Humanities and Social Sciences **2023**
Research Journal 30, No. 4 (2023) – part I, pp 7-24 **October-December**

Received: April 2023
Accepted: December 2023
DOI: 10.7862/rz.2023.hss.39

Robert BIAŁOSKÓRSKI[1]

THE THEORETICAL CONCEPT OF INFORMATION WARFARE: A GENERAL OUTLINE

This article presents the results of research on the theoretical paradigm of information warfare. The research methodology is based on political realism in international relations and observations of the war in Ukraine since 2014. It assumes that the main feature of the international system is the distribution of power and intersections between rival power centers. The principal roles are now played by states and groups of states as basic political units. From a broader perspective, in the future, the importance of non-state actors will also increase. The research produces a general outline of the theoretical concept of information warfare. According to the accepted terminology, information warfare is a process of achieving the strategic goals (interests) of any organization by offensive and defensive activities in the information space (infosphere), inspired and carried out against other organizations for self-protection and self-defense. The research indicates three key interconnected structures (components) of the concept of information warfare: participants (actors), tools (operators), and the information domination subprocess.

Keywords: cybernetic warfare, information warfare, information operations, information power, information geopolitics.

1. INTRODUCTION

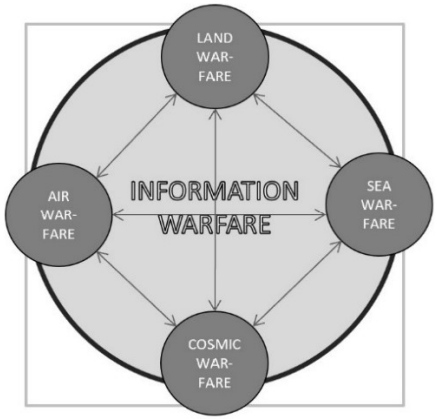
Information warfare (IW) is an important element of the process of hybridisation of war consisting primarily of the growing role of the information domain in the management of contemporary armed conflicts. The experience of the battlefield, especially in the war in Ukraine, initiated by the Russian annexation of Crimea in 2014, and next by the military invasion in 24 February 2022, demonstrates in practice the evolutionary directions of development of the information warfare.

Progressing of digitization increases the involvement of nonmilitary means of the battlefield at all stages of war: preconflict, active conflict, and postconflict. The scope of the military impact of the information domain is in practice the most significant among the other kinetic domains: land, air, sea, and cosmic (Warden III, 1995). Any kinetic military operation begins, continues, and ends in the information domain. It brings the information domain to the rank of sine qua non factor of the success of any military operation. Simultaneously at the same war does not mean operating only in the information domain

[1] Robert Białoskórski, University of Siedlce, Poland; e-mail: robert.bialoskorski@uws.edu.pl. ORCID: 0000-0003-3038-7560.

without the support of any other kinetic domain. It is the result of the military technological development (intelligent robotization) of the modern battlefield. In NATO terminology, it is called 'multi-domain operations' instead of the 'joint operations' strategy (Drawing 1).

In this context, we should rather talk about 'information warfare', not 'information war'. This latter term should be treated more as journalistic metaphor for information warfare (Triqui, 2015), than scientific. But this approach is also found in scientific papers, political strategies and doctrines, and cybersecurity dictionaries (Maurer, Morgus, 2014).

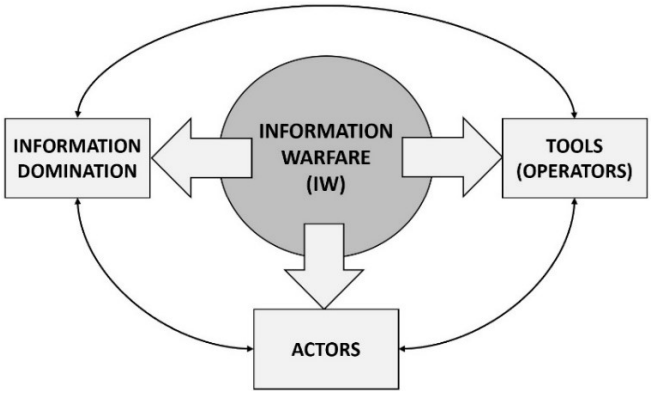


Drawing 1. The multi-domain military operations strategy

Source: own elaboration.

According to this research study, **information warfare is a process of achieving strategic goals (interests) of any organization by offensive and defensive activities in the information space (infosphere) inspired and carried out against other organizations for self-protection and self-defence**.

In this context, three key components of this model must be defined, such as actors, tools (operators), and the information domination subprocess (Drawing 2).



Drawing 2. Key components of the concept of information warfare

Source: own elaboration.

The adopted definition of IW refers to any state and non-state organization able to conduct IW, as an actor of this process[2]. Researching the theoretical aspects of IW is critical to develop its effective information doctrine and strategy in decision-making practise and activities. **Information domination is the acquisition of information advantage from an organization in offensive and defensive actions against other organizations during geopolitical struggle or armed conflict.** Two key tools (operators) of IW, such as **psychological information operations (PIOs) and cybernetic information operations (CIOs)**, are considered.

2. BRIEF REMARKS ON THE LITARATURE

The literature on information warfare is quite extensive. However, a gap should be noted in the systematic approach to this concept. The content of most books and papers concerns the discussion about the different definitional concepts, evolution, strategies, deterring, and case studies (especially in the aspect of hybrid warfare) of IW, as well as methods and techniques of IT attacks (e.g. J. Andress, R.A. Clarke, D.E. Denning, B. Gardner, J.J. Garstka, K. Giles, A. Greenberg, F. Kaplan, S. Komov, S.T. Lawson, D. Lonsdale, M. Libicki, T. Rid, T.A. Schnaufer II, D.C. Schleher, P.W. Singer, M. Snegovaya, R. Stiennon, R. Stengel, E. Waltz, S. Winterfeld). Studies on the information and cybernetic power are explored by a rather small group of researchers (Ch.L. Barry, D.J. Betz, D. Cassidy, W. DeSombre, M.A. Gomez, C.S. Gray, I. Hemani, S. Jones, A. Klimburg, D. Kuehl, D.T. Kuehl, A. Schwarzenbach, T. Stevens, J. Voo, E. Zimet).

3. INFORMATION WARFARE ACTORS

The information warfare actors are de facto all actors of the international relations. It can be divided into state and non-state and internal and external actors. However the role of non-state actors (e.g. transnational corporations) is increasing, but it is still the states (as well as the intergovernmental organizations) as the principle political units with their holistic material and intangible resources (potential) playing a key role in the international system. And according to the theory of political realism, the most important feature of every international system is the distribution of power (Aron, 2017).

