UDC 355.01:004(73:510:470)
DOI: https://doi.org/10.18485/iipe_ria.2022.73.1185.3
Biblid 0543-3657, 73 (2022)
Vol. LXXIII, No. 1185, pp. 51–71
Original article

CONCEPTS OF INFORMATION WARFARE (OPERATIONS) OF THE UNITED STATES OF AMERICA, CHINA AND RUSSIA

Dejan V. VULETIĆ[1]
Petar STANOJEVIĆ[2]

Abstract: The paper emphasises the importance of information and communication technologies (ICT) in modern society. In the introductory part of the paper, the authors describe different terms, such as "information environment", "information superiority", "information warfare" (IW), and "information operations" (IO). The authors analyse the concepts of IW of the United States of America (US), China, and Russia. The mentioned research subject is directly related to the objective of the paper, aimed at emphasising and explaining strategic documents, manuals, handbooks, and other documents, given in the second part of the paper. The result of the research is the identification of similarities and differences in perceptions and views about information warfare. The authors conclude that at the present moment, all three countries are aware of the importance of information and ICT, especially in the case of armed conflict. The information space is increasingly an area of conflict between the mentioned countries, both in peace and in war. It is estimated that their importance will grow in the future. The advantage and dominance that the US used to have are decreasing in relation to the competitors.

Keywords: information; superiority; operations; warfare; US; China; Russia.

[1] Research Fellow, The Strategic Research Institute, University of Defence in Belgrade, Belgrade. E-mail: dejan.vuletic@mod.gov.rs, https://orcid.org/0000-0001-9496-2259

This research was supported by the Science Fund of the Republic of Serbia, Grant No. 2803/2021, Management of New Security Risks-Research and Simulation Deveopment – NEWSIMR&D.

[2] Associate Professor, The Faculty of Security Studies, University of Belgrade, Belgrade. E-mail: petar.stanojevic@fb.bg.ac.rs, https://orcid.org/0000-0002-4964-9113

INTRODUCTION

The dominant process in the third technological revolution, characterised by the rapid development of science and technology, is the informatization of society. This period of development is often called the "information revolution". Society today has reached new levels of development, and the achieved level has led to the fact that the pursuit of interests is not primarily done by the use of armed force but by other means. Due to the technological progress of society, the physiognomy of armed conflicts has changed in the last few decades. The role of non-military content and its impact on the outcome of the conflict is growing (Kreveld 2010, 11; Vračar 2019, 449–450; Milenković i Vračar 2022, 159). Certain strategists and theorists, such as Gray (2007, 15–19), hold traditional views, arguing that the nature of war has not changed, but only its characteristics. Another group of theorists, advocates of modern thinking, such as Kreveld (2010, 49–55) and Kaldor (2005, 13–29), believe that existing knowledge about the nature of war is outdated. Despite some disagreement about the change in the nature of war, they agree that there was a change in his physiognomy because modern conflicts reflected the growing presence of unarmed content of war, which clearly made them different from previous (traditional, classical) conflicts (Vuletić i Vračar 2018, 142–143).

All conflicts are based on information. In the modern information age, information has become even more important. The expansion of information warfare began in the 20th century with the development of information and communication technologies. That development enabled achievements in weapons and accompanying equipment, which affected the way warfare changed. Information warfare involves taking action to achieve information superiority by attacking adversary information, information-based processes, and information systems while defending one's own information, information-based processes, and information systems (Schleher 1999, 3). Information warfare includes, among other things, striving to find out as much as possible about your opponent and preventing your opponent from knowing a lot about your forces (Arquilla and Ronfeldt 1995). This information enables the optimal functioning of the decision-making process by military commanders. The optimal decision implies the best choice from a set of several options to achieve the desired goal. In order to achieve that, a large amount of timely, relevant, current, and accurate information is necessary. Information can also be used in a negative context, to disorganise governance, organise protests by anti-government organisations, influence public opinion, and reduce an adversary's will to oppose.

The history of the conflict testifies to numerous examples that indicate the importance of information and the achievement of information superiority over an adversary (in relation to the opponent). Information superiority is the

operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (FM 3-0 2017). Control of information communicated to adversaries, for example, through deception and concealment, can create a reality misperception for an adversary. Information warfare uses information to influence an adversary's perception in order to subdue its will to fight, in place of physical force. The goal of subject "A" is to influence and force subject "B" to act in a way that is favourable to subject "A". The ultimate goal of each warring party is to induce an adversary to act in the desired manner: to surrender, make a mistake or fail, withdraw its forces, stop hostilities, etc. An attacker can use force or other available resources to achieve this goal. A defender may make a decision known to be in favour of subject "A" (e.g., admit defeat and surrender) or may become a victim of seduction or deception and unknowingly make decisions in favour of subject "A" (Sheen 2020, 1). Information superiority is the basis of the functioning of armies and is one of the key success factors in a possible conflict (Metz 2018, 21; Hammond-Errey 2019, 3).

