Review

Impact of Cyber Space on Security in the Context of Armed Conflicts: Towards Disaster Risk Resilience

Dalibor Milenković , Vladimir M. Cvetković * , Aleksandar Ivanov , Renate Renner

Posted Date: 12 December 2024

doi: 10.20944/preprints202412.1099.v1

Keywords: cyberspace; security; armed conflicts; disaster risk resilience; hybrid warfare; artificial intelligence; Internet of Things; regulatory frameworks; operational capabilities; resilience building

 doi:10.20944/preprints202412.1099.v1

Review

Impact of Cyber Space on Security in the Context of Armed Conflicts: Towards Disaster Risk Resilience

Dalibor Milenković [1,2], Vladimir M. Cvetković [1,2,3,4,*], Aleksandar Ivanov [1,4,5] and Renate Renner [4]

[1] Scientific-Professional Society for Disaster Risk Management, Dimitrija Tucovića 121, 11040 Belgrade, Serbia
[2] International Institute for Disaster Research, Dimitrija Tucovića 121, 11040 Belgrade, Serbia
[3] Department of Disaster Management and Environmental Security, Faculty of Security Studies, University of Belgrade, Gospodara Vučića 50, 11040 Belgrade, Serbia
[4] Safety and Disaster Studies, Department of Environmental and Energy Process Engineering, Montanuniversität of Leoben, Franz Josef-Straße 18, 8700 Leoben, Austria;
[5] Faculty of Security—Skopje, University St. Kliment Ohridski Bitola, 7000 Bitola, North Macedonia
* Correspondence: vladimir.cvetkovic@unileoben.ac.at

Abstract: The rapid evolution of cyberspace has profoundly impacted security dynamics and the conduct of armed conflicts. As an integral domain in modern warfare, cyberspace intertwines with traditional conflict factors, such as human and material resources, space, time, and information, redefining their roles and interactions. This paper explores the influence of cyberspace on security within the context of armed conflicts, highlighting its dual nature as a battlefield and a tool for shaping strategic outcomes. Emphasis is placed on integrating advanced technologies, including artificial intelligence and the Internet of Things (IoT), in enhancing operational capabilities and addressing hybrid and informational warfare. Furthermore, the study examines the critical role of disaster risk resilience in mitigating the cascading effects of cyber-related disruptions during conflicts. The findings underscore the need for a comprehensive approach combining technical innovations, organizational strategies, and robust regulatory frameworks. The paper concludes that achieving resilience in cyberspace requires multidisciplinary collaboration, continuous capacity building, and the alignment of security policies with emerging technological challenges. The findings highlight the critical importance of integrating digital infrastructures, regulatory frameworks, and innovative technologies, such as artificial intelligence and the Internet of Things (IoT), to mitigate cascading effects during armed conflicts. By emphasizing adaptive strategies and capacity-building, the paper offers actionable insights for policymakers and practitioners aiming to strengthen societal and infrastructural resilience in the face of hybrid threats.

Keywords: cyberspace; security; armed conflicts; disaster risk resilience; hybrid warfare; artificial intelligence; Internet of Things; regulatory frameworks; operational capabilities; resilience building

1. Introduction

Civilizational development viewed through the prism of technological progress and the improvement of comprehensive social relations, along with the constant striving for something new, as the basic determinant of all modern states, imposed the necessity of dealing with, often completely new fields, that is, the circumstances in which organized societies must function (Friedmann, 1952; Kolganov, 2022; Stepanyants, 2022; Zgirovskaya, 2023; Ноономика et al., 2022). The pursuit of progress imposed the need for an intensified connection of all social segments that in the past were even separated and distant by default. It was the merging and synchronization of certain social segments that contributed to an even greater acceleration of progress, to which even developed countries often failed to respond adequately and cope with the changes completely successfully.

 doi:10.20944/preprints202412.1099.v1

The acceleration of all processes in modern societies has created a sense of constant tension or friction between what has become old and what is considered new. The answer to these circumstances is to define such a situation as a crisis. It is precisely the increasingly frequent crises that impose conflicts as a response. War, as the ultimate origin of social conflicts, aims to change and impose the will, i.e. the continuation of life in new circumstances imposed by the winner. In the recent past, the will was imposed by the concrete disintegration of the adversary or its resources.

Today, imposing a will and changing circumstances does not require such brutality as was used in the previous period (Alemzadeh, 2023; Bandura, 1999; Dobash, Dobash, Cavanagh, & Lewis, 1996; Hall, 2018; Hubert, 2017; López, 2020; Schinkel, 2004; Townsend et al., 2023; Urbatsch, 2021; Van Swol, Prahl, MacGeorge, & Branch, 2019). All-out destruction of opponents is becoming less necessary but is still often a key way to resolve social conflicts. Precisely because of this, the perception of war is actively changing and its conduct is increasingly influenced by completely new segments in social development. Societies that perceive the impact of new circumstances, go to meet them. Some societies, instead of action, function on the principle of reaction when a new circumstance causes problems or damage, which can often be irreparable.

Especially because of the above, i.e. the evolution of the classic military conflict as a way of conflict resolution, it is necessary to look at certain new segments of social development with the factors of armed struggle, which represents the basic content of war. In the context of the above, information and communication technologies (ICT) can be considered as new segments of social development, i.e. cyberspace itself is viewed as a place where certain elements of the factors of armed struggle, reflected in human and material resources, space, time and information, are intertwined.

In the context of disaster risk resilience, the integration of cyberspace and its associated technologies plays a crucial role in mitigating the cascading effects of armed conflicts on societies (Cvetković & Šišović, 2024; Milenković, Cvetković, & Renner, 2024). Resilience is not solely about enduring disruptions but also about adapting and thriving amidst challenges. Cyberspace, as a domain, offers unprecedented opportunities to enhance early warning systems, optimize resource allocation, and ensure the continuity of critical functions during conflicts. By leveraging innovations such as artificial intelligence and the Internet of Things (IoT), this paper emphasizes the potential of resilient digital infrastructures to protect human and material resources, preserve critical information, and maintain societal stability. This aligns with the broader objective of fostering adaptive capacities and reducing vulnerabilities in the face of hybrid and technological threats.

The aim of this paper is to explore the impact of cyberspace on security in the context of armed conflicts, with a particular focus on disaster risk resilience. By examining cyberspace as a pivotal factor in modern conflicts, the study analyzes how technological innovations, such as artificial intelligence and the Internet of Things (IoT), can contribute to the resilience of communities and infrastructure against the destructive effects of conflicts. This underscores the necessity of integrating technical solutions and risk management strategies to enhance resilience and mitigate the effects of hybrid and informational threats in contemporary society.

2. Characteristics of Modern War

War has always been one of the ultimate ways of resolving conflicts between two social entities (Cvetković, 2024a, 2024b; Cvetković & Šišović, 2024; Grozdanić & Cvetković, 2024; Tanasić & Cvetković, 2024). Although it has traditionally been expressed throughout history as a desire to physically destroy the opponent in any form and then impose one's will, it also implied other aspects of social conflicts, which, however, were not so efficient and effective. Therefore, looking at earlier periods, wars can be divided into several eras. According to the character of armed struggle and its evolution, William Lind and George Thiele (Lind & Thiele, 2015) formulate the division of wars into four generations with all the specificities that these generations carried.