Therefore, it is no exaggeration to say that the IW is currently a key tool in the geopolitical rivaling of states for the best possible position in the structure of the international system. A stronger position means greater power and opportunities to influence the international distribution of power (IDP) as a game of powers and interests in a global, regional, or local dimension. The rivalry between states is a so-called zero-sum game, where winning one side is a loss of the other side with the same size. In the IDP, a global power is always equal to 100%, while the ratio of states power is constantly changing. Rivalry between states for limited global resources (‘source of survival energy’)

[2] The author has also developed a narrow definition of information warfare based on a multi-indicator model of defining and identifying cyber threats. This model is based on four indicators matrix: 1) attacking subject (agresor), 2) attacked subject (victim), 3) result, 4) purpose/motivation). According to this concept, information warfare is ‘various actions in cyberspace inspired and directly or indirectly conducted by States and/or international organizations (attacking subject) directed against other States, international organizations and/or non-State actors (attacked subject), which directly or indirectly lead to injure or death people and damage or destroy the elements of critical infrastructure (result), in order to achieve the State’s national interests or the interests of the organization (purpose/ motivation)’ (Białoskórski, 2012).

takes two forms: (1) cooperation (trade resources) or (2) struggle (taking other people's resources). Cooperation is a so-called positive sum game, where all players profit, though to a different degree. Struggle (in different spheres: information, political, economic, military, etc.) is a so-called negative-sum game in which all players lose, though to a different degree. Therefore, in constant competition for the maximum share of power, states alternate between cooperation and struggle, depending on specific conditions (Sułek, 2013) (Sułek, 2020). Studying changes in the IDP in economic, military and geopolitical dimensions, the current international system can be reliably determined, especially in geostrategic studies (Białoskórski, 2018, 2020, 2021).

The political, economic, military, technological, and cultural capabilities and influence of states are widely known in the social sciences domain. However, in the context of the IW, the special role of the system of state authorities, secret services, actors of military and civilian information domains (such as military reconnaissance), state society ('ordinary people'), and non-state actors must be taken into account. Secret services (intelligence and counterintelligence), as well as special operations forces, are the sensors ('eyes and ears') of the army in the harassment zone in front and behind enemy lines. There is also a category of people called 'useful idiots' who, without external inspiration, favour hostile interests with their views and actions. Non-state actors, such as cybercorporations, private military companies (PMC), such as the russian 'Wagner' and „Reduta" very active from the beginning of the Ukraine war, international cyber terrorist organizations (ICTOs), organized international cybercriminals groups (OICGs) covert or overt employment in cyberspace operations mostly as volunteers in state-to-state conflicts (Sigholm, 2013). In this case, the cooperation between ICTOs and OICGs is already an unusual and particularly dangerous cyberthreat. As an example, the joined operatives aligned between the Tunisian Cyber Army (TCA) and al-Qaeda Electronic Army (AQEA) and their assault on US government websites for US Customs and Border Protection and the Office of Personnel Management in 2015. The role of supporting actor in the information warfare process is also played by the civilian society. This applies to ordinary citizens who play the role of 'war singalists' taking advantage of home. The dictionary term 'signalist' means someone who makes signals or communicates intelligence by signaling („Signalists", 2022). This term comes from the English word "whistleblower" and refers to a social phenomenon that has long been present in various countries and societies. It literally means blowing a whistle and refers to the act of summoning help, alerting, and signaling danger. It was proposed by Ralph Nader, an American lawyer and social activist in the 1970s. It meant the action of a prosocially motivated individual informing the environment that its organization violates the public interest. War signalists can inform the state authorities about the dislocation and movements of the occupying forces. It is necessary to include them in an organized information system, i.g. by mobile phones with emergency calls. There are known cases of monitoring and informing about the positions and mobility of Russian troops by Ukrainian citizens during the war in Ukraine. For some of them, spying on the Russians is even part of their own daily routine, playing a key role in guiding Ukrainian precision combat strikes. In particular, this applies to military operations in the Donbass. This is clearly evidenced by the statement of a Ukrainian security official: 'These people see Russian tanks moving, they see where the troops go to dinner, where they party, where they do their laundry, and they share that information with us' (Luxmoore, 2022).

Every country, the most intergovernmental organizations, such as EU and NATO lead cyber activities and policies such as the establishment of national (international) cyber strategies, enhancing research and development efforts, and strengthening international

cyber collaborations and regulations. The governments undertake defensive and offensive cybersecurity operations (officially announced in 2016) (Baram et al., 2018). This requires the building and involvement of an national information power in both civilian and military domains. Cyber-army and army intelligence play a special role in various forms (kinetic and non-kinetic) of international conflict. Their permanent tasks are monitoring and processing of information flow streams in the state critical infrastructure security system, as well as the fight against all form of cyber-threats and cyber-attacks, such as: cyberwarfare, cyberespionage, cyberterrorism and cybercrime (Białoskórski, 2012).

During military operations, army intelligence has issued a wide range of fully integrated aerial, ground, and cyber sensors based on intelligence, surveillance, and reconnaissance (ISR) capabilities to support kinetic fighting forces on the battlefield. To be effective against a networked enemy, it is demanded abilities such as full-motion video (FMV), signals intelligence geo-location, exploitation of captured documents and media (DOMEX), biometrics, advanced analytics, and more robust human and technical collection (Legere, 2012). It requires to be organised such branches as a special cyber defence centre (e.g., in the structure of General Staff), as well as similar centres in each military district and type of the armed forces. It is also necessary to create a military cybernetwork based on the intranet (without any connection to the internet) with multilevel protection abilities to prevent any offensive cyber-attacks. Beyond the information and communication technology (ICT) aspects, the most important is the protection of financial support and the hiring of professional military and civilian personnel.

It is clear that the Army needs fully integrated intelligence, security, information operations, and related support from the government and private ICT innovation sector. Covers areas such as intelligence collection and analysis, information operations, support of intelligence operations, facilities and systems, and support services.

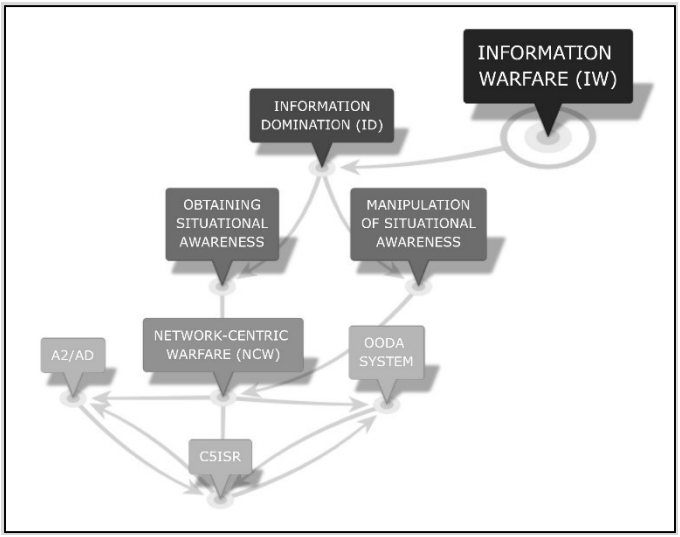
4. INFORMATION DOMINATION

Information domination (ID) is the obtaining of information advantage of an organization in offensive and defensive actions against other organization during geopolitical struggle or armed conflict. The key factors for ID are the achievement of self-situational awareness (self-awareness) and the manipulation of situational awareness, own and rival(s) (Drawing 3). This process is based on network-centric warfare (NCW), acting as the ‘brain’ of the information warfare process. It is an emerging theory of war in the information age ('Vice Admiral (Ret.) Arthur K. Cebrowski, Director, Office of Force Transformation, interview with Frank Swofford', 2004).

