Internal Security Review

2024, no. 31, pp. 279–320

CC BY-NC-SA 4.0 https://doi.org/10.4467/20801335PBW.24.027.20804

ARTICLE

The potential of Cyber Threat Intelligence analytical frameworks in research on information operations and influence operations

KAMIL BARANIUK

Faculty of Social Sciences, University of Wrocław
Polish Association for National Security
https://orcid.org/0000-0002-8071-434X

PIOTR MARSZAŁEK

Polish Association for National Security
https://orcid.org/0009-0000-0362-4132

Abstract

The article's aim is to evaluate the utility of using the Cyber Threat Intelligence (CTI) approach in analysing information and influence operations. The study was carried out by a comparative method based on the technique of desk research. The point of comparison for the CTI methodology were methods originated in communicology, which are relatively popular in the study of propaganda. The authors try to answer the question of what methodological contribute to the study of the discussed phenomena – and thus to the practical potential of the analyst's workshop – is the adoption of a paradigm for the analysis of information operations and influence operations based on models of tactics, techniques, and procedures (TTPs) recognition and taxonomy of ICT incidents or typification of CTI threat actors. The central focus of the study is a critical analysis of English-language publications discussing the use of CTI in disinformation analysis. The main conclusion from the analysis includes a thesis about the limited methodological benefits of CTI based methods, while using their technical and organisational strengths to research elements of information operations and influence operations in which cyberspace is used.

Keywords information warfare, influence operations, information operations, disinformation, cybersecurity, CTI

Introduction

Cyber Threat Intelligence (CTI) is now an integral part of the process of ensuring cyber security[1] in areas where there is an alleged adversary. The development of this discipline, linked to the need to respond to the increasing creativity and sophistication of adversaries, is helping to encompass ever new elements of evolving cyber threats into the analysis process. The use of a common conceptual apparatus, models and standards greatly enhances the cooperative potential of cyber security professionals. The ambition of CTI experts is to ensure the ability of organisations, including the state and its citizens, to take pre-emptive action calculated to eliminate or minimise, e.g. through active defence, the effects of malicious actions.

The aim of the authors of the article was to assess the usefulness of using the CTI approach in the analysis of information operations and influence operations, i.e. proposals currently popularised by, among others, the European Union Agency for Cybersecurity (ENISA)[2]. The authors attempted to answer the question of what methodological contribution to the research of the phenomena in question – and thus to the practical potential of an analyst's workshop – is provided by the adoption of a model for analysing information and influence operations based on the recognition of tactics, techniques, and procedures (TTPs), threat actors and inspiration from the terminology of ICT incidents.

[1] 'Cyber security' and other terms used in this article are defined later on.

[2] See in more detail: *Cybersecurity and Foreign Interference in the EU Information Ecosystem*, ENISA, 8 XII 2022, https://www.enisa.europa.eu/news/cybersecurity-foreign-interference-in-the-eu-information-ecosystem [accessed: 20 IX 2024]; *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape*, ENISA, 8 XII 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape [accessed: 20 IX 2024].

The authors achieved the stated aim using the assumptions of the general methodology – analysis and synthesis – which were carried out using the comparative method and the technique of analysing existing sources.

In the first part of the article, a source analysis aimed at discussing the basics of CTI and the analytical models used within its framework was carried out. In the second part, the authors attempted to define the essence of information operations and influence operations on the basis of examples of publicly available materials and literature produced by institutions that are obliged to deal with such phenomena, i.e. institutions of the security sector (mainly normative documents of the Western armed forces in the form of doctrines and instructions, as well as literature related to the functioning of special services in the form of professional glossaries, dictionaries and lexicons). It discusses the understanding of these phenomena by actors in the social platform and IT industries. The social networks Facebook and X as well as Microsoft were used as examples. The aim of this part of the article was to analyse the relationship of influence and information operations with cyber security and cyberspace. In the third and fourth parts of the article, the authors synthesised the academic literature and other literature on the subject to compare methods of analysing information operations and influence operations using research methods derived from communication sciences and – adapted for these purposes – models used in CTI.

Cyber Threat Intelligence as part of ensuring cyber security

A discussion of the essence of CTI should begin by outlining the area of cyber security for which it is responsible. The cyber threat sphere[3] is growing rapidly, both qualitatively and quantitatively. This is due to the constant increase in the number

[3] The concept of cyberspace, which is used by academics and experts alike, has its origins in popular culture and - in a nutshell - can be assumed to refer to a vast sphere alternative to the real (physical) world, based on the links between telecommunications and information devices. See: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni* (Eng. Definition outline of cyberspace), "Przegląd Bezpieczeństwa Wewnętrznego" 2013, no. 9, pp. 225–226. The term 'cyberspace' also functions in Polish legal circulation and means, in accordance with Article 2(1)(1b) of the *Act of 29 August 2002 on martial law and the competences of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland*, '(…) the space for processing and exchanging information created by ICT systems (…) together with the links between them and the relations with users'. Polish legislation, on the other hand, defines the term 'ICT system' as, pursuant to Article 3(3) of the *Act of 17 February 2005 on Informatisation of the Activities of Entities Performing Public Tasks*, '(…) a set of cooperating IT devices and software ensuring processing, storage, as well as sending and receiving data via telecommunication networks by means of a telecommunication terminal device appropriate for a given type of network, within the meaning of the provisions of the Act of 12 July 2024 - Electronic Communications Law'.

of threat actors, highly motivated to exploit the opportunities created by virtual reality to carry out actions that harm the assets of others. Depending on their motivation (e.g. financial or political), these actors target individuals (e.g. identity theft) as well as organisations (e.g. financial fraud) and state entities (e.g. cyber espionage, computer sabotage).

Providing any organisation, state, but also an individual with cyber security in the broadest sense would therefore not be complete if, in identifying and countering threats in cyberspace, a deeper knowledge of the threat creators was not sought. Actions taken in cyberspace, although benefiting from its various facilities[4], do not take place without leaving traces and leads (i.e. data) that can be collected and taken into account in retrospective analysis. This data can also be used to take pre-emptive action, which is the most advantageous move in certain situations.

An area of knowledge with the ambition of strengthening an organisation's defensive capabilities in cyberspace, developed at the intersection of computer science, cyber security and intelligence studies, is CTI[5]. There are many definitions of this concept[6]. This is related, among other things, to the commercial development of the cyber security industry, within which CTI functions as a product or service (e.g. paid access to threat intelligence feeds) and is subject to the laws of the commercial market and marketing needs[7]. To a lesser extent, CTI is a domain of scientific research, including methodological research, remaining an area requiring theoretical reflection[8].

For the purpose of this article, the authors adopted the definition of CTI proposed in the *CTI-CMM Cyber Threat Intelligence Capability Maturity Model* document. According to it, it is a discipline focused on understanding

[4] These facilities, compared to the physical dimension of the information environment, increase the possibilities of hiding or falsifying identities and make the actions taken geographically unconstrained.

[5] K. Oosthoek, Ch. Doerr, *Cyber Threat Intelligence: A Product Without a Process?*, "International Journal of Intelligence and Counter Intelligence" 2021, vol. 34, no. 2, p. 301. https://doi.org/10.1080/08850607.2020.1780062.

[6] It is not uncommon for the term *cyber threat intelligence (CTI)* to be used interchangeably with *threat intelligence (TI)*, a concept that is meaningfully broader. As Scott J. Roberts and Rebekah Brown point out, TI is the analysis of adversaries, their capabilities, motivations and goals, while CTI is the analysis of how adversaries use cyberspace to achieve their goals. See: S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response. Outwitting the Adversary*, Sebastopol 2017, pp. 2–3.

[7] *An introduction to threat intelligence*, CERT-UK, https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf, p. 2 [accessed: 10 IX 2024].

[8] K. Oosthoek, Ch. Doerr, *Cyber Threat Intelligence*…, pp. 301–302.

the capabilities, intentions, motivations and opportunities of cyber adversaries and their associated tactics, techniques and procedures[9] of action (TTPs)[10].

Framing CTI as a process involves, among other things, organising and systematising the activities undertaken in the form of an intelligence cycle, aiming to produce useful knowledge that meets the information needs of the recipient. Drawing extensively on the heritage of intelligence analysis is intended to ensure, or rather impose, appropriate rigour and quality on the analytical process. Therefore, constant elements of CTI lectures are: the use of structured analytical techniques (e.g. competitive hypothesis analysis) and the use of standardised language expressing the degree of certainty of judgements made or the degree of probability of events described[11].

As in intelligence analysis[12], CTI information products are divided into three levels: tactical, operational and strategic. Thus, they direct the knowledge obtained to the appropriate decision-making level. The lowest level, tactical, comprises information that has a short lifecycle but is necessary for the direct detection and mitigation of a threat by technical teams monitoring the cyber security of systems or incident response teams. At this level, the primary forms of information provided by CTI are indicators of compromise (IoC), i.e. artefacts such as IP address, domain, file hash. Their presence in a protected system indicates a breach of its security. The operational level usually includes information about the campaign (operation) conducted by the adversaries, together with characteristics of the modus operandi and motive (e.g. data theft). This level includes the behavioural dimension (i.e. TTPs), describing how the attacker achieves their goal. Linking the behavioural observations to information about the infrastructure used in the operation, as well as interpreting the motivation and intended objectives of the operation, can provide the basis for attribution, i.e. the assignment of the operation to a particular actor, e.g. an APT

[9] On the importance of TTPs in CTI, see: *TTP in cybersecurity*, Sekoia, https://www.sekoia.io/en/glossary/ttp-cyber-tactics-techniques-and-procedures/ [accessed: 9 IX 2024].

[10] M. DeBolt et al., *CTI-CMM Cyber Threat Intelligence Capability Maturity Model*, Version 1.0, https://d39ec1uo9ktrut.cloudfront.net/Datasheets/CTI-CMM-Cyber-Threat-Intelligence-Capability-Maturity-Model.pdf, p. 70 [accessed: 22 VIII 2024]. The CTI-CMM (version 1.0) is a document describing the maturity model of an organisation's CTI programme, published in 2024 and developed as a consensus of a group of 27 experts from the private and public sectors.

[11] See: *Words of Estimative Probability, Analytic Confidences, and Structured Analytic Techniques*, Center for Internet Security, https://www.cisecurity.org/ms-isac/services/words-of-estimative-probability-analytic-confidences-and-structured-analytic-techniques [accessed: 23 VIII 2023]. The scale of the actual use of methods and tools drawn from intelligence analysis in the work of CTI teams may be greatly overstated, being a postulate rather than a daily routine for CTI practitioners. See: K. Oosthoek, Ch. Doerr, *Cyber Threat Intelligence*…, pp. 304–305.

[12] See: *Words of Estimative Probability, Analytic Confidences*…

(advanced persistent threat) group[13]. The strategic level meets the information needs of top-level audiences, e.g. those creating an organisation's or state's cyber security policy, and enables strategic cyber security actions, supported by a structured intelligence process[14].