Information superiority means dominance in the information environment over opponents. An information environment is a set of individuals, organisations, and systems that collect, process, or otherwise act on information. This environment consists of three interrelated dimensions (physical, informational, and cognitive). The physical dimension involves military forces, units, means, facilities, etc. The informational dimension is characterised by the flow of information (collection, processing, distribution, display) and serves to communicate and exchange information between all participants in operations. The cognitive dimension includes motivation, vulnerabilities, perception, education, understanding, beliefs, values of participants, etc (JP 3-13 2014; Alberts et al. 2001, 10; ATP 3-13.1 2018). The information environment is an environment that consists of different complex elements where the human factor is the most important and unavoidable part of that system. The information environment is a key component of the broader operational environment of the commander and has a huge impact on the decision-making process of the commander (DoD Strategy 2016, 3). The operational environment is a phrase that is most often used in military terminology and refers to a set of conditions in which, based on the commander's decisions, forces are used in the operation and which affect its outcome. The operational environment is a combination of conditions, circumstances, and influences that affect the engagement of capabilities and influence the decisions of the commander. Understanding the operational environment helps the commander to better identify the problem, predict potential outcomes, and better understand the various activities of the enemy and how these actions affect the achievement of a military state of emergency.

Some actions can be performed within an information environment, and they can have military or commercial goals. The critical infrastructure of one country can also be a goal. The military has traditionally attacked military targets with military weapons, but IW implies that all national sources are potential weapons. Therefore, they may be considered targets. Information superiority is the ultimate goal of information warfare or operations (Sheen 2020, 1).

IO provide units with support and the increased understanding of the situation with the aim of dominating the battlefield. An information operation is the joint engagement of Information Related Capabilities (IRCs)[3] during military operations, consistent with other operations that affect, disrupt, compromise, or impede the decision-making process of adversaries and their allies (JP 3-13 2014; IO 2014). The preparation of IO is complex and integrates numerous activities. It is the integration and synchronisation of information-related capabilities that enables the desired effects in the information environment at specific times and in specific locations. By carrying out information operations activities, it is possible to influence the will, morale, and perception of opponents' decision-makers (commanders of all levels, important personalities) and other participants in operations, information flows of opponents who distribute information and serve as support in the decision-making process as well as means of collecting and processing information in the enemy's command system (means of monitoring, surveillance, reconnaissance, and processing).

IW and IO are not synonims. IW is an information operation conducted during crises or conflicts. IW is carried out in times of crisis and IO at any time (JP 3-13 2014; Poisel 2013, 34). Information operations can be defined as activities that affect the content, flow, and other operations for the purpose of information superiority (Poisel 2013, 50). The term "information operation" has only been used in official US strategic documents in recent years. The IO force consists of units, staff, and individuals; military professionals, active and reserve; as well as civilians in the Ministry of Defense who perform or support the integration of action against the enemy and potential enemy (IO 2017).

[3] Information-Related Capabilities (IRCs) are all available means of the state that are used to create adequate conditions for the operation of combat units and other formations. (DoD Dictionary 2021, 104).

CONCEPTS OF IW OF THE WORLD'S LEADING POWERS AND OPERATIONALISATION THROUGH STRATEGIC DOCUMENTS

The concept of IW in the US

Accelerated, primarily technological development, requires new concepts, so the terminology has developed rapidly in recent years, from multidimensional battle through multidimensional operations to operations in all domains. A multi-domain operation basically explains how US forces will deter and defeat an adversary in a crisis situation or in the case of a conflict situation. This concept enables US forces to physically, virtually, and cognitively overcome their opponents, using combined weapons in all domains. US strategists estimate that, for the US military to maintain its superiority in capabilities over advanced technologies and enemy concepts, better integration of all forces must take place. According to expert estimates, the current system does not sufficiently integrate all domains, such as technological integration. Certain weaknesses were also noticed when it comes to the real-time command and control system (Vuletić et al. 2021, 4; TRADOC 2018).

The analysis of US strategic documents shows a change in the concept of how to act in the information space. In the earlier period, the emphasis was placed more on the defensive aspect, calculating that domination and demonstration of abilities in the information space would deter potential attackers. Such a concept did not prove to be effective in practice, and preventive, offensive action was taken against rivals in the information environment (Vuletić et al. 2021, 5).

The central idea is the rapid and continuous integration of all domains of warfare in order to deter the adversary and gain an advantage in armed conflict. The US Army in Multi-Domain Operations 2028 concept, developed by the Training and Doctrine Command (TRADOC) in 2018, proposes solutions to conflicts in various domains. The Air Force 2025 study was also the basis for new and creative thinking. The study covers topics such as information warfare, unmanned aerial combat platforms, organisations dealing with the situation between peace and war, and ways to most effectively degrade enemy unity and will (Metz 2018, 27).

According to their understanding, the new Concept will change the character of modern warfare. Every action of joint forces, every written or spoken word, displayed or transmitted image, has an informative character. The usual concept of working in an information environment assumes that the Joint Forces know how to handle information and various information activities in order to achieve information superiority. The Joint Forces use information power to achieve various goals, such as changing or maintaining perceptions, attitudes, and other elements that trigger desired adversary behaviours; protecting and securing the

perceptions, attitudes, decisions, and behaviours of their own forces; and also the collection, processing, distribution, and use of data to enhance combat power (JCOIE 2018).