Roughly speaking, under modern, or fourth-generation war, we can consider those that have taken place in the last three decades, that is, in such a way that a neutral observer who is a layman can notice all the changes compared to previous wars and conclude certain regularities. This does not mean that in the previous historical period, what was sought in wars from the recent past was not

 doi:10.20944/preprints202412.1099.v1

sought, but that at that time there were no objective possibilities and knowledge to realize these aspirations.

A characteristic of the wars of the last generation is the complete involvement of all segments of society in the war. This is understood to mean that the entire population and territory of an entire country or region are involved in the conflict, along with all the available resources that a society or country has at its disposal. Such conflicts, due to their comprehensiveness and asymmetry, are considered and called hybrid wars. This form of war involves a set of actions that can affect certain segments of society and influence the outcome of the armed conflict. "The rise of this type of conflict does not represent the end of conventional warfare, but it is a factor that greatly complicates defence planning in the 21st century." (Hoffman, 2007, p. 9).

Hybrid warfare involves armed conflict that simultaneously involves military and non-military means intending to direct the enemy towards activities that he would not voluntarily undertake" (Hybrid Warfare: A New Phenomenon in Europe's Security Environment, 2016, pp. 10-11). The main role in hybrid warfare belongs to several subversive activities through special operations, combined with economic or commercial pressure. In addition, in addition to regular military operations, those that are considered irregular can also be used. All activities can be directed both at the entire society and at individuals or certain segments of society, such as political structures, state bodies or the enemy's armed forces themselves (*Hybrid Warfare: A New Phenomenon in Europe's Security Environment*, 2016).

3. Factors of Armed Conflict

The understanding of what constitutes a modern army is closely linked to the circumstances and factors surrounding the defence system in a society and its immediate and broader international environment (Creveld, 1992; Gareev, 2001; Kier, 1995; Kristoferson, 1981; Milinovic & Ivaniš, 2015; Santala, 2004; Westing, 1988; Wilén & Strömbom, 2021). A proper understanding of the relevant circumstances and factors is a prerequisite for quality planning of the use of armed forces, which demonstrates its affirmation through effectiveness in practice during the execution of the basic assigned tasks. The armed forces of a modern country, in addition to the capacity for immediate use, in the current circumstances must also represent a factor of deterrence and prevention that is used together with other social segments.

To implement this, the armed forces must have achieved the desired operational capabilities. For what is considered operational capabilities, the definition in the Serbian Army can be taken as an example, which states that they represent the ability of the army or its parts to achieve the desired operational effects, within a given time and under certain standards and conditions, by combining forces, means and methods of performing tasks (Serbian Army, 2022). However, classic war, manifested by armed conflict as a basic phenomenon, has remained the main ultimate way of imposing the will of one side on the other. The use of organized armed violence and its nonlinearity and asymmetry is a consequence of the different overall levels of development of the conflicting parties. The goal is to inflict as much damage as possible on the enemy and deviate from the rules of combat that are imposed.

Armed struggle, as a fundamental element of war and armed conflict, is a way to cause changes through combat actions that imply political, economic, military and other goals. Armed struggle is characterized by duration, hierarchy, intensity, manoeuvre, interdependence and coordination. The course and outcome of armed struggle are influenced by the following factors: human resources; material resources; space; time and information. Here, the context of the elaboration of the aforementioned factors, which in this case are closely related to armed struggle, must be particularly taken into account.

Human resources, as in the civilian sector, are today becoming a decisive factor for the successful functioning of the armed forces. Adaptive management of this resource in times of constant changes in use but also in living and working conditions requires monitoring of needs, demographic and economic potential. They include the demographic capacity of the country that can be used effectively

 doi:10.20944/preprints202412.1099.v1

for military purposes in an armed conflict. The term effectively means their exploitation to a reasonable extent and in a way that optimally utilizes the potential of each individual.

Material resources today represent the most complex factor of armed struggle. They encompass the entire social potential reflected in natural, industrial, financial, energy information and communication potentials. Planning, construction, use and resilience of the above segments of material resources represent a basic prerequisite for armed conflict or its prevention in terms of building a deterrent factor about a potential adversary.

Space as a factor in the classical sense represents the place where armed struggle is waged. Space includes land, sea and air. In the past, these three segments of space were a limiting factor and were largely defined by the line along which armed struggle took place. Today, in modern conflicts, these three segments of space include not only what is possessed by the two entities in conflict, but also wider parts related to foreign or international space. In this context, the most developed countries in the world consider space as one of the physical segments of space and actively exploit it. In general, there is no clear marking of the space in which armed struggle is carried out, there is no background or depth of territory that would be inaccessible to the enemy.

Time as a factor of combat manifests itself as a determinant of the duration of an activity, as the time of day or year, or as a meteorological phenomenon. In the modern context of armed conflicts, time becomes an essential resource and all processes in armed conflict are drastically accelerated, which is why the flow of time often becomes a decisive factor for the implementation and conduct of armed conflict. In addition to the above, in terms of meteorological conditions, time becomes a less significant factor with the application of more advanced technologies, i.e. the limitations for conducting armed conflict are becoming smaller.

Information as a factor implies the availability of knowledge and data necessary for the successful conduct of armed conflict. Possession of the necessary information reduces the uncertainty of the successful implementation of necessary tasks. Possession of quality information in the required period enables the successful achievement of set goals or the prevention of undesirable outcomes. The specific feature of information as a factor is that it has the greatest degree of interaction and influence on other factors of armed conflict. It represents a vital resource that is the product of the collection, processing and exchange of data on other factors of armed conflict (2010).

4. Cyberspace

Technological progress, especially in developed countries, is often closely linked to development projects of the army or defence system in a broader sense (Chkhikvishvili & Beridze, 2024; Dexia, 2012; Gilli & Gilli, 2019; Herolf, 1988; Howe, 2006; Kupchyn, Dykhanovskyi, & Kolotukhin, 2020; Pysarenko et al., 2024). The development of each new detail is always placed in the context of its impact on the ability to defend or threaten society, regardless of what is meant by the defence. Every technological "breakthrough" in a certain scientific field always has an impact on the context of material resources as a factor in armed conflict. The acceleration of development and the complementarity of new knowledge and products have created the interpenetration and interdependence of all parts of society, where the development of ICT plays a special role in connecting them. The emergence of ICT and their development have completely changed the classic armed conflict, both directly and indirectly. Directly because they have changed and are changing the degree of influence of the factors of armed struggle or conflict, and indirectly because they change the perception of armed conflict, the need for its intensity, purposefulness, etc. Because of the above, Putnik states that "information and communication technologies have a special influence on the beginning, course and outcome of the conflict." (Путник, 2022, p. 42).