Analytical models and information exchange platforms in CTI

The dynamic development of threat defence methods and techniques, driven by the need to balance or exceed the potentials between defenders and attackers, has resulted in the development of analytical models (analytical frameworks), taxonomies, ontologies or data exchange standards (e.g. STIX format, structured threat information eXpression)[15]. Leading analytical models used in CTI include: Cyber Kill Chain, MITRE ATT&CK and Diamond Model.

The Cyber Kill Chain model, proposed and characterised by Eric M. Huthins and others at Lockheed Martin in the article *Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*[16], is a decomposition of a cyber attack into seven consecutive stages that an attacker must complete to achieve his goal. These are:

1) reconnaissance,
2) weaponization,
3) delivery,
4) exploitation,
5) installation,
6) command & control, C2,
7) actions on objectives.

[13] The issue of attribution in CTI is an important element of it, as it answers the fundamental question – who generates the threat? This kind of question can usually only be answered partially or uncertainly, which is due, among other things, to the fact that many actors hide their true identity. On the attribution of CTI, see: J. Collier, S. Ronis, *Navigating the Trade-Offs of Cyber Attribution*, https://cloud.google.com/blog/topics/threat-intelligence/trade-offs-attribution/ [accessed: 22 VIII 2024].

[14] S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response*…, pp. 24–25.

[15] On the taxonomy, ontology, data exchange standards (STIX) in CTI see: V. Mavroeidis, S. Bromander, *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*, https://arxiv.org/pdf/2103.03530 [accessed: 24 VIII 2024] – preprint from a paper presented at the 2017 European Intelligence and Security Informatic Conference; *Introduction to STIX*, https://oasis-open.github.io/cti-documentation/stix/intro.html [accessed: 24 VIII 2024].

[16] E.M. Hutchins, M.J. Cloppert, R.M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [accessed: 24 VIII 2024].

From a defensive perspective, aborting an attack at any stage, preferably as early as possible, results in its thwarting. Among other things, this model supports the abstraction of the TTPs and facilitates the understanding of the actions taken by the attacker[17].

Another analytical tool is the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) model[18], which is a knowledge base that currently includes more than 200 unique techniques and more than 400 sub-techniques used by attackers, categorised under 14 tactics. The inclusion of these techniques in the model is a result of observations of intrusions that have occurred, so the model is constantly expanding. ATT&CK allows the actions of a specific attacker, such as an APT group, to be modelled through the lens of techniques used in earlier campaigns. For example, the APT29 group[19], associated with the Foreign Intelligence Service of the Russian Federation, used more than 40 techniques in its hacking campaign against the US IT service provider – SolarWinds[20]. Among these, the technique of acquiring the infrastructure (technique), i.e. the internet domains (sub-technique)[21] necessary to establish a command and control (C2) mechanism, can be mentioned as an example. The defensive application of MITRE ATT&CK involves, among other things, the implementation of technical solutions that mitigate or detect the use of a specific technique known to be used by an attacker interested or likely to be interested in the protected organisation or sector[22].

The diamond model (Figure 1), described by Sergio Caltagirone et al. in their article *The Diamond Model of Intrusion Analysis*, bases its structure on four interdependent elements. These are: adversary, victim, infrastructure and capability. As the authors of this publication point out, the *adversary* uses his or her capabilities through a specific infrastructure against the victim[23]. The adversary is assumed to be an entity, e.g. an individual or an organisation, aware of its objectives and the means necessary to achieve them, with specific intentions, requiring an attempt to break into

[17] S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response…*, pp. 35–36. The Cyber Kill Chain model has seen many extensions, such as the Unified Kill Chain model. See in more detail: P. Pols, *The Unified Kill Chain. Raising resilience against advanced cyber-attacks*, https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf [accessed: 24 VIII 2024].

[18] See: *ATT&CK Matrix for Enterprise*, Attack. Mitre, https://attack.mitre.org/ [accessed: 24 VIII 2024].

[19] *APT29*, Attack. Mitre, https://attack.mitre.org/groups/G0016/ [accessed: 24 VIII 2024].

[20] *SolarWinds Compromise*, Attack. Mitre, https://attack.mitre.org/campaigns/C0024/ [accessed: 24 VIII 2024].

[21] *Acquire Infrastructure: Domains*, Attack. Mitre, https://attack.mitre.org/techniques/T1583/001/ [accessed: 24 VIII 2024].

[22] Many techniques have assigned methods for their detection and mitigation along with an identifier.

[23] S. Caltagirone, A. Pendergast, Ch. Betz, *The Diamond Model of Intrusion Analysis*, https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf, p. 7 [accessed: 24 VIII 2024].

a computer network or system. On the attacker's side, a distinction is made between the operator (the contractor, the 'hacker') and the customer (the principal) who derives the ultimate benefit from the action. Capabilities refer the tools and techniques used in a specific act of intrusion (event), such as malware. The infrastructure element is the physical or logical resources used by the attacker to deliver and maintain the capability and gain the effects of the capability. These include, for example, used email addresses, social media accounts, C2 servers, planted USB sticks. The victim affected by a capability can be a person, an organisation (victim persona) or a related asset (victim asset), such as a network, device or website. An important concept organising the analysis in the model is the diamond event. According to the axioms of the model, for every intrusion there is an adversary taking a step towards the intended goal through the use of a capability. The events are autonomous (a single, indivisible step) and comprise a time-ordered activity threads, i.e. a sequence of logically related actions of the adversary. The accumulation of information from the analysed events allows us to broaden our knowledge of the nodes of the diamond, while moving along its edges (pivoting) exposes the relationships between them. Building an in-depth picture of the adversary's actions also includes such meta-features as timestamp, result, methodology and others[24].

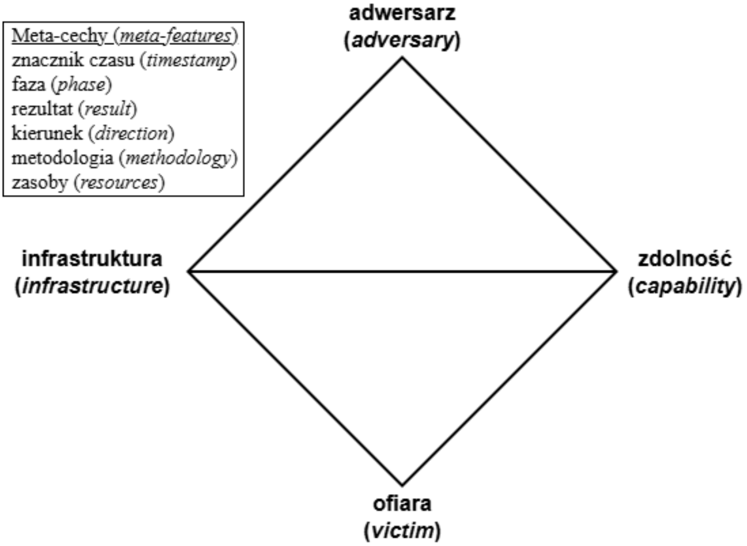

Figure 1. Visualisation of the diamond model.

Source: own elaboration based on: S. Caltagirone, A. Pendergast, Ch. Betz, *The Diamond Model of Intrusion Analysis*, Active Response, https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf, p. 9 [accessed: 24 VIII 2024].

[24] Ibid., pp. 7–13; S.J. Roberts, R. Brown, *Intelligence-Driven Incident Response*..., pp. 49–50.

The use of the analytical models presented has been limited to the three most popular, but sufficient to indicate the analytical potential arising from their use in the investigation of intentional cyber threats. These models are complementary, allowing the analytical process to be structured, including the identification of areas of high assurance and usability or that represent intelligence gaps[25].

Organisations with a similar threat profile or facing potentially the same adversary have an incentive to combine efforts in the area of threat intelligence[26]. This cooperation is often institutionalised, such as within information sharing and analysis centres (ISAC)[27]. The practice in this area is to automate information sharing, especially at the tactical and operational level, through the use of threat intelligence (TI) platforms, e.g. the open-source MISP Threat Sharing (Malware Information Sharing Platform)[28] or OpenCTI[29].

Defining information and influence operations

What needs to be confronted is the relationship between cyber security and information operations as well as influence operations, and how disjoint in meaning the two types of activities are. According to the Oxford English Dictionary, the term 'operation' originated in French and Latin. The sources of its modern understanding emerged in the 18th century, at which time it began to be used in mathematics and the military, among other fields[30]. Following the Cambridge Dictionary, it can be assumed that in a general sense the term 'operation' means 'an activity that is planned to achieve something'[31]. A similar formulation can be found in the Dictionary

[25] For a comparison of the models in question, see: F.M. Ferazza, *Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model: a comparison of cyber intrusion analysis models*, https://www.royalholloway.ac.uk/media/20188/techreport-2022-5.pdf.pdf [accessed: 25 VIII 2024].

[26] On the exchange of information in the CTI area, see: T.D. Wagner et al., *Cyber Threat Intelligence Sharing: Survey and Research Directions*, https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf [accessed: 24 VIII 2024].

[27] See: *Information Sharing and Analysis Centres (ISACs). Cooperative models*, ENISA, 2017, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/@@download/fullReport, pp. 7–8 [accessed: 24 VIII 2024].

[28] *MISP. Threat Sharing*, https://www.misp-project.org/ [accessed: 24 VIII 2024].

[29] *OpenCTI*, https://filigran.io/solutions/open-cti/ [accessed: 24 VIII 2024].

[30] *Oxford English Dictionary*, https://www.oed.com/dictionary/operation_n?tab=factsheet&tl=true#33665121 [accessed: 28 XII 2023].

[31] *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/operation [accessed: 28 XII 2023].

of the Polish Language (inter alia: 'actions aimed at accomplishing a specific task')[32]. For the purposes of the article, the authors assume that an operation means a set of purposeful activities, depending on the industry and field, aimed at achieving various objectives.

In the theoretical heritage of the US Army, the term 'information operations' (InfoOps) has been around since 1996, when activities in this area were included in the *Joint Doctrine for Command and Control Warfare* (C2W)[33]. The term 'command and control warfare (C2W)' was used to describe information warfare (i.e. actions taken to achieve information superiority) conducted as part of military operations. In US C2W doctrine at the time, this included the integrated use of psychological operations (PSYOPS), military deception, operations security (OPSEC), electronic warfare and physical destruction, supported by intelligence to impede an adversary's ability to access information, degrade, destroy or influence his command capability and, at the same time, defend against such actions[34]. The US Army's field manual FM 100-6, published in 1996, states that all aspects of information are integrated in the information operations to its full potential in the conduct of military operations. It was further pointed out that in the information age, the commander operates in an increasingly complex information environment, which includes both military and non-military (global) information environment issues. This environment is made up of, among others, foreign governments, political leaders, the media, international organisations and even individuals. It is worth noting that already at that time the range of activities covered by information operations was wide – they were both techno – and anthropocentric in nature[35]. Influenced by subsequent changes made to US Army doctrine, the term 'information operations' began to be equated with the C2W activities described earlier. These activities were expanded to include other types

[32] *Słownik języka polskiego PWN* (Eng. PWN Dictionary of the Polish Language), https://sjp.pwn.pl/szukaj/operacja.html [accessed: 3 VII 2024].

