The Cyber Era`s Character of War

Maija Turunen
Finnish National Defence University, Helsinki, Finland
maijaturunen@yahoo.com

Abstract: The nature of war is often considered unchanged, although in the cyber era the concept of war, weapon, and fighter have become blurred. Instead, the character of war is constantly changing and is always unique. The character of war is not similar at different battle domains or levels of warfare, which complicates the course of war. A serious deviation from a strategic-level perception of war character in relation to an operational or tactical level perception character of war can result in defeat. The fog of war has intensified, although the situational awareness of conventional battlefields has clarified due to advances in technology. Technology is a key factor in shaping the war character of the cyber era, depending on the point of view, in 4th or 5th generation warfare. The nature of the next generation warfare and the formation of the character of war may be determined by the Artificial Intelligence or other Emerging and Disruptive Technologies, which itself develops and uses technology or some other technology, not yet known to us. This paper seeks to find factors that influence the formation of the cyber era`s war character and its transformation in Western and Russian military thinking. The aim is to describe the opportunities and challenges associated with the use of advanced technology in the military purpose. This review is based on the NATO`s and the Russia`s strategy papers. Theoreticallly, this paper draws on the theory of the character of war, which is applied to the question under study through the theory of strategic culture. An integrative literature analysis has been used as the research method. The key findings of the paper are that Russia and the West share the view that a warlike battle is already under way in the cyberspace. That requires an faster and better capacity to utilize advanced technologies as part of or in support of weapons systems. Russia and the West are struggling with the moral, legal, and technical problems associated with the use of advanced technology, but are aware of its necessity in the cyber warfare.

Keywords: character of war, cyber warfare, Russia, NATO, artificial intelligence

1. Introduction

The motives behind to prepare for war and the warfare: honour, fear, and interests (Chance, 2012, 13), and some features, like as dominant role of policy and strategy, psychological factors, irrationality, violence and uncertainty (Vego, 2011, 64) have remained the same and universal throughout the history of warfare. The nature of war is often considered unchanged, although in the cyber era the concept of war, the weapon, and the fighter have become blurred.

The character of war is not stable but in constant change. The character of war is changing with the development of an international and interactive political process and technology driven and conditioned by social and economical changes. The character of war is tied to its creator: knowledge of what is available, the ability to interpret and utilize this knowledge. The character of war is a position and culture bound concept that can be shaped for example through strategic communication, reflexive control or information operations. Because the war is always a unique, circumstantial, and dynamic activity between two or more parties, involving the unpredictable changes, each party to the war has its own character of war. (Gray, 2010, pp. 12-13; Vego, 2011, 61, 64; Gerasimov, 2013) The character of war is not similar at different battle domains or levels of warfare, which complicates the course of war.

The history of modern warfare can be divided into eras or generations, at the beginning of which there was a significant change in the way a war was waged and in the character of war. Modern warfare can be considered to have begun in the mid-17th century, when the Treaty of Westphalia sought to create a straightforward and systematic means of war based on nation states. The first generation of warfare was characterized by mass armies, mobile footsteps, and static fire stations. The second-generation warfare can be considered to have begun in the 19th century, when the motorization of the troops, the development of weapons and communication systems allowed for faster movement and fire, and smaller troop divisions. Something about the pace of change in the development of warfare is that the third-generation warfare can be considered to have begun as early as the 20th century, when the advanced aeronautical technology made it possible to strike at enemy targets faster and over long distances. The fourth-generation warfare was characterized by an expanding range of means of asymmetric strategies and tactics designed to challenge the values and social system of the adversary using information, psychological, and lawfare methods. (Paronen, 2016; Lind & all, 1989, 23; Ahvenainen, 1994, 96-97)

The fifth-generation warfare is marked by its invisibility, which blurs and creates uncertainty about the difference between war and peace. The focus is on non-kinetic interference, such as information and cyber operations, which seek to undermine the non-military resilience of the adversary and obscure the adversary's situational awareness, as well as deny the adversary right to use military force. (Paronen, 2016; Abbott, 2010, 20). The strong and fast development of information, cyber, autonomous and hypersonic weapons, as well as artificial intelligence (AI), quantum computing, and robotics, can also be considered in the fifth-generation warfare, which current phase could also be called the cyber era`s warfare. Even the term "sixth-generation warfare" (Slipchenko, 2013) has been used in the Russian scientific debate. However, the sixth-generation warfare is counted as the New Generation Warfare. (Bērziņš, 2019, 167, 170, 176).