The following are the key principles (according to the DoD Strategy 2016, 6):

1. IO is an important component at all stages of an operation or campaign, including the shaping of peacetime activities. Planning, integration activities, and coordination with other joint operations are crucial for success.
2. In some cases, joint operations in the information environment require close cooperation not only within the ministry but also within the US government (inter–agency process).
3. Although information activities can be carried out in peacetime and in conflict, some of them are limited by policies, doctrines, or operational plans that will require a high level of permission to carry them out. Procedures for managing information activities in an appropriate way through conflict levels have been established.
4. The Ministry of Defence seeks to deter attacks and defend the state from any adversary trying to harm them. To this end, the Ministry of Defence develops capabilities and capacities and seeks to integrate them into other aspects of the country's defence.
5. Ongoing intelligence support is needed to succeed. Due to dynamic and rapid changes, some old processes and tools may not be responsible enough, and new methods may be needed for reading, evaluating, managing, and controlling.
6. In order to provide EW at the current level, certain resources are allocated. In order to succeed, it is necessary to build capacity and increase efficiency, which can be achieved by informing about priorities or by resource compensation. In this context, the DoD provides unique approaches, capabilities, and capacities that are necessary for success.
7. The Ministry must coordinate and synchronise influence activities with information activities, primarily public affairs, which publish information that becomes immediately available to the general public, including opponents and potential opponents.

The US Army's publication "Information Operations" (JP 3-13 2014) provides a common doctrine for planning, preparing, executing, and evaluating specific types of operations, such as information operations. Handbook FM 3-13 is a basic document for the operationalization actions in the information space. The handbook contributes to better harmonisation of military doctrine with the joint doctrine while recognising uniform requirements for information operations to support ground forces. FM 3-13 clarifies the place and goal of information

operations in today's complex global security environment (technological capabilities, interpersonal skills, individual possibilities, etc.) (FM 3-13 2016). The purpose (goal) of the IO is to create desired effects that give commanders a decisive advantage over enemies and opponents. Commanders achieve this advantage by preserving and facilitating decision-making and the impact of decision-making while influencing, hindering, or degrading the decision-making of adversaries; obtaining more timely, relevant, accurate, and complete information from the enemies or opponents; or influencing the attitudes and behaviour of the relevant audience that have an impact on operations and decision-making (FM 3-13 2016).

Guidelines for the implementation of IO have been developed through ATP 3-13.1 "Conducting Information Operations". It is primarily intended for IO officers and planners or those who have been assigned responsibilities for fulfilling duties related to information operations. It also provides useful material for commanders, operational officers, intelligence officers, and other staff members who oversee, coordinate, or provide support in the IO's planning, preparation, execution, and evaluation. ATP Manual 3-13.1 states that the three levels of warfare (strategic, operational, and tactical) shape the relationship between national objectives and tactical actions. Command layout, unit size, equipment types and types, and the position of forces or components can often be related to a particular level: strategic, operational, or tactical. The purpose of their engagement depends on the nature of their task, mission, or goal (ATP 3-13. 1. 2018).

The concept of IW of the People's Republic of China

The Chinese concept of integrated strategic deterrence has an increasing emphasis on space and information and communication technologies. China's assessment is that military competition in the information space is intensifying and the struggle for dominance in the field of information is likely to prove decisive in future wars (DoD Strategy 2016, 2). China increasingly sees space and cyberspace as an important arena for both achieving domination and the spread of Chinese interests, but at the same time as a potential vulnerability (Chase and Chan 2016, 118). China's position, in line with its strategic goals, places more emphasis on control of its information space. Chinese authorities put priority on the issue of information security, and that concept emphasises the importance of controlling the narratives, information, and content distributed to their citizens. China stands for sovereignty in information (cyberspace), i.e., control of what is distributed to citizens through ICT (Raud 2016, 6–10).

China's real capabilities in IW and cyber warfare remain unknown. Gaining power and superiority in cyberspace has become an important issue in China. In

general, the level of military development is measured by the level of information warfare capabilities. China plans to build capacity, have trained personnel, and provide the forces and resources to win information wars before 2050 (Ventre 2010, 2). War is evolving in form towards information warfare, i.e., the form of war is accelerating its evolution to informationization. In order to achieve information dominance, China's armed forces will speed up weaponry and equipment upgrades and work to develop a weaponry and equipment system that can effectively respond to informationized warfare and help fulfil missions and tasks. China's armed forces will continue with the strategic project for personnel training that can meet the demands of informationized warfare (China's National Defense 2010; China's Military Strategy 2015; Bebber 2016, 45).

The Chinese concept related to information capabilities is aimed at positioning China as one of the world's leading powers in the information space. In addition, huge attention is paid to the control and management of the information domain at the national level by providing the so-called "digital sovereignty". They are aware of the risks associated with social networks and try to advise but also control citizens to use social media responsibly. A large amount of personal information relevant to competitors is stored on these platforms. Social networks can be a threat to national security and political stability, especially given that the creators of these networks come from certain countries marked as competitors (Ventre 2010, 3).

China has developed its own concept of IW, different from the concept of leading Western countries, which may have served only as the basis for their development. Chinese experts believe that the essence of the information ability is to break the will of the opponents, their attitudes and beliefs, which would affect the will and morale of the opponents to continue to fight. According to the Chinese concept, information warfare has an offensive and defensive aspect. Both aspects are important for the normal functioning of the state and the protection of its own interests. It will be especially important to ensure the functioning of critical information infrastructures, which will be the main targets of enemy attacks (Anand 2006, 782–786).