[33] I.R. Porche et al., *Redefining Information Warfare Boundaries for an Army in Wireless World*, https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf, p. 103 [accessed: 28 XII 2023].

[34] *Joint Doctrine for Command and Control Warfare (C2W)*, https://apps.dtic.mil/sti/pdfs/ADA357635.pdf, pp. 14–15 [accessed: 28 XII 2023].

[35] Headquarters Department of the Army, *FM 100-6, Information Operations*, Washington 1996, https://www.hsdl.org/?view&did=437397, pp. 5–12 [accessed: 28 XII 2023]. It should be emphasised that, doctrinally speaking, information operations can be carried out in three dimensions of the information environment – cognitive (human-related), informational (data-related) and physical (related to the material, real sphere). See: *Information Operations. Joint Publication 3-13*, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf, pp. 7–8 [accessed: 30 I 2023].

of activity, including computer network operations (such changes occurred in FM 3-13 document). In subsequent doctrinal documents (JP 3-13), the concept of strategic communication emerged, encompassing both information operations and activities at the level of public affairs and defence support for public diplomacy[36].

NATO Allied Joint Publication-10.1 (*Allied Joint Doctrine for Information Operations*) states that information operations are activities that can be used in peacetime as well as in times of crisis and conflict to provide a comprehensive understanding of the information environment, in particular the audience, and give the opportunity to plan specific activities to achieve cognitive effect and support in other areas of operations[37]. The details of the doctrine point, among other things, to the role of influence on the audience through action based on NATO narrative-led execution[38].

In the case of both NATO doctrine and the previously cited US Army documents, the concept of influence operations does not appear, although influencing audiences, decision-making, troop morale and enemy command staffs is embedded in their essence. Attempts to create a definition of this concept for doctrinal purposes do appear in expert studies, but these most often emphasise the complexity of operations and their strategic level, i.e. the characteristics of strategic communication activity[39].

[36] On developments in the doctrines, see in more detail: I.R. Porche et al., *Redefining Information Warfare Boundaries…*, pp. 103–112.

[37] Literal definition: "Information operations (InfoOps) is applicable in peace, crisis and conflict throughout the continuum of competition. It provides a comprehensive understanding of the information environment and, in particular audiences, the ability to plan specific activities for cognitive effect and provides support to planning of all activities in the engagement space, which are then assessed to enable refinement of plans to meet objectives". See: *Allied Joint Doctrine for Information Operations (AJP-10.1)*, UK Ministry of Defence, https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101, p. 11 [accessed: 28 XII 2023].

[38] Ibid., p. 12.

[39] See: E.V. Larson et al., *Foundations of Effective Influence Operations. A Framework for Enhancing Army Capabilities*, Rand Corporation, 2009, https://www.rand.org/pubs/monographs/MG654, pp. 2–6 [accessed: 18 XI 2024]. Understanding an influence operation as planned, directed towards the achievement of set objectives, utilising the broad resources and instruments of the state (within foreign policy, military, intelligence, media) and coordinated by the highest levels of the state administration may be legitimate, but from the perspective of the article does not represent a qualitative change to the activities undertaken in strategic communication. In NATO nomenclature, strategic communication primarily refers to the coordination and appropriate use of communication activities and capabilities in support of Alliance policy, operations and activities. StratCom activities include: public diplomacy, civilian and military public affairs activities,

In the view of the authors of this article, the rationale for distinguishing influence operations as a distinct type of planned activity lies primarily in their specific means of implementation, namely the agents of influence. The term appears in the glossary of intelligence definitions and terms published by the Central Intelligence Agency (CIA) and describes a person manipulated by an intelligence organisation in order to use his or her position to influence public opinion or the decision-making process in a way that favours the goal of the country for which the organisation is acting[40]. The term 'agent of influence' also appears in a glossary of terms published in 2011 by one of the institutions dealing with, inter alia, counterintelligence in the defence ministry in the United States (Defense Counterintelligence and Human Intelligence operating within the Defense Intelligence Agency). This publication also assumes that it is a person who uses his or her position to influence public opinion or make decisions to benefit the country with which the service for which the agent is acting is associated. In doing so, it is pointed out that the term is derived from terminology

information operations (including psychological operations). See: *About Strategic Communications*, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/about_us/about-strategic-communications/1 [accessed: 10 VII 2024]. The doctrinal basis for StratCom within NATO has been developed since 2009. On this subject, see in more detail: D. Niedzielski, *Wojskowa doktryna komunikacji strategicznej NATO i jej znaczenie dla Polski* (Eng. NATO's military strategic communications doctrine and its relevance to Poland), "Akademickie Centrum Komunikacji Strategicznej" 2022, no. 3, https://www.wojsko-polskie.pl/aszwoj/u/af/14/af143adc-70e6-463a-8448-faaf0df61e9a/biuletyn_nr_3.pdf, pp. 46–53 [accessed: 10 VII 2024]. A similar, i.e. emphasising the importance of coordinating communication activities, understanding of this aspect is found in the non-military part of the state security system. This is evidenced, for example, by the postulate formulated in the 2020 National Security Strategy of the Republic of Poland (hereinafter: NSS), indicating the necessity of creating a unified system of strategic communication of the country in the context of ensuring the secure functioning of the state and citizens in the information space. See: *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020* (Eng. National Security Strategy of the Republic of Poland 2020), https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, p. 21 [accessed: 10 VII 2024]. In the 2020 NSS, 'information space' is defined as 'the interpenetrating layers of space: virtual (systems, software and applications layer), physical (infrastructure and hardware) and cognitive'. The cognitive sphere of information space is therefore an essential element that broadens it objectively compared to the concept of cyberspace (see note 4). At the same time, it should be noted that the optics of information space adopted in the 2020 NSS are in line with the perception of the dimensions of the information environment on the basis of NATO doctrines. See in more detail: Z. Modrzejewski, *Information operations from the Polish point of view*, "Obrana a strategie" (Defence and Strategy) 2018, no. 1, pp. 118–119. https://doi.org/10.3849/1802-7199.18.2018.01.113-130.

[40] *Glossary of Intelligence Terms and Definitions*, https://www.cia.gov/readingroom/docs/CIA-RDP80M00596A000500020003-7.pdf, p. 1 [accessed: 28 XII 2023].

created by the Soviets[41]. Similarly, the term is defined in the *Great Lexicon of the World's Special Services* by Jan Larecki. There is also a conscious cooperation of a person with a foreign intelligence service in order to use his or her political, social or professional position to promote the objectives of another state, influence the decision-making process, the economic situation, etc. Larecki draws attention to the strategic and long-term nature of influence operations, their high degree of secrecy, as well as the particularly valuable nature of influence agency and its difference from 'classical' (information-gathering) agency[42].

Influence operations will thus be intelligence activities carried out using agent intelligence resources to influence another state, e.g. in the sphere of foreign and security policy, the conduct of socio-political activity resulting in the destabilisation of the state, the financing from foreign sources of political corruption activities or the conduct of illegal economic lobbying. It should be emphasised that the scope and means of implementing influence operations are constantly expanding. According to the Federal Bureau of Investigation (FBI), this type of activity currently also includes activities in cyberspace. With regard to this space, US counterintelligence primarily points to attacks on targets related to the electoral process, i.e. voting infrastructure, candidates in elections[43]. Viewing cyberspace as an area where influence operations are carried out is a broader trend. Another example of adopting this perspective is the US agency responsible for cyber security and the coordination of critical infrastructure protection efforts, the Cybersecurity & Infrastructure Security Agency (CISA). The agency identifies a wide range of threat-generating sources, assuming that these are malicious actors, and that the influence operations themselves consist of, among other things, information manipulation techniques

[41] *Terms & Definitions of Interest for DoD Counterintelligence Professionals*, https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf, p. 4 [accessed: 28 XII 2023].

[42] J. Larecki, *Wielki leksykon służb specjalnych świata* (Eng. Great lexicon of the world's special services), Warszawa 2007, pp. 30–31. Mirosław Minkina refers to activities that by their scope and objectives are the same as influence operations by the terms: 'clandestine operations' and 'non-influence operations'. In doing so, he emphasises their distinctiveness from 'classical' intelligence activities aimed at gathering information. In this view, information operations/influence operations are: covertly supporting a friendly state, influencing the perception and evaluation by states of intelligence interest, influencing the perception and evaluation by the public of a state of intelligence interest, supporting friendly political movements, and influencing events with violence. See in more detail: M. Minkina, *Sztuka wywiadu w państwie współczesnym* (Eng. The art of intelligence in the modern state), Warszawa 2014, pp. 227–245.

[43] *Combating Foreign Influence*, FBI, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [accessed: 2 XI 2024].

(misinformation, disinformation, malinformation)[44] through which foreign actors achieve their own objectives[45].

From the perspective of the nomenclature used in the force sector (military, special services), information operations and influence operations are therefore different types of activity, although similar to some extent. Influence operations, due to their access to clandestine (covert) means of implementation, are characteristic of the activities of intelligence services and their most important objective is to support the broader state policy (mainly foreign and security). As such, they are defined by specific attributes characteristic of intelligence activities, including: institutions of covertness, methods of recruiting and conducting influence agents, as well as communication channels used to finance and task them[46]. Influence operations in cyberspace (the term 'cyber influence operation' is used in expert discourse[47]) on the other hand, can consist of, for example, hack and leak operations.

[44] Some experts dealing with threats in the information space use the distinction between disinformation and the related – but ambiguous – terms *malinformation* and *misinformation*. The term *disinformation* is associated with the deliberate and intentional dissemination of false information with the aim of causing harm. *Misinformation* is assumed to be the dissemination of false information but without the intention to cause harm, and *malinformation* is assumed to be the use of truthful information to cause harm. On this subject, see in more detail: C. Wardle, H. Derakhshan, *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe report DGI(2017)09, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html, pp. 20–22 [accessed: 10 VII 2024].

[45] *Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure*, https://www.cisa.gov/sites/default/files/2023-01/cisa_insight_mitigating_foreign_influence_508.pdf, p. 1 [accessed: 29 XII 2023].

[46] For a comprehensive description of a contemporary Russian FSB special service influence operation aimed at destabilising, dismantling and then seizing power in Ukraine in 2022 using influence agents, see the study published by the UK-based think-tank Royal United Services Institute. See: J. Watling, O. Danyluk, N. Reynolds, *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023*, https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf [accessed: 10 VII 2024]. In the Polish literature, an in-depth analysis of this operation was conducted by Marek Świerczek. See: M. Świerczek, *Working methods of the Russian secret services in the light of the Oleg Kulinich case*, "Internal Security Review" 2023, no. 29, pp. 289–322. https://doi.org/10.4467/20801335PBW.23.031.18773. It should be noted that the nomenclature for influence operations is not uniform in the Western intelligence community either and is constantly expanding. In 2024, the US National Intelligence Council published a glossary of several pages of terms for so-called 'grey area' activities. Its scope includes, inter alia, influence operations and other definitively similar terms, such as covert operation, foreign influence and unconventional warfare. See: *Updated IC Gray Zone Lexicon: Key Terms and Definitions*, https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf [accessed: 11 VIII 2024].