Throughout history, the development of ICT has had various impacts on armed conflict. The impact has changed over time, becoming more complex and multidimensional. More complex, because it initially enabled faster transmission of messages, and with later development, it began to affect all factors of armed conflict, while today it has its unequivocal great impact on all flows before, during and after armed conflict. To be precise, it permeates the entire process of relations between two opposing entities, where armed conflict is only one of the phases of conflict resolution. This has

 doi:10.20944/preprints202412.1099.v1

also been contributed to by the availability of technologies throughout the world, where the advantage of using ICT is no longer only for richer societies.

As a consequence of the presence of ICT and its development, the term cyberspace has been actively used since the beginning of the 21st century (Babulak, 2010a, 2010b; Chatinakrob, 2024; Kellerman, 2010; Lan, 2021; Mbanaso & Dandaura, 2015; Muller, 2015; Sim, 2023). It generally refers to electronic communication networks that are connected to devices or groups of interconnected devices that have the property of automatic operation using computer programs (Information Security Act, 2019). Initially, the perception of cyberspace as a segment in which conflict can be waged or a type of space that can affect the armed conflict itself was not given much importance, primarily because there was no awareness of its use or the consequences of its use. Technological development has influenced cyberspace to expand and enter every socio-social activity, from the life of an individual to the use of the most complex means of warfare.

The doctrines of the most militarily developed countries in the world and military alliances have placed cyberspace on the same level as land, sea, air and space (North Atlantic Treaty Organization, 2022). It has become a place for defence but also a place or means for attacking the enemy. Accordingly, the last two decades have marked a period of the emergence of military "cyber capacities", which were reflected in the development of human and material capacities for conducting cyber activities (protection and attack). Just as classical forces (army, navy, air force) have developed, so too has the continuous development of military cyber capacities been noticeable. It can be said that they are not only complementary to other types of military but that they are becoming an element that permeates through the aforementioned classical types and that this interpenetration becomes their "bloodstream", without which they will not be able to function shortly.

The US Department of Defense's definition, in the context of armed combat factors, even more closely states (clarifies) that "cyberspace is an area in the information environment consisting of independent networks of information structures, including the Internet, telecommunications networks, computer systems, embedded processors, and controllers." (*Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms*, 2016, p. 58).

Due to the above, it is particularly important to emphasize that the perspective of cyberspace in the future is to cease to be a segment of space as a factor of armed struggle and to become one of the key independent factors of armed struggle.

4.1. Cyberwar

Information as a starting point in any military armed conflict or battle represents the essence and potential to win or avoid defeat (Bogdanoski & Milkovski, 2015; Johnson et al., 1997; Libicki, Gompert, Frelinger, & Smith, 2007; Neculcea, 2021a, 2021b; Reese, 2020; Serrano & López, 2008; Toroi, 2021). For a set of objective facts, converted into data and shaped into information, often in the past, more important than the quality itself was how quickly it would reach the user who makes decisions in the conflict. With the development of technologies that enabled two-way and one-way communication, information consumers were born and developed. It is easiest to divide them into two groups, primary, those for whom the information is important for decision-making, as well as secondary, for whom the information is of less direct importance, but who ultimately decide on the course of events (conflict).

During the 20th century, if we exclude the standard two-way communication channels for command in conflict, the most important step was made in one-way communication channels towards the ordinary person, embodied in radio and television. The importance of these two forms of communication was quickly recognized and exploited to the extent that it often played a decisive role in influencing all aspects of armed conflict, before the conflict as preparation, during the conflict to shape it, and finally to indicate the achieved goal and purpose of the completed conflict.

The end of the last century and the beginning of the present century brought the possibility of instant two-way communication between the recipient and the sender of information via computer networks in the broadest sense of the word. The possibilities of this type of communication and its fundamental importance were not understood by many countries or societies even in the second

 doi:10.20944/preprints202412.1099.v1

decade of this century. In addition to the above, comprehensive social development has integrated ICT into all aspects of the functioning of a state, to the extent that almost everything functions when it is "on a network". This fact has not bypassed more complex systems or means of military technology in modern armies, where in addition to the transmission of information, the newly created space enables the autonomy of the action of these means and their implications for the physical world.

There are still active scientific debates about establishing and defining a term for the newly emerging space, or rather the conflict in it, that would be generally accepted and that would shape the relevant topic. Thus, Putnik and Milošević state that cyber warfare is a continuous conflict between national armies or guerrilla groups in cyberspace, which involves conducting attacks on the opponent's information infrastructure using malware and other cyber tools and techniques, as well as conducting propaganda activities, to cause damage to the opponent and weaken his defensive capacities in the cyber and physical world (Putnik & Milošević, 2018). The above definition represents the sublimation or genesis of a larger number of definitions, primarily modern military ones, that treat the concept of cyber warfare.

The essence of cyber warfare is that it takes place in a space that is separate and distinct from the others that are incorporated into the classical space as a factor of armed combat. It is also characterized and shaped by the computers and computer networks in which it can take place.

4.2. The Impact of Cyberspace on the Factors of Armed Conflict

Modern armies and military alliances have become increasingly aware of the advantages and dangers that cyberspace brings with it in its current state of development. That is why, in the first decade of the 21st century, they placed this type of space on an equal footing with other segments of space as a factor in armed conflict (National Security Strategy, 2022). They began to actively develop human and technical capacities for defensive and offensive actions in cyberspace. Initially, these were smaller units, almost experimental in nature, today they are equal formations with organizational structures and a way of functioning that is almost the same as in other types of armies. Regardless of all the facts and objective circumstances, there are still armies that strive to be modern, but do not have defined, regulated and rounded cyber capacities in their formations. It can be said that these compositions are in experimental stages and that they are a full decade behind objective reality and the needs of the future.

In the militaries of states that are facing future circumstances, there is a noticeable tendency to expand cyber capabilities in such a way that they become integral parts of other classical aspects in a single army or military alliance. Their role and complementarity are becoming an indispensable factor and prerequisite for the successful use of armed forces.

Considering the influence of the factors of armed conflict, with their mutual intertwining, on the course and outcome of an armed conflict, it is necessary to consider in what ways cyberspace as a place of cyberwar can individually influence each factor of armed conflict. First of all, it should be taken into account that two types of cyber operations take place in cyberspace: internal, which relate to security and defense, and external, which relate to attack or exploitation of cyberspace. ("Cyberspace Operations," 2018). „Cyber operations are the use of cyberspace capabilities to achieve objectives in or through cyberspace.“ (*Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms*, 2016, p. 58).

When it comes to human resources as a factor in armed conflict, the influence of cyberspace can be divided into two segments. The first is the one that precedes the armed conflict itself in which the goal is to obtain enemy data or to protect as much as possible of one's data about individuals or the entire human resources of society that are available for armed confrontation with the enemy. Today's functioning of each individual is unthinkable outside the virtual world where, intentionally or not, a huge amount of data is left behind that can be used to reach conclusions, or information that can be used or be of key importance for the outcome of an armed conflict.