China is taking a number of steps to develop information warfare capabilities, including the development of computer network capabilities. China's cyber capabilities can help the People's Liberation Army (PLA) gather information for intelligence purposes or carry out a cyber attack. The PLA achieves dominance in the information space by relying on its computer networks and information systems, denying the opponent the opportunity to do the same. The PLA understands information warfare as an important means of reducing the impact of high-tech adversaries in the conflict with China. Information and communication tools could be used in conjunction with conventional and cyber attacks on enemy radars and other types of electronic equipment, reducing the

enemy's ability to use information to its advantage and allowing China to take the initiative. China is also investigating and deploying its forces and resources for information warfare beyond national borders (Chase and Chan 2016, 126; MSDIPRC 2015, 37–37).

PLA strategists understand the increase in competition between the great powers, which is intensifying due to their increasing dependence on computer networks for a wide range of military and economic functions. Measures are being taken and preparations are being made to achieve information superiority over their opponents in the war. According to PLA strategists, there is already a struggle in the information space for information and peace. Chinese strategists see the US and other countries with powerful military forces as a threat to China's national interests (Chase and Chan 2016, 122). The goal of the PLA is to build adequate forces and obtain an information war. In Nanjing, the PLA has developed more than 250 Trojans and similar tools. The Chinese Academy of Sciences, which has an advisory role in national information security policy and law, has established a state laboratory for information security. The laboratory launched the "National Attack Project" as one of its research programs. Also, certain professionals have been recruited into military organisations to strengthen their combat capabilities in future wars. China pays great attention to the offensive component in the information space, although it concentrates primarily on the defence aspect (Medeiros et al. 2004, 242; Anand 2006, 782–786). In July 2010, the PLA announced the establishment of an Information Protection Base. China's decision to create such a base was made soon after the United States formed the Cyber Command (Ball 2011, 81).

The PLA has spent more than a decade examining US military publications on network-oriented warfare and US information warfare doctrines. Prior to building their own capacities, the achievements of developed countries, primarily the US, were studied over a long period of time, as were experiences from the application of various forms of IR in conflicts in the late 20th and early 21st century. Concepts and strategic and other documents have been adopted in line with the country's specifics, size, vulnerability, national interests, tradition and degree of technological development. Great funds have been allocated for modernization and capacity building for the application of various forms of information warfare in the event of a conflict. Increasing emphasis is being placed on intelligence-reconnaissance and cyber warfare (Wortzel 2014, 1).

For the PLA, special attention is paid to the detection of information exchange devices, information channels, information processing, and decision-making systems. The goals are information superiority, disruption of enemy control of information and information capabilities, and maintenance of one's own information systems and capabilities. For decades, China's military culture

has emphasised the importance of people, not equipment, in warfare (Wortzel 2014, 1).

The PLA views cyber warfare as part of information warfare. These operations are designed to access, exploit, and possibly damage, through electronic means, the enemy's information systems and networks, computers, communication systems, and supporting infrastructure. Like other developed countries, China is highly dependent and relies heavily on computer networks. These operations are being prepared for a number of reasons, such as (Wortzel 2014, 16–17; Sheldon 2011, 36–51):

1. Strengthening China's political and economic power;
2. Complementing other forms of intelligence gathering and collecting economic, military, or technological information;
3. Reconnaissance, mapping, and collection of targeted data in foreign military, governmental, civilian infrastructure, or corporate networks for subsequent exploitation or attack;
4. Conducting exploitation or attacks using the information collected and
5. Improving the capacity and ability to perform, primarily, defence operations.

The concept of IW in the Russian Federation

According to Russia's strategic documents, IW is the main tool for achieving various strategic goals. In that sense, an information attack is realised to degrade or disable the functioning of information and communication systems of the enemy, but not necessarily for their destruction. In Russia's strategic documents, technological and psychological means of IW have been constantly evolving and are characterised by a high degree of integration. Russia has also developed a high level of warning about threats coming from the information space (Devai 2020, 34).

According to the Russian view, information warfare is seen as a conflict between two or more states in the information space with the aim of damaging information systems, processes and resources, critical and other structures, undermining the political and economic situation in a country, mass psychological manipulation, destabilisation of the state and society, and thus affects the decision-making process of the enemy (Porche III 2020, 25). Russia sees information superiority in the mass and widespread use of various devices, systems, and platforms that are necessary for a positive outcome in a potential conflict. Modern conflicts involve the use of the military but also non-military and non-violent measures that include various activities in the information space in order to achieve information superiority. Contemporary conflicts will be accompanied by increased activity on various social networks, blogs, forums, discussion groups, etc., which will have a great influence

on public opinion and attitudes towards the conflicting parties (Akimenko and Giles 2020, 68; Giles 2016, 6–7).

The National Security Strategy of the Russian Federation (Strategy RF 2015) explains that information security is a part of national security and that national security is provided by information means. The role and importance of the media as an unavoidable segment of modern conflict were emphasised. Critical information infrastructure is one of the objects of information threats. Certain updates and amendments to the Strategy were implemented in 2021, primarily in the field of threats in cyberspace and the development of forces and capabilities to act in that domain. In 2017, Defence Minister Sergei Shoigu announced the establishment of information-operations forces within the Russian armed forces. The training of military information-security specialists is mainly undertaken by Krasnodar Higher Military School (IISS 2022, 509).