There is no broad consensus on the division of the strategic, operational, tactical and technical levels of warfare into generations or what stage they are at. However, it can be seen that generational change in warfare involves key ideas common to all changes, such as changes in perception on the battlefield, changes in the mobility and the speed of hostilities, and the goals (enemy forces, political system, critical infrastructure), and the objectives (destroy vs. collapse). (Lind & all, 1989, 23; Paronen, 2016). Gray (2010, 11-12) has listed five significant changes in the contexts that shape contemporary war and strategy. They are: 1) The development of cyber power (all future wars will harbor integral cyber warfare); 2) Space warfare; 3) The rise of a global electronic media with real-time access to events; 4) An information-led revolution in the military affairs (RMA); and 5) Belligerents and irregular warfare.

The era of cyber warfare can be considered to have begun in the 1960s with the proliferation of computers and the invention of the Internet. The cyber warfare is affected by the general functional dimensions of warfare, such as human, technology, organizational skills, logistics, knowledge, doctrines, time, space, and energy. In the cyber domain, there is an ongoing struggle between attackers and defenders. The durability and extensibility of the "Red Lines" set by the states are tested all the time. The success of this struggle in the militarization of information and new technologies, especially artificial intelligence, acts as a game changer (Edmonds, 2021, 79-83).

1.1 Theoretical background

This research is based on the application of the theory of character of war. The character of war can be defined as follows: The character of war means the common perceptions in the international system of the nature, needs and possibilities of the use of armed forces, as well as the effective principles and operating models of the armed forces. In the theory of character of war, war was viewed as a pragmatic and changing phenomenon. The war character is connected in the international system and security environment, as well as in operational logic, strategic communication, rules, and influence of the new technological advances. It also constructs association with identities of the actors. Through the character of war, the creator of the character of war seeks to outline the prevailing military threats against which one must be able to wage war; the situation in which war may be waged; the methods by which war is to be fought; the factors that can be used to increase credible military power; and the objectives of warfare. (Raitasalo – Sipilä, 2008, 9; Vego, 2011, 64; JDN 1-8, 2018, I-4).

The theory of strategic culture plays a central role in understanding Russian art of warfare, but is also suitable for explaining the factors behind the Western perception of the character of war. The strategic culture can be explained as a set of persistent and consistent historical patterns of how the state`s leadership thinks about the use of force to achieve political goals. The preferences originate in the historical experiences related to the threat and use of force by the state and are influenced by the philosophical, political, cultural, and cognitive experiences and characteristics of the state (Kari, 2019, 71; Johnston, 1995).

Integrative literature analysis were used as the research method. By integrating and analysing the strategic documents and literature on the current perception to future cyberwarfare, the aim is to consider what kind of factors influence the formation of the war character of the cyber era and its transformation in Western and Russian military thinking. The purpose is to position the examination of the research question as part of the scientific debate on the topic.

2. Russian perception of the character of cyberwar

The National Security Strategy (2021), the Russian Military Doctrine (2014), the Information Security Doctrine (2016) and National Strategy for the Development of Artificial Intelligence for the period until 2030 (2019) are the main official public documents outlining the formation of the Russian perception about the character of cyber war and warfare. They highlight in particular the various threats as well as identify and provide to the authorities, including army, and obligation to respond vigorously to these threats in all domains. They also include clear measures for managing the cyber environment and consider the entire world as a theatre of operations and information space as the battlefield, not just the information space under Russian control. In other words, these documents are used by Russia to legitimize its own actions (Bērziņš, 2014, 3; Thomas, 2016, 22). Strong legalism is emphasized as part of Russian society in its power structures and their supporting activities. Unlike most Western countries where the powers of the authorities are limited by the law, in Russia the law is confirmed obligations to the public authorities from doctrines and strategies, while giving them powers to carry out these tasks.

