DOCTRINAL INTEROPERABILITY IN THE NORTH ATLANTIC ALLIANCE IN RELATION TO RUSSIAN AND CHINESE APPROACH TO INFORMATION OPERATIONS

Lieutenant Assist. Prof. Cosmina-Andreea NECULCEA

"Henri Coandă" Air Force Academy, Brașov

Major General (r.) Prof. Florian RĂPAN, PhD

"Dimitrie Cantemir" Christian University, Bucharest

DOI: 10.55535/RMT.2023.1.4

Interoperability is described as the ability of member states to act together coherently and effectively to achieve tactical, operational and strategic objectives. In particular, interoperability allows forces, units and/or systems to operate together and use shared concepts. At the operational and tactical level, there are numerous challenges regarding interoperability, and one of these challenges consists of doctrinal differences. The purpose of this article is to identify these differences, through the brief analysis of the doctrine projections of NATO, USA and Romania. There are significant differences both in understanding the concept of information operations from a conceptual and practical point of view and in terms of these subsumed operations. Also, in order to identify one's vulnerabilities, we think that the analysis of strategies and tactics based only on a Western empirical approach is insufficient, and we aim at comparing the effectiveness of information operations from the Russian and Chinese perspectives, as well.

Keywords: information operations (InfoOps); comparative doctrine analysis; doctrine interoperability; differences; NATO; Russia;

INTRODUCTION

At the level of the North Atlantic Alliance and its member states, information operations/InfoOps[1] have known increasing attention, as a result of the people's awareness that the environment in which they live is dominated by information. The information environment, with its three dimensions, cognitive, physical and virtual, has altered the nature of war and has become a global battlefield, where conflicts seem to have no identifiable boundaries. Conducted at all operational levels and throughout all phases of a conflict, InfoOps integrate all aspects of information, supporting and enhancing elements of the combat power.

The information environment, with its three dimensions, cognitive, physical and virtual, has altered the nature of war and has become a global battlefield, where conflicts seem to have no identifiable boundaries. Conducted at all operational levels and throughout all phases of a conflict, InfoOps integrate all aspects of information, supporting and enhancing elements of the combat power.

Furthermore, there is increasing overlapping between the field of military actions and the field of civil actions and vice versa and the speed with which information is transmitted may represent both an advantage and vulnerability. Following the same rationale, we may assert that InfoOps are not as costly as classic operations and they represent an advantage in relation to saving human lives. The matter of interoperability has been perceived as being as old as the military operations, whereas joint operations are an essential condition for operational efficiency. This challenge is also underlined by the famous quote of General and theoretician Ferdinand Foch, assigned to take command of the allied coalition against Germany in 1918, who "*is supposed to have remarked that after directing a coalition, he lost some of his admiration for Napoleon*" (Neiberg, 2010, p. 699).

The procedural dimension of interoperability focuses on doctrines and procedures and involves the standardisation of capabilities, including the level of communication and terminology, or with regard to tactics, techniques and procedures. At first glance, the terminology, resources, tactics, techniques and procedures of states and units vary. Therefore, the lack of standardisation will affect interoperability, including combat power. In the same vein, we could say that, at the operation and tactical level, doctrinal differences represent a real challenge.

[1] For the coherence and conceptual unity of the current article, we will use the abbreviation InfoOps, as it appears within the Romanian doctrines.

In our analytical approach, we aim, in the first phase, to identify differences in the InfoOps sphere, through the comparative analysis of specific doctrinal projections at the level of NATO, USA and Romania. The parallel analysis of InfoOps doctrines reveals numerous differences both in relation to the understanding of the concept and in terms of coordination and harmonization of subordinate capabilities.