In addition, cyberspace allows for the manifestation of an immediate and constant influence on the enemy's human resources, but also on one's people, which can change things on the ground in an instant. The second segment of influence is the one that is realized during the immediate armed

 doi:10.20944/preprints202412.1099.v1

conflict. The goals are the same as in the first segment, but with a far greater influence of other factors of armed struggle, where, primarily due to the acceleration of the flow of information, the processes of influencing human resources are simplified and accelerated, all to collect data on people as quickly and easily as possible and reach individuals who will receive the data or information with an easily understandable message, which will influence them, a group or the entire composition of the enemy.

Due to all of the above, a very important prerequisite for building human resource resilience in modern armed forces lies in raising awareness and educating personnel, clear and precise regulations, and internal cyber operations that will increase security, enable the flow of information, and exercise control over cyberspace.

Material resources, as the most complex factor of armed struggle, are directly related to the level of development of a particular society. Also, the achieved level of development of a society unambiguously indicates the impact of cyberspace on material resources, primarily because they represent the entire potential of society sublimated into natural, industrial, financial, energy and ICT capacities. Any modern society is capable of waging an armed conflict only if it has built high-quality and comprehensive resistance of the aforementioned segments, but also the ability to constantly threaten enemy material resources with its capacities.

One of the segments of this resilience and capability is the protection and threat of this factor of armed struggle in cyberspace. This is primarily important because today, both in peace and in war, almost no segment of material resources can be used or used for defence without being in some direct or indirect connection with cyberspace, whether it is coal mining or the use of the latest means of warfare. The resilience of material resources in cyberspace is ensured by striving for optimal autonomy, clear and precise regulation, improvements and raising of the work safety culture, and comprehensive cyber operations to increase the security and control of cyberspace.

In every armed conflict, space as a physical phenomenon is divided into several entities (land, sea, air, space). In the past, these entities were divided and had less mutual influence. With technological progress, the entities of space became complementary, with greater interaction, that is, the growth of mutual influence. Today, armed conflict cannot be imagined and waged without the absence of some of the entities of space. Cyberspace, unlike the aforementioned physical entities, has become a place where the entire physical space is unified. Today, it is not possible to wage a modern conflict without the existence of technologies that are connected to such an extent that systems must be developed that help other systems distinguish who is the enemy and who is the friend during the conflict (Identification, friend or foe – IFF), and in what can be called the space of armed conflict. In recent decades, cyberspace has contributed to the loss of a clear definition of space or one of the entities of space, or rather, to the absence of its clear boundaries. It has become irrelevant where and what the "background" is and where the depth of the territory, one's own or the opponent's, is.

The successful functioning of the armed forces in space, and the resilience of the synchronized use of all its components, are conditioned by the capabilities in cyberspace, primarily in the application of a set of state-of-the-art technologies for protection, but also the possibility of unhindered use of all systems that improve the complementarity of the use of military equipment in all components of space. Here, as with the previous factors, legal regulations must be taken into account, as well as the scope of cyberspace used by the armed forces, the security of the aforementioned scope, the development of ICT and the ability to use it.

Time in the context of armed conflict factors manifests itself in many ways. As a determinant of the duration of an activity, as the time of day or year, or as a meteorological phenomenon. Considering that the most important part of this factor is time as a determinant of the duration of an activity, it is easy to conclude how much cyberspace has contributed to the acceleration of activity during armed conflict in recent decades. In earlier times, activity was often conditioned not only by information but also by the speed of its distribution. Often, some of the active actions were implemented in a short time, but the path to it, primarily waiting for the exchange of data, took the most time and therefore the conflicts lasted longer, with a lower degree of loss of effectiveness (people and equipment). Today, with the development of new data transmission technologies that take place in real-time, the duration of armed conflict has been drastically reduced, but also the effectiveness

 doi:10.20944/preprints202412.1099.v1

and efficiency of the use of military equipment have been increased, which in turn has greatly contributed to conflicts ending earlier due to the accelerated loss of human and material resources.

Information as a factor of armed struggle represents the availability of knowledge and data that are necessary for success in a conflict. In addition to the speed of availability of certain information, which is considered timeliness, possession of the necessary reliable information is a prerequisite for victory or avoidance of defeat. The specificity of information lies not only in its complementarity with other factors but also in the fact that in a modern conflict, it has perhaps the greatest influence on the outcome of the same. Information itself is created by collecting, processing and exchanging data on the facts of one's own and enemy factors of armed struggle. It is precisely the development of cyberspace that has enabled the exponential rise of information as a key element for a successful positive end to the conflict.

The development of ICT has enabled, in addition to accessibility, the storage and processing of available information. This has contributed to a change in the balance of power between individual states, because it has made the disposal of military resources in the classical sense less competitive. The war for information, through information and against information in cyberspace itself has in many ways made classical armed struggle much more complicated to wage. Putnik states that "the mastery of information and the establishment of control over it have promoted it into the basic object of cyber warfare, and cyber warfare into the primary form of conflict. Victory in the war for information has become a prerequisite for victory in a traditional military conflict" (Putnik, 2022, p. 90).

Building resilience in the handling of information, its distribution and exploitation represents, in addition to material resources, not only the most complex but also the most important prerequisite for the successful conduct of armed conflict. The set of measures, actions and procedures that must be taken with this goal requires the mobilization of all available resources. The above implies investment in technological progress, the autonomy of ICT systems, comprehensive legal regulation, the security aspect in the broadest sense, but also internal and external cyber operations of the defence system during an armed conflict ("Cyberspace Operations," 2018).

5. The Impact of Artificial Intelligence on the Factors of Armed Struggle

The development of science in most parts of the world is closely linked to military or security issues. Very often, it is the armies that become the first users, even experimental ones, of the latest inventions in science. Putting cyberspace about the factors of armed struggle, it is very easy to conclude that it is precisely military elements that are the actors in the implementation of a large number of activities in cyberspace, which to a certain extent are also characterized as cyber attacks on other entities, broadly speaking.

Modern armies have been actively using artificial intelligence as a tool for working in cyberspace for many years. The reason for using artificial intelligence for military purposes lies in its recognizable definition as a device or set of connected devices that can implement activities that require human intelligence (Galan, Carrasco, & LaTorre, 2022). Although there are levels of artificial intelligence in theoretical considerations, today the artificial intelligence that has segmented capabilities in one field for which it is specialized is still used in practice. Currently, the factors of armed combat abound in enormous amounts of data, be it human resources, material resources, information, and even time as a factor with all its constituent segments. The above data represents an area where, among other things, modern armed forces use artificial intelligence to process this data and obtain conclusions that require the same quality as if a human had analyzed it with his intelligence.

Due to the speed of arrival, quantity and diversity, traditional methods of storing and working with data, such as relational databases, have been replaced by artificial intelligence that allows for almost instantaneous processing of the same. The essence of large amounts of data is not only in processing and analyzing it, but also in predicting and influencing the future with it (Cintiriz, Buhur, & Sensoy, 2015). If data of importance to the armed forces are divided by source, we can classify them as: public (government and public administration); private (legal entities and individuals); data from social networks; secondary data and data on the behaviour and actions of the entity. During an armed

 doi:10.20944/preprints202412.1099.v1

conflict, in addition to the above data sources, a huge number of specific data are obtained from intelligence and reconnaissance activities (George, Haas, & Pentland, 2014).