Russia's new National Security Strategy (NSSRF) can be described as a manifesto, a defiant declamation to the rest of the world and a narrative for citizens emphasizing to victimizing and to sacrifice for Russian sovereignty and traditional values. The strategy explicitly states that: “Space and information space are being actively explored as new spheres of warfare.” Development of a safe information space, protection of Russian society from destructive information and psychological impact are mentioned as one of Russia’s national interests and strategic national priorities. (NSSRF, 2021, 4-6, 8). Particular attention is paid to the timely consideration of trends in the changing nature of modern wars and armed conflicts, the creation of conditions for the fullest realization of the combat capabilities of troops (forces), the development of requirements for prospective formations and new means of armed combat and ensuring the technological independence of the defense-industrial complex of the Russia. (NSSRF, 2021, 11-14)

Russia accuse foreign states for computer attacks, resistance to their initiatives in the field of international information security and activities of special services to conduct reconnaissance and other operations in the Russian information space. Also Russia complains, that armed forces of foreign states are practicing actions to disable critical information infrastructure facilities of Russia. Russia intends to fight against such activities, e.g. by the development of forces and means of information confrontation and improvement of means and methods of information security based on the use of advanced technologies, including artificial intelligence and quantum computing technologies. And finally, the Strategy states ominously: “The Russian Federation considers it legitimate to take symmetric and asymmetric measures necessary to suppress such unfriendly actions and to prevent their recurrence in the future.” (NSSRF, 2021, 19-22, 39)

The General Staff Commander of the Russian Army, General Gerasimov, has stressed the importance of researching the nature of modern warfare, military and non-military means of waging war, and the problems of strategic deterrence, which means finding ways to prevent hybrid pressure and the ability to maintain a strategic initiative for the possibility of admission (Thomas, 2016, 18-19; Krasnaya Zvezda, 2019). Sukhankin (2019, 332) considers with reference Gerasimov (2016), the militarization of information as Russia's information strategy the most important pillars. Worth noting is that Russia considers cyber and electronic warfare capabilities to be part of information security and Russia'swde21 Anti-Access/Area-Denial (A2/AD) strategy. The difference between technological and psychological information control is clear, but both are crucial to achieving the goals already in the initial period of war by taking control of the adversary’s information space. Where Western countries emphasize the freedom of information, the right to information, the protection of privacy, and information as the key to truth, in Russian thinking, the information weapon is a weapon like others are and the moral-based and self-restraining attitude of the Western states towards information opens up vulnerabilities that can be exploited through information operations (Kucharsky, 2018, 2).

Russian military thinking also involves creating an alternative reality or realities. The idea is that in a state under threat of war, society’s support for the state’s strategic goals - in other words, the legitimacy of war - is essential to achieve a victory. The Russians have placed the idea of influence on the center of its operative planning. Examples of such influence are both internal and external communication, deception operations, and psychological operations. (Bērziņš 2019, 166-167, 170-171). Also Kasapoglu (2015, 5-6) estimates that Russia's hybrid warfare is aimed at creating a fog of hallucinatory warfare and it consists of consistent delusions not intended to paralyze Western intelligence and proactive capabilities, but to changes Western analysis results and perceptions of Russia’s strategic intentions.

The Russian Military Doctrine (2014) sees that there are military dangers and threats are increasingly moving into the information space and information acts as a justification for military action. The use of cyber methods is suitable for the implementation of the basic principles of Russian operative thinking, like surprise and confusion. These methods have subtle nature and they left space for speculation. The use of cyber methods and the need to protect against them are most evident in the Information Security Doctrine (2016), which defines that Russia's national interests in the information space contain e.g. maintaining continuous and smooth information operations in information infrastructure.