According to the Military Doctrine of the Russian Federation (Doctrine RF 2014), military threats are present in the information space and their seriousness, role, and importance for the outcome of the conflict were emphasised. The role and importance of the media and social networks in forming attitudes and reactions to the use of military force by various international organisations, associations, and individual states were also considered. The Doctrine of Information Security of the Russian Federation, approved in December 2016, contains similar provisions as the National Security Strategy, which emphasises the growing threats to Russia. The information space is defined more broadly than in the previous version of the same doctrine from 2000. "Informatization" is a key term, which refers to the economic and technical processes for adoption and widespread use of ICT across the country and providing access to information resources. This change indicates an understanding of the growing importance of ICT and technological development and, most importantly, it considers this domain a tool for changing society. The greater need and importance of Internet governance, information security, and risk management in ICT systems are emphasised, as well as the necessity of relying on domestic ICT products and resources (Akimenko and Giles 2020, 69).

Maintaining continuous, uninterrupted, and well-prepared information operations is particularly emphasised. Special emphasis is placed on critical information infrastructure and imminent threats that may endanger their functioning during the war. The Doctrine also emphasises geopolitical interests, the importance and influence of intelligence, psychological, and other means by which to influence the situation in the country, as well as in different regions of the world (Doctrine RF 2016).

Through its strategic documents, Russia seeks to establish a comprehensive and coordinated approach to security and the successful pursuit of its interests.

This effort is conceived as a joint action of state institutions and non-governmental actors. In fact, the strategy, doctrine, and narratives promoted by the government suggest that Russia's national interests require the involvement of numerous and diverse social actors. While Russia is increasingly emphasising non-military means and activities, the process of military modernization is constantly being carried out. According to Russian General Valeri V. Gerasimov, the relationship between non-military and military measures in the modern security environment is 4:1 (Tachev et al. 2019, 133). He thinks that the key feature of warfare is the simultaneous effects on the entire depth of enemy territory, in all physical media and in the information domain (Giles 2016, 77).

IW, and thus cyber warfare, has become a legitimate means of peace and war. According to General Gerasimov, the line between war and peace is blurred in the 21st century, which is amplified by the fact that wars are no longer declared. In addition to that, IW and thus cyber warfare have become a legitimate means of peace and war. The experience of military conflicts, including the so-called "colour revolution" in North Africa and Ukraine, confirms that a perfectly successful state can enter the arena of fierce armed conflict, become a "victim" of foreign intervention, and fall into chaos, humanitarian catastrophe, and civil war in a matter of months or even days (Connell and Vogler 2017, 4). Russia's IW is uninterrupted and constant. While Western nations tend to differentiate between war and peace, in Russian thinking, states are constantly in the process of fighting for the protection of national interests, security, influence, and resources (Tachev et al. 2019, 141).

Russia's approach is characterised by the so-called non-linear approach to military strategy, which essentially implies that war and peace as they once were are disappearing, and that continuous warfare can become a regular form of relations between states. IW is at the core of this non-linear strategy. Methods and ways of acting are changing depending on the situation on the terrain. The conflict in Ukraine is proof of this, where information warfare techniques and tools have been actively tested on the ground (Molder and Sazonov 2018, 327). Chekinov and Bogdanov believe that the critical component of IW is the beginning of information activities in order to prepare the battlefield for action by other means. This perspective is in accordance with Gerasimov's observation that IW is largely the basis for victory (Chekinov and Bogdanov 2013, 12–23).

A characteristic of the Russian position on the issue of information flow is the intention to control information processes within state borders. Russia's defence includes protecting infrastructure and increasing digital sovereignty by improving preparedness and capabilities with various measures and solutions, such as isolating the Russian segment of the Internet (Kari 2019, 89–92). Russia stands for multilateral regulatory procedures for the use of ICT for various purposes, especially criminal and terrorist ones (Vuletić i Đorđević 2021, 240).

Russian officials are convinced that they are in a constant struggle with certain countries and organisations that want to endanger its security. Globalization, together with the free flow of information it creates, is both a threat and an opportunity. According to Russian strategic documents, there is no clear distinction between peacetime and wartime (Connell and Vogler 2017, 27–28). According to the Russian perspective, the number and seriousness of threats to Russia have increased, and those threats are being transferred to the internal sphere of Russia. Russia's national interests may be threatened on or through the Internet. Terrorists and extremists can carry out attacks on resources and infrastructure of strategic importance, disrupt the management and decision-making system, and paralyse Russia's strategic leadership. In addition, cybercriminals can threaten Russia's critical infrastructure in or through cyberspace by infiltrating state information systems (Doctrine RF 2016; Strategy RF 2015; Doctrine RF 2014).

SIMILARITIES AND DISTINCTIONS IN THE VIEWS OF THE US, CHINA AND RUSSIA REGARDING IW (IO)

There is still no consensus among the world's leading powers on many issues related to the use of ICT for military purposes, although there have been several initiatives within international organisations on this issue. Regarding the use of terms such as IW, Psychological Operations (PsyOps), Computer Network Operations (CNO), and others, there is a lot of confusion because there are many conflicting definitions, and these terms are used in different contexts to describe different goals and actions (Giles 2016, 6–7).

By analysing the strategic documents of the considered countries, it can be concluded that the importance of information and achieving information superiority is recognised in all three countries, especially in armed conflicts. Russia and China observe IW more broadly, in both peacetime and wartime, whereas the United States' perspective is narrower and only refers to wartime. Russia and China do not have official doctrines or other documents related to IW and IO known to the public. In contrast, the US has certain publications, manuals, handbooks, etc. (Heickero 2010, 23–24).