In the second phase, we have considered it challenging but also necessary to scan how Russia and China approach InfoOps. Both Russia and China see influence activities, including disinformation, as common activities that they carry out domestically to control people's minds, through manipulation and censorship. However, there are many differences between the two approaches. One of these differences could be reinforced by the metaphor used by the director of cyber-security of the American National Security Agency, Rob Joyce, who stated: "*I kind of look at Russia as the hurricane. It comes in fast and hard. China, on the other hand, is climate change: long, slow, pervasive*." (Vilmer, Charon, 2020). In this context, we can say that the Chinese state takes a much more moderate approach to information dissemination or offensive cyber tactics. While Russia is one of the most active adversaries, at least against the US, in the information environment and cyberspace, China appears to be taking a much more centralised, controlled, and enduring view of InfoOps. That is why Russia's visibly disruptive actions are associated with a *hurricane*, and China's slow and pervasive actions are compared to *climate change*. At the same time, the interactions between China and Russia in recent years could raise some problems, including in relation to the InfoOps approach, because both countries have dramatically expanded their disinformation actions in the last year.

Both Russia and China see influence activities, including disinformation, as common activities that they carry out domestically to control people's minds, through manipulation and censorship. However, there are many differences between the two approaches.

COMPARATIVE ANALYSIS OF INFOOPS DOCTRINES IN RELATION TO NATO, USA AND ROMANIA

In order to identify the doctrinal differences at the Alliance level, we have focused our attention both on the InfoOps doctrines at the level of NATO, USA and Romania (NATO – Allied Joint Doctrine for Information Operations/AJP-3.10/2015; USA – Information Operations/ JP 3-13/2014; Romania – Doctrina Operațiilor Informaționale/ nformation Operations Doctrine/2017), as well as on the doctrines of subordinate operations. Access to the entire documentation was straightforward for the reason that both the NATO and the US doctrines are available on the internet, whereas the Romanian doctrines can be accessed in their printed format.

The first difference derives from the definitions attributed to InfoOps, in the three doctrinal projections. At the Alliance level, InfoOps are defined as "*a staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives*" (AJP-3.10, 2015, p. 1-5), definition which is completed by another expression, in respect of information activities which represent "*actions designed to affect information or information systems. Information activities can be performed by any actor and include protection measures*". (AJP-3.10, 2015, p. 1-5). At the national level, the equivalent of the AJP-3.10/2015 doctrine is the Information Operations Doctrine of 2017, with some small variation. The definition of InfoOps in the Romanian conceptual framework is similar to that of the allied doctrine, emphasising at the same time the offensive aspect or the impact of information on the information systems of the enemy, as well as the defensive aspect, namely, the protection of own resources and systems.

USA has a slightly different approach to InfoOps, characterising them as "*the integrated employment, during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own*" (JP 3-13, 2014, p. ix). IRC or information capabilities are "*the tools, techniques, or activities that affect any of the three dimensions of the information environment.*" (JP 3-13, 2014, p. x). The doctrine emphasises the integration of IRC during the joint operations planning process and describes these capabilities as tools available to the commander to affect the cognitive, physical and virtual dimensions of the information environment.

Another difference between the three doctrine projections is related to the establishment of the principles of information operations. For example, the American doctrine for information operations does not provide a description or enumeration of InfoOps principles, as we find it in the other two doctrine projections under scrutiny. On the other side, in the previous doctrine *JP 3-13/ Information Operations* of 2006, under the heading **Planning and Coordination**, the following clarification appears: "*The planning of Information Operations follows the same principles and processes established for the planning of joint operations*" (JP 3-13, 2006, p. xiii). In other words, InfoOps planning must aim to coordinate and synchronse capabilities to meet the Joint Force Commander's objectives. Also, InfoOps must be an integral part of the overall planning effort and their use ever since the early

At the Alliance level, InfoOps are defined as "a staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives".

phases of operations planning can influence the effort required for the following phases.

Regarding the principles of Joint Operations, at the level of the US, the turning point in relation to the establishment of principles is represented by the terrorist attacks of September 11, 2001. At that time, the *warfare principles*, as they were called in the doctrines of those times, and which had a broad strategic utility, were renamed the *Principles of Joint Operations*, which implied a much narrower purpose. Secondly, the experiences in Iraq and Afghanistan, adjoining the challenges of those irregular wars, led to the addition of three new principles: *restraint, perseverance and legitimacy*.