Modern armed forces use large amounts of data for direct and indirect needs. When it comes to direct needs, these are: familiarization with the intelligence situation and knowledge management; knowledge of the operational situation; decision-making process; cyber defence and attack; information management; military forensics, and geographic information systems. The indirect spectrum of needs is broader and more comprehensive and refers to more complex terms, namely: conventional warfare; counterinsurgency actions; hybrid warfare, asymmetric threats; counter-terrorism; logistics; command and control operations and technology development for military needs (Cintiriz, Buhur, & Sensoy, 2015).

Data processing for the above direct and indirect needs is performed using machine learning. "Machine learning is a branch of artificial intelligence and computer science that focuses on using data and algorithms to imitate the way human learning works, gradually improving its precision or accuracy" (www.ibm.com, 2017). Data processing in this way is necessary not only because of the shorter period until conclusion but also because it processes a large amount of data independently or with minimal human corrective role in the processing process. Machine learning allows for the detection of difficult-to-see logical patterns in data. If we consider the sources of data, their volume, and the needs of the armed forces that can be met by them, the most common areas in which machine learning is applied for military purposes are:

- Combat platforms – They include complex combat systems such as armoured infantry systems, vessels, aircraft, artillery and missile systems, anti-aircraft defence systems, etc. Their characteristic, which are achieved by machine learning, is minimal human intervention during operation, better synergy of all subsystems, and reduced need for maintenance, which collectively implies improving the autonomy and firepower of these assets;
- Cybersecurity of defense capabilities – These capabilities mainly include systems for command, control, communications, computers and computer networks, systems for collecting intelligence, reconnaissance and surveillance, as well as systems for finding, tracking and selecting enemy threats and targets. Machine learning enables the automatic protection of networks, programs and data they use from unauthorized access. In addition, they monitor cyber-attack patterns and develop counterattack tools;
- Logistics and transport – This area uses applications that enable the optimization of defense logistics and transport systems. During armed combat, it is crucial to make the optimal allocation of material resources, military equipment, ammunition, etc. The implementation of machine learning in this area enables timely supply, cost reduction and engagement of the human factor. The use of machine learning is also used at the tactical level, which, for example, in the US armed forces allows for the prediction of necessary maintenance and the prediction of failures in armoured combat vehicles;
- Systems for finding, tracking and selecting threats and targets – In addition to being used for their security in cyberspace, machine learning is also used to understand the zone of operation, through the analysis of intelligence, reconnaissance and other reports, documents and other forms of information obtained from a large number of integrated sensors of various nature, which is a prerequisite for situational awareness on the battlefield, i.e. finding, tracking and selecting threats and targets. These systems are multidisciplinary in nature and are used by all types of armed forces. They are mainly integrated into combat platforms;
- Medical support – Autonomous platforms are used on the battlefield to extract wounded members of the armed forces, and their further medical care, as well as for rapid identification of injuries and diagnoses in combat conditions;
- Training – It involves the use of platforms for exercises through computer simulations and the use of combat platform simulators. Machine learning, through these two platforms, allows the creation of a completely realistic situation for personnel training. In this way, more comprehensive training is achieved for different types and conditions of force engagement and drastic savings of money and time for training purposes are achieved; (Abell, 2020).

 doi:10.20944/preprints202412.1099.v1

In order to be able to round off the issue of the influence of cyberspace and artificial intelligence on the factors of armed conflict, it is necessary to take into account the tendency of development of the so-called Internet of Things (IoT), their connection with cyberspace, the role of artificial intelligence and the further perspective of their use in armed conflicts (for military purposes). Specifically, "the Internet of Things represents an interdisciplinary technology that connects networks, embedded hardware, software, sensor technologies, information management, data analysis and visualization in a single object, while the term thing refers to any controlled device that can be communicated with at a distance and that can collect data (Suri et al., 2016).

The essence of the functioning of IoT is in networking, or the use of networks, therefore their influence permeates all factors of armed combat almost evenly and therefore will not be considered individually for each factor, but rather the focus is on their definition and analysis by certain factors. Currently, modern armed forces mostly use IoT for C4ISTAR systems, which means: command, control, communications, computers, intelligence and surveillance, target selection and reconnaissance. In parallel with the use and procurement of these systems, in recent years, a fifth letter "C" (C5ISTAR) has been added to them, which implies cybersecurity of the use of the system. In other words, IoT for these purposes is improved with a component that enables safe use in cyberspace to the extent possible (www.adsinc.com, 2021). The aforementioned system involves the integrated use of a larger number of devices and platforms. These are networked communication and information devices and platforms (communications means); multi-sensor devices and platforms for data collection, i.e. radars, satellites and unmanned aerial vehicles; electronic warfare systems (electronic reconnaissance and counter-electronic effects) such as specially equipped aircraft, ships or vehicles; a large number of sensors that are integrated on combat and non-combat platforms to collect the necessary data.

The characteristic of IoT for use in the armed forces is that it must be standardized and secure, can connect via wire, satellites, mobile network, radio connection, etc. They use special servers, but also dedicated and public servers depending on the needs and apply modern methods of storing and analyzing large amounts of data using machine learning. Military IoT uses a large number of sensors to collect the largest possible range of data, these sensors, among others, can be: audio, video, biological, atomic, chemical, thermal, radar, laser, RF, infrared, electro-optical, geolocation, for performance measurement, RFID, energy, etc. Devices and platforms on which IoT is used can be personal portable devices, vehicles, ships, aircraft, unmanned systems (air, land and water) and computing devices. The above includes almost the entire spectrum of modern military equipment currently in use. Even devices belonging to the third (obsolete) generation of military equipment have been upgraded in the last ten years in such a way that they can be considered IoT. All of the above devices have their own purpose for which they are used. If we take this purpose as a criterion for division, IoT is divided into:

- Personal IoT – They include tactical communication and information platforms that enable horizontal (between soldiers) and vertical (through the chain of command) communication, as well as platforms that monitor a person's health parameters;
- IoT for situational awareness – They enable satellite navigation, digital maps, the position and layout of their own and enemy forces, monitoring activities and coordination and control on the battlefield. For command personnel, these IoTs provide a broad picture of the operation zone, which is formed by collecting data from subordinate platforms directly on the ground;
- IoT for fire control – They are used in all types of armed forces, primarily for artillery and anti-aircraft fire, for guided missiles on land assets, aircraft, ships, etc. They enable fully autonomous capabilities for the use of firepower. It is reflected in the control of the fire system, tracking over 100 targets simultaneously, target selection and fire that is pinpoint accurate because IoT segments are integrated into the ammunition itself, i.e. in the missiles and artillery shells used today. For this purpose, unmanned aerial vehicles are also widely used, which have become an indispensable integrated part of the fire control system;
- Logistic IoT – They involve the use of IoT for logistics and transport capacities. They are used to monitor the status of stored assets, delivery requests and their transport. In addition to the

 doi:10.20944/preprints202412.1099.v1

above, they can monitor basic logistical parameters of importance on the battlefield. The use goes so far that it is even possible to monitor the use of fuel in military equipment and its availability at distribution points;

- The use of IoT for personnel training – A set of sensors implemented on military equipment enables an exercise in which the participants are fully monitored in real-time. Their activities are sublimated so that trainers have the opportunity to guide the trainees in their actions in real-time. An example of the use of IoT can be taken as the use of the MILES (Multiple Integrated Laser Engagement System). It simulates real infantry combat but uses lasers instead of ammunition. During the exercise, soldiers run out of ammunition, are hit by "bullet or artillery fire" and are thrown out of the vehicle ("wounded or eliminated"). In addition, trainers have an instant overview of the complete situation in an imaginary armed battle. (Zheng & Carter, 2015).