In the Chinese view, IO is a component of IW, as opposed to the American view. Russia's view is much closer to the understanding of the People's Republic of China, according to which IW is conducted in peace and war (less, more constantly) at several levels and dimensions (Heickero 2010, 23–24). According to the US view, IW are information operations conducted during crises or conflicts, while IO is conducted at any time. According to the US, IW involves the more limited use of forces and resources.

Russia's approach to understanding information operations differs in some elements from the US approach. Information has its value and must be protected in peace and war, as it is emphasised in Russian strategic documents. Information protection is of strategic importance and is a key factor for the functioning of the society, political stability, and opportunities for action and victory in potential conflict. Military doctrine indicates the role of the IW during the initial phase of the conflict, but also the conduct of an information campaign during the conflict and how important it is for the final outcome and victory (Heickero 2010, 23–24). From the standpoint of Russia, IW is focused predominantly on the cognitive layer of the opponent, while the US has given priority to the physical layer with similar or identical goals. Technological, psychological, and other means of information warfare are constantly evolving, and they are much more integrated into the activities of the armed forces of the Russian Federation (Devai 2020, 34).

The advantages in the capabilities that the US had in the past regarding IW are diminishing in relation to other leading world powers (DoD Strategy 2016, 2). According to the opinion of certain experts (Singer and Friedman 2014, 94; Cheung et al. 2015, 3; Yavuz 2019, 236) China lags behind the US and is not capable of carrying out a complex attack in cyberspace. Others believe that China has the capabilities and the will to surpass the West in military capability. However, no one is sure how far China's current strengths, long-term plans, technical solutions, and achievements in the field of ICT can reach. China is the country with the economic and military capacity to truly challenge the US and to disrupt the international system it presides over. The internet is an increasingly critical part of that system. Consequently, cyberspace will be an important battlefield that will primarily affect the final outcome of the conflict (SGI, 2018).

In recent years, China has shown great progress in improving its forces and resources, which has direct implications for the national security of the US. China's ability to wage an information war against the US in peace and war could pose a serious challenge to American strategists. China seeks to build capacity and reach such a level of development to become a leading player internationally in the field of IW, with a special focus on cyber warfare. China's intentions to endanger US infrastructure are obvious, as evidenced by many examples, as well as China's intention to become an active player in the arms race in the information space and its efforts to become the world's leading power in this field.

CONCLUSION

The mass use of ICT has enabled access to a huge amount of data and the connection of a large number of entities, both state and non-state. Modern society with the achieved technological progress compared to the previous one is characterised by various forms of communication, information exchange and

an increasing number of interoperable, interconnected, digital devices (DoD Strategy 2016, 4). In today's world, ICT is not just a privilege of developed countries. Certain countries, often with the involvement of non-state actors, try to endanger the resources of the opposite side (Proroković 2017, 402–403). In order to realise their activities, they use various techniques and tools.

Accelerated development and the increasing use of ICT on a large scale have hung the modern world. Changes in the information environment make information superiority a key factor in achieving success in a conflict. Contemporary conflicts are also strongly characterised as struggles in the information domain. Among the key factors in the international community, there is a commonality in understanding the importance of information, but there are some differences in terms of place and role, as well as the application of information operations.

Modern conflicts are accompanied by very intense information warfare. The greatest intensity is at the beginning of the armed conflict, but it is being waged continuously all the time. The various techniques, methods, and tools used in IW have a strong impact on the warring parties and enable the realisation of the information superiority of the dominant party in the conflict. The actions and goals of IW are planned long before the beginning of the armed conflict. Different forms of IW are escalating in scope, sophistication, and better coordination.

In the US, there is an obvious shift in the concept, with an increasing emphasis on offensive action in the information space. The current concept of action enables the better use of resources and the rational use of forces. The US approach differs from the views of other considered world powers on the issue of IW. It is considered primarily during the war.

The People's Republic of China's concept is very similar to the Russian one. It differs from the US, and it is probably based on a long-term study of the actions of other world and regional powers in the conflicts initiated and led by these countries. China has developed its own model, striving to improve capabilities and deter potential attackers. China, like Russia, is trying to achieve so-called digital sovereignty, i.e., control of its own information space. Both mentioned countries believe that the information war is being waged continuously, both in peace and war.

The analysis of strategic and other documents reveals all the complexity of IW (IO) as well as different approaches. IO are regarded today as an integral part of warfare. These terms, IW and IO, cover a number of aspects, including psychological, electronic, cyber, etc. What they have in common is that all three countries are investing more and more funds in information warfare, and that the latest technological achievements are being used for that purpose as well.

In recent years, there has been a considerable increase in the role and relevance of IO in relation to other types of operations (land, air, naval, and other sorts of operations). The emphasis in all three countries considered is on the defensive aspect of action and the protection of one's own interests. The principles of efficiency, timeliness, speed, and integration of all capacities are especially emphasised. Concepts and views have more similarities than differences. They share the employment of various forms of information warfare for geopolitical reasons and the realisation of national interests, among other things. However, the analysis of certain events shows that they are conceptually different from the real things. Many activities are carried out "under the cloak" of protection of human rights and democratic values.