The US Joint Doctrine lists 12 principles of Joint Operations, which are applicable to InfoOps as well: o*bjective, offensive mass, manoeuvre, economy of force, unity of command, security, surprise, simplicity, restraint, perseverance, legitimacy.* (JP 3-0, 2017, p. ix). These principles are applicable to both traditional and irregular forms of warfare.

The US Joint Doctrine lists 12 principles of Joint Operations, which are applicable to InfoOps as well: objective, offensive mass, manoeuvre, economy of force, unity of command, security, surprise, simplicity, restraint, perseverance, legitimacy.

At the national level, the *Information Operations Doctrine* lists a number of 10 specific InfoOps principles, the first nine being taken from AJP-3.10 of 2009 and the set was completed with the tenth principle, *adaptability*. On the other hand, the current NATO doctrine, AJP 3.10/2015 differs from the previous doctrine by a new set of principles, some taken from the old one, others different *(focused and integrated, coherent and consistent, comprehensive understanding, centralized planning and decentralized execution, continuous, Monitoring and assessment, agility)* (AJP-3.10, 2015, p. 1-9).

The third difference concerns key areas. The indigenous doctrine projects 12 capabilities subordinated to InfoOps, which it calls *key domains* coordinated within InfoOps. These are Psychological Operations (PSYOPS), Presence, Profile and Posture (PPP), Operations Security (OPSEC), Information Security (INFOSEC), Military Deception (MILDEC), Electronic Warfare (EW), Physical Destruction, Key Leader Engagement (KLE), Military Engagement, Cyberspace Operations, Cyber Defense and Civil-Military Cooperation (CIMIC) and can be considered *"InfoOps activities only when they are directly aimed at the understanding and perception, will and capabilities or means of the adversary, the potential opponent or other approved entities"* (DOI, 2017, p. 22).

The NATO Doctrine, AJP-3.10/2015, includes the operations subsumed to InfoOps, in a distinct category, entitled *Capabilities and*

Techniques Integrated Through Information Operations. Although the list is not exhaustive, the capabilities and techniques listed represent the basis of most InfoOps activities. Furthermore, the current doctrine completed the list of *Capabilities, Tools and Techniques Used in Support of Information Operations Objectives* from the previous doctrine with three other capabilities such as *Special Capabilities, Military Public Affairs and Cultural Understanding and Engagement and Excluded Information Security/INFOSEC* (AJP-3.10, 2015, 1-10).

In the USA, the information operations doctrine of 2014, JP 3-13, lists a broader set of *capabilities that contribute to InfoOps*, which it places under the title of *Relationship and Integration, as follows: Strategic Communication, Joint Interagency Coordination Group, Public Affairs, Civil-Military Operations, Cyberspace Operations, Information Assurance, Space Operations, Military Information Support Operations/ MISO (in previous editions of the doctrines), Psychological Operations, Intelligence, Military Deception, Operations Security, Special Technical Operations, Joint Electromagnetic Spectrum Operations, Key Leader Engagement* (JP 3-13, 2014, II-5).

In the USA, the information operations doctrine, lists a broader set of capabilities that contribute to InfoOps, which it places under the title of Relationship and Integration, as follows: Strategic Communication, Joint Interagency Coordination Group, Public Affairs, Civil-Military Operations, Cyberspace Operations, Information Assurance, Space Operations, Military Information Support Operations/ MISO, Psychological Operations, Intelligence, Military Deception, Operations Security.