Unlike Russia's Information Security Doctrine, their National Strategy for the Development of Artificial Intelligence for the period until 2030 (2019), despite its ambitious goals, is quite modest when it comes to utilizing AI for the military use. Robotics and unmanned vehicle control are mentioned in related areas of the use of AI (NSDAI, 2018, 4). The Russian Artificial Intelligence Strategy also includes the principles which are obligatory during the implementation of that strategy: a) the protection of human rights and liberties; b) security; c) transparency; d) technological sovereignty; e) innovation cycle integrity; e) reasonable thrift; and g) support for competition (NSDAI, 2018, 7-8). Russia's military thinking recognizes the risks associated with the development and use of AI, but considers it inevitable that some military systems will become completely autonomous. The Syrian war provided a good opportunity for Russia to test its autonomous weapons systems and a concept of limited action warfare beyond its borders. (Edmonds, 2021, 80, 115; McDermott, 2019).

Russia's strategy papers emphasize the goal of protecting Russia's world of values and ideas, as well as culture, and creating a unified character of Russia as a strong nation. In this context, the information confrontation and psychological warfare play a key role, highlighted by the effective use of AI and other advanced technologies (Edmonds, 2021, 82-83). According to Bērziņš (2019, 165-166): "The Russian view of modern warfare is based on the idea that the main battlespace is the mind. As a result, new-generation wars are to be dominated by information and psychological warfare in order to achieve superiority in troops and weapons control, morally and psychologically depressing an enemy's armed forces personnel and civilian population." As in his speech in 2017, Gerasimov (Komsomolskaya Pravda, 2017), seems to focus on the fight in the minds of the citizens, the sixth dimension of battlefields.

In summary, it can be said that the lines between war and peace and between defensive and offensive methods have been deliberately blurred in Russian military thinking (Foxall, 2021, 18). Unlike in the West, where peace is in principle considered a normal interstate situation, in Russian thinking wars and armed conflicts will continue uninterrupted. (Giles, 2021, 16-17). While Russia fears the use of asymmetric measures to influence its citizens, it also favours the use of these measures in creating a fog of war and influencing its adversaries. Information confrontation, information weapons (including cyber weapons utilizing AI) and informational-psychological operations has a centric position in Russian asymmetric warfare strategic planning.

3. Western perception of the character of cyberwar

The Strategic Concepts (2010, will be updated on 2022), the Emerging and Disruptive Technologies Coherent Implementation Strategy (2021), the NATO Warfighting Capstone Concept (NWCC, 2021) and the NATO Artificial Intelligence Strategy (2021) are key documents in mapping NATO's public stance on the character of war of the cyber era.

NWCC is adversary-centric and designed to acting across three operational contexts: shaping, contesting and fighting. It sets out five Warfare Development Imperatives: 1) Cognitive superiority; 2) Layered resilience; 3) Influence and power projection; 4) Integrated multi-domain defence; and 5) Cross-domain command (Tammen, 2021). The purpose of the NWCC is to create a vision for Alliance Warfare Development up to 2040 to allow the Alliance to protect NATO's core security interests in the future (Sweijs & all, 2020, 2).

A specialists are estimated, that Emerging and Disruptive Technologies (EDTs) are a challenge but also opportunity for NATO and the alliance to achieve dominance in key EDTs must be a strategic priority for the Alliance: "EDTs will disrupt, degrade and enable NATO military capabilities in the 2020-2040 timeframe. Such characteristics of modern technologies are drivers of the current evolution and revolution in data, AI, autonomy, space, quantum, hypersonics, biotechnologies and materials. Alone or in combination, they define the technological edge necessary for NATO's operational and organisational effectiveness." (Reflection Group, 2020, 13, 39).

