyberspace must be governed commensurate to their business, moral, social, economic or political interests.[79] Examples of this direct and indirect norm-making capacity by ICTC are Apple with global standards based on patents such as iOS and the Apple Store where quality standards are set; policies for content moderation (e.g. how to handle hate speech); and lobbying to influence government policy and regulation to protect their interest.[80]

---

[75] Very few states produce their own hardware and software, often via state-controlled or owned companies. Examples are China, Russia, India, Iran and North-Korea.

[76] Examples of such ecosystems are those offered by Apple with iOS and the App Store, the marketplace and cloud services of Amazon, and the search engines, e-mail service Gmail and operating system Android of Google.

[77] Examples are Palo Alto Networks, CrowdStrike, Fortinet, and CloudFlare.

[78] Examples are Facebook, X ,YouTube, Instagram, LinkedIn, TikTok, Snapchat, WhatsApp, WeChat and Discord.

[79] Udi Sommer, Eviatar Matania, and Nir Hassid, "The rise of companies in the cyber era and the pursuant shift in national security," *Political Science*, 75, no.2: 148. 140-164, DOI: 10.1080/00323187.2023.2278499.

[80] For example, companies such as Google and Facebook actively participated in the debate around the GDPR in the EU.

This brief oversight demonstrates that ICTC represent various expressions of informational power. This has – at least – two implications for states and warfare. First of all, informational power (by virtue of the ICTC) is used alongside military power in conflict and war. This is evident when looking at strategic cyber enabled influence operations. Secondly, informational power is also recognized as a key feature in military power as some of the capacities (e.g. satellite connectivity) or concepts (e.g. information manoeuvring) rely on the provision of ICTC's services. In the next paragraph we will explain what this means for military power.

5.2. Implications for Military Power

Previously, we concluded that the information environment serves as a resource for forms of information taken from the cognitive, virtual and physical dimensions enabling understanding, decision making, a backbone for communication and information sharing and as an arena for action (in various dimensions). In this arena actions, operations, are planned and executed. Given ICTC's roles and position in cyberspace and subsequent significance for the utility of the information environment, it is not surprising that states rely on and closely work together with ICTC for the development of and support to fighting power.

First of all, as ICTC have a dominant role in cyberspace and hence in the virtual dimension of the information environment, it is - in general terms - obvious that by virtue of their structural and institutional power, ICTC enable the use of cyberspace (and the information environment). As such, they contribute to military power and contribute to the effectiveness of capacities and concepts. Looking at the examples taken from the Ukrainian war, it became clear that various ICTC have been providing resources (i.a., cyber threat intelligence, satellite imagery, geo positioning data) that were used to generate understanding, enabling decision making, orchestrations and ultimately action. Additionally, the backbones, i.e. the various communication systems owned or provides by ICTC, be it satellite, GSM or ISP, enable the activities undertaken in the information environment: observe, understand, decide, orchestrate and act (see Figure 2). Starlink is the obvious example used for communication and orchestration. Another example is Twitter as a platform, providing the @ITArmyUKR account used for communication, acquisition and harvesting potential vulnerabilities. In terms of components of military power, these features qualify as capacities (in the physical (including non-kinetic) component.

Secondly, considering the opportunities to wield compulsory and productive power, it also fair to say that ICTC enable action, or in military terms, operations. Action can be recognized in the examples above. Taking a broad approach, it is the shutting down of services upon request (PayPal) or the refusal to do so (ICANN) that represents the use of compulsory power that can be exercised indirectly through the ICTC. The use of social media platforms, whether by President Zelensky or by the SBU and HUR, to launch and conduct cyber-enable influence campaigns to generate international (public, political, economic and military) support serves as a clear example of productive power. So do Russia's disinformation campaigns launched through RT or Sputnik (although hampered abroad through sanctions). Once again, these services can be regarded as capacities, part of military power.