The differences listed above reinforce the idea that InfoOps remain a complex topic occurring in a field under continuous evolution, the information field. Therefore, there is a need for better insight and clarity in defining InfoOps, because the absence of a clear definition of InfoOps can lead to strategic failure. At the same time, the complex and evolving nature of InfoOps reveals more than ever the need to develop a clear and concise understanding of this concept. In turn, the InfoOps principles represent one of the durable components of the doctrine, because they represent the basis of the conduct of military operations. The fact that the principles of InfoOps in the three analysed doctrinal projections differ or are even missing can also be regarded as a simple conceptual gap. We may assert that there is a practical need to achieve coherence between the NATO doctrines for Information Operations and those of the allied states. At least at the operational and tactical level, interoperability depends on these doctrinal differences. Therefore, the higher the degree of doctrinal correspondence between the NATO, US and Romanian doctrines, the more interoperability can be achieved without irregularity. Otherwise, the complexity of InfoOps will increase, becoming more and more sensitive, leading to increased confusion rather than clarification of the nature of InfoOps, which is constantly changing.

APPROACHING INFOOPS FROM THE RUSSIAN PERSPECTIVE

Compared to the Western states, the Russians approach InfoOps in a different manner. The Russian military thinking is influenced by culture, politics, economy, technological advancement, as well as military experience. Similarly, the attitude of Russians towards InfoOps is strongly affected by the lower technological class and they perceive the use of InfoOps by foreigners as a threat to the political and cultural vulnerabilities of their society.

Regarding the InfoOps approach, one of the aspects identified is in relation to the availability of doctrines. Both the Russians and the Chinese do not publish the doctrines as the NATO or other member states do and even public writings can be inconsistent with actual practice, intentionally or unintentionally confusing.

Regarding the InfoOps approach, one of the aspects identified is in relation to the availability of doctrines. Both the Russians and the Chinese do not publish the doctrines as the NATO or other member states do and even public writings can be inconsistent with actual practice, intentionally or unintentionally confusing.

The characteristics of modern warfare have led the Russian military to revise its own conceptualisation of warfare, and InfoOps appear to be essential. Just as information superiority over the adversary is critical and essential to war time, so can InfoOps serve as a cohesive and vital agent.

In the Russian perception, NATO and the US represent an increasingly pronounced threat, including in the sphere of Russian influence. According to the Military Doctrine of the Russian Federation, NATO represents the main external military risk *["build-up of the power potential of the North Atlantic Treaty Organization (NATO) and vesting NATO with global functions carried out in violation of the rules of international law, bringing the military infrastructure of NATO member countries near the borders of the Russian Federation, including by further expansion of the alliance"]* (Military Doctrine of the Russian Federation, 2014).

In recent years, Russia and China have developed closer relations, by expanding trade and defence relations, up to the point of perceiving themselves as strategic partners. This partnership was described by the presidents of the two states as one with *no limits*[2], with an emphasis on cooperation, including in the field of defence or collaboration in the outer space. On the other side, the so-called *closeness* could be intensified precisely by their common rivalry with the US, more than any other natural affinity. In turn, the two states are considered by the US as *great power rivals* (Fact Sheet – US National Defense Strategy, 2022).

[2] *"Friendship between the two states has no limits, there are no ‹forbidden› areas of cooperation".* (Munroe, Ozborn, Pamuk, 2022).

Since 2003, Russia and China have carried out joint military exercises aimed at increasing interoperability and mutual trust between their armed forces, but their partnership can also be considered a message addressed to NATO, the US or other European states. A recent example, after the outbreak of the Ukraine War, is the Russian-Chinese military exercise carried out over the Sea of Japan, with Russian Tu-95 strategic bombers and Chinese Xian H-6 aircraft (Digi24.ro, 2022), in the context in which the American President, Joe Biden, was visiting Tokyo.

Since 2003, Russia and China have carried out joint military exercises aimed at increasing interoperability and mutual trust between their armed forces, but their partnership can also be considered a message addressed to NATO, the US or other European states. A recent example, after the outbreak of the Ukraine War, is the Russian-Chinese military exercise carried out over the Sea of Japan, with Russian Tu-95 strategic bombers and Chinese Xian H-6 aircraft, in the context in which the American President, Joe Biden, was visiting Tokyo.