The NCW concept broadly describes the combination of strategies, emerging tactics, techniques, and procedures, and organizations that a fully or even a partially networked force can employ to create a decisive warfighting advantage (Garstka, 2003). There are three elements clearly distinct from the NCW definitions, that is, the impetus of NCW, the means to establish it, and the outcome/benefits it aims to achieve, that is, enhanced combat capabilities and their five attributes, such as extensive connectivity and interoperability, common and shared situational awareness, cooperative detection, cooperative detection, and compression of time and space (Soon-Chia, 2004).

The attribute of common and shared situational awareness decides on the ability to achieve ‘[…] a complete picture for the entire Area of Operation (AOR). NCW, enabled by increased network bandwidth, will see a proliferation of Common Operating Pictures (COPs) transcending through and distributed across the military hierarchies, from the

strategic level to the lower echelons (Soon-Chia, 2004). This tactic of armed war is based on the idea of swarming (BattleSwarm). It is based on systematic, pulsating and simultaneous multi-impacts from all diffused operation directions by specialized military componnets connected in NCW system. The permanent "pulsation" of power and high dynamics and pace of kinetic impact is a characteristic feature of the swarm's tactics, making it difficult for the opponent to respond effectively (Olszyk, 2019).



Drawing 3. Information domination process

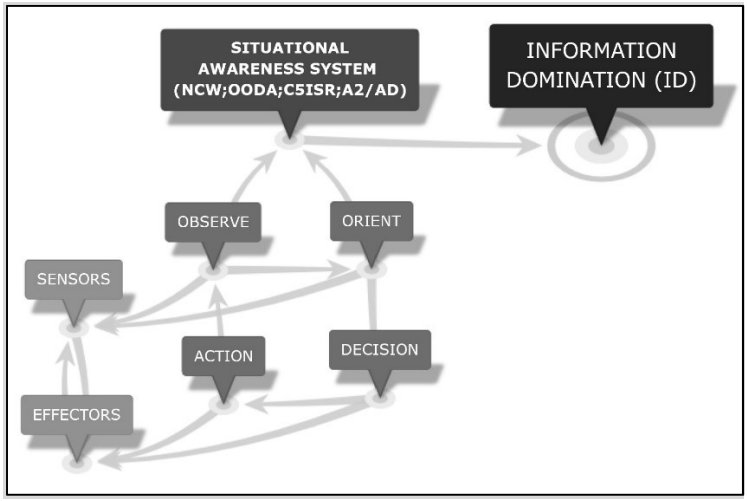
Source: own elaboration.

The operational success of the concept of the NCW process depends mainly on the OODA (observe, orient, decision, and action), C5ISR (command, control, communication, computers, cyber, intelligence, surveillance, reconnaissance), and A2/AD (anti-access/area denial) systems (Drawing 4).

The OODA loop strategy is a concept of situational awareness first developed in the mid-1950s, by USAF Colonel John Boyd (Kelly and Heliskiing, 2014) (Rađenović, no date). The OODA is the information management and control system of any organization. In the military aspect, it is the C5ISR system of the armed forces, during the period of peace (P) and war (W). The concept of the OODA system is based on the implementation of four circularly interconnected activities: observation (observe), orientation (orient), decision, and action. Observation and orientation act as sensors, while decision and action are the functions of effectors. The OODA concept is also the framework of a more advanced intelligence circle process (Krizan, 1999).

In the Ukrainian war, a special role of sensors is played by satellite and operational intelligence capabilities, including intelligence data of NATO mamber states and and radio-electronic warfare (REW) systems, such as the western Airborne Early Warning And Control (AWACS) or Russian Palatin. From the operational and tactical point of view, an important role plays played by artillery reconnaissance and strike systems, such as Himmars and Gladius. This war showed the omnipresence of sensors and effectors almost

in all changing battlefield conditions, regardless of the season, day and night, or weather conditions. This is the first drone war with the complex of sensors and effectors (loitering munitions, kamikaze drones), where it is hard to hide.



Drawing 4. Situational awareness system

Source: own elaboration.

These experiences have also proven the particular usefulness of network-centric systems installed on mobile devices (smartphones), as an element of the military communication, reconnaissance, decision-making and strike network, such as TAK (Tactical Assault Kit-military, and Team Awareness Kit-civilian versions). TAK uses the CoT (Cursor on Target) information exchange protocol, e.g., to inform about the deployment of own and enemy forces (blue force tracking), map events, ability reporting, command forwarding, and obtaining information from sensors by users connected to the system, such as drone image. The main advantage of TAK is its simplicity, enabling very quick implementation and integration of various types of system, communications, sensors, and even effectors (Szopa, 2023).

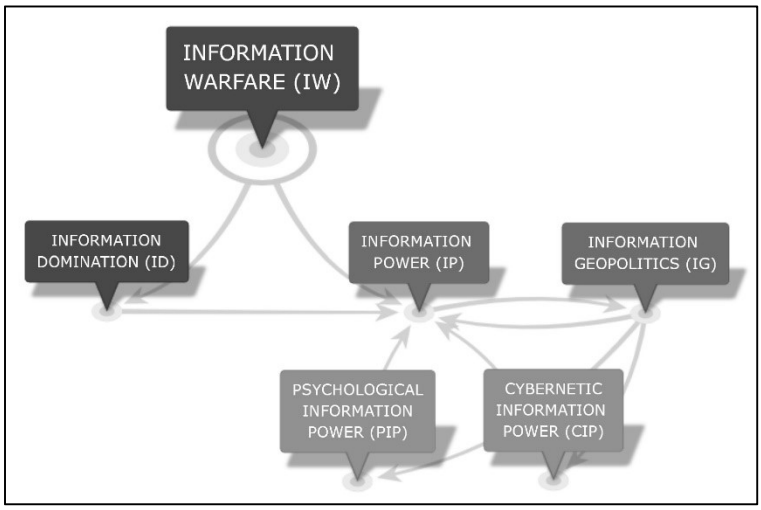
5. INFORMATION POWER AND INFORMATION GEOPOLITICS

At the beginning of the considerations, it is worth quoting two statements from the theory of international relations. The fundamental concept in social science is power in the same sense in which energy is the fundamental concept in physics (Russell, 1996). In a general sense, power is the ability to do, make, or destroy. […] An individual's power is his ability to act, but above all to influence the actions or feelings of other individuals. On the international scene, power should be defined as the capacity of a political unit to impose its will on other units. In short, political power is not an absolute; it is a human relationship (Aron, 2017).