[47] P. Brangetto, M.A. Veenendaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Cyberattacks in Support of Influence Operations*, in: *8th International Conference on Cyber*

These operations consist of obtaining information by illegal means (e.g. through hacking activities) and then using it in the information space to achieve specific objectives, e.g. destabilising the political system by compromising a particular politician, as happened in the United States in 2016, during the campaign for the presidential election[48]. In NATO doctrinal terms, information operations encompass a wide variety of activities that, in addition to information and communication activities aimed at achieving cognitive objectives[49], may also integrate activities related to, among other things: protecting one's own information environment (OPSEC) and operational masking, cyberspace operations and even electronic warfare[50]. All of these types of activities are distinct, highly complex and multidimensional activities. If cyberspace occurs within information operations, it is one of many possible spaces for their implementation[51].

The optics of the digital platform industry and, above all, social media, are also important in understanding the adaptability of the body of knowledge related to cyber security for disinformation recognition. These are environments heavily exploited in disinformation and influence operations conducted in cyberspace. According to Meta (formerly Facebook), influence operations are (…) *coordinated efforts made to manipulate or corrupt public debate for a strategic goal*[52]. In the company's nomenclature, influence operations involve violations of its internal security policy for the prevention of coordinated inauthentic behaviour (CIB) on the platform. Between 2017 and 2020, the company

Conflict. Proceedings 2016, N. Pissanidis et al. (sci. eds.), https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf, pp. 113–126 [accessed: 10 VII 2024]; *Cyber Influence Operations,* https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-cyber-influence-operations [accessed: 10 VII 2024].

[48] J. Shires, *Hack-and-leak operations and U.S. cyber policy*, War on the Rocks, 14 VIII 2020, https://warontherocks.com/2020/08/the-simulation-of-scandal/ [accessed: 10 VII 2024].

[49] More on communication operations later in the article. It should be mentioned that the distinction between information operations and psychological operations has also been adapted in Russian information warfare theory. It is worth noting, however, that at the same time there is a category of combined operations in Russian nomenclature, referred to by the term information-psychological operations. On this subject see in more detail: M. Wojnowski, *"Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.* (Eng. 'Reflective management' as a paradigm for Russian information-psychological operations in the 21st century.), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 12, pp. 15–17.

[50] *Allied Joint Doctrine for Information Operations (AJP-10.1)…*, pp. 32–37 [accessed: 17 XI 2024].

[51] The information environment in this view is divided into three dimensions: virtual, physical and cognitive. See: ibid., pp. 16–17.

[52] *Threat Report. The State of Influence Operations 2017–2020*, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf, p. 3 [accessed: 10 VII 2024].

recognised 150 such operations[53]. It is worth noting that Meta maintains a public repository on the social networking site GitHub, which contains, among other things, TTPs recognised in CIB detection, as well as more detailed information, such as the names of propagated domains, which, as in cyber security, is defined by the term compromise indicator. Meta declares using a general data analysis method based on the Kill Chain model for this purpose[54]. It should be noted that the various platforms have different policies for sharing and countering knowledge of detected information and influence operations. A few years ago, the social network Twitter (currently X) was also active in this respect, making available to researchers large datasets of profiles identified as being involved in inauthentic and coordinated information campaigns carried out on this platform (these were referred to as inauthentic influence campaign)[55]. Currently, the platform does not have such extensive activities in this area. Analysing influence operations in cyberspace is increasingly becoming part of the practice of global IT and cyber security companies, not just social media platforms. Microsoft's policy can be cited as an example. It has dedicated a separate chapter to influence operations in some of its annual digital threat reports and has used elements of cyber security terminology adapted for this purpose (e.g. the term advanced persistent manipulators referring to advanced persistent threat) to describe them[56]. The theoretical heritage of digital companies and platforms is not as extensive and in-depth as that of state actors in the national security sector, as the meaningful sense of these definitions derives from a different practice and from the needs of the industry.

Despite the indicated remarks on the distinction between information operations and influence operations in the remainder of the article, the authors will use these terms interchangeably, as such a distinction is also not used in the further literature on the subject discussed later in the article. As

[53] *Threat Report: Combating Influence Operations*, Meta, 26 V 2021, https://about.fb.com/news/2021/05/influence-operations-threat-report/ [accessed: 11 VIII 2024].

[54] *Facebook. Threat research*, GitHub, https://github.com/facebook/threat-research [accessed: 11 VIII 2024]. Example of a report: *Facebook. Threat Research. Indicators. CSV. Q4_2023*, GitHub, https://github.com/facebook/threat-research/blob/main/indicators/csv/Q4_2023/Q4_2023_China_based_CIB_network.csv. More on the adaptation of cybersecurity analysis methodology for information and influence operations in cyberspace later in this article.

[55] For more on this topic, see the archived version of the social media site Twitter. See: *Information Operations*, http://web.archive.org/web/20201226185947/https://transparency.twitter.com/en/reports/information-operations.html [accessed: 11 VIII 2024].

[56] *Microsoft Digital Defence Report 2022*, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us, p. 72 [accessed: 11 VIII 2024].

a conclusion, however, it should be emphasised that cyberspace represents only one segment of the information environment in which such complex operations are conducted.

Methods for analysing information/influence operations by components of the communication process

A common feature of information operations/influence operations is that, at some stage of their implementation, they may involve communication activities aimed at changing or perpetuating the behaviour and attitudes of specific individuals or social groups (political, professional, religious). In NATO information operations doctrine, such objectives are pursued, inter alia, through psychological operations defined as (…) *planned psychological activities using methods of communications and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives*[57]. In the case of influence operations, affecting the attitudes and behaviour of recipients may take various forms, including disinformation as part of the intelligence activities of a foreign state. In Poland, such activity has been criminalised and defined in detail in the Criminal Code, amended in 2023. In the legal definition of the concept of disinformation, the legislator included not only the condition of linking the person involved in the disinformation process with foreign intelligence, but also the qualitative dimension of these activities (an attempt to cause serious damage to the Republic of Poland, an allied state or an international organisation) and specified the manner of their implementation – it is the dissemination of a specific type of information (false or misleading)[58].

[57] See: *Allied Joint Doctrine for Psychological Operations (AJP-3.10.1)*, UK Ministry of Defence, https://www.gov.uk/government/publications/ajp-3101-allied-joint-doctrine-for-psychological-operations, p. 18 [accessed: 5 VII 2024]. In the cited NATO doctrinal document on information operations (AJP-10.1), PSYOPS activities are listed as one of two communication capabilities used within INFOOPS (the other type of capability is military public affairs). See: *Allied Joint Doctrine for Information Operations (AJP-10.1)*, pp. 30–31. Information operation and psychological operation are thus separate terms, but interrelated, as INFOOPS is overarching PSYOPS. On the semantic differences and the history of the formation of the term 'information operations', see: T. Kacała, *Tendencje rozwojowe współczesnych działań psychologicznych prowadzonych przez Siły Zbrojne RP* (Eng. Developmental trends of contemporary psychological activities carried out by the Polish Armed Forces), in: *Innowacja i synergia w Siłach Zbrojnych RP*, vol. 1, A. Lis, R. Reczkowski (eds.), Bydgoszcz 2012.

[58] Article 130(9) of the Criminal Code: 'Whoever, taking part in the activities of a foreign intelligence service or acting on its behalf, conducts disinformation, consisting in the dissemination of false or misleading information, with the aim of causing serious disturbances in the system or economy of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member, or inducing a public authority of the Republic of Poland, an allied state or

In the literature on the subject, a popularised and capacious term for shaping attitudes and behaviour is 'propaganda'. Among the many definitions of the term, for the purposes of this article, it is assumed to be understood as the mass, methodical and intentional dissemination of specific content in an effort to influence a specific audience[59]. It is worth mentioning that propaganda can be carried out using media with varying degrees of secrecy. 'White' propaganda is referred to as activities carried out by a well identified source (e.g. state media). In the case of 'grey' propaganda, there is the problem of identifying the correct source of the content in question, which at the same time makes it difficult to assess the author's intentions. 'Black' propaganda, on the other hand, is characterised by complete secrecy of the source of the message and the dissemination of false content. This type of propaganda is often equated with disinformation[60]. Propaganda can therefore encompass some of the activities carried out in psychological operations or disinformation, but it is a much broader concept. At the same time, it is a well-established term in the literature that refers to intentional and structured communication activities aimed at influencing the attitudes or behaviour of an audience.

What both influence operations, psychological operations and propaganda have in common is that they can be considered as a communicative process. Most models of the communication process distinguish the following components[61]:

- the participants, i.e. the senders (the actual authors/sources of the message) and the receivers (the addressees, the audience);

an international organisation of which the Republic of Poland is a member to take or refrain from taking certain actions, shall be subject to a penalty of deprivation of liberty for a period of not less than 8 years'.

[59] There are many definitions of propaganda in the literature. Edward Bernays, one of the forerunners of research on propaganda and public relations, believed that no ethical value should be placed on the term, as it has a purely technical meaning and denotes '(…) a consistent and sustained effort directed at creating or shaping events that influence the public's relationship with a company, an idea or a particular group'. See: E.L. Bernays, *Propaganda*, New York 1928, p. 15. On the definition of propaganda, see: R. Rajczyk, *Nowoczesne wojny informacyjne* (Eng. Modern information warfare), Warszawa 2016, pp. 22–24.

[60] B. Dobek-Ostrowska, J. Fras, B. Ociepka, *Teoria i praktyka propagandy* (Eng. Theory and practice of propaganda), Wrocław 1999, p. 36.

[61] B. Dobek-Ostrowska, *Podstawy komunikowania społecznego* (Eng. Fundamentals of social communication), Wrocław 1999, p. 15. There are also other, more complex communication models in the literature that highlight, for example, the roles of opinion leaders (two-stage communication flow model) and information selectors – so-called gatekeepers (topological communication model). See in more detail: B. Dobek-Ostrowska, *Komunikowanie polityczne i publiczne* (Eng. Political and public communication), Warszawa 2007, p. 36.

- the message (communication message), the content of which is contained in the meanings and symbols encoded by the sender and decoded by the receiver;
- the channel, i.e. the route of the communication message, through which it is transferred by the sender to the receiver (e.g. mass media, social media, as well as verbal and non-verbal communication);
- feedback that informs the recipient's reaction to the communication message, through which the sender learns whether it has been received and understood;
- noise that interferes with the effectiveness of the communication process, which can be internal (e.g. a person's limitations due to his or her psychological predisposition or emotional state), external (e.g. physical conditions such as weather or interference with the functioning of the communication channel) and semantic (e.g. inappropriate selection or reception of the meaning or symbol contained in the message);
- context, i.e. the conditions (social, cultural, historical or physical) in which the communication process takes place (Figure 2).