The new technologies will change the nature of warfare, and enable new forms of attacks (Reflection Group, 2020, 16, 18, 31). NATO sees interoperability, a mix of old legacy systems and new weapon systems, the technopolicy, legal and ethical issues as a challenge in the use and further development of AI and other EDTs (NSTO, 2020, 26, 39, 55). NATO's Artificial Intelligence Strategy (2021) identifies these challenges and sets out common principles to which the NATO and its Allies have committed themselves in developing and to use of AI and its applications: 1. Lawfulness; 2. Responsibility and Accountability; 3. Explainability and Traceability; 4. Reliability; 5. Governability; and 6. Bias Mitigation (NATO, 2021). These principles emphasize responsibility and, more broadly, Western values and norms in the theatre of future warfare, where AI offers immeasurable opportunities. As an example of these opportunities, AI can be used to enhance intelligence, surveillance and reconnaisance capacity in continuously ongoing Command and Control operations. The capability of advanced AI systems to collect, analyze, generate, and manipulate information opens new posibilities for information superiority at all levels of operational decision-making. Advanced artificial intelligence systems can create their own killing chains, mutable cyber weapons or even rewrite themselves, thus will be revolutionizing military operations at all levels. In the flexible defence or response cyber operations, the ability of AI to generate unique effects, randomly select locations for launching surprise operations and generate various responses, makes it difficult for an attacker to determine what kind of and where the countermeasures are needed. (Edmonds, 2021, 82; Chen, 2017, 104-105).

Artificial Intelligence and Robotic Autonomous Systems (RAS) are already here, but their advanced application for military purposes could give to states a significant military advantage, revolutionise military and strategic affairs and change the character of war (Tonin, 2019, 4). There are countless opportunities in the military sector to exploit AI and RAS. These can be used, for example, to facilitate autonomous and remote operations, operations both on physical and virtual A2/AD zones, to intensify the informed military decision making at all levels, to improve the situational awareness and resource management, and to increase the speed and scale of military action (Gray and Ertan, 2021, 22; Sayler and Hoadley, 2020; Tonin, 2019, 8).

But, there are also many challenges to development and use the advanced technologies to military purpose: Firstly, as with all weapons systems, there are ethical, political and legal issues, and especially when dealing with the international law and politics, issues of trust; secondly, there will be significant technological challenges: AI technology and systems use by that, need to be integrated into existing systems and ensure their interoperability. AI may be unpredictable or vulnerable to unique forms of manipulation or human based programming errors and cyber attacks. AI systems are brittle, opaque, and reliant on good data, and any failure in an AI enabled military system could have catastrophic consequences; and thirdly, challenges may be caused by a lack of financial and intellectual resources in the state seeking to exploit AI. The development of AI and related systems not only requires skilled and innovative people, but also changes the strategic military thinking and the allocation of available resources. (Gray and Ertan, 2021, 22; Sayler and Hoadley, 2020; Tonin, 2019, 6-8)

Western experts estimate that tomorrow’s conflict will be characterized by the widening of the battlespace, the fusion of dimensions and the rise of borderless warfare. Future wars will include societal warfare (focused on disrupting and coercing societies) and cognitive warfare (focused on creating civilian disorder), alongside high-end conventional wars and wars fought by proxy (Sweijs & all, 2020, 3-4). However, the perception of the character of war is still hampered by traditional thinking about the distinction between peace, crisis and conflict paradigm (Tammen, 2021) An ability to project hard power will retain its place in the multi-domain warfare of the future. In multi-domain warfare, it is also necessary to develop A2/AD zones in order to reflect military strength in controversial areas based on technological advancements. Strategically future warfare is required for example cognitive superiority, full-spectrum engagement, and agile ways of adaptation. (Sweijs & all, 2020, 9, 11).

4. Conclusions

An examination of both Russia's and NATO's strategy documents shows that the use of AI and other EDTs in military activities and weapon systems, political will, and military strategic thinking, can been seen as key factors that will influence the formation of the character of war of the cyber era.