From the theory of social cybernetics, durign the international game of power and interests, the states pursue their strategic goals by the increasing (maximizing) the national power (NP) as a form called by Marian Mazur as **'sociological power'** in contrast to

'material (kinetic) power' (Mazur, 1996). In a mathematical formula, NP can be defined as a potential product (capability) and employing social support (will) and an appropriate strategy. It can also be expressed as a product of tangible (that is, material factor), intellectual (that is, information factor), and spiritual potential, as well as a product of national resources (potential, that is, material factor), strategy (that is, information factor) and the desire to pursue national strategy by the political unit (Sułek, 2010; Moczulski, 1999). The formula for the mathematical product means that all factors must be met for the power to be greater than zero. The Ukrainian conflict clearly showed the importance of the third factor of NP - spiritual, the will to fight for the life and survival of the nation and state. Victory on the battlefield is ensured by the synergy of will to fight, training, and technology. The bravery and heroism of the Ukrainian nation in the face of the overwhelming material ('kinetic') power of the enemy surprised and amazed not only the Russian aggressor, who was unable to break it, but also the entire international community.

This leads directly to a terminological convention, that **the information power (IP) is the organization's ability to pursue its strategic goals by influencing the information space (infosphere).** Contrary to the already relatively developed research on the kind of 'material (kinetic) power', the study of IP is still in an early stage. The approach presented mostly in the literature treats IP as a 'cyber power (CP)' (Kuehl, 1997; Barnett, Duvall, 2005; Kuehl, 2009; Zimet, Barry, 2009; Stevens, 2010; Nye, 2010; Klimburg, 2011; Betz, Stevens, 2011; Gray, 2013; Yuen, 2015; Langner, 2016; Domingo, 2016; Van Haaster, 2016; Bebber, 2017; Knox, 2018; Voo et al., 2020a; Voo et al., 2020b; *Global Cybersecurity Index 2020. Measuring commitment to cybersecurity*, 2020; Cho, 2020; Gomez, no date). Tt is not and should not be treated in the same way as IP. The above results from the fact that IP is a kind of hybrid structure of two integrated components: 'psychological information power' (PIP), as a kind of 'soft information power' and 'cybernetic information power' (CIP), as a kind of 'hard information power' (Drawing 5).



Drawing 5. Information power and information geopolitics in information warfare

Source: own elaboration.

Both of these new terms are precisely correlated with two IW key operators, i.e. psychological information operations (PIOs) and cybernetic information operations (CIOs). Therefore, '**psychological information power' (PIP) is the organization's ability to pursue its strategic goals by 'psychological information operations' (PIOs) and 'cybernetic information power' (CIP) is the organization's ability to pursue its strategic goals by 'cybernetic information operations' (CIOs).**

The measurement of IP is the level of effectiveness of the implementation of strategic interests by any organization by the activities in the infosphere. It is expressed in the form of various indicators. There are known such indicators as: Cyber Power Index (CPI) (*Cyber Power Index. Findings and Methodology*, 2011), National Cyber Power Index (NCPI) (Voo et al., 2020b), Global Cybersecurity Index (GCI) (*Global Cybersecurity Index 2020. Measuring commitment to cybersecurity*, 2020). This issue requires further theoretical and empirical research.

In a broader sense, these considerations directly lead to the concept of information geopolitics (IG). This new direction of geopolitics research results mainly from the growing importance of the information power in relation to material (kinetic) power in the international system (Białoskórski, 2022). The main reason is the currently emerging polycentric nature of the international system, dominated by the United States and China, and the dominance of 'hybrid conflicts' ('nonlinear conflicts' in Russian terminology) and 'diffusion (dispersed) conflicts' over classic 'kinetic (linear) conflicts' (Siverson, Starr, 1991; Lawson, 2014; Gardner, 2018).

Geopolitics of information is one of the developing subdisciplines of geopolitics. However, in the literature it also appears as a synonym of 'information geopolitics' and 'geopolitics of information', as well as the related terms: 'geopolitics of cyberspace', 'networked geopolitics', 'corporate geopolitics', or 'geopolitics of technology'. The etymology of the term information geopolitics is related to the evolution of geopolitics as a scientific discipline, from classical geopolitics to contemporary geopolitics. In the classical (traditional) sense of geopolitics, these are geographical conditions. The modern (new, critical) geopolitics concept has a multidimensional and real-time variable nature strongly associated with the impact of information stream flows in the infosphere. Moreover, it significantly deepens the classically understood geographical research area of geopolitics, redefining the space-time concept. It is already not only a geographical chessboard, but also a network of connections between various space-time factors and their geopolitical context interpretation. As a result, it is significantly more important in the science and practice of international relations.

This also gives grounds for the separation and development of **information geopolitics as a subdiscipline of geopolitics dealing with the study of the impact of the information space (infosphere) on the process of making strategic decisions (particularly political) by geopolitical actors creating the distribution of power and interests, as the main feature of the international system** (Białoskórski, 2022).

An important factor that determines information geopolitics is a '**strategic culture' (SC)** of geopolitical actors that formulate information policy, as well as strategies, concepts, and doctrines. The essence of considerations on SC is Carl von Clausewitz's theory that the goal of war is not only to defeat the enemy physically but also to incapacitate psychologically (Lantis, 2002, 2005). In the general sense, 'strategic culture' is culturally conditioned patterns and perception schemes characteristic of a given community (nation). It affects the perception of the security environment, the assessment of security threats, and the crisis management process (Snyder, 1977; Klein, 1991; Zaman, 2009). For example,

Russia's strategic culture is different from American, as well as American differs from Chinese one.

In the aspect of the war in Ukraine, the main features of the strategic culture of the Russian aggressor are important. Three of them are the most important: 1) relative historical durability and militarization (coexistence with military culture), 2) militarization of public space (interpenetration of the military sphere and the dominant state ideology), 3) traditional militaristic expansionism (Budzisz, 2021). This finds its expression in the 'spirit' and 'word' (content) of the Russian perspective of imperial geopolitics (Dugin, 2014) and mental (psychological) warfare strategy (ИЛЬНИЦКИЙ, 2021). This is also reflected in the theory of 'reflexive control' and, more broadly, in the 'reflective psychology' initiated by Vladimir A. Lefebvre. Reflection means the ability to create in our consciousness an image of 'inner world' of other human beings and assessing how others perceive us (Lefebvre, 1987). The goal of reflexive control is to 'control' the 'reflex' of the opponent by creating a certain model of behavior in the system it seeks to control (Kowalewski, 2017). The effect of his scientific work is the foundation of the theory and practice of Russian information warfare. This is the paradigm of techniques and methods of Russian psychological information operations (PIOs), as well as cybernetic information operations (CIOs) developing after the Second World War (Giles, Sherr, and Seaboyer, 2018).