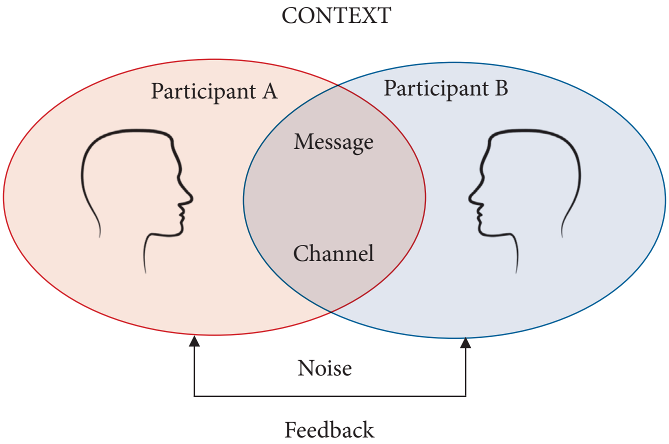

Figure 2. Components of the communication process.

Source: own elaboration based on: B. Dobek-Ostrowska, *Komunikowanie polityczne i publiczne* (Eng. Political and public communication), Warszawa 2007, The PWN Publishing House, p. 64.

The ability to isolate the components of the communication process creates a common methodological starting point for the analysis of the communicative aspect of information (psychological)/influence operations. With regard to the above-mentioned components, it is important to recall the research of the American political scientist and propaganda researcher Harold Lasswell, who conducted a study of the communicative process in terms of its function and, in 1948, created a model of the persuasive act. His premise was based on the precisely distinguished roles of sender and receiver and the unidirectional nature of communication, used by the sender for a clearly defined purpose - to cause a specific effect (outcome) in the receiver. The essence of communication according to Lasswell is encapsulated in the answer to the five questions concerning the elements of the communication process described earlier[62]:

1. Who is speaking? (question about the sender of the message).
2. What is the sender saying? (question about the content of the message).
3. Through which channel does the sender speak? (question about the channel of the message).
4. To whom is the sender speaking? (question about the recipient of the message).
5. With what effect does the sender speak? (question about the effectiveness of the message).

Lasswell's research can still be used to analyse psychological actions, as evidenced by a study by Tomasz Kacała and Justyna Lipińska entitled *Strategic communication and public affairs*, published by the Military Centre for Civic Education. It contains a scheme for the analysis of hostile propaganda taking into account five categories: source, content, audience, media used and effects achieved[63]. The publication details the areas of interest and supporting questions for those researching propaganda messages. Selected elements are presented in Table 1.

[62] B. Dobek-Ostrowska, *Komunikowanie polityczne…*, p. 32.

[63] T. Kacała, J. Lipińska, *Komunikacja strategiczna i public affairs* (Eng. Strategic communication and public affairs), Warszawa 2014, pp. 155–160.

Table 1. Components of propaganda analysis in relation to elements of the communication process based on the study by Tomasz Kacała and Justyna Lipińska.

A component of the communication process **(research focus area)**	**Examples of analytical questions**
Sender - source analysis	Actor Who is the person/group delivering the message?
	Authority Who patronises an opponent's activities or gives value to their actions?
	Author Who created/developed the propaganda material analysed?
	Disseminator Who is responsible for disseminating the message to the objects of influence?
	Authenticity and credibility Is the source of the message identifiable? (type of communication source by degree of secrecy 'white', 'grey', 'black')
Message – content analysis (What does propaganda communicate? What is it trying to persuade the objects of influence to do?)	Purpose of the message What behaviour/attitudes of the object of influence is the sender trying to elicit?
	Lines of persuasion What argumentation, techniques and symbolism does the sender use in the message?
	Inadvertent information What unintended information did the sender include in the message?
	Inaccuracy of the message What elements make the message inconsistent or erroneous - including in comparison with previous material?
Recipient – recipient analysis (Who is the recipient?)	Apparent object of influence Who appears to be the recipient of the message at first?
	Final (target) object of the impact Who is the target, intended recipient of the message?
	Indirect object of influence Who is the indirect recipient of the message, i.e. the one through whom the sender is trying to reach the ultimate object of influence?

A component of the communication process **(research focus area)**	**Examples of analytical questions**
Channel - media analysis (Which media were used? Why these?)	Media types: radio, television, print, internet What information gaps exist (e.g. frequency, location, place of origin, technical characteristics, method of dissemination)?
Feedback - performance analysis (What effect does propaganda have?)	What events, incidents, reactions can demonstrate the effectiveness of the impact of the message?

Source: own elaboration based on: T. Kacała, J. Lipińska, *Komunikacja strategiczna i public affairs* (Eng. Strategic communication and public affairs), Warszawa 2014, pp. 155–160.

The advantages of Lasswell's model appear to be its simplicity and relatively high source availability, since the required minimum for its use is the content layer of information operations/influence operations, which – at least in the case of mass communication (e.g. propaganda) – is by definition visible and widely available[64]. At the same time, it should be emphasised that the peculiarities of contemporary media complicate basing the research procedure of information operations/ influence operations on clearly defined elements of the communication process. This is influenced by the interactivity of the new type of media[65] (particularly high in the case of social media), which makes it difficult to precisely isolate the basic elements of the communication process (sender, medium, addressee), and the algorithmisation of content selection (resulting in information bubbles) further increases the importance of context as an essential element of this process[66].

[64] In order to solve the task of carrying out an analysis according to the questions indicated in Table 1, Tomasz Kacała and Justyna Lipińska provide only one example of a propaganda text from the Diwaniyah province from the period of the stabilisation mission of the Polish Military Contingent in Iraq in 2006. See: T. Kacała, J. Lipińska, *Komunikacja strategiczna*..., pp. 159–161.

[65] On the interactivity of new media, see: J. van Dijk, *Społeczne aspekty nowych mediów* (Eng. Social aspects of new media), Warszawa 2010, p. 18; G.S. Jowett, V. O'Donnell, *Propaganda and Persuasion. Fifth Edition*, Los Angeles–London–New Delhi–Singapore–Washington 2012, p. 366.

[66] On the subject of propaganda under the conditions of algorithmisation of the message, see: S.C. Woolley, P.N. Howard, *Introduction: Computational Propaganda Worldwide*, in: *Computational*

Methods for analysing information operations/influence operations based on the achievements of the cyber security industry

Reflection on the use of the legacy of cyber threat research methodologies in the study of information operations and disinformation is present both in academic papers and in the expertise of analysts and governmental, international and non-governmental institutions, as well as commercial actors of the cyber security industry. By way of introduction, reference can be made to an article by three American researchers associated with the University at Albany, State University of New York entitled *The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats*. Its authors point out that the extent to which disinformation affects the confidentiality, integrity and availability of information makes it necessary to view it not only as an information disruption phenomenon, but also as a form of cyber attack[67]. The article compares disinformation with other categories of cyber threats, such as social engineering, attacks on web applications, DDoS attacks, malware, ransomware, activities of APT groups, zero-day threats. The comparison was made with regard to the threat actors, their source (external or internal from an information system perspective), the motivations and goals of the adversaries, the attack vector, the attacked network layer according to the Open System Interconnection Model (OSI), as well as the impact of the attack on the system and its users and ways to mitigate the associated threats. The US researchers argue that the result of their comparative analysis showed many similarities between disinformation and the types of attacks established in the taxonomy of cyber threats. For example, the similarities between disinformation and social engineering are based on human weaknesses (e.g. the tendency to behave unthinkingly when given information in a manipulated context) and, when compared with ransomware and malware attacks, involve similar consequences – reduced reputation, generation of financial losses and loss of trust for the victim of the attack. The researchers also point to similarities with the activities of APT groups, which are characterised by a prolonged action on the victim's network (similar to, for example, the disinformation process

Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media, S.C. Woolley, P.N. Howard (eds.), Oxford 2018, p. 4. https://doi.org/10.1093/oso/9780190931407.001.0001.

[67] K.M. Caramancion et al., *The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats*, "Data" 2022, vol. 7, no. 4, p. 1. https://doi.org/10.3390/data7040049.

on social media)[68]. It is worth noting that, according to them, an adversary carrying out disinformation in cyberspace attacks the last layer of the OSI model, the application layer, and the attack vectors are search engines, online advertisements and social media platforms[69].

An important contribution to the adaptation of the cybersecurity industry's body of work to the needs of identifying information operations and disinformation comes from Clint Watts, an expert on security, information warfare and disinformation, who has been involved with the US military and FBI in the past and is now a research fellow at the Foreign Policy Research Institute and a specialist at the Alliance for Securing Democracy. Watts points out that social media is being targeted by groups of APMs (advanced persistent manipulators), defined by him as (…) *an actor or combination of actors perpetrating an extended, sophisticated, multiplatform, multi-media information attack on a specified target*[70]. The term *advanced persistent manipulators* refers to the term *advanced persistent threats*, commonly used in the cybersecurity industry to describe threat actors (mainly state actors) capable of generating advanced and persistent cyber threats by penetrating a victim's network and remaining undetected for a prolonged period of time. APM groups operate similarly to APT groups in the sense that they consistently pursue their objectives, so that the threat they generate is not mitigated by, for example, the closure or temporary blocking of an account on a social networking platform. APM groups use a combination of manipulation techniques and have sufficient resources to conduct long-term propaganda and disinformation campaigns. In doing so, they are able to collect, aggregate and analyse user data, as well as adapt techniques and circumvent social media account and content controls. Watts identifies a wide variety of APM-type groups: state actors, extremist groups, activists, politicians, and lobbyists and PR companies[71].

A strongly developed strand of research into the adaptability of cyber security industry experience for disinformation recognition is the building of analytical models (frameworks). They enable the standardisation of the research process and thus make it easier for experts to exchange information and knowledge, to compare and generalise the conclusions of the analysis,

[68] Ibid., p. 15.

[69] Ibid., p. 10.

[70] See: C. Watts, *Advanced Persistent Manipulators, Part One: The Threat to Social Media Industry*, Alliance for Securing Democracy, 12 II 2019, https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/ [accessed: 11 VII 2024].

[71] C. Watts, *Advanced Persistent Manipulators*…

and consequently to achieve measurable analytical results, e.g. attribution (attribution of perpetration) of information (psychological)/influence operations to individual actors, i.e. to APMs. Before discussing example solutions, it is worth recalling the perception of this issue by experts from the NATO Strategic Communication Centre of Excellence (NATO StratCom) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). They point out that a significant problem in identifying information operations/influence operations is the varying type of data on which analysts work. NATO StratCom and Hybrid CoE experts have divided them into three categories: technical, behavioural and contextual. In addition, they differ by the degree of availability. The first category of sources is publicly available (open source) data. In this category, technical data would be, for example, the IP address and owner of a website or the openly displayed economic relationships of the entities used in a specific operation (e.g. information from business registers or financial statements). Behavioural data extracted from open sources will be, for instance, the exemplary activity of a particular account or page, message propagation patterns and communication techniques observed by the analyst, and connections demonstrated through social network analysis. Contextual data in this case may relate to the geopolitical situation (e.g. linking a particular event to an actor on the basis of motive probability), as well as being the result of narrative (content) analysis and linguistic characteristics of the material in question (e.g. propaganda). Another category is proprietary sources, i.e. information sources that can only be accessed by the owners of the data (e.g. social media platforms), e.g. users' IP address, geo-location, the entire scope of account activity. The third type of information is classified source data, which is mainly accessed by government institutions. This is data collected through, for example, intelligence activities. The authors also point out that legal and ethical considerations must be taken into account in the collection and processing of all data from the above types of sources (Table 2)[72].