It may be particularly interesting to consider the currently current personal IoT and those that a soldier will use in armed combat shortly. Modern armed forces currently use personal IoT that is predominantly related to communication and is reflected in a networked multifunctional horizontal and vertical connection with other participants in armed combat. Soon, personal IoT is expected to be used in communication (similar to now); situational awareness (tactical multifunctional mobile devices with a large number of additional sensors); medical surveillance (a platform that monitors vital health parameters and diagnoses); electronic warfare (electronic signal jamming devices) and independent power supply of all devices that are expected to be used by a soldier in the future (Fraga-Lamas, 2016).

6. Strategic and Normative Framework

For law, cyberspace represents a new, very dynamic and still incompletely regulated place in which perhaps too rapid changes are taking place, for which the legal order of a society or international organization does not always have an immediate and adequate response. This arises because the law itself represents a set of norms according to which an individual or community should function over a longer period. All norms codified in normative acts shape the legal system that, through public authorities, regulates all aspects of the functioning of the individual and society in general. Unlike law, cyberspace has not been limited by physical boundaries since its inception, and its technological side has enabled rapid changes and evolution of the form and method of functioning (Putnik, 2022).

This situation has forced societies and organizations to actively create and adapt strategic and normative frameworks to changes in cyberspace. Due to the complexity and development of cyberspace, modern societies recognize the need to establish international standards and norms that, following their specificities, would be transferred to the national level. However, establishing these standards, as well as applying existing ones at a time when cyberspace has become very topical and with a large number of states and entities that can exploit it, represents a serious challenge. The securitization of cyberspace is a current international topic with different views on it. Some countries, led by the USA, advocate the application of existing international norms, while others, such as the Russian Federation, emphasize the need to harmonize separate international agreements that would regulate this area.

The absence of a specific and clear source of international law leaves the possibility for countries to independently decide whether, for example, some cyber activity in cyberspace is equated with a kinetic armed attack. In general, taking into account the UN Charter and relevant UN resolutions, it has become an acceptable opinion that cyber operations whose effects are reflected in the destruction or incapacitation of human or material factors of the enemy party can be considered the use of force in international relations, regardless of the weapon used, because they produce the same effects as classical kinetic weapons. However, the question arises as to what to do with those cyber activities that do not do the above, but still have serious consequences for the functioning of society. In addition, it must be further considered that according to UN principles, it is acceptable to use classical armed self-defence only if there is an armed attack on the country.

 doi:10.20944/preprints202412.1099.v1

Due to the existence of a legal vacuum, and the impossibility of fully applying the principle of legal succession, because cyberspace and activities in it differ from the starting principles in international law, i.e. the postulates of the UN, various initiatives have emerged that have addressed this issue. One of the most significant is the NATO initiative, which, over a long period, has brought together interested, prominent experts from several countries who are engaged in studying and organizing the most important facts when it comes to the use of the principles of international law in cyber warfare. So far, this initiative has resulted in the publication of manuals known as the first and second Tallinn Manuals (published in 2013 and 2017 by the University of Cambridge, while the third is currently under development as of 2021). Although they do not represent a legally binding interpretation, they reflect the positions of the authorities of the countries that initiated their publication (primarily NATO countries). Thus, the first manual opens up the possibility of self-defence with kinetic weapons if a cyber attack causes the destruction or incapacitation of the country's human and material factors. The second includes even more broadly the areas that may be affected by cyber activities and establish positions and guidelines for potential action.

At the national level, the success of regulating cyberspace is defined by high-quality inter-sectoral cooperation and a complementary approach to defining norms related to cyberspace. This is achieved through documents such as, in the case of the Republic of Serbia, the Strategy for the Development of the Information Society and Information Security. The general goal of this strategy is, among other things, a developed information society and information security of citizens, public administration and the economy (Strategy for the Development of the Information Society and Information Security in the Republic of Serbia for the Period from 2021 to 2026, 2021). When it comes to the country's defence, the National Security Strategy and the Defense Strategy of the Republic of Serbia are of particular importance. of Serbia, which were adopted in 2019 and which only then, unlike the previous ones from 2009, recognize cyberspace, cyber security and cyber defence as factors influencing the overall security and defence of the country.

The National Security Strategy, when defining the issues of the strategic environment, recognizes that cyber threats can endanger the security of cyberspace through cyber espionage, attacks on critical infrastructure, unauthorized penetration of secret databases, as well as the spread of fake news and disinformation, while the part related to national security policy states that, when it comes to cyber security, it is stated that the ability and capacity to process, transfer and protect information and information and communication systems and defence against hybrid and information warfare techniques in information and cyberspace should continue to be improved. It is also stated that significant attention will be paid to the development of a general security culture of all citizens (National Security Strategy of the Republic of Serbia, 2019).

The Defense Strategy recognizes cyber attacks as part of the factors that negatively affect the security environment through attacks on critical infrastructure facilities and the spread of fake news and disinformation within the concept of hybrid and information warfare. When it comes to challenges, risks and threats, it is stated that cyber attacks on critical infrastructure facilities, high-tech crime, endangerment of information and communication systems, as well as the spread of fake news and disinformation within the concept of hybrid and information warfare, can negatively affect the functioning of elements of the defence system. Therefore, it is necessary to continuously develop technological and information protection of elements of the defence system at all levels of the organization. In the part related to defence policy and protection of the security of the state and citizens, the need to improve cybersecurity is recognized through improving the capabilities and capacities for coordinating work aimed at achieving cybersecurity and protecting against security risks in information and communication systems. The need to formulate a clear and coherent policy to increase the resilience of the aforementioned systems to incidents, to establish a network of competent entities for the fight against cyber actions and crime, as well as to improve cooperation between the public and private sectors in the field of cybersecurity is also recognized (Defense Strategy of the Republic of Serbia, 2019).

When, after the strategic framework, the normative framework is taken into consideration, it is important to first point out that it must, in addition to monitoring the development of cyberspace,

 doi:10.20944/preprints202412.1099.v1

also have a guiding role based on the prediction of the further development of that space in a particular society but also internationally. In the case of the Republic of Serbia, by assuming or accepting international obligations, the normative framework for cyberspace began to develop almost two decades ago by adopting laws and enacting individual bylaws that elaborated the laws in more detail. At the very beginning, the Criminal Code and the Code of Criminal Procedure were amended, which defined the penalties and criminal procedure by which a criminal offence is established in cyberspace (Criminal Code, 2019) (Criminal Code, 2021).