6. INFORMATION WARFARE TOOLS (OPERATORS)

In the concept of IW, two types of information operations have been distinguished: psychological information operations (PIOs) as an operator of some kind of information 'soft-power' and cybernetic information operations (CIOs), as an operator of some kind of information 'hard-power'. It should be noted that these operations are carried out in the form of offensive and defensive by both the civilian and military security sectors, with CIOs, as a kinetic form, dominating the military sphere.

6.1. Psychological Information Operations (PIOs)

The PIOs are defensive and offensive information activities that shape mental maps of social awareness in the process of decision-making information. They are based on more spectrum of social management (social engineering) techniques feeding an opponent special selected (prepared) information to influence the opponent to make decisions favourable to the attacker. These activities are conducted firstly in non-autonomous (external) information system, towards the foreign environment, but also in autonomous (internal) information system, according to a native society. The Russian theory of information warfare (e.g. Sergey Komov) distinguishes such PIOs techniques as: Distraction, by creating a real or imaginary threat to one of the enemy's most vital locations (flanks, rear, etc.) during the preparatory stages of combat operations, forcing him to reconsider the wisdom of his decisions to operate along this or that axis; • Overload, by frequently sending the enemy a large amount of conflicting information; • Paralysis, by creating the perception of a specific threat to a vital interest or weak spot; • Exhaustion, by compelling the enemy to carry out useless operations, thus entering combat with reduced resources; • Deception, by forcing the enemy to reallocate forces to a threatened region during the preparatory stages of combat operations; • Division, by convincing the enemy that he must operate in opposition to coalition interests; • Pacification, by leading the enemy to believe that pre-planned operational training is occurring rather than offensive

preparations, thus reducing his vigilance; • Deterrence, by creating the perception of insurmountable superiority; • Provocation, by forcing the commander to take action advantageous to your side; • Suggestion, by offering information that affects the enemy legally, morally, ideologically, or in other areas; • Pressure, by offering information that discredits the government in the eyes of its population (Giles, Sherr, and House, 2018) – Quoted for: (Komov, 1997). Taking into account the 'reflexive interaction categories' defined and practised by Russian in the IW from the 1980s, it can be recognised as follows: Transfer of an image of the situation: Provide an opponent with an erroneous or incomplete image of the situation. • Creation of a goal for the opponent: putting an opponent in a position in which he must select a goal in our favour (e.g., for provoking an enemy with a threat to which he must rationally respond). • Form a goal by transferring an image of the situation: feigning weakness or creating a false picture. • Transfer of an image of one's own perception of the situation: providing an opponent with false information or portions of the truth based on one's own perception of the situation. • Transfer of an image of one's own goal. • Transfer of an image of one's own doctrine: giving a false view of one's procedures and algorithms for decision making. • Transfer of one's own image of a situation to make the opponent deduce his own goal: present a false image of one's own perception of the situation, with the additional level of risk (Giles, Sherr, and House, 2018) – Quoted for: (Reid, 1987).

In the last decade, Russia has conducted IOPs in Georgia (7–8 August 2008) and still in Syria (since 30 September 2017) and Ukraine (since 2014) on the battlefield (in classic and hybrid forms). It is clear that a significant part of the streams of IOPs flow in **electronic media** (traditionally and modern), especially **social media** through various internet platforms and many providers, such as: social networks (e.g. Facebook, LinkedIn), video content (e.g. YouTube, Periscope), picture content (e.g. Instagram, Snapchat), book content (e.g. Goodreads, WeRead), training content (e.g. Garmin Conect, Strava), instant messaging (e.g. WhatsApp, Telegram), blogs (e.g. WordPress, Blogspot), micro-blogging (e.g. Twitter, Friendfeed), analytics tools (e.g. Klout, Geofeedia), crowd-sourcing (e.g. InnoCentive, Patreon), location services (e.g. Tinder, TripAdvisor) (Giles, Sherr, and House, 2018). There are many definitions with different approaches to social media and the discussion is still open (Giles, Sherr, House, 2018).

The Russian-Ukrainian war began in 2014 with the Russian military invasion and finally annexation of Crimea (10 March) and Russian military support of separatism separatist movements in the Donbas (symbolic so-called Putin's 'green men'). After six years of 'hybrid war', it took the form of an open kinetic conflict (called 'military special operation' by Russian authorities) since February 24, 2022. From the beginning, both sides are conducting an information warfare in the external and internal environment. In the first phase of this conflict (2014–2021), Russia proved to be more effective in IOPs. As a result, Russia obtained one main geopolitical and geostrategic goal – the annexation of Crimea (territorial success) by a 'soft' international response (political success). From the first days of its second phase, Ukraine surprised Russia with the dynamics and effectiveness of PIOs. This shows well the training of the Ukrainian security sector by information warfare specialists from western countries. Ukraine and its supporting countries have successfully blocked Russian PIOs to undermine the Western consensus on supporting Ukraine, justify the war by Russia, and conceal war crimes. Russian campaigns addressed to both Russian and foreign societies are carried out by disseminating false information on social media using fake accounts, trolls, and bots, most often on several platforms at the same time. Increasingly, campaigns use artificial intelligence to create fictitious user accounts, photos,

videos, or satellite maps, or to send large numbers of messages at once. They use websites pretending to be well-known news sites, such as the BBC, CNN, and DW, or promote pseudo-scientific publications (Kaca, 2022).

However, the situation will escalate as the conflict continues. Although the instruments of Moscow's propaganda and information influence on the West are not so effective as before February 24, mass activity of Russians is visible in social networks aimed at creating further divisions within the Western world. Constantly aggressive Russian rhetoric, regular threats nuclear weapons, the desire to deepen the energy and economic crisis in the EU are intended to lead to the fatigue of Western elites and societies and to submission to Moscow's demands (Konończuk, 2023).

In addition, the impact of Russian IPOs on its own nation will be maintained and even intensified. Their advanced forms are 'false flag operations' (FFO). This is the type of 'camouflage' operation (Russian: 'maskirovka') practiced by secret services. It consists of impersonating foreign secret services, hiding the real identity. An example is the case of an alleged Ukrainian sabotage diversion in the Bryansk region on Russian territory in March 2023. Ukraine's authorities have denied these actions and point to Russian provocation in the form of FFOs to more strongly intimidate and control the Russian society (Bruszewski, 2023).