Over the last few years, there has been a growing confrontation in the information environment and more and more mutual accusations between the US, on the one hand, and Russia or China, on the other hand, for acting due to interference in internal affairs and destabilization, such as presidential elections, territorial integrity, theft of intellectual property, etc. Many things related to information security are among the most closely guarded secrets, so it is difficult to say with certainty which of the considered world powers is dominant in the information space. There is no doubt that this aspect of warfare and various soft power mechanisms has an increasingly important role in achieving foreign policy goals (Stojanović i Đorđević 2017, 479; Kostić 2018, 407; Vuletić 2018, 274). In this constant rivalry, the achievements of potential opponents are analysed, special forces are formed, increasing funds are allocated, and strategies, doctrines, and other regulations are adopted, all with the goal of achieving information superiority over adversaries.

REFERENCES

Akimenko, Valeriy and Keir Giles. 2020. "Russia's Cyber and Information Warfare". *Asia Pacific* 27 (1): 67–75.

Alberts, David, John Garstka, Richard Hayes and David Signori. 2001. *Understanding Information Age Warfare*. Washington: CCRP.

Anand, Vinod. 2006. "Chinese Concepts and Capabilities of Information Warfare". *Strategic Analysis* 30 (4): 781–797.

Arquilla, John and David Ronfeldt. 1995. *Network war and cyberwar: A copy of the study publication in Comparative Strategy*. U.S.: RAND Corporation.

[ATP 3-13.1] Army Techniques Publication No. 3-13.1 The Conduct of Information Operations. 2018. https://irp.fas.org/doddir/army/atp3-13-1.pdf

Ball, Desmond. 2011. "China's cyber warfare capabilities". *Security Challenges* 7 (2): 81–103.

Bebber, Robert. 2016. "Information War and Rethinking Phase 0". *Journal of Information Warfare* 15 (2): 39–52.

Chase, Michael and Arthur Chan. 2016. "China's Evolving Strategic Deterrence Concepts and Capabilities". *The Washington Quarterly* 39 (1): 117–136.

Chekinov, Sergey and Sergey Bogdanov. 2013. "The Nature and Content of a New-Generation War". *Military Though* 4 (1): 12–23.

[China's Military Strategy] China's Military Strategy. 2015. The State Council Information Office of the People's Republic of China. http://eng.mod.gov.cn/publications/2021-06/23/content_4887928.htm

[China's National Defense] China's National Defense in 2010. 2010. Information Office of the State Council the People's Republic of China. http://eng.mod.gov.cn/publications/2021-06/23/content_4887922.htm

Connell, Michael and Sarah Vogler. 2017. *Russia's Approach to Cyber Warfare*. Washington: Center for Naval Analyses.

Devai, Dora. 2020. "An Overview of the Development of the Russian Information Warfare Concept Part 1". *Hadtudományi Szemle* 13 (1): 27–35.

[Doctrine RF] Voennaia doktrina Rossiiskoi Federatsii. 2014. *President of the Russian Federation*, No. 2976/2014. http://www.scrf.gov.ru/security/military/document129/

[Doctrine RF] Doctrine of Information Security of the Russian Federation. 2016. *President of the Russian Federation*, No. 646/2016. https://publicintelligence.net/ru-information-security-2016/

[DoD Strategy] Department of Defense Strategy for Operations in the Information Environment. 2016. https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

[DoD Dictionary] DoD Dictionary of Military and Associated Terms. 2021.https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

[FM 3-13] Field Manual No. 3-13 Information Operations. 2016. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf

[FM 3-0] Field Manual No. 3-0 Operations.2017. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6687_FM%203-0%20C1%20Inc%20FINAL%20WEB.pdf

Giles, Keir. 2016. *Handbook of Russian Information Warfare*. Rome: NATO Defense College.

Gray, Colin. 2007. *War, Peace, and International Relations: An Introduction to Strategic History*. Abingdon: Routledge.

Hammond-Errey, Miah. 2019. "Understanding and Assessing Information Influence and Foreign Interference". *Journal of Information Warfare* 18 (1): 1–22.

Heickero, Roland. 2010. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stocholm: Swedish Defence Research Agency.

[IO] Information Operations Air Force Policy Directive 10-7. 2014. https://irp.fas.org/doddir/usaf/afpd10-7.pdf

[IO] Information operations Directive number 3600.01. 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf

[IISS] International Institute for Strategic Studies. 2022. "The annual assessment of global military capabilities and defence economics". *Military Balance* 122 (1): 1–529.

[JP 3-13] Joint Publication 3-13 Information Operations. 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

[JCOIE] Joint Concept for Operating in the Information Environment. 2018. Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf

Kaldor, Meri. 2005. *Novi i stari ratovi – organizovano nasilje u globalizovanoj eri*. Beograd: Beogradski krug.

Kari, Martti. 2019. *Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats*. Doctoral Dissertation. Faculty of Information Technology University of Jyväskylä Finland.

Kostić, Marina. 2018. "Čija hegemonija? - Svet u uslovima takmičenja za novu globalnu vladavinu". *Međunarodni problemi* 70 (4): 391–411.

Kreveld, Martin. 2010. *Transformacija rata*. Beograd: Službeni glasnik i Fakultet bezbednosti.

Lindsay Jon, Cheung, Tai Ming and Derek Reveron. 2015. *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. New York: Oxford University Press.

Medeiros, Evan, Roger Cliff, Keith Crane and James Mulvenon. 2005. *A New Direction for China's Defense Industry*. Santa Monica: RAND Corporation.

Metz, Steven. 2018. *Armed conflict in the 21st century the information revolution and post-modern warfare*. New York: Nova Science Publishers, Inc.

[MSDIPRC] Military and Security Developments Involving the People's Republic of China. 2015. *Annual Report to Congress*. Washington, D.C.: Office of the Secretary of Defense.