Also, back in 2005, among other things, the law regulated the detection, prosecution and trial of criminal offences against the security of computer data as defined in the Criminal Code (Law on the Organization and Competence of State Bodies for the Fight against High-Tech Crime, 2023). The aforementioned law is constantly being adapted so that it experienced its last amendments in early 2023. After the above, when it comes to comprehensive cybersecurity, the Law on the Security and Information Agency and the Law on the Military Security and Military Intelligence Agency are characteristic. The former, in certain cases, allows, with the consent of the court, secret surveillance and recording of communications regardless of the form and technical means used, as well as static electronic surveillance of communications and information systems (Law on the Security and Information Agency, 2018). The second one regulates that the Military Security Agency implements measures to preserve the security of assets, data, industry, information and communication systems and cryptographic protection, as well as to detect and investigate acts that threaten classified data and the security of computer data. It also regulates that the Military Intelligence Agency may acquire, develop and use information systems and data transmission systems, as well as means of protecting information (Law on the Military Security and Military Intelligence Agency, 2013). Following these laws, laws dealing with data protection were successively adopted in the Republic of Serbia. These laws regulated the collection, processing and protection of personal data, information of public importance, secret data, business and professional secrets (Law on the Protection of Personal Data, 2018) (Law on the Protection of Business Secrets, 2021). In parallel with these laws, due to the expanding use of ICT, the Law on Electronic Communications was adopted, which comprehensively regulated electronic communications and electronic communications networks, and in a certain way regulated their security with the associated characteristics and priorities of the use of information networks for security and defense purposes (Law on Electronic Communications, 2023).

Following the above regulations, as a result of the further expansion of the use of cyberspace and the importance of the actions taking place in it, the obligation and need to adopt the Law on Information Security (first adopted in 2016, with the latest amendments and supplements in 2019) became mandatory. The above regulation establishes a system for the detection and prevention of cyber attacks, defines the obligations, powers and coordination of existing and new entities (created by the adoption of the law) in cyberspace and in the event of cyber attacks. The law establishes the basic principles of the protection of information and communication systems (risk management, comprehensiveness, as well as awareness and capability). Systems of particular importance are defined, which to a certain extent coincide with the factors of armed conflict, primarily when it comes to human and material resources, but also time, space and information. The National Center for the Prevention of Security Risks in Information and Communication Systems (better known as the National CERT) has been established, as well as centers of government bodies and independent system operators with their respective areas of competence. The system for the functioning of cryptosecurity and protection against compromising electromagnetic radiation has been completed (Information Security Act, 2019).

Despite the progress made so far in the aforementioned strategies and laws, this progress is not sufficient in itself; rather, for the sake of a comprehensive and clear state response to contemporary challenges, risks and threats, it is necessary to adopt, following the example of most modern societies, an adequate national cybersecurity strategy and a national cyber defense strategy, which would be accompanied by additional legal solutions. The adoption of the aforementioned strategies and laws would be a prerequisite for creating an adequate legal framework for cybersecurity that includes "regulations regulating the responsibilities of authorities for managing security risks in information

 doi:10.20944/preprints202412.1099.v1

and communication systems and suppressing actions that threaten or disrupt the functioning of these systems, as well as norms on protection techniques, methods and procedures, coordination between protection actors, their responsibility and supervision over the implementation of legal powers and obligations" (Milošević & Putnik, 2017, p. 180).

To develop a comprehensive and complete strategic or legal framework for cybersecurity, it is necessary to understand and understand the principles of cyber warfare. The first eight principles were defined by Parks and Duggan at the beginning of the 21st century (Parks & Duggan, 2001). They are: (1) Cyber warfare must have concrete effects in the real world; (2) One party may take active steps to hide in the cyber world, but everything someone does is visible, the only question is whether anyone is watching; (3) There is no unchanging behavior in cyberspace, except for that which requires action in the physical world; (4) Some entities in the cyber world have authorization to enter or perform any action that the attacker wants to be performed. The attacker's goal is to take the identity of these entities; (5) Cyber warfare tools have a dual role; (6) Attackers and defenders control a very small portion of the cyberspace they use. Whoever controls the portion of cyberspace used by an adversary can control the adversary; (7) Cyberspace is inconsistent and unreliable; (8) Physical constraints such as distance and space are not applicable in cyberspace.

Finally, the ninth principle, which emerged in the past decade, is defined by Putnik and Milošević as follows: “The assessment of security risks and threats in cyberspace is based primarily on the exponential law, while in the physical world it is based on the law of normal distribution” (Putnik, Milošević, & Bošković, 2017, p. 181).

One’s own military power, as well as that of the opponent, is traditionally viewed through the factors of armed combat. Often, these factors are easily measurable and comparable in armed conflict (number and training of personnel, types and number of military equipment, “depth of territory”, infrastructure, etc.). However, with the emergence of cyberspace and the shaping of the principles of cyber warfare, the initial assumptions about one’s own and the enemy’s capacities are being questioned. The aforementioned principles of cyber warfare today change the perspective of armed combat factors in such a way that their importance is quite easily changed, or reduced.

Adopting appropriate strategies and further regulating the normative framework of cyberspace requires a different methodology than that applicable in the physical world. “Cyberspace is a realm of extreme events. Strategies that are considered good in physical warfare may be ineffective, even dangerous, in cyberspace. Entities in cyberspace behave significantly differently from what military experts are used to. It is almost certain that most entities within cyberspace, such as the physical and organizational topology of the network, undergo changes, most often in accordance with the exponential law. All activities that are carried out with the aim of carrying out attacks in cyberspace and causing damage to the adversary are also subject to this law. An adequate cyberspace defence policy should properly anticipate the challenges of exponential distribution, but also fully respect other principles of cyber warfare, which undoubtedly question traditional principles of defence planning, both from an organizational and economic perspective.” (Putnik, Milošević, & Bošković, 2017, p. 183).

The normative framework, developed on the above-mentioned principles, will enable the development of comprehensive resilience and protection of the factors of the armed struggle of a society in cyberspace. It will also have elements of prediction and successful guidance for the further development of cyberspace. In addition, it will contribute to raising awareness, knowledge and security culture in the broadest sense of the word, regardless of whether it is an ordinary citizen, a public institution, a private company or a scientific institute.

7. Conclusion

The general acceleration of processes in modern societies enabled by cyberspace and the development of ICT has brought a still unimaginable leap forward in overall progress. With it, the processes that bring about conflicts have also accelerated. Modern conflicts have changed their physiognomy compared to the conflicts that marked the 20th century, however, the goals for which they are fought have remained the same. Modern conflicts, although shorter, have become more

 doi:10.20944/preprints202412.1099.v1

comprehensive because they include all aspects of a society participating in an armed conflict. The factors of armed conflict represent everything decisive that a society can include in an armed conflict. Modern conflicts are also characterized by greater interconnectedness and mutual influence of the factors of armed conflict. Cyberspace, as a new circumstance, in the context of the history of armed conflicts, has brought about major changes, that is, its influence on the factors of armed conflict.