[72] See in more detail: J. Pamment, V. Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, https://stratcomcoe.org/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf, pp. 15–24 [accessed: 18 VIII 2024].

Table 2. Types of data considered in influence/information operations analysis according to James Pamment and Victoria Smith.

	Technical evidence	**Behavioural evidence**	**Contextual evidence**	**Legal & ethical assessment**
Open source	domain owner, IP addresses, economic links	account activity, page activity, posting/cross-posting, sharing, watching, network activity	media content, discourse and narratives, linguistics, political context, *cui bono*	risk of litigation, research ethics, risk of becoming a target
Proprietary source	data collected by the backend of (internet) platforms	as above, with more data from (online) platforms	as above and data from deleted content (takedowns) with suspicious links	protection of political and commercial interests, data protection
Classified source	SIGINT, proprietary source data obtained under a warrant	as above and SIGINT, HUMINT	as above and implicit geopolitical assessments	actor-specific strategy, protection of political interests, data protection

Source: own elaboration based on: J. Pamment, V. Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, https://stratcomcoe.org/publications/download/Nato-Attributing-Information-Influence-Operations-DIGITAL-v4.pdf, p. 15 [accessed: 18 VIII 2024].

Based on the results of their analysis of the diversity of types and sources of data, the experts of NATO StratCom and EU Hybrid CoE highlight the problems in investigating, and consequently countering, disinformation. One of their arguments is that digital platforms are reluctant to share their technical and behavioural data. They explain this, for example, by the need to protect users' privacy and the secrecy of commercial activities[73]. As necessary in overcoming the difficulties, experts see building transparent methodologies for recognising information/influence operations and opening up to the sharing of information on recognised techniques, tactics and procedures, and using consistent data formatting to enable cross-platform analysis[74]. In the following section, analytical models (frameworks) popularised in the literature will be discussed.

[73] Ibid., p. 27.

[74] Ibid., p. 26.

Kill Chain

The postulation of adapting the Cyber Kill Chain model for the analysis of influence operations in cyberspace was made in the article *Understanding Influence Operations in Social Media* by Arlid Bergh of the Norwegian Defence Research Establishment. The text appeared in *the Journal of Information Warfare* in 2020[75]. Bergh emphasises that relying on a quantitative approach to the study of influence operations (e.g. by analysing the number of shares of false material) is insufficient to fully recognise and understand them, and therefore advocates the need to include sociotechnical issues in the analysis. In his view, the sociotechnical layer of influence operations can be deepened by including in its analysis a methodology based on the phases of a cyber attack of the Kill Chain model, consisting of:

- reconnaissance – identifying weaknesses in the target that can be exploited during the attack;
- weaponisation – selecting social media and creating content to be used in the attack;
- delivery – using social media channels to spread the content;
- exploitation – generating audience interest (e.g. using clickbait techniques or influencing opinion leaders);
- installation – embedding the propagated content in the audience's news feed. Bergh proposes the concept of online information sediments in this context. With it, he points out that content skilfully introduced into the information circuit persists in it for a long time. Even if they do not have the potential for impact, their very presence (persistence) in the information circuit gives them utility from an influence operations perspective (e.g. they can be used to increase the credibility of other narratives or influence content recommendation algorithms in social media);
- command and control – influencing and affecting the meaning-making process of specific individuals and groups;
- action on objectives – seeking to elicit specific actions (behaviour) from defined audiences (e.g. social protests).

Summarising the Kill Chain model, it is worth noting that in this view, an influence operation is effective when the objectives are met in all the phases mentioned above. The effectiveness of such an operation thus goes well beyond the situation in which the material has only been effectively disseminated online (even if it is permanently there), as what matters most is the effectiveness of influencing the cognitive sphere and – as a consequence – shaping specific

[75] A. Bergh, *Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach*, "Journal of Information Warfare" 2020, vol. 19, no. 4, pp. 113–121.

attitudes or inducing desired behaviour in the audience. Bergh also points out that the operation of influence is circular (rather than linear), making the information processing highly dependent on external factors (e.g. the engagement of social media users)[76]. This implies the need to consider the activities that are elements of information operations/influence operations in cyberspace in a broad context and with a view to their long-term nature.

Diamond model

Analyst Charity Wright associated with the Insikt Group (part of the wider Recorded Future commercial cyber security entity), and in the past with the US military and the National Security Agency[77], has published a report with a proposal to use the diamond model for analysing influence operations in cyberspace. The premise of this model is based on the centrality of the narrative as the most important element of an influence operation and its connection to four components[78]:

1) the influencer, who may be the person or organisation carrying out the harmful activity;
2) the public (audience), who can be the persons or groups targeted by the influencing operation;
3) the infrastructure, which includes the technical and physical means used to create and distribute the materials used in the influencing operation;
4) capabilities, consisting of TTPs used by the influencer (Figure 3).

The effectiveness of influence operations depends on all these elements, each of which can also be analysed separately. In the diamond model, there are two types of narrative linkages - sociopolitical and technical. The first type is the linkage of the narrative to the influencer and the recipient and can refer, for example, to the influencer's knowledge of the recipient's weaknesses that enable the influencer to conduct an effective influence operation. On the other hand, the linkage of the narrative to infrastructure and capabilities is technical in nature – these include the identified media used in the operation and the techniques used to support the influence or propagation of the message (e.g. data on the audiovisual materials used)[79]. Analysing the relationships between the various elements of the model allows for a better understanding of the objectives of the campaign,

[76] Ibid., p. 122.

[77] C. Wright, *The Diamond Model for Influence Operations Analysis*, https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf [accessed: 28 VII 2024].

[78] Ibid., pp. 3–7.

[79] Ibid.

identifying the weaknesses of the audience, predicting the influencer's next actions and recommending countermeasures[80].

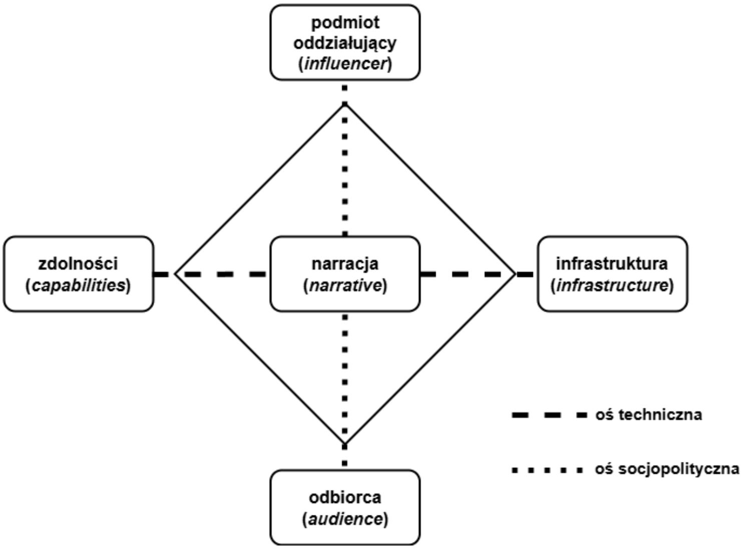
podmiot oddziałujący (*influencer*)
zdolności (*capabilities*)
narracja (*narrative*)
infrastruktura (*infrastructure*)
odbiorca (*audience*)
oś techniczna
oś socjopolityczna

Figure 3. Components and links of the diamond model in Recorded Future's analysis of information operations/influence operations.

Source: own elaboration based on: C. Wright, *The Diamond Model for Influence Operations Analysis*, Active Response, https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf, p. 1 [accessed: 28 VII 2024].

DISARM Framework

The DISARM Framework (Disinformation Analysis and Response Measures) is of a different nature to the concepts discussed above, in that it focuses more on the operationalisation of the processes involved in analysing and preventing information operations/influence operations, and less on the theoretical and methodological issues of this aspect (although it also makes some claims in this regard). According to information provided by the DISARM Foundation[81],

[80] Ibid., p. 10.

[81] An entity established to promote and develop the DISARM Framework. Its members are information security industry managers, analysts and experts with experience working or serving in US public institutions, commercial entities and third sector organisations. See: *DISARM Foundation*, https://www.disarm.foundation/about-us [accessed: 5 VIII 2024].

the DISARM Framework refers to expert Sara-Jayne Terp's[82] 2017-2018 work on the adaptability of information security tools for the study of disinformation, and the concept itself took shape in 2019-2020. During its several years of evolution, it was influenced, according to information provided by the DISARM Framework, by a number of organisations in the cybersecurity industry (the model was previously called AMITT). The development of the concept was based on a standardised system of information sharing and the inclusion of both offensive (red team) and defensive (blue team) side in the TTPs information gathering process. Currently, the DISARM Framework is presented as a tool based on solutions similar to MITRE ATT&CK[83]. The foundations of the DISARM Framework were presented by Sara-Jane Terp and Pablo Breuer of the DISARM Foundation at the 2022 CogSIMA conference (Conference on Cognitive and Computational Aspects of Situation Management). The authors suggest that, from a practitioner's perspective, it is useful to adopt the optics of cognitive security[84], which allows disinformation to be viewed more holistically. In doing so, they suggest that the cognitive security perspective is related not only to 'large-scale social engineering', but also to the problem of machine learning in information security (MLSec), i.e. the use of artificial intelligence technology, its models based on human thought processes, to attack information systems and other artificial intelligence systems[85]. The authors therefore suggest that not only elements of the cybersecurity analytics acquis (particularly the Kill Chain model as well as the MITRE ATT&CK formula information and knowledge sharing platform), but also research in the cognitive sphere, e.g. related to marketing techniques (e.g. evaluation of a given content by a targeted group or individual) or psychological activities, should be used to identify and prevent disinformation[86].

The DISARM Framework's information collection and processing method is based on the assumption that an individual disinformation case should be treated in the category of an incident (as in the case of computer incidents), which

[82] Sara-Jayne Terp's interests focus on cognitive security and disinformation analysis and prevention. See: SJ Terp, https://www.infosecurity-magazine.com/profile/sj-terp/ [accessed: 5 VIII 2024].

[83] On this subject see: *DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/ [accessed: 5 VIII 2024].

[84] Terp and Breuer define the term as: *application of information security principles, practices, and tools to misinformation, disinformation, and influence operations*). See: SJ Terp, P. Breuer, *DISARM: A Framework for Analysis of Disinformation Campaigns,* 2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogsSIMA), https://ieeexplore.ieee.org/document/9830669, p. 3 [accessed: 5 VIII 2024].