CONCEPT

When considering the information environment and cyberspace as an arena is which action – offensively or in defence – is taken (using compulsory and/or productive power) it is also fair to state that tools (instruments or weapons) and vectors (the Internet or glass fibre seabed cables) used to address targets (virtual identities and objects) are part of the infrastructures owned or services offered by the ICTC. Once again, this tooling (or weaponeering) and the vectors, can be regarded (non-physical and physical) capacities. Moreover, viewing the information environment as the operational context, the conceptual notion of information manoeuvring contributes to fighting power as it explains how the use of capacities can be planned and executed to acquire beneficial 'positions' or outcomes and effects.[81]

5.3.The Other Side of the Coin

It is clear from the paragraphs above that – directly and indirectly – using or profiting from the services and powers ICTC represent, ultimately offers advantages for states and their armed forces. In general, ICTC contribute to – at least – capacities as part of the (non-)physical component and the conceptual component of military powers as it increases effectiveness of military action and power.

Nevertheless, there's also another side of the coin. First, the dominant position of ICTC in cyberspace raises concerns on the functioning of the information environment. This can be attributed to, what has been dubbed as, 'digital feudalism': by exploiting existing legal frameworks and policies in some areas and the absence thereof in others, ICTC – Big Tech in particular – essentially control whether, where, when, how and under which conditions data and information can be digitally created, stored, analysed, structured, disseminated, manipulated, used, et cetera.[82] A consequence of this is the monopolisation of information. With their use of features like content moderation, paywalls, AI and algorithms, as well as their regulatory power, ICTC are in a position to limit the access to, the diversity of, and quality of information. In essence, for billions of customers all over the world, including governments and armed forces, ICTC are the gatekeepers of the virtual dimension and are therefore the decisive factor in how other actors in the information environment perceive information, what they decide and subsequently where and how they act. This not only impacts individuals, but first and foremost states: as ICTC literally 'sit' on information, their information position has become stronger than that of states and their intelligence services.[83] Combined with their enormous financial power, which in some instances exceeds that of states,[84] ICTC have used their structural power

[81] See the definition of Information Manoeuvre above in paragraph 3.2, footnote 42.

[82] Reijer Passchier, *De vloek van Big Tech* (Boom Juridisch, 2024). Examples of existing laws and policies are free trade rules, patent and copyright laws, and tax laws; domains that remained unregulated for a long time are data and privacy protection and laws and policies against disinformation and hate speech.

[83] For example, the provision of intelligence products by private companies – using open source information – is a fast growing sector, with governments and the private sector as clients. See, for example, Katherine Tucker and Maria Robson-Morrow, "Intelligence outsourcing for non-traditional clients: the rise of private sector intelligence providers," *Intelligence and National Security*, January 3, 2025, https://doi.org/10.1080/02684527.2024.2437958.

[84] Some ICTC are wealthier than the GDP of certain countries. For an overview, see Ruslana Lishchuck, "How Large Would Tech Companies Be if They Were Countries?," *MacKeeper Blog*, August 13, 2021, https://mackeeper.com/blog/tech-giants-as-countries/. See also the yearly "Global Ranking of the Top 100

CONCEPT

(or 'platform power')[85] and institutional position to gain privileged access to public authorities and international fora, to set standards and to form coalitions to protect their interests, as recent examples demonstrate.[86] In doing so, ICTC are increasingly injecting themselves in, interfering with or seem to be taking over traditional governmental functions, including in the realm of national and international security.[87]

A second negative effect is the change in participative behaviour of actors in the information environment as a consequence of the erosion of user trust regarding ICTC's handling of data and information. This follows, firstly, from the ICTC's role in relation to manipulated and harmful information, such as misinformation, disinformation and hate speech. As owners of the main social media platforms, ICTC are the principal enablers of this type of information. Examples of the impact thereof on democratic processes,[88] public discourse and social cohesion[89] are numerous. Likely on economic grounds, ICTC have been reluctant to take preventive or mitigating measures. Measures that have been introduced – such as fact checking and internal oversight boards – have been criticized for failing to meet basic standards, such as transparency and independency.[90] In other instances, ICTC have overhauled preventive

Public Companies by Market Capitalisation" provided by Price Waterhouse Coopers, see for example their 2024-report at https://www.pwc.co.uk/services/audit/insights/global-top-100-companies.html?WT.mc_id=CT1-PL50-DM2-TR3-LS3-ND30-TTA9-CN_Captial-Markets-Assurance-Global-Top-100-Companies-Annual-Report-. See also Forbes, "Top 100 Digital Companies," https://www.forbes.com/top-digital-companies/list/.