NATO and Russia both emphasize the importance of cyber methods, and in particular the development and exploitation of the opportunities offered by AI and RAS now and in a future warfare. Similarly, the creation of A2/AD zones and the ability to extend the battle to the adversary’s A2/AD zones are seen as a significant factor in the military strategic thinking of both actors in cyber warfare. Both actors also recognize the key integration problem associated with the development of AI and RAS. New technology-based C5ISR and weapons systems should be able to be used integrated or at least in parallel with older systems, which are often expensive to be replaced and designed to have a long life cycle. The third common view is that there is already a war-like struggle in cyber domain and the permanent and effective ability to perform different and various levels of cyber operations is essential. This means that the use of advanced technology in surveillance and intelligence systems or in data collection and analysis alone is not enough. Operational efficiency also requires allowing the advanced technology to develop, to use and to real-time operate, for example, self-correcting and mutation-capable cyber weapon systems.

One of key difference between those actors is in the strategic communication, in the national narrative: Russia emphasizes the threat posed to the Russian people by the West and the readiness for sacrifices required to protect from it, while the West believes that citizens are safe and their information rights and freedoms must be protected and promoted. NATO and Russia share respect for human rights and security as common values in developing of AI and RAS, but otherwise the emphasis of values differs from emphasizing NATO's responsibility to promoting Russia's digital sovereignty goals. Both sides have their own values, their protection and the commitment of their citizens, as a basis for preparing for the war of the future. Indeed, the sixth generation war may be resolved by the minds of the people (soldiers, citizens and politicians): what kind of technology and what kind of weapon systems they are willing to accept and to use.

References

Abbott, D. (2010). The Handbook of Fifth-Generation Warfare. Nimble Books.

Ahvenainen, S. (1994). Sodankäynnistä, elektroniikasta ja elsosta. Tiede Ja Ase, 52(52), pp. 91–139. https://journal.fi/ta/article/view/47764.

Bērziņš J. (2014) Russia`s New Generation Warfare in Ukraine. Implications for Latvian Defence Forces, National Defence Academy of Latvia Center for Security and Strategic Research, 2014. http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx.

Bērziņš J. (2019) Not 'Hybrid' but New Generation Warfare. https://jamestown.org/wp-content/uploads/2019/02/Russias-Military-Strategy-and-Doctrine-web.pdf?x29008&x87069.

Chance, A. (2012) Motives Beyond Fear: Thucydides on Honor, Vengeance, and Liberty. https://dlib.bc.edu/islandora/object/bc-ir:101441/datastream/PDF/view.

Chen, J. (2017) Cyber Deterrence by Engagement and Surprise. PRISM 7, NO. 2, 2017. pp.101-107. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_7-2/prism_7-2.pdf.

Edmonds, J. and all (2021) Artificial Intelligence and Autonomy in Russia https://www.cna.org/CNA_files/centers/CNA/sppp/rsp/russia-ai/Russia-Artificial-Intelligence-Autonomy-Putin-Military.pdf

Foxall, A. (2021) Changing Character of Russia`s Understanding of War: Policy Implications for the UK and Its Allies. https://static1.squarespace.com/static/55faab67e4b0914105347194/t/60ad0d070095631c778111fe/1621953799713/How+Russia+Understands+War+2021.pdf.

Gerasimov, V. (2016): По опыту Сирии. 7.3.2016 Военно-промышленный курьер. https://vpk-news.ru/articles/29579.

Giles, K. (2021) What deters Russia. Enduring principles for responding to Moscow https://www.chathamhouse.org/sites/default/files/2021-10/21-09-23-what-deters-russia-giles.pdf.

Gray, C.S. (2010) War—Continuity in Change, and Change in Continuity. The US Army War College Quarterly: Parameters 40, 2. https://press.armywarcollege.edu/parameters/vol40/iss2/5.

Gray, M. & Ertan, A. (2021) Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment. NATO CCDCOE. https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_A4.pdf.

Johnston, A. (1995). Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. Princeton University Press 1995.

Kari, M. J (2019) Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats. JYU DISSERTATIONS 122.

Kasapoglu, C. (2015) Russia`s Renewed Military Thinking: Non-Linear Warfare and Reflexive Control. Research Division – Nato Defence College, Rome – No. 121 – November 2015

Komsomolskaya Pravda, 26.12.2017: Начальник Генштаба Вооруженных сил России генерал армии Валерий Герасимов: «Мы переломили хребет ударным силам терроризма» http://archive.redstar.ru/index.php/component/k2/item/35551-my-perelomili-khrebet-udarnym-silam-terrorizma.