[85] Ibid., p. 3.

[86] Ibid., p. 6.

should be catalogued and then analysed (e.g. in terms of answering questions about the individual components of the incident, their interdependence and their relationship to other events and propaganda campaigns). In the paper, Terp and Breuer presented a disinformation/propaganda incident template, which consists of nine categories of information. These include descriptive information such as: the name and summary of the incident, hypotheses about the perpetrator of the attack (attribution), the duration of the incident, the moment of occurrence, the likely targets of the adversaries, their methods, methods of counteraction and other, potentially related, incidents. In the DISARM Framework, access to the incident database is open source and is intended to be fed by a variety of sources – academics, researchers of disinformation phenomena[87]. According to the data provided, the database contains information on 66 incidents and is limited to the years 2014-2020[88]. It contains a list of 142 techniques (for some, sub-types are included, so this number is actually higher) characterising the actions of offensive and defensive teams. These techniques include observed ways of manipulation used in the message, ways of introducing or perpetuating it in the information flow, as well as recommendations for defensive actions aimed at mitigating threats generated by adversaries[89]. The techniques have been assigned to 16 tactics, which in turn correspond to four phases of action[90].

Summary

The analytical models discussed in the text are not exhaustive of all proposals for the use of cyber security industry experience in information operations/influence operations analysis[91]. The compilation includes only those aspects that the authors considered relevant from the perspective of the objectives of this article. In conclusion, common features justifying the adaptation of the conceptual and methodological foundations of CTI for the study of information operations/influence operations should be identified:

[87] Ibid.

[88] See: *DISARM Frameworks – incidents*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/incidents_index.md [accessed: 31 VIII 2024].

[89] See: *DISARM Frameworks – techniques*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques_index.md [accessed: 31 VIII 2024].

[90] See: *DISARM Frameworks – phases*, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/tree/main/generated_pages/phases [accessed: 31 VIII 2024].

[91] For other analytical models, see: *IO-Campaign-Collections*, GitHub, https://github.com/tripkrant/IO-Campaign-Collections [accessed: 31 VIII 2024].

- The main argument is the operation of APM-type groups in information spaces, i.e. entities permanently and methodically infecting the infosphere through various methods of manipulation (including disinformation) in order to induce a certain behaviour or shape the attitudes of decision-makers, opinion leaders or more or less broad social groups. APMs may be politically motivated (e.g. power sector institutions conducting influence operations in cyberspace on behalf of foreign states), business motivated (e.g. illegal lobbying, black PR online) and ideologically motivated (e.g. extremist organisations). Their actions can have immediate or lasting effects negatively affecting the functioning of states and its institutions, society and individual citizens. In this sense, the information space is therefore threatened by the negative impact of these actors in much the same way that ICT networks are threatened by the actions of state actors (e.g. APTs), criminal groups or hacktivists.
- The activity of APM-type groups requires mitigating the various risks and threats they generate. To this end, efforts should be made, inter alia, by analogy with CTI, to identify their activity in the information space by examining the TTPs they employ, the infrastructure they use and, on this basis, to make attribution with a specific entity (e.g. a state, an institution, an organisation, a commercial entity).
- APM-type groups carry out activities in different areas of the information space (e.g. different social media) and the effects of their activities are studied and analysed by a community of different people and actors using different models and methodologies of analysis. It is therefore necessary to standardise procedures in order to enable knowledge sharing and synergies. The literature points to the relevance of using threat intelligence platforms, e.g. OpenCTI, to improve the collection and analysis of traces of APM activity (IoC, TTP, etc.) and the exchange of knowledge within agreed taxonomies (these are used, for example, in the database at MITRE ATT&CK). Solutions similar to MITRE ATT&CK are currently being developed, an example being the DISARM Framework.
- Authors of material on the adaptation of CTI for the analysis of information operations/influence operations are aware of its dissimilarity to 'classical' CTI due to the socio-political nature of the issues under study. This can be seen at the level of both general and specific postulates and concepts, as exemplified by the diamond model in which narrative is central to the analysis.

The importance of the latter point is worth noting. The collection and analysis of text data containing a specific message is different from the processing of data such as packets sent between specific IP addresses or the analysis of activity logs in a network infected by the actions of an adversary (hacker group). This characteristic of the phenomena under study limits the possibility of fully adapting the methodology and work of CTI for the analysis of influence operations. However, developments in technologies related to artificial intelligence, especially natural language processing (NLP), may reduce this methodological gap in the future.

It should also be mentioned that the currently popularised frameworks do not emphasise the legitimacy of pre-emptive detection of (recipient) vulnerabilities to various forms of manipulation, which could enable or increase the effectiveness of information/influence operations. Such vulnerabilities can be technical (e.g. the possibility of registering or using domains for disinformation[92] or the possibility of creating and long-term use of a network of accounts for the purpose trolling on a specific topic) and social (e.g. the degree of trust in public institutions, the potential for polarisation and social radicalisation or the media competence of citizens). It would seem that this type of activity, aimed at actively seeking threats, would be close to another concept supporting CTI, i.e. threat modelling. A signal of interest in these issues is the considerations of the authors of the DISARM Framework concept, referred to in this article, concerning the perception of information operations/influence operations from a 'cognitive security' perspective. It can be assumed that, in the future, this strand of reflection will be deepened and enriched with specific case studies or the creation of a theoretical and methodological basis to study the type of phenomena in question.

Conclusions

The authors assess that the adaptation of CTI experience in the framework of the study of information operations/influence operations in the methodological layer has certain research qualities, although they do not constitute a significant qualitative change in relation to the approach discussed in the article developed in the social sciences, primarily in communicology. This is because the adapted CTI methodology focuses on assumptions similar to the analysis based on the elements of the communication process, i.e.: the adversary (i.e. the sender of the message), his

[92] The identification of ventures involving the registration of domains with names resembling official government websites that could in future be used in socio-technical activities, including disinformation, was reported by the CSIRT GOV team in its 2023 report. See: *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku* (Eng. Report on the state of Poland's cybersecurity in 2023), CSIRT GOV, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html, p. 20 [accessed: 31 VIII 2024].

actions (the message) and the infrastructure used (the media used to communicate the message), and the object of attack (the audience of the message). In addition, CTI adaptation postulates do not seem to emphasise the importance of analysing the impact of information operations/influence operations. This significantly reduces the possibility of a holistic and in-depth understanding of them, and this issue is in turn immanent to an analysis based on elements of the communication process. In contrast, a methodological variation on the communicology-based methods described above is the inclusion of the chronology and phases of the information operation/influence operation in its characterisation. Adopting such an approach makes it possible to define adversarial behaviour more precisely in the form of a TTP.

An unquestionable advantage of the CTI is the existing achievements in the organisation of work with information, including the endeavour to standardise procedures (terminology, typologies) for the collection and processing of data and the development of organisational and technical conditions for their exchange. This lends great merit to the adaptation of CTI for the study of information operations/influence operations and means that this postulate should be seen not as a proposal for a new method of studying these phenomena, but more broadly as a certain organisational and methodological approach. Evaluating the CTI acquis from this perspective and bearing in mind the conclusions of the analysis of the literature on the subject, it should be concluded that the validity of the adaptation of CTI for the recognition of information operations/influence operations depends on the answers to the following questions:

1. What is being analysed? As indicated in the section on defining information and influence operations, cyberspace is only one of the environments in which they are carried out. The legitimacy of the adaptation of CTI models therefore only applies to a specific type of these operations.
2. What is the purpose of the analysis? CTI methodology enables efficient data grouping, which facilitates data processing and knowledge sharing. It thus increases the possibilities for building situational awareness of cyber threats. However, this approach does not seem to bring us any closer to answering questions about the broader dimension of analysis, such as the effectiveness of adversaries. This is due, among other things, to the omission of the aspect of studying the effect of actions (cognitive, social, political, etc.).
3. What sources does the analyst have access to? From the Hybrid CoE and NATO StratCom expert studies cited above, it appears that the range of data that can be accessed as part of an information operation/influence operation study is very broad. In some cases, however, access to the data is only available to specific organisations (social media platforms, state intelligence institutions). This access therefore affects the positioning

of the analyst in the process of gathering information on the phenomenon and determines the range of research questions that can be answered on the basis of the data.

Bibliography

Bergh A., *Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach*, "Journal of Information Warfare" 2020, vol. 19, no. 4, pp. 110–131.

Bernays E.L., *Propaganda*, New York 1928.

Caramancion K.M. et al., *The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats*, "Data" 2022, vol. 7, no. 4, pp. 1–18. https://doi.org/10.3390/data7040049.

Dijk J. van, *Społeczne aspekty nowych mediów* (Eng. Social aspects of new media), Warszawa 2010.

Dobek-Ostrowska B., *Komunikowanie polityczne i publiczne* (Eng. Political and public communication), Warszawa 2007.

Dobek-Ostrowska B., *Podstawy komunikowania społecznego* (Eng. Fundamentals of social communication), Wrocław 1999.

Dobek-Ostrowska B., Fras J., Ociepka B., *Teoria i praktyka propagandy* (Eng. Theory and practice of propaganda), Wrocław 1999.

Jowett G.S., O'Donnell V., *Propaganda and Persuasion. Fifth Edition*, Los Angeles–London–New Delhi–Singapore–Washington 2012.

Kacała T., *Tendencje rozwojowe współczesnych działań psychologicznych prowadzonych przez Siły Zbrojne RP* (Eng. Developmental trends of contemporary psychological activities carried out by the Polish Armed Forces), in: *Innowacja i synergia w Siłach Zbrojnych RP*, vol. 1, A. Lis, R. Reczkowski (eds.), Bydgoszcz 2012, pp. 87–118.

Kacała T., Lipińska J., *Komunikacja strategiczna i public affairs* (Eng. Strategic communication and public affairs), Warszawa 2014.

Larecki J., *Wielki leksykon służb specjalnych* świata (Eng. Great lexicon of the world's special services), Warszawa 2007.

Minkina M., *Sztuka wywiadu w państwie współczesnym* (Eng. The art of intelligence in the modern state), Warszawa 2014.

Modrzejewski Z., *Information operations from the Polish point of view*, "Obrana a strategie" (Defence and Strategy) 2018, no. 1, pp. 115–132. https://doi.org/10.3849/1802-7199.18.2018.01.113-130.

Oosthoek K., Doerr Ch., *Cyber Threat Intelligence: A Product Without a Process?*, "International Journal of Intelligence and Counter Intelligence" 2021, vol. 34, no. 2, pp. 300–315. https://doi.org/10.1080/08850607.2020.1780062.

Rajczyk R., *Nowoczesne wojny informacyjne* (Eng. Modern information warfare), Warszawa 2016.

Roberts S.J., Brown R., *Intelligence-Driven Incident Response. Outwitting the Adversary*, Sebastopol 2017.