[85] José van Dijck, David Nieborg, and Thomas Poell, "Reframing Platform Power," *Internet Policy Review*, 8(2). DOI: 10.14763/2019.2.1414.

[86] See, for example, Elon Musk's meetings with European party leaders Farage (Reform UK, UK), Meloni (Fratelli d'Italia, Italy), Weidel (AfD, Germany), Cat Zakrzewski, "Elon Musk goes global with his playbook for political influence," *The Washington Post*, January 5, 2025, https://www.washingtonpost.com/politics/2025/01/04/elon-musk-uk-germany-canada-far-right/. See also Meta's CEO, Mark Zuckerberg's decision to cancel its fact-checking program to protect his interests under the Trump-reign: Naomi Nix, Will Oremus, and Aaron Gregg, "Meta Ends Fact-Checking, Drawing Praise from Trump," *The Washington Post*, January 7, 2025, https://www.washingtonpost.com/technology/2025/01/07/meta-factchecking-zuckerberg/. See also Shaleen Khanal, Hongzhou Zhang, and Araz Taeihagh, "Why and How is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI," *Policy and Society*, 2024, https://doi.org/1093/polsoc/puae012.

[87] Sommer, Matania, and Hassid, "The rise of companies in the cyber era and the pursuant shift in national security."

[88] A recent example is the role of TikTok to influence the 2024 elections in Romania, Joseph Mann, "Covert TikTok Campaign Blamed in Pro-Russian Romanian Candidate's Surge," *The Washington Post*, 5 December 2024, https://www.washingtonpost.com/technology/2024/12/05/tiktok-romania-president-russia-influence/.

[89] See, for example the polarizing effects of social media content on the Israel-Hamas conflict, Elizabeth Dwoskin, "A Flood of Misinformation Shapes Views of Israel-Gaza Conflict," *The Washington Post*, October 14, 2023, https://www.washingtonpost.com/technology/2023/10/14/propaganda-misinformation-israel-hamas-war-social-media/. See also Stefan Stieglitz and Björn Ross, "The Impact of Social Media on Social Cohesion: A Double-Edged Sword, *Media and Communication*, 10, no.2, 2022, https://doi.org/10.17645/mac.v10i2.5792. Shumpenthung Ezung and Kekhronei O Koza, "The Influence of Social Media on Public Discourse: Examining How Social Media Shape Popular Opinion," *International Journal of Contemporary Research in Multidisciplinary*, 3 no. 6, 2024, DOI: https://doi.org/10.5281/zenodo.14252454.

[90] See, for example, Adam Satariano, "Facebook's Oversight Board Faults its Policy on Preferential Treatment," *The New York Times*, October 21, 2021, https://www.nytimes.com/2021/10/21/business/facebook-oversight-board-members-criticism.html. On basic standards for improvement of transparency, see for example Amnesty International, "Amnesty International Position on the Proposals for a Digital Services Act and a Digital Markets Act, March 2021," https://www.amnesty.eu/wp-content/uploads/2021/04/Amnesty-International-Position-Paper-Digital-Services-Act-Package_March2021_Updated.pdf.

measures.[91] At the same time, ICTC use their power to influence initiatives by states to regulate ICTC's role in the spread of disinformation[92] or to challenge existing laws.[93] In other instances, states are too slow to adopt laws[94] or allow disinformation to take place under the pretext of free speech.[95] Ultimately, this undermines the confidence of audiences with respect to accountability and governance of ICTC and the ability of the information environment to assist them in making decisions based on information from sources that have historically been considered relatively credible, such as news media, scientific institutions and government organizations. Eventually, the loss of confidence causes people to retreat into online communities that reinforce their own beliefs, further limiting their access to diverse and credible information and critical thinking. Its polarizing effects ultimately not only negatively affects dialogue and cooperation on individual and group level, but also undermine broader societal and democratic processes, such as elections.