The outbreak of the war in Ukraine can be considered a turning point that put China in an uncomfortable position and which could influence the durability and stability of the relationship between the two states. However, China has never condemned Russia's actions in Ukraine, blaming NATO and the US for challenging Russia (Business-Standard.com, 2022).

Compared to the Western approach, which is conditioned by legal and political constraints and assumes the distinction between peace and war, the Russian approach seeks to capitalise on all the instruments of national power, in a continuous confrontation, in which the whole society is involved: *"In fact, the body of strategies, doctrines, and government-promoted narratives suggests that the successful promotion of Russia's national interests requires the involvement of the entire society"* (Tashev, Purcell, McLaughlin, 2019, p. 133). Also, regarding the nature of the confrontation, Russia seems to have reached a consensus, describing the relations between the states as *"inherently and constantly competitive"* (Tashev, Purcell, McLaughlin, 2019, p. 135).

The Russians see InfoOps as a dynamic process, which makes the approach evolve and adapt. Also, when one approach appears to be failing, the Russians seek to adopt a new one, and when one approach is successful, they reinforce it. Another characteristic of the Russian approach is that Russians take the *cognitive dimension* very seriously, which they constantly seek to control by familiarising themselves with the history, ideology, culture, experiences or influences that affect the decision-making of the target group.

The term preferred by Russians to describe Russia's actions in the informational sphere is that of *information confrontation*, and the use of the term *information operations* in the Russian literature constitutes a point of reference in relation to the doctrines of NATO or the member states. Moreover, in their theory and practice, the Russians even borrowed certain Western terms that they adapted to traditional activities (Darczewska, 2015, p. 38).

The InfoOps approach from the Russian perspective differs from the Western one through different cultural and cognitive practices. This underlines the increasing importance given to non-military measures. The role of non-military means was even quantified by General Gerasimov through a ratio of 4 to 1, a ratio that practically highlights the magnitude of non-military measures in the conflict.

APPROACHING INFOOPS FROM THE CHINESE PERSPECTIVE

China's Army or the People's Liberation Army (PLA) is the largest army in the world and is under the leadership of the Chinese Communist Party. At the moment, China is engaged in a series of territorial disputes, whereas the US, for example, has stable and undisputed borders.

China's latest strategies refer to a local war, different from the total war, having limited goals and taking place in a certain area where China's sovereignty is endangered, such as disputes in the South China Sea, Taiwan, Nepal or the border with India. Also, with the passage of time, China has moved towards several variants of local war, the most recent being the Informationised Local War.

China's latest strategies refer to a local war, different from the total war, having limited goals and taking place in a certain area where China's sovereignty is endangered, such as disputes in the South China Sea, Taiwan, Nepal or the border with India. Also, with the passage of time, China has moved towards several variants of local war, the most recent being the *Informationised Local War*.

Relative to the USA, which seeks to build alliances, reaching a number of 35 allies, China has only one formal ally, North Korea, alliance established following the signing of the *Treaty of Friendship, Cooperation and Mutual Assistance*, in the year of 1961. Japan is also considered a threat to China, due to its military alliance with the U.S.A., but also taking into account the historical aggression against China. Currently, the territorial dispute over the Senkaku/Diaoyu islands in the East China Sea, in which the US is also involved, based on the *Treaty of Mutual Cooperation and Security between Japan and the United States*, further increases the tensions between China and the USA.

With the proliferation of computers and telecommunications technology, information has become an essential part of national security considerations, a process called *informationisation* (Cheng, 2017, p. 1). At the same time, the PLA must improve its ability to conduct joint operations, in which information warfare is an essential part. Information, as emphasised by the doctrine in force, enjoys a central position, being considered both a field of confrontation and a condition or a means to win the war.

As part of the PLA modernisation process, a concept with a relatively clumsy description appears in Chinese strategic documents: *Non-war*

Military Activities/NWMA[3]. Through this concept, China seeks to adopt a favourable posture, able to face the challenges brought by economic growth or global expansion.