6.2. Cybernetic Information Operations (CIOs)

CIOs are defensive and offensive cybernetic activities that affect critical infrastructure (people and objects). This is the principle military information domain involving the armed forces (cyber-army, cyber-soldiers) and military secret services. CIOs are conducting during classical linear war, as well as nonlinear (hybrid) war. Their main operators are electronic warfare components with such operational tasks as: 1) permanent or temporary destruction of enemy electronic (cybernetic) systems, 2) electronic defense against enemy electronic attack, 3) electronic intelligence and counterintelligence.

Ad 1) Permanent or temporary destruction of enemy electronic systems (incl. autonomous weapons) is conductig by electronic attack (*use of electromagnetic energy for offensive purposes*) in its electromagnetic vulnerability (the characteristics of a system that cause it to suffer degradation in performance of, or inability to perform, its specified task as a result of electromagnetic interference). Electronic defence, as the use of electromagnetic energy to provide protection and to ensure effective friendly use of the electromagnetic spectrum, is an electronic countermeasures (that division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum through the use of electromagnetic energy. There are three subdivisions of electronic countermeasures: electronic jamming, electronic deception and electronic neutralization) (*Słownik terminów i definicji NATO (AAP-6)*, 2014).

Ad 2) There are many electronic passive and active rotective measures (countermeasures) of a defense strategy against an enemy electronic attack such as: electronic intelligence and surveillance, electronic neutralization, electromagnetic interference, electronic masking, barrage jamming, electronic jamming; jamming; spot jamming; sweep jamming, electronic deception and others. An important part of this strategy is military cyber networks isolated from the global network with multi-layered cyber protection system. The implementation of this strategy belongs to new special military scientific divisions as cyber-army, cyber-commands, cyber-soldiers, and intelligence corps.

Ad 3) The components of electronic intelligence and surveillance are the main components of electronic defence. It consists of the use of electromagnetic energy for the purpose of preemptive situational awareness and data intelligence. To the main components belong: SIGINT (Signals Intelligence), COMINT (Communication Intelligence), and ELINT (Electronic Intelligence), MASINT (Measurement and Signature Intelligence). Of course, activities within the framework of HUMINT (Human Intelligence) and OSINT (Open-Source Intelligence) are always important.

During the war in Ukraine, the most advanced and effective russian CIOs occurred during the Russian annexation of Crimea. The effective attack on the communication systems of Ukrainian soldiers and politicians led to information chaos and paralyzed retaliatory actions (Kozłowski, 2014). Then, the Ukrainian cyber troops began to take over the operational initiative.

7. CONCLUSIONS

The presented research outcome fills a gap in the information warfare literature. The study of information warfare in the aspect of the war in Ukraine made it possible to verify and modify its theoretical paradigm. The result of this study is a new systemic concept of information warfare as a process of achieving strategic goals (interests) of any organization by offensive and defensive activities in the infosphere inspired and carried out against other organizations and for self-defence.

This model assumes the interaction of three of its key components, such as actors, information domination, and tools (operators) of information warfare. Among the actors of the IW, the main role is still played by the states as the principal political units. However, the growing importance of non-state actors, especially digital transnational corporations, needs to be observed and researched.

The sine qua non condition for the effectiveness of the information warfare is information dominance, as the obtaining of information advantage of an organization in offensive and defensive actions against other organization during geopolitical struggle or armed conflict. It means the ability to achieve self-situational awareness (self-awareness) and the manipulation of situational awareness, both own and rival(s). It depends on the efficiency of network-centric warfare (NCW) acting as the ‘brain’ of the information warfare process.

This concept involves the interaction of two categories of information warfare tools (operators): psychological information operations (PIOs) as an operator of some kind of information ‘soft-power’ and cybernetic information operations (CIOs), as an operator of some kind of information ‘hard-power’. Both categories of IW operators use different methods and techniques to influence offensive and defensive information.

This requires increasing their information power, as the organization's ability to pursue its strategic goals by influencing the information space (infosphere). This also gives grounds for the separation and development of information geopolitics as a subdiscipline of geopolitics dealing with the study of the impact of the information space (infosphere) on the process of making strategic decisions (particularly political) by geopolitical actors creating the distribution of power and interests, as the main feature of the international system. In this sense, the factor of the the strategic culture of organization plays an important role.

REFERENCES

Aron, R. (2017). *Peace and War: A Theory of International Relations*. New York: Routledge.

Baram, G., Paikowsky, D., Pavel, T., Ben-Israel, I. (2018). *Trends in Government Cyber Security Activities in 2016.* „Social Science Research Network". DOI: 10.2139/ssrn. 3113106.

Barnett, M., Duvall, R. (2005). *Power in International Politics*. „*International Organization"*, 59(1).

Bebber, R. (2017). *Cyber Power and Cyber Effectiveness An Analytic Framework*. „*Comparitive Strategy"*, 5.

Betz, D.J., Stevens, T. (2011). *Cyberspace and the State. Towards a Strategy of Cyber-Power*. New York: Routledge.

Białoskórski, R. (2012). *Cyberthreats in the Security Environment of the 21st Century*. „*Journal of Security and Sustainability Issues"*, 2 [Access: 3.03.2023]. Access on the internet: http://jssidoi.org/jssi/volume-1-number-4-2012-june.

—— (2018). *The Geostrategic Position of the Russian Federation. A Powermetric Study*. Siedlce: Scientific Publishing House of the Siedlce University of Natural Sciences and Humanities.

—— (2020). *The Global Balance of Power After the Cold War. A Powermetric Approach.* „*Journal of Security And Sustainability Issues"*, 9(3).

—— (2021). *The Regional Security System after a Cold War – A Game of Power and Interests.* „*Przegląd Geopolityczny"* (eng. *„Geopolitical Review"*), 35.

—— (2022). *Wzrost znaczenia potęgi informacyjnej jako przyczynek do koncepcji geopolityki informacyjnej* [In:] Popławski, D., ed., *Studia nad potęgą państw* (eng. *Studies on the Power of States*). Warszawa: Scholar.

Bruszewski, M. (2023). *Prowokacja Putina w stylu gliwickiej radiostacji? „Ukraińska grupa sabotażowa przedarła się pod Briańsk".* „*Defence24"* [Access: 3.03.2023]. Access on the internet: https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/prowokacja-putina-w-stylu-gliwickiej-radiostacji-ukrainska-grupa-sabotazowa-przedarla-sie-pod-briansk.

Budzisz, M. (2021). *Wszystko jest wojną. Rosyjska kultura strategiczna*. Warszawa: Zona Zero.

Cho, S. (2020). *An Assessment Model for Defense Cybersecurity Capability.* „*Journal of Defense Acquisition and Technology"*, 2(2).

Cyber Power Index. Findings and Methodology. (2011). *Economist Intelligence Unit* [Access: 3.03.2023]. Access on the internet: http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf.