As becomes clear, ICTC near-absolute dominance in cyberspace has created an information environment that makes it possible to handle information in ways that were previously unthinkable. On the other hand, it has created an unbalanced relationship between ICTC and the users of its products and services; a relationship that is characterized by an almost complete degree of dependence. Put otherwise, if ICTC-dominance were to implode suddenly, it would affect almost every aspect of our daily lives, with severe consequences for global economy, safety and society. It is therefore fair to say that ICTC practically keep the world in a stronghold, notwithstanding the moral and legal shortcomings of their practices. These dynamics also applies to the relationship of states with ICTC with respect to the fighting power of their armed forces.

6. Concluding remarks

The information age, being society's development after the creation of cyberspace and its increased use after (mobile) Internet connectivity spread around the world, now connecting a majority of over 5 billion people worldwide, resulted in a change in character of social behaviour.[96] Interaction changed as a result of virtualisation and digitisation,[97] and as a result, the niche social interaction called war changed as well. Departing from a strategic notion of states' instruments of power, it is evident that both informational power and military power have evolved over time.

[91] Nix, Oremus and Gregg, "Meta Ends Fact-Checking, Drawing Praise from Trump."
[92] Max Bank and Bram Vanken, "How Big Tech's Revolving Doors Erode EU Antitrust Laws," *EU Observer*, October 28, 2024, https://euobserver.com/news/ar1234f8b4.
[93] See Amelia Minkin and Michael Beckel, "Big Tech Ramps Up Lobbying as Industry Seeks to Thwart Legislation to Protect Kids Online," *IssueOne*, October 22, 2024, https://issueone.org/articles/big-tech-ramps-up-lobbying-as-industry-seeks-to-thwart-legislation-to-protect-kids-online/
[94] Passchier, *De vloek van Big Tech.*
[95] See, for example, the Executive Order of President Trump issues on 25 January 2025, in which he forbids federal censorship to secure the freedom of speech, see The White House, "Restoring Freedom of Speech and Ending Federal Censorship," January 25, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship/.
[96] See e.g. Jonathan Haidt, *The Anxious Generation. How the Great Rewiring of Childhood is Causing an Epidemic of Mental Illness* (Penguin, 2024).
[97] See van Keulen, "*Digital Force"*; van Haaster, "*On Cyber."*

CONCEPT

Digital warfare took the fore through connectivity, digitisation and virtualisation. It was found that ICTC play a major role in this development. As was demonstrated by assessing cases taken from the war in Ukraine, the ICTC's structural and institutional power basis as well as compulsory and productive power enabled military capacities and ultimately capabilities (or fighting power). This explains the increased appearance of ICTC on the frontlines of war and underscores our assessment that they will play a prominent role in future warfare.

ICTC provide the backbone of cyberspace enables communication. They facilitate the collection of information from the cognitive, virtual and physical dimension enabling understanding, the subsequent decision making and orchestration of action, and finally the action itself. As an arena where digitised social interaction (*in ultimo* including warfighting) takes place, these ICTC provide for information on threats, vulnerabilities to be exploited through tooling (instruments or 'weapons'). Their networks serve as a vector for the tools targeting the virtual identities, virtual objects or hardware and are therefore crucial in the development of a state's ability to exercise military power. Ultimately, as capacities and concepts benefit from the services offered by ICTC, these entities contribute to the effectiveness of fighting power.

Apart from the fact that ICTC play a crucial role in the development of fighting power of state in the physical dimension, cyberspace and the wider information environment in itself provide an independent way of deploying fighting power – a cyberwar where states are no longer the dominant actors.

However, as a result of their vital position and contribution to cyberspace and the information environment, depending and relying on these ICTC comes at a price. Firstly, overdependence on digital technology will involve operational vulnerabilities. Drones are not effective if there is a scarcity in SIM-card or when the wifi-signal is weak. Secondly, the allegiance or enduring loyalty of ICTC bring about risks. An ICTC can withdraw its support if the endeavours in warzones are too costly, when there are security concerns for personnel, or when the support will cause reputational damage. We should not be naive and realise that also states can change their stances when the incumbent governments changes, but ICTC – and non-state actors in general – usually have a more complex set of interests when involved in an armed conflict.