From the point of view of the evolution of Chinese strategies, we can see that the strategies of the last decades refer to *active defence*, a strategy that China describes as *essentially defensive but operationally offensive* (China Military Power Report, 2019, p. 15), the PLA being prepared to carry out offensive actions at all three levels – tactical, operational and strategic –, according to the principle *"We will not attack unless we are attacked, but we will surely counterattack if attacked".* (Blasko, 2017).

China's idea of winning the informationised war, as it appears in the current doctrine, suggests that the Chinese posture is not only limited to the conventional sphere but also extends to non-conventional areas. In this sense, Chinese literature particularly emphasizes the role of the *Three Warfare Strategy*, emblematic of the Chinese political warfare strategy, which includes *Public Opinion Warfare, Psychological Warfare, and Legal Warfare*. The use of *Three Warfare Strategy* implies *"a perceptual preparation of the battlefield that is seen as critical to advancing its interests during both peace and war"*. (Kania, 2016)

Psychological warfare from the Chinese perspective involves actions of propaganda, military deception, threat or even restraint, with the aim of affecting the adversary's ability to make decisions. The second type of warfare, that of the public opinion, is the dissemination of information for public consumption with the aim of influencing and directing public opinion and gaining support from domestic or international audiences. By using national and international laws, all under the dome of legal warfare, the aim is to gain international support as well as influence the target audience.

China's military strategy, characterised as one of active defence, has its origins in the idea that armed conflicts should not be initiated, but if the adversary challenges its sovereignty, unity or national interests, China will respond firmly. In other words, China will never lead an invasion or expansion, but also will never allow any piece of Chinese territory to be separated from China.

China's military strategy, characterised as one of *active defence*, has its origins in the idea that armed conflicts should not be initiated, but if the adversary challenges its sovereignty, unity or national interests, China will respond firmly. In other words, China will never lead an invasion or expansion, but also will never allow any piece of Chinese territory to be separated from China (Wen, Blanchard, 2017).

The way war is waged from the Chinese perspective has changed considerably since 20 years ago, but this does not mean that it is entirely new. Like Russia, China does not distinguish between peace and war

[3] This concept, Non-war military activities/NWMA, has its origins in the *concept of Military Operations Other Than War/ MOOTW*, from the American doctrine, and some Chinese writings prefer to use the American version.

and focuses on winning the informationised warfare. At the same time, while under Chinese President Hu Jintao, informationised warfare was a condition, under Xi Jinping, China has become a world power, both economically and militarily, and the concept of *informationised warfare* plays a prominent role in PLA preparation for a possible conflict.

CONCLUSIONS

Starting from the differences in doctrine projection at the level of the Alliance (e.g. definitions, principles, key domains) and the need to obtain coherence between the doctrines for information operations of the NATO member states and the allied doctrine, an essential condition in ensuring interoperability and continuing with the analysis approach to InfoOps from Russian and Chinese perspectives, we may affirm that InfoOps remain a complex, evolving and essential topic in the conceptualisation of warfare. While NATO and USA doctrinal publications are available to the public, the roughly similar Russian and Chinese documents are not available nor discussed in the public space. Also, while the West distinguishes between peace and war, the Russians and Chinese adopt the non-binary view of warfare in which war and peace are two distinct dimensions.

At the same time, the basic line of the war, centred on the use of armed forces, has expanded and presupposes an increasingly pronounced use of non-military measures. For example, the Russian approach seeks to capitalise on all national instruments, by involving both national institutions and non-governmental actors, in a continuous confrontation with current or potential adversaries.

General Gerasimov even stated that Russia must learn not only from its own operations but also from the way the West engaged in operations in Afghanistan or Iraq. At the same time, the General emphasised the fact that warfare cannot be stereotyped, because each conflict has its own logic, and new technologies give a new impetus to the way of thinking about military art. Just as Russia or China have learned from the mistakes of the Americans and not only, so can the American scientists or those who write the doctrines learn from the Russian or Chinese writings and practices. There is a vast literature on this topic, and contrasting these approaches reveals significant differences, which can contribute to the improvement of Western doctrines.