Domingo, F.C. (2016). *Explaining Great Power Competition in Cyberspace* [Access: 3.03.2023]. Access on the internet: https://www.academia.edu/12966842/Explaining_Great_Power_Competition_in_Cyberspace.

Dugin, A. (2014). *Geopolityczna przyszłość Rosji*. *Klub Jagielloński* [Access: 3.03.2023]. Access on the internet: https://klubjagiellonski.pl/2014/12/07/dugin-geopolityczna-przyszlosc-rosji/.

Gardner, B. (2018). *Social Engineering in Non-Linear Warfare.* „*Journal of Applied Digital Evidence"*, 1(1) [Access: 3.03.2023]. Access on the internet: https://mds.marshall.edu/cgi/viewcontent.cgi?article=1000&context=jade.

Garstka, J.J. (2003). *Network-Centric Warfare Offers Warfighting Advantage*. „Signal" [Access: 3.03.2023]. Access on the internet: https://www.afcea.org/signal-media/network-centric-warfare-offers-warfighting-advantage.

Giles, K., Sherr, J., House, C. (2018). *Russian Reflexive Control*. Kingston: Royal Military College of Canada [Access: 3.03.2023]. Access on the internet: https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control.

Global Cybersecurity Index 2020. *Measuring commitment to cybersecurity* (2020). The International Telecommunication Union (ITU) [Access: 3.03.2023]. Access on the internet: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Gomez, M.A. (no date). *Identifying Cyber Strategies vis-a-vis Cyber Power* [Access: 3.03.2023]. Access on the internet: http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power.

Gray, C.S. (2013). *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Strategic Studies Institute and U.S. Army War College Press [Access: 3.03.2023]. Access on the internet: https://ssi.armywarcollege.edu/2013/pubs/making-strategic-sense-of-cyber-power-why-the-sky-is-not-falling/.

Kaca, E. (2022). *Countering Russian Disinformation about Ukraine in the EU*. The Polish Institute of International Affairs, 145 [Access: 3.03.2023]. Access on the internet: https://www.pism.pl/publications/countering-russian-disinformation-about-ukraine-in-the-eu.

Караяни, А.Г. (2023). *Информационно-психологическое противоборство в современной войне* (*Information and psychological confrontation in modern warfare*) [Access: 10.10.2023]. Access on the internet: https://armyrus.ru/index.php?option=com_content&task=view&id=739.

Kelly, M., Heliskiing, A. (2014). *The OODA Loop (Observe, Orient, Decide, Act). Applying Military Strategy To High Risk Decision Making and Operational Learning Processes for On-Snow Practitioners. „International Snow Science Workshop, Banff"* [Access: 3.03.2023]. Access on the internet: https://arc.lib.montana.edu/snow-science/objects/ISSW14_paper_P3.45.pdf.

Klein, I. (1991). *A theory of strategic culture.* „*Comparative Strategy"*, 10(1).

Klimburg, A. (2011). *The Whole of Nation in Cyberpower.* „*The Georgetown Journal of International Affairs"* [Access: 3.03.2023]. Access on the internet: https://www.jstor.org/stable/43133826.

Knox, B.J. (2018). *The Effect of Cyberpower on Institutional Development in Norway.* „*Frontiers in Psychology"*, 9. DOI: 10.3389/fpsyg.2018.00717.

Komov, S. (1997). *About Methods and Forms of Conducting Information Warfare.* „*Military Though"*, 4.

Konończuk, W. (2023). *One year of war. Russia's imperial maximalism versus Ukraine's resistance. „Center for Eastern Studies"*, 495 [Access: 3.03.2023]. Access on the internet: https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2023-02-28/imperialny-maksymalizm-rosji-kontra-upor-ukrainy.

Kowalewski, A. (2017). *Disinformation and Reflexive Control The New Cold War. „Georgetown Security Studies Review"* [Access: 3.03.2023]. Access on the internet: https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/.

Kozłowski, A. (2014). *Cyberwojownicy Kremla. „Amicus Europea"*, 6 [Access: 3.03.2023]. Access on the internet: https://fae.pl/biuletynopiniefaecyberwojownicykremla.pdf.

Krizan, L. (1999). *Intelligence Essentials For Eveeyone, Joint Military Intelligence Collage. „Joint Military Intelligence Collage"* [Access: 3.03.2023]. Access on the internet: http://www.scip.org/files/Resources/Krizan-Intelligence-Essentials.pdf.

Kuehl, D. (1997). *Defining Information Power. „Strategic Forum”*, 115 [Access: 3.03.2023]. Access on the internet: https://universityofleeds.github.io/philtaylorpapers/vp01ee6b.html.

Kuehl, D.T. (2009). *From Cyberspace to Cyberpower: Defining the Problem* [In:] Kramer, D., Stuart, H., Wentz, L.K., eds., *Cyberpower and National Security Policy*. National Defense University, Potomac Books, Inc [Access: 3.03.2023]. Access on the internet: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf.

Kuleshov, Yu et al. (2014). 'Информационно-психологическое противоборство в современных условиях: теория и практика' (Information-Psychological Warfare In Modern Conditions: Theory And Practice), *Vestnik Akademii Voyennykh Nauk*, *1*.

Кулешов, Ю.Е., Жутдиев, Б.Б., Ничипорович О.С., Федоров, Д. А. (2014). *Теоретические аспекты информационно-психологического противоборства в современных условиях* (*Theoretical aspects of information-psychological warfare in modern conditions*), „*ВЕСЦІ НАЦЫЯНАЛЬНАЙ АКАДЭМІІ НАВУК БЕЛАРУСІ”,* 3 [Access: 20.10.2023]. Access on the internet: https://vestihum.belnauka.by/jour/article/view/39/40.

Langner, R. (2016). *Cyber Power – an Emerging Factor in National and International Security. „Horizon: Journal of International Relations and Sustainable Development”*, 8.

Lantis, J.S. (2002). *Strategic Culture and National Security Policy.* „*International Studies Review”*, 4(3).

—— (2005). *Strategic Culture: From Clausewitz to Constructivism. „Strategic Insights”,* IV(10) [Access: 3.03.2023]. Access on the internet: https://www.hsdl.org/?view&did=457637.

Lawson, S.T. (2014). *Nonlinear Science and Warfare. Chaos, complexity and the U.S. military in the information age*. New York: Routledge.

Lefebvre, V.A. (1987). *The Fundamental Structure of Human Reflexion. „Journal of Social and Biological Structures”*, 10. DOI: 10.1016/0140-1750(87)90004-2.

Legere, M.A. (2012). *Army Intelligence 2020: Enabling Decisive Operations. While Transforming in the Breach.* „*Army”* [Access: 3.03.2023]. Access on the internet: https://docslib.org/doc/3769146/army-intelligence-2020-enabling-decisive-operations-while-transforming-in-the-breach.