When war is taken to cyberspace, the ICTC – not the states - are the dominant actor providing the communication backbone, and repository of data to support decision making, and control the vectors (the Internet and social media) to target opposing actors. In the relation between states and ICTC, the question then emerges, who is supposed to be loyal to whom?

7. Bibliography

Books and Journal Articles

Bateman, Jon. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," *Carnegie Endowment for International Peace,* December (2022), p. 14.

CONCEPT

Barnett, Michael, and Raymond Duvall, "Power in International Politics." *International Organisation* 59, no.1 (2005): 39-75.

Ducheine, Paul. "Non-Kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting." In *Targeting: Challenges of Modern Warfare*, edited by Paul Ducheine, Michael Schmitt, and Frans Osinga. TMC Asser Press, 2015.

Ducheine, Paul, Jelle van Haaster, and Richard van Harskamp. "Manoeuvring and Generating Effects in the Information Environment." In *NLARMS 2017: Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis*, edited by Paul Ducheine and Frans Osinga. TMC Asser Press, 2017.

Ducheine, Paul and Peter Pijpers. "The Missing Component in Deterrence Theory: The Legal Framework." In *NLARMS 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, edited by Frans. Osinga and Tim Sweijs. TMC Asser Press, 2021. Available at https://ssrn.com/abstract=3748348

Dijck, José van, David Nieborg, and Thomas Poell. "Reframing Platform Power." *Internet Policy Review*, 8, no. 2. DOI: 10.14763/2019.2.1414.

Giumelli, Francesco, "Winning Without Killing: The Case for Targeted Sanctions." In *Winning without Killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, ed. Paul Ducheine and Frans Osinga, Netherlands Annual Review of Military Studies 2017 (TMC Asser Press, 2017).

Haaster, Jelle van, "*On Cyber: The Utility of Military Cyber Operations during Armed Conflict.*" PhD diss., University of Amsterdam, 2019.

Keulen, Roy van. "Digital Force: Disrupting Life, Liberty and Livelihood in the Information Age." PhD diss. Leiden University, 2018.

Łoś, R. "U.S. and China: Hard and Soft Power Potential," *International Studies. Interdisciplinary Political and Cultural Journal*, 22, no. 1 (2018): 39-50, https://doi.org/1018778/1641-4233.22.03.

Mann, Michael, "The Sources of My Sources," *Contemporary Sociology*, 42 no. 4, 499-502.

McCreadie, Maureen, and Ronald Rice. "Trends in Analyzing Access to Information. Part I: Cross-Disciplinary Conceptualizations of Access." *Information Processing and Management* 35 (1999): 45–76.

Ministry of Defence of the Kingdom of the Netherlands. *Netherlands Defence Doctrine.* June 2019.

NATO, *AJP-01 Allied Joint Doctrine*, Edition F Version 1. December 2022.

NATO *AJP-3.10 Allied Joint Doctrine for Information Operations*. November 2009.

NATO. *AJP-3.20, Allied Joint Publication for Cyber Operations*, Edition A Version 1. January 2020.

NATO. *MC 422/3, NATO Military Policy for Information Operations.*

Nye Jr, Joseph, "Hard, Soft, and Smart Power." In *The Oxford Handbook of Modern Diplomacy*, edited by Andrew Cooper, Jorge Heine, and Ramesh Thakur. Oxford University Press, 2013.

Reijer Passchier. *De vloek van Big Tech*. Boom Juridisch, 2024.

Pijpers, Peter, and Kraesten Arnold. "Conquering the Invisible Battleground." *Atlantisch Perspectief*, 44, no. 4 (2020).

CONCEPT

Pijpers, Peter B.M.J., and Paul A.L. Ducheine. "'If You Have A Hammer': Shaping the Armed Forces' Discourse on Information Maneuver." *International Journal of Intelligence and Counter-Intelligence* 36, no. 3 (2023).

Pijpers, Peter B.M.J., and Paul A.L. Ducheine. "Influence Operations in Cyberspace: How They Really Work." In *Hybridity, Conflict, and the Global Politics of Cybersecurity*, edited by Fabio Cristiano and Bibi van den Berg, Rowman & Littlefield, 2023.