While NATO and USA doctrinal publications are available to the public, the roughly similar Russian and Chinese documents are not available nor discussed in the public space. Also, while the West distinguishes between peace and war, the Russians and Chinese adopt the non-binary view of warfare in which war and peace are two distinct dimensions.

BIBLIOGRAPHY:

1. Cheng, Dean, (2017). *Cyber Dragon, Inside China's Information Warfare and Cyber Operations, the Changing Face of War.* James Jay Carafano, Series Editor. Praeger Security International. California: Santa Barbara.
2. Darczewska, J. (2015). *The Devil is in the Details. Information Warfare in the Light of Russia's Military Doctrine*. Ośrodek Studiów Wschodnich im. Warsaw: Marka Karpia/Centre for Eastern Studies.
3. Kania, E. (2016). *"The PLA's Latest Strategic Thinking on the Three Warfares"*. China Brief, vol. 16, nr. 13, https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/, retrieved on 22 September 2022.
4. Munroe, T., Osborn, A., Pamuk, H. (2022). *China, Russia Partner up against West at Olympics Summit.* Reuters, https://www.reuters.com/world/europe/russia-china-tell-nato-stop-expansion-moscow-backs-beijing-taiwan-2022-02-04/, retrieved on 20 September 2022.
5. Neiberg, M. (2010). *United States Army War College and the University of Southern Mississippi*. H-France Review, vol. 10 (October), nr. 161, p. 699, https://www.h france.net/vol10reviews/vol10no161Neiberg.pdf, retrieved on 20 September 2022.
6. Tashev, B., Lieutenant Colonel (ret.) Purcell, M., Major (ret.) McLaughlin, B. (2019). *Russia's Information Warfare. Exploring the Cognitive Dimension.* MCU Journal, vol. 10, nr. 2, https://www.usmcu.edu/Portals/218/MCUJ_Fall2019_10_2_web.pdf, retrieved on 21 September 2022.
7. Vilmer, J.-B. J., Charon, P. (2020). *Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare*. War on the rocks. Texas National Security Review, https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/, retrieved on 21 September 2022.
8. Wen, P., Blanchard, B. (2017). *President Xi Says China Loves Peace but Won't Compromise on Sovereignty.* Reuters. Aerospace and Defense, https://www.reuters.com/article/us-china-defence-idUSKBN1AH2YE, retrieved on 20 September 2022.
9. AJP-3.10, Allied Joint Doctrine for Information Operations (2009, 2015).
10. Doctrina Operaţiilor Informaţionale (Information Operations Doctrine), (2017) 2nd Edition.
11. The Military Doctrine of the Russian Federation, 2014, https://rusemb.org.uk/press/2029, retrieved on 20 September 2022
12. JP 3-13, Joint Publication 3-13, Information Operations (2006, 2014).
13. JP 3-0, Joint Publication 3-0, Joint Operations (2017).
14. Fact Sheet – US National Defense Strategy (2022). US Department of Defense, https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF, retrieved on 19 September 2022.
15. https://www.business-standard.com/article/international/china-blames-us-nato-expansion-for-russia-ukraine-war-122040100760_1.html, retrieved on 21 September 2022.
16. http://en.kremlin.ru/supplement/5770, retrieved on 19 September 2022.
17. https://www.digi24.ro/stiri/externe/o-provocare-rusia-si-china-si-au-trimis-avioanele-de-razboi-deasupra-marii-japoniei-in-timpul-vizitei-lui-biden-1950723, retrieved on 22 September 2022.

While NATO and USA doctrinal publications are available to the public, the roughly similar Russian and Chinese documents are not available nor discussed in the public space. Also, while the West distinguishes between peace and war, the Russians and Chinese adopt the non-binary view of warfare in which war and peace are two distinct dimensions.