Molder, Holger and Vladimir Sazonov. 2018. "Information Warfare as the Hobbesian Concept of Modern Times - The Principles, Techniques, and Tools of Russian Information Operations in the Donbass". *The Journal of Slavic Military Studies* 31 (3): 308–328.

Milenković, Miloš i Milinko Vračar. 2022. "Politička korisnost vojne moći u savremenim međunarodnim odnosima". *Politička revija* 72 (1): 157–175.

Poisel, Richard. 2013. *Information Warfare and Electronic Warfare Systems*. Boston & London: Artech House.

Porche III, Isaac R. 2020. *Cyberwarfare an Introduction to Information-Age Conflict*. Boston & London: Artech House.

Proroković, Dušan. 2017. "Geopolitičke determinante spoljnopolitičkog pozicioniranja Srbije na početku 21. veka". *Međunarodni problemi* 69 (4): 401–422.

Raud, Mikk. 2016. *China and Cyber: Attitudes, Strategies, Organisation*. Tallin: Cooperative Cyber Defence Centre of Excellence.

Schleher, Curtis. 1999. *Electronic Warfare in the information age*. Massachusetts: Artech House.

[SGI] Stratfor Global Intelligence. 2018. The Uncertain Future of Warfare. https://worldview.stratfor.com/article/uncertain-future-warfare

Sheldon, Robert. 2011. "China's Great Firewall and Situational Awareness". *Strategic Insights* 10 (1): 36–51.

Sheen, Ariel. 2020. "Notes from Information Revolution Principles and Operations", *Digital Portfolio, Academic Journal and Creative Writings,* May 12. https://arielsheen.com/index.php/2020/05/12/notes-from-information-warfare-principles-and-operations/

Singer, Peter, Waren, and Allan Friedman. 2014. *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press.

Stojanović, Stanislav i Branislav Đorđević. 2017. "Svetsko društvo rizika i zaštita nacionalnih interesa Republike Srbije". *Međunarodni problemi* 69 (4): 465–482.

[Strategy RF] O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii. 2015. *President of the Russian Federation*, No. 683/2015. http://pravo.gov.ru/proxy/ips/?docbody=&nd=102385609

Tachev, Blagovest, Michael Purcell and Brian McLaughlin. 2019. "Russia's Information Warfare Exploring the Cognitive Dimension". *MCU Journal* 10 (2): 129–147.

[TRADOC] Training and DoctrineCommand. 2018. The U.S. Army in Multi-Domain Operations 2028. https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

Ventre, Daniel. 2010. "Chinese Information and Cyber Warfare", *E-International Relations*, Aprli 13. https://www.e-ir.info/pdf/3845

Vračar, Milinko. 2019. "Fizionomija rata u postmoderni: Studija slučaja sirijskog oružanog sukoba". *Međunarodni problemi* 71 (4): 447–474.

Vuletić, Dejan, Miloš Milenković i Anđelija Đukić. 2021. "Sajber prostor kao područje sukobljavanja: Slučaj SAD – Iran i Severna Koreja". *Vojno delo* 73 (1): 1–14.

Vuletić, Dejan. 2018. "Psihološka dimenzija hibridnog ratovanja". *Vojno delo* 70 (6): 274–281.

Vuletić, Dejan i Branislav Đorđević. 2021. "Problemi i izazovi upravljanja internetom na međunarodnom nivou". *Međunarodni problemi* 73 (2): 235–258.

Vuletić, Dejan i Milinko Vračar. 2018. "Promena fizionomije savremenih sukoba". In: *Upotreba sile u međunarodnim odnosima*, edited by Ž. Novičić, 137–153. Beograd: Institut za međunarodnu politiku i privredu.

Wortzel, Larry. 2014. *The Chinese People's Liberation Army and information warfare*. Pennsylvania: Strategic Studies Institute.

Yavuz, Akdag. 2018. "The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective". *Journal of Chinese Political Science* 24 (2): 225–247.

КОНЦЕПТИ ИНФОРМАЦИОНОГ РАТОВАЊА (ОПЕРАЦИЈА) СЈЕДИЊЕНИХ АМЕРИЧКИХ ДРЖАВА, КИНЕ И РУСИЈЕ

Апстракт: У раду се истиче значај информационо-комуникационих технологија (ИКТ) у савременом друштву. У уводном делу рада аутори описују различите појмове као што су "информационо окружење", "информациона супериорност", "информационо ратовање" (ИР) и "информационе операције" (ИО). Аутори анализирају концепте ИР Сједињених Америчких Држава (САД), Кине и Русије. Наведени предмет истраживања је у директној вези са циљем рада, који је усмерен на истицање и објашњење стратешких докумената, упутстава, приручника и других докумената, датих у другом делу рада. Резултат истраживања је идентификација сличности и разлика у перцепцијама и ставовима о информационом ратовању. Аутори закључују да су у овом тренутку све три земље свесне значаја информација и ИКТ, посебно у случају оружаног сукоба. Информациони простор је све више подручје сукоба наведених држава, како у миру тако и у рату. Процењује се да ће њихов значај у будућности расти. Предност и доминација коју су САД имале се смањују у односу на конкуренте.

Кључне речи: информације; супериорност; операције; ратовање; САД; Кина; Русија.

Received: 21 April 2022
Accepted: 08 June 2022