Schrijver, Peter. 'The Wise Man Will Be Master of the Stars'. The Use of Twitter by a Military Intelligence Service in Wartime: The Case of the GUR 77. In *Reflections on the Russia-Ukraine War*, edited by Maarten Rothman, Lonneke Peperkamp, and Bas Rietjens. Leiden University Press, 2024.

Schrijver, Peter and Paul Ducheine. "Cyber-enabled Influence Operations: the Case of the Belarusian Cyber-Partisans." *Militaire Spectator* 192, no.11 (2023), 284-295.

Schroeder, Ralph. " Introduction: the IEMP Model and its Critics." In *An Anatomy of Power: The Social Theory of Michael Mann*, edited by J.A. Hall and Ralph Schroeder. Cambridge University Press, 2015.

Sommer, Udi, Eviatar Matania, and Nir Hassid. "The Rise of Companies in the Cyber Era and the Pursuant Shift in National Security," *Political Science*, 75, no.2: 140-164, DOI: 10.1080/00323187.2023.2278499

Timmer, Marije, and Paul Ducheine. "Conceptual Manoeuvring: The Interpretation of Information Manoeuvre within the Netherlands Ministry of Defence." *Militaire Spectator* 192, no. 11 (2023): 542-555.

UK Ministry of Defence, *Joint Doctrine Publication 0-01: British Defence Doctrine* (2011).

US Joint Chiefs of Staff, *Joint Publication 1: Doctrine for the Armed Forces of the United States* (2013).

Wiltenburg, Ivor. "Security Force Assistance: Practised but not Substantiated." *Militaire Spectator* 188, no. 2, 88-99.

Reports and Online Sources:

Amnesty International. *Amnesty International Position on the Proposals for a Digital Services Act and a Digital Markets Act, March 2021*. https://www.amnesty.eu/wp-content/uploads/2021/04/Amnesty-International-Position-Paper-Digital-Services-Act-Package_March2021_Updated.pdf.

Bank, Max and Bram Vanken. *How Big Tech's Revolving Doors Erode EU Antitrust Laws*. EU Observer, October 28, 2024. https://euobserver.com/news/ar1234f8b4.

Bateman, Jon. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." Carnegie Endowment for International Peace, December 2022. https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en.

Bellinger, John III. Suing China over the Coronavirus Won't Help. Here's What Can Work. *The Washington Post*, April 23, 2020. https://www.washingtonpost.com/opinions/2020/04/23/suing-china-over-coronavirus-wont-help-heres-what-can-work/.

CONCEPT

Bond, Shannon, and Bobby Allyn. *Russia is Restricting Social Media. Here's What we Know*. NPR, March 21, 2022. https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban (updated)

Brandom, Russell. *Google launches new anti-DDoS service called 'Project Shield*.' The Verge, 21 October 2013. https://www.theverge.com/2013/10/21/4862724/google-launches-new-anti-ddos-service-called-project-shield

Dave, Paresh, and Jeffrey Dastin. "Ukraine Has Started Using Clearview AI's Facial Recognition During War." *Reuters*, March 14, 2022. https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

Dwoskin, Elizabeth. A Flood of Misinformation Shapes Views of Israel-Gaza Conflict. *The Washington Post*, October 14, 2023. https://www.washingtonpost.com/technology/2023/10/14/propaganda-misinformation-israel-hamas-war-social-media/.

European Council, "EU sanctions against Russia explained", via: https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/

Farrow, Ronan. *Elon Musk's shadow rule*. *The New Yorker*, August 21, 2023. https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule.

Fedorov, Myhailo: Tweet ("while you try to colonize Mars …"), Twitter (now X), February 26, 2022. https://x.com/FedorovMykhailo/status/1497543633293266944

Google Threat Analysis Group and Mandiant. "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape." February 2023. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

Isidore, Chris. *Why many businesses are getting tougher on Russia than sanctions require*. CNN, 2022. https://edition.cnn.com/2022/03/03/business/business-go-beyond-russian-sanctions/index.html

Horowitz, Jason. *Italy Orders Seizure of Migrant Rescue Ship.* New York Times, November 20 2018. https://www.nytimes.com/2018/11/20/world/europe/italy-aquarius-seizure-order.html.