Luxmoore, M. (2022). *Ukraine's Secret Weapon Is Ordinary People Spying on Russian Forces. „Wall Street Journal”* [Access: 3.03.2023]. Access on the internet: https://www.wsj.com/articles/ukraines-secret-weapon-is-ordinary-people-spying-on-russian-forces-11671012147.

Maurer, T., Morgus, R. (2014). *Compilation of Existing Cybersecurity and Information Security Related Definitions. „New America”* [Access: 3.03.2023]. Access on the internet: https://www.giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf.

Mazur, M. (1996). *Cybernetyka i charakter* (eng. *Cybernetics and Character)*. Podkowa Leśna: Aula.

Moczulski, L. (1999). *Geopolityka. Potęga w czasie i przestrzeni* (eng. *The Geopolitics. Power in Time and Space*). Warszawa: Bellona.

Nye, J.S. (2010). *Cyber Power*. Harvard Kennedy School. Belfer Center for Science and International Affairs [Access: 3.03.2023]. Access on the internet: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

Olszyk, S. (2019). *Metody i techniki działań sieciocentrycznych. Wojna sieciocentryczna.* „*Bezpieczeństwo Międzynarodowe”*, 13(2). DOI: 10.34862/rbm.2019.2.10.

Ососков, Г.В. (2020). *Информационно-психологическое противоборство как важнейшая функция военно-политических органов по организации военно-политической пропаганды и агитации* (*Information And Psychological Warfare as the Most Important Function of Military-Political Propaganda And Agitation*). „*Гуманитарный вестник военной академии ракетных войск стратегического назначения",* 3 [Access: 10.10.2023]. Access on the internet: https://www.elibrary.ru/item.asp?id=44911055.

Rađenović, S. (no data). *Observe-Orient-Decide-Act (OODA) by John Boyd*, academia.edu [Access: 3.03.2023]. Access on the internet: https://www.academia.edu/8347535/Observe_Orient_Decide_Act_OODA_by_John_Boyd.

Reid, C. (1987). *Reflexive Control in Soviet Military Planning* [In:] Dailey, B., Parker, P., eds., *Soviet Strategic Deception*. Stanford: The Hoover Institution Press.

Russell, B. (1996). *Power: A New Social Analysis*. New York: Routledge.

Sigholm, J. (2013). *Non-State Actors in Cyberspace Operations. „Journal of Military Studies"*, 4(1). DOI: 10.1515/jms-2016-0184.

Signalists (2022). *WordSense Dictionary* [Access: 3 March 2023]. Access on the internet: https://www.wordsense.eu/signalists/.

Siverson, R.M., Starr, H. (1991). *The Diffuzion of War. A Study of Opportunity and Willingness.* Michigan: Michigan Publishing University of Michigan Press.

Słownik terminów i definicji NATO (AAP-6) (2014) [Access: 3.03.2023]. Access on the internet: https://wcnjik.wp.mil.pl/u/AAP6PL.pdf.

Snyder, J.L. (1977). *The Soviet Strategic Culture Implication for Nuclear Operations*. RAND [Access: 3.03.2023]. Access on the internet: https://www.rand.org/pubs/reports/R2154.html.

Soon-Chia, L. (2004). *Network centric warfare: A command and control perspective*. Monterey: Naval Postgraduate School [Access: 3.03.2023]. Access on the internet: https://core.ac.uk/download/pdf/36695391.pdf.

Stevens, T. (2010). *Reading Power in UK Cybersecurity* [Access: 3.03.2023]. Access on the internet: https://www.academia.edu/1157394/Reading_Power_in_UK_Cybersecurity.

Sułek, M. (2010). *Prognozowanie i symulacje międzynarodowe* (eng. *The International Forecasting and Simulations*). Warszawa: Scholar.

—— (2013). *Potęga państw. Modele i zastosowania* (eng. *Power of States. Models and Applications)*. Warszawa: Rambler.

—— (2020). *Measurement of national power – A powermetric model*. „*Przegląd Geopolityczny"* (eng. „*Geopolitical Review"*), 32.

Szopa, M. (2023). *TAK – system mapowy jak szwajcarski scyzoryk [ANALIZA]*, „*Defence24"* [Access: 3.03.2023]. Access on the internet: https://defence24.pl/technologie/tak-system-mapowy-jak-szwajcarski-scyzoryk-analiza.

Triqui, Y. (2015). *Is there such a thing as a cyberwar? Does the debate matter?* [Access: 3.03.2023]. Access on the internet: https://www.academia.edu/es/33578279/Is_there_such_a_thing_as_a_cyberwar_Does_the_debate_matter_.

Van Haaster, J. (2016). *Assessing Cyber Power.* 2016 8th International Conference on Cyber Conflict (CyCon). DOI: 10.1109/CYCON.2016.7529423.

Vice Admiral (Ret.) Arthur K. Cebrowski (2004). *Director, Office of Force Transformation, interview with Frank Swofford*', „*Defense AT&L"* [Access: 3.03.2023]. Access on the internet: https://www.dau.edu/library/defense-atl/DATLFiles/2004_03_04/ceb-ma04.pdf.

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., Schwarzenbach, A. (2020a). *Reconceptualizing Cyber Power. Cyber Power Index Primer.* „*Harvard Kennedy School*

[Access: 3.03.2023]. Access on the internet: https://www.belfercenter.org/sites/default/files/2020-04/ReconceptualizingCyber.pdf.

—— (2020b). *National Cyber Power Index 2020. Methodology and Analytical Considerations.* „*Belfer Center for Science and International Affairs"* [Access: 3.03.2023]. Access on the internet: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.

Warden III, J.A. (1995). *The Enemy as a System. „Airpower Journal"* [Access: 3.03.2023]. Access on the internet: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf.

Yuen, S. (2015). *Becoming a Cyber Power. China's cybersecurity upgrade and its consequences.* „*China Perspectives"*, 2. DOI: 10.4000/chinaperspectives.6731.

Zaman, R.U. (2009). *Strategic Culture: A „Cultural" Understanding of War. „Comparative Strategy"*, 28(1). DOI: 10.1080/01495930802679785.

Zimet, E. and Barry, C.L. (2009). *Military Service Cyber Overview* [In:] Wentz, L.K., Barry, C.L., Starr S.H., eds., *Military Perspectives Cyberpower 2009*. Washigton D.C.: Center for Technology and National Security Policy At The National Defense University [Access: 3.03.2023]. Access on the internet: https://apps.dtic.mil/sti/pdfs/ADA505424.pdf.

Ильницкий, А.М. (2021). *Ментальная война России*. „*Военная мысль"* [Access: 3.03.2023]. Access on the internet: https://vm.ric.mil.ru/Stati/item/336904/.