Each of the factors of armed conflict in the last few decades, due to the emergence of cyberspace, has begun to change almost completely, and the mutual influence has become such that the factors have become intertwined and dependent on each other. Cyberspace is still something new for some armed forces, for some, it is largely a part of space as a factor of armed conflict, while for a certain number of armed forces cyberspace has taken shape and can be considered a separate factor of armed conflict. It is unnecessary to talk about the connection and dependence of the human factor on cyberspace when every person is "online". The same can also be said for information. Material resources are currently characterized by the greatest changes, because in addition to technological progress, ICT with all its features are being implemented in. For modern armed forces, material resources represent a connection between cyberspace and the physical world. Artificial intelligence capabilities, interconnected resources and the development of IoT have completely changed the capabilities of the armed forces. Cyberspace for the armed forces represents the potential for victory but also the danger of losing in an armed conflict. The legal framework and normative order in a society must keep pace with the development, opportunities and dangers of cyberspace. The above can be considered preventive action and a prerequisite for building resilience to the factors of armed conflict.

The coming decades will be challenging for modern armed forces because cyberspace will require a change in the factors of armed combat compared to today's. Completely different capacities and abilities will be required from people. Completely new means of warfare will be used, which will be almost entirely IoT. Material resources and the optimization of their use through new scientific achievements will have much greater importance for armed conflict. The availability and flow of information will take on a completely different dimension. Time and space will lose the importance they had and still have, except for time as a determinant of the duration of activities because many processes will take place almost instantly, unlike today.

Due to its connection and influence on other factors of armed combat, cyberspace will take on the characteristics of a separate factor, which, according to its characteristics, will be the most important and decisive factor of armed combat shortly.

Funding: This research was funded by the Scientific–Professional Society for Disaster Risk Management, Belgrade (https://upravljanje-rizicima.com/, accessed on 24 September 2024), and the International Institute for Disaster Research (https://idr.edu.rs/, accessed on 24 September 2024), Belgrade, Serbia.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Acknowledgements: The authors acknowledge the use of Grammarly Premium and ChatGPT 4.0 in the process of translating and improving the clarity and quality of the English language in this manuscript. The AI tools were used to assist in language enhancement but were not involved in the development of the scientific content. The authors take full responsibility for the originality, validity, and integrity of the manuscript.

References

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. (2023). *"Službeni glasnik RS", br. 61 od 18. jula 2005, 104 od 16. decembra 2009, 10 od 9. februara 2023, 10 od 9. februara 2023 – dr. zakon*.

(2017, mart 17). Preuzeto Januar 15, 2023 sa www.ibm.com: https://www.ibm.com/topics/machine-learning

(2021, oktobar 21). Preuzeto januar 14, 2023 sa www.adsinc.com: https://www.adsinc.com/news/c4isr-vs-c5isr-what-is-the-difference

Abell, N. (2020, oktobar 2). Preuzeto januar 15, 2023 sa https://medium.com: https://medium.com/@nqabell89/7-key-military-applications-of-machine-learning-9818dfa2ea86

Cintiriz, H., Buhur, M. N., & Sensoy, E. (2015). Military Implications of Big Data. *Proceedings of the International Conference on Military and Security Studies 2015* (str. 55-60). Istanbul: Turkish Army War College.

Cyberspace Operations. (2018, jun 8). Preuzeto januar 13, 2023 sa https://irp.fas.org/doddir/dod/jp3_12.pdf

Fraga-Lamas, P. F.-C.-A.-L. (2016). A Review on Internet of Things for Defense and Public Safety. *Sensors, 10*. doi:https://doi.org/10.3390/s16101644

Galan, J. J., Carrasco, R. A., & LaTorre, A. (2022, april 22). Military Applications of Machine Learning: A Bibliometric Perspective. *Mathematics, 10*.

George, G., Haas, M., & Pentland, A. S. (2014). Big Data And Management. *Academy of Management Journal*, 321-326.

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of The Hybrid Wars.* Arlington: Potomac Institute for Policy Studies.

Hybrid Warfare: A New Phenomenon in Europe's Security Environment. (2016). Prague: Jagello 2000 for NATO Information Centre in Prague.

Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms. (2016). Washington, D.C.: Joint Chiefs of Staf.

Lind, W. S., & Thiele, G. A. (2015). *4th Generation Warfare Handbook.* Kouvola, Finland: Castalia House.

National Security Strategy. (2022, oktobar 12). Preuzeto decembar 15, 2022 sa whitehouse.gov: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

North Atlantic Treaty Organization. (2022, mart 23). Preuzeto decembar 25, 2022 sa https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

Parks, R. C., & Duggan, D. P. (2001). Principles of Cyber-warfare. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 122-125.

Putnik, N., & Milošević, M. (2018). Trends in Peace Research - Can Cyber Detente Lead to Lasting Peace. U B. Cook (Ur.), *Handbook of Research on Examining Global Peacemaking in the Digital age* (str. 1-19). Hershey: IGI Global.

Suri, N., Tortonesi, M., Michaelis, J., Budulas, P., Benincasa, G., Russell, S., & Winkler, R. (2016). Analyzing the applicability of internet of things to the battlefield environment. *2016 international conference on military communications and information systems (ICMCIS)*, (pp. 1-8). Brussels. doi:10.1109/ICMCIS.2016.7496574

Zheng, D. E., & Carter, W. A. (2015). *Leveraging the Internet of Things for a More Efficient and Effective Military.* Washington, DC: Center for Strategic and International Studies.

Vojska Srbije. (2010). Preuzeto decembar 10, 2022 sa https://www.scribd.com/doc/270209153/Doktrina-Vojske-Srbije-kraj

Vojska Srbije. (2022). Preuzeto januar 10, 2023 sa https://www.vs.rs/sr_cyr/medjunarodna-saradnja/partnerstvo-za-mir/koncept-operativnih-sposobnosti

Zakon o Bezbednosno-informativnoj agenciji. (2018). *„Službeni glasnik RS", br. 42 od 19. jula 2002, 111 od 29. decembra 2009, 65 od 27. juna 2014 - US, 66 od 29. juna 2014, 36 od 10. maja 2018.*

Zakon o Vojnobezbednosnoj i Vojnoobaveštajnoj agenciji. (2013). *„Službeni glasnik RS", br. 88 od 28. oktobra 2009, 55 od 1. juna 2012 - US, 17 od 21. februara 2013.*

Zakon o elektronskim komunikacijama . (2023). *"Službeni glasnik RS", broj 35 od 29. aprila 2023.*

Zakon o zaštiti podataka o ličnosti. (2018). *"Službeni glasnik RS", broj 87 od 13. novembra 2018.*

Zakon o zaštiti poslovne tajne. (2021). *"Službeni glasnik RS", broj 53 od 28. maja 2021.*

Zakon o informacionoj bezbednosti. (2019). *Službeni glasnik RS br. 6 od 28. januara 2016, 94 od 19. oktobra 2017