Howell O'Neill, Patrick. *Russia hacked an American satellite company one hour before the Ukraine invasion.* MIT Technology Review, May 10, 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

ICANN (2 March 2022), Letter from Göran Marby to Mykhailo Fedorov, via: https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

Khanal, Shaleen, Hongzhou Zhang, and Araz Taeihagh. *Why and How is the Power of Big Tech Increasing in the Policy Process? The Case of Generative AI*. Policy and Society, 2024. https://doi.org/10.1093/polsoc/puae012.

Lishchuck, Ruslana. *How Large Would Tech Companies Be if They Were Countries?*. *MacKeeper Blog*, August 13, 2021. https://mackeeper.com/blog/tech-giants-as-countries/.

Madory, Doug. *Updated: Cogent and Lumen curtail operations in Russia*. Kentik, March 7, 2022, https://www.kentik.com/blog/cogent-disconnects-from-russia/.

CONCEPT

Malik, Aisha. *Google Adds Air Raids Alerts to Android Phones in Ukraine*. TechCrunch, March 10, 2022. https://techcrunch.com/2022/03/10/google-adds-air-raid-alerts-to-android-phones-in-ukraine/?guccounter=2.

Man, Joseph. *Covert TikTok Campaign Blamed in Pro-Russian Romanian Candidate's Surge.* The Washington Post, December 5, 2024. https://www.washingtonpost.com/technology/2024/12/05/tiktok-romania-president-russia-infulence/.

Marquardt, Alex, "Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab," CNN, October 14, 2022, https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

Martin, Alexander. US Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command. Sky News, 2022. https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139.

McDaid, Cathal, and Rowland Corr. "The Mobile Network Battlefield in Ukraine - Part 3." *Adaptive Mobile Security*, 2022.

Meta. Meta's Ongoing Efforts Regarding Russia's Invasion of Ukraine. February 26, 2022. https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/.

Microsoft Threat Intelligence Centre. *Destructive Malware Targeting Ukrainian Organizations.* January 15, 2022.

Microsoft Threat Intelligence Centre. *A Year of Russian Hybrid Warfare in Ukraine*. March 15, 2023. https://nsarchive.gwu.edu/sites/default/files/documents/s9zfme-rssdn/2023-03-15-Microsoft-A-year-of-Russian-hybrid-warfare-in-Ukraine-MS-Threat-Intelligence.pdf

Microsoft. *Microsoft suspends new sales in Russia*. Microsoft Official Blog, 2022, https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/.

MilitaryNewsUA, 25 January 2024, Tweet ("Ukrainian Saker Scout drone with artificial intelligence"), via: https://twitter.com/i/status/1750444954298577263.

Minkin, Amelia and Michael Beckel. *Big Tech Ramps Up Lobbying as Industry Seeks to Thwart Legislation to Protect Kids Online*. IssueOne, October 22, 2024, https://issueone.org/articles/big-tech-ramps-up-lobbying-as-industry-seeks-to-thwart-legislation-to-protect-kids-online/.

Musk, Elon (@elonmusk), Twitter (now X), February 26, 2022, https://x.com/elonmusk/status/1497701484003213317.

Nix, Naomi, Will Oremus, and Aaron Gregg. *Meta Ends Fact-Checking, Drawing Praise from Trump*. The Washington Post, January 7, 2025, https://www.washingtonpost.com/technology/2025/01/07/meta-factchecking-zuckerberg/.

O'Neill, Patrick Howell. *Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion.* MIT Technology Review. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

Paresh, Dave, and Jeffrey Dastin. "Ukraine Has Started Using Clearview AI's Facial Recognition During War." *Reuters*, March 14, 2022.

CONCEPT

https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

Price Waterhouse Coopers. *Global Ranking of the Top 100 Public Companies by Market Capitalisation – Global Top 100 Companies – April 2024.* https://www.pwc.co.uk/services/audit/insights/global-top-100-companies.html?WT.mc_id=CT1-PL50-DM2-TR3-LS3-ND30-TTA9-CN_Captial-Markets-Assurance-Global-Top-100-Companies-Annual-Report-.

Radio Free Europe, "Ukraine Tells UN's Top Court Russia Using 'False' Genocide Allegations As Pretext For War," https://www.rferl.org/a/ukraine-tells-un-russia-false-genocide-war-pretext/32599619.html, September 19, 2023.