Krasnaya Zvezda (4.3.2019): Векторы развития военной стратегии. http://redstar.ru/vektory-razvitiya-voennoj-strategii/.

Kucharsky, L. (2018) Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe. https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf.

Lind, W.S and all (1989) The Changing Face of War: Into the Fourth Generation Marine Corps Gazette (pre-1994); Oct 1989; 73, 10; ProQuest Direct Complete pp. 22-26

McDermott, R. (2019): Russia's Military Scientists and Future Warfare. https://jamestown.org/program/russias-military-scientists-and-future-warfare/

NATO (2021) Summary of the NATO Artificial Intelligence Strategy. https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

NATO Warfighting Capstone Concept (2021) https://www.act.nato.int/nwcc.

NATO Science & Technology Organization (2020): Science & Technology Trends 2020-2040 Exploring the S&T Edge. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

Paronen, A. (2016) Onko Suomi sodassa? – Sodankäynnin viides sukupolvi. The Ulkopolitist. https://ulkopolitist.fi/2016/02/10/onko-suomi-sodassa-sodankaynnin-viides-sukupolvi/.

Reflection Group (2020) NATO 2030. United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

Sayler, K. M. and Hoadley, D. S. (2020) Artificial Intelligence and National Security. CRS Report R45178. https://sgp.fas.org/crs/natsec/R45178.pdf.

Slipchenko, V. (2013) "Information Resource and Information Confrontation: their Evolution, Role,and Place in Future War," Armeyskiy Sbornik (Army Journal), No. 10 2013, pp. 52-57,

Sukhankin, S. (2019) Russia's Offensive and Defensive Use of Information Security. In "Russia`s Military Strategy and Doctrine." Howard, G. and Czekaj, M (Eds.) The Jamestown Foundation, Washington, DC February 2019, pp. 302 – 342.

Sweijs, T. et all (2020) The NATO Warfighting Capstone Concept: Key Insights from the Global Expert Symposium Summer 2020. Hague Centre for Strategic Studies. https://www.jstor.org/stable/resrep26765.

Tammen, J.W. (2021) NATO Review (9.7.2021) NATO's Warfighting Capstone Concept: anticipating the changing character of war. https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html.

The Doctrine of Information Security of the Russian Federation (2016). http://www.mid.ru/en/foreign_policy/official_documents/asset_publisher/CptICkB6BZ29/content/id/2563163

The Military Doctrine of the Russian Federation (2014). https://rusemb.org.uk/press/2029.

The National Security Strategy of the Russian Federation (2021). https://www.academia.edu/49526773/National_Security_Strategy_of_the_Russian_Federation_2021.

The National Strategy for the Development of Artificial Intelligence for the period until 2030 (2019). Center for Security and Emerging Technology, Trans.), October 10, 2019. https://cset.georgetown.edu/wp-content/uploads/Decree-of-the-President-of-the-RussianFederation-on-the-Development-of-Artificial-Intelligence-in-the-Russian-Federation-.pdf.

Thomas, T. (2016) Thinking Like A Russian Officer: Basic Factors And Contemporary Thinking On The Nature Of War. Foreign Military Studies Office. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/194971.

Tonin, M. (2019) 'Artificial Intelligence: Implications for NATO's Armed Forces'. NATO Science and Technology Committee Sub-Committee on Technology Trends and Security. 13 October 2019. https://www.nato-pa.int/document/2019-stcttc-2019-report-artificial-intelligence-tonin-149-stctts-19-e-rev1-fin.

U.S Joint Chief of Staff (2018) Joint Doctrine Note 1-18. Strategy. (JDN 1-8) https://fas.org/irp/doddir/dod/jdn1_18.pdf.

Vego, M. (2011) On Military Theory. Issue 62, 3 d quarter 2011 / JFQ. https://apps.dtic.mil/dtic/tr/fulltext/u2/a546600.pdf pp.60-67.