Świerczek M., *Working methods of the Russian secret services in the light of the Oleg Kulinich case*, "Internal Security Review" 2023, no. 29, pp. 289–322. https://doi.org/10.4467/20801335PBW.23.031.18773.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni* (Eng. Definition outline of cyberspace), "Przegląd Bezpieczeństwa Wewnętrznego" 2013, no. 9, pp. 225–234.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.* (Eng. 'Reflective management' as a paradigm for Russian information-psychological operations in the 21st century), "Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 12, pp. 11–36.

Woolley S.C., Howard P.N., *Introduction: Computational Propaganda Worldwide*, in: *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, S.C. Woolley, P.N. Howard (eds.), Oxford 2018, pp. 3–18. https://doi.org/10.1093/oso/9780190931407.001.0001.

Internet sources

About Strategic Communications, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/about_us/about-strategic-communications/1 [accessed: 10 VII 2024].

Acquire Infrastructure: Domains, Attack. Mitre, https://attack.mitre.org/techniques/T1583/001/ [accessed: 24 VIII 2024].

Allied Joint Doctrine for Information Operations (AJP-10.1), UK Ministry of Defence, https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations--ajp-101 [accessed: 28 XII 2023].

Allied Joint Doctrine for Psychological Operations (AJP-3.10.1), UK Ministry of Defence, https://www.gov.uk/government/publications/ajp-3101-allied-joint-doctrine-for-psychological-operations [accessed: 5 VII 2024].

An introduction to threat intelligence, CERT-UK, https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf [accessed: 10 IX 2024].

APT29, Attack. Mitre, https://attack.mitre.org/groups/G0016/ [accessed: 24 VIII 2024].

ATT&CK Matrix for Enterprise, Attack. Mitre, https://attack.mitre.org/ [accessed: 24 VIII 2024].

Brangetto P., Veenendaal M.A., *Influence Cyber Operations: The Use of Cyberattacks in Support of Cyberattacks in Support of Influence Operations*, in: *8th International Conference on Cyber Conflict. Proceedings 2016*, N. Pissanidis et al. (sci. ed.), https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence--Operations.pdf, pp. 113–126 [accessed: 10 VII 2024].

Caltagirone S., Pendergast A., Betz Ch., *The Diamond Model of Intrusion Analysis*, https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf [accessed: 24 VIII 2024].

Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/operation [accessed: 28 XII 2023].

Collier J., Ronis S., *Navigating the Trade-Offs of Cyber Attribution*, https://cloud.google.com/blog/topics/threat-intelligence/trade-offs-attribution/ [accessed: 22 VIII 2024].

Combating Foreign Influence, FBI, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [accessed: 2 XI 2024].

Cybersecurity and Foreign Interference in the EU Information Ecosystem, ENISA, 8 XII 2022, https://www.enisa.europa.eu/news/cybersecurity-foreign-interference-in-the-eu-information-ecosystem [accessed: 20 IX 2024].

Cyber Influence Operations, https://www.microsoft.com/en-us/security/business/microsoft--digital-defense-report-2022-cyber-influence-operations [accessed: 10 VII 2024].

DeBolt M. et al., *CTI-CMM Cyber Threat Intelligence Capability Maturity Model*, Version 1.0, https://d39ec1uo9ktrut.cloudfront.net/Datasheets/CTI-CMM-Cyber-Threat-Intelligence--Capability-Maturity-Model.pdf [accessed: 22 VIII 2024].

DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/ [accessed: 5 VIII 2024].

DISARM Foundation, https://www.disarm.foundation/about-us [accessed: 5 VIII 2024].

DISARM Frameworks – incidents, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/incidents_index.md [accessed: 31 VIII 2024].

DISARM Frameworks – phases, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/tree/main/generated_pages/phases [accessed: 31 VIII 2024].

DISARM Frameworks – techniques, GitHub, https://github.com/DISARMFoundation/DISARMframeworks/blob/main/generated_pages/techniques_index.md [accessed: 31 VIII 2024].

Facebook. Threat research, GitHub, https://github.com/facebook/threat-research [accessed: 11 VIII 2024].

Ferazza F.M., *Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model: a comparison of cyber intrusion analysis models*, https://www.royalholloway.ac.uk/media/20188/techreport-2022-5.pdf.pdf [accessed: 25 VIII 2024].

Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape, ENISA, 8 XII 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape [accessed: 20 IX 2024].

Glossary of Intelligence Terms and Definitions, https://www.cia.gov/readingroom/docs/CIA-RDP80M00596A000500020003-7.pdf [accessed: 28 XII 2023].

Headquarters Department of the Army, *FM 100-6, Information Operations*, Washington 1996, https://www.hsdl.org/?view&did=437397 [accessed: 28 XII 2023].

Hutchins E.M., Cloppert M.J., Amin R.M., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [accessed: 24 VIII 2024].

Information Operations, http://web.archive.org/web/20201226185947/https://transparency.twitter.com/en/reports/information-operations.html [accessed: 11 VIII 2024].

Information Operations. Joint Publication 3-13, https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf [accessed: 30 I 2023].

Information Sharing and Analysis Centres (ISACs). Cooperative models, ENISA, 2017, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/@@download/fullReport [accessed: 24 VIII 2024].

Introduction to STIX, https://oasis-open.github.io/cti-documentation/stix/intro.html [accessed: 24 VIII 2024].

IO-Campaign-Collections, GitHub, https://github.com/tripkrant/IO-Campaign-Collections [accessed: 31 VIII 2024].

Joint Doctrine for Command and Control Warfare (C2W), https://apps.dtic.mil/sti/pdfs/ADA357635.pdf [accessed: 28 XII 2023].

Larson E.V. et al., *Foundations of Effective Influence Operations. A Framework for Enhancing Army Capabilities*, Rand Corporation, 2009, https://www.rand.org/pubs/monographs/MG654.html [accessed: 18 XI 2024].

Mavroeidis V., Bromander S., *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*, https://arxiv.org/pdf/2103.03530 [accessed: 24 VIII 2024].

Microsoft Digital Defence Report 2022, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us [accessed: 11 VIII 2024].

MISP. Threat Sharing, https://www.misp-project.org/ [accessed: 24 VIII 2024].

Niedzielski D., *Wojskowa doktryna komunikacji strategicznej NATO i jej znaczenie dla Polski* (Eng. NATO's Military strategic communications doctrine and its relevance to Poland), "Akademickie Centrum Komunikacji Strategicznej" 2022, no. 3, https://www.wojsko-polskie.pl/aszwoj/u/af/14/af143adc-70e6-463a-8448-faaf0df61e9a/biuletyn_nr_3.pdf, pp. 46–53 [accessed: 10 VII 2024].

OpenCTI, https://filigran.io/solutions/open-cti/ [accessed: 24 VIII 2024].

Oxford English Dictionary, https://www.oed.com/dictionary/operation_n?tab=factsheet&tl=true#33665121 [accessed: 28 XII 2023].

Pamment J., Smith V., *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, https://stratcomcoe.org/publications/download/Nato--Attributing-Information-Influence-Operations-DIGITAL-v4.pdf [accessed: 18 VIII 2024].

Pols P., *The Unified Kill Chain. Raising resilience against advanced cyber attacks*, https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf [accessed: 24 VIII 2024].

Porche I.R. et al., *Redefining Information Warfare Boundaries for an Army in Wireless World*, https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf [accessed: 28 XII 2023].

Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure, https://www.cisa.gov/sites/default/files/2023-01/cisa_insight_mitigating_foreign_influence_508.pdf [accessed: 29 XII 2023].

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku (Eng. Report on the state of Poland's cybersecurity in 2023), CSIRT GOV, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-staniebezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html, p. 20 [accessed: 31 VIII 2024].

Shires J., *Hack-and-leak operations and U.S. cyber policy*, War on the Rocks, 14 VIII 2020, https://warontherocks.com/2020/08/the-simulation-of-scandal/ [accessed: 10 VII 2024].

SJ Terp, https://www.infosecurity-magazine.com/profile/sj-terp/ [accessed: 5 VIII 2024].

Słownik języka polskiego PWN (Eng. PWN Dictionary of the Polish Language), https://sjp.pwn.pl/szukaj/operacja.html [accessed: 3 VII 2024].

SolarWinds Compromise, Attack. Mitre, https://attack.mitre.org/campaigns/C0024/ [accessed: 24 VIII 2024].

Terms & Definitions of Interest for DoD Counterintelligence Professionals, https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf [accessed: 28 XII 2023].

Terp SJ, Breuer P., *DISARM: A Framework for Analysis of Disinformation Campaigns*, 2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), https://ieeexplore.ieee.org/document/9830669 [accessed: 5 VIII 2024].

Threat Report: Combating Influence Operations, Meta, 26 V 2021, https://about.fb.com/news/2021/05/influence-operations-threat-report/ [accessed: 11 VIII 2024].

Threat Report. The State of Influence Operations 2017–2020, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf [accessed: 10 VII 2024].

TTP in cybersecurity, Sekoia, https://www.sekoia.io/en/glossary/ttp-cyber-tactics-techniques-and-procedures/ [accessed: 9 IX 2024].

Updated IC Gray Zone Lexicon: Key Terms and Definitions, https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf [accessed: 11 VIII 2024].

Wagner T.D. et al., *Cyber Threat Intelligence Sharing: Survey and Research Directions*, https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf [accessed: 24 VIII 2024].

Wardle C., Derakhshan H., *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Council of Europe report DGI(2017)09, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html [accessed: 10 VII 2024].

Watling J., Danyluk O., Reynolds N., *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023*, https://static.rusi.org/202303-SR-Unconventional-Operations-Russo-Ukrainian-War-web-final.pdf.pdf [accessed: 10 VII 2024].

Watts C., *Advanced Persistent Manipulators, Part One: The Threat to Social Media Industry*, Alliance for Securing Democracy, 12 II 2019, https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/ [accessed: 18 VIII 2024].

Words of Estimative Probability, Analytic Confidences, and Structured Analytic Techniques, Center for Internet Security, https://www.cisecurity.org/ms-isac/services/words-of-estimative-probability-analytic-confidences-and-structured-analytic-techniques [accessed: 23 VIII 2023].

Wright C., *The Diamond Model for Influence Operations Analysis*, https://go.recordedfuture.com/hubfs/white-papers/diamond-model-influence-operations-analysis.pdf [accessed: 28 VII 2024].

Legal acts

Act of 17 February 2005 on the computerisation of the activities of entities performing public tasks (Journal of Laws of 2024, item 1557).

Act of 29 August 2002 on martial law and the competences of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland (Journal of Laws of 2022, item 2091).

Act of 6 June 1997 – Criminal Code (Journal of Laws of 2024, item 17).

Other documents

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 (Eng. National Security Strategy of the Republic of Poland 2020), https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [accessed: 10 VII 2024].

Kamil Baraniuk, PhD

Doctor of Political Science and Administration, graduate of the Faculty of Social Sciences, University of Wrocław.

Contact: kam.baraniuk@gmail.com

Piotr Marszałek

Cyber security expert at the Polish Association for National Security.

Contact: piotr.marszalek@ptbn.online