Rodriguez, C.A., T.C. Walton and C. Hyong, "Putting the "fil" into "dime": growing joint understanding of the instruments of power", *Joint Force Quarterly*, 97 no.2 (2020).

Roulette, Joey, "SpaceX curbed Ukraine's use of Starlink internet for drones -company president," *Reuters*, February 9, 2023, https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/.

Sanger, Andrew (17 March 2022). "Piercing the State's Corporate Veil: Using Private Actors to Enforce International Norms". EJIL: Talk! via https://www.ejiltalk.org/piercing-the-states-corporate-veil-using-private-actors-to-enforce-international-norms/.

Sari, Aurel, "Hybrid threats and the law: Concepts, trends and implications," *Hybrid Centre of Excellence Trend Report* 3 (April 2020), https://www.hybridcoe.fi/wp-content/uploads/2020/05/Hybrid-CoE-Trend-Report-3.pdf.

Satariano, Adam. *Facebook's Oversight Board Faults its Policy on Preferential Treatment*. The New York Times, October 21, 2021. https://www.nytimes.com/2021/10/21/business/facebook-oversight-board-members-criticism.html.

Shumpenthung Ezung and Kekhronei O Koza. *The Influence of Social Media on Public Discourse: Examining How Social Media Shape Popular Opinion*. International Journal of Contemporary Research in Multidisciplinary, 3 no. 6, 2024, DOI: https://doi.org/10.5281/zenodo.14252454.

Soesanto, Stefan. "The IT Army of Ukraine: Structure, Tasking, and Ecosystem." CSS Cyberdefense Report, June (2022). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf.

Sonne, Paul, Missy Ryan, and John Hudson. *Russia Planning Potential Sabotage Operations in Ukraine, U.S. Says.* The Washington Post, January 14, 2022. https://www.washingtonpost.com/national-security/russia-ukraine-invasion-sabotage-operations/2022/01/14/769314a2-754f-11ec-8ec6-9d61f7afbe17_story.html

Stieglitz, Stefan, and Björn Ross. *The Impact of Social Media on Social Cohesion: A Double-Edged Sword*. Media and Communication, 10, no.2, 2022. https://doi.org/10.17645/mac.v10i2.5792.

Sullivan, Eilleen, and Benjamin Weiser. *U.S. Seizes North Korean Ship for Violating Sanctions*. New York Times, 9 May 2019. https://www.nytimes.com/2019/05/09/us/politics/wise-honest-north-korea-ship-seized.html.

CONCEPT

The White House. *Restoring Freedom of Speech and Ending Federal Censorship*. Executive Order, January 25, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship/.

Tucker, Katherine, and Maria Robson-Morrow. *Intelligence outsourcing for non-traditional clients: the rise of private sector intelligence providers.* Intelligence and National Security, 1-20. https://doi.org/10.1080/02684527.2024.2437958© 2025.

US Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and, October 19, 2020;

US Department of Justice, "Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government," https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government, September 6, 2024;

Valovic, Tom. *Big Tech Companies Are Becoming More Powerful Than Nation-States*. Metapsychisis – Journal of Consciousness, Literature and Art, May 13 2024. https://metapsychosis.com/big-tech-companies-are-becoming-more-powerful-than-nation-states/.

Weymouth, Lally. *Volodymyr Zelensky: 'Everyone Will Loss' If Russia Invades Ukraine.* The Washington Post, January 20, 2022, https://www.washingtonpost.com/outlook/2022/01/20/ukraine-russia-zelensky-interview/.

Yenin, Yevgeny. Deputy Minister of Foreign Affairs of Ukraine. Source: Clearview AI. Retrieved June 28, 2024. https://www.clearview.ai/ukraine.

Young, N. *The Cultural Crusades*. New Internationalist 423, https://newint.org/features/2009/06/01/culture.

Zakrzewski Cat. *Elon Musk goes global with his playbook for political influence*. *The Washington Post*, January 5, 2025. https://www.washingtonpost.com/politics/2025/01/04/elon-musk-uk-germany-canada-far-right/.

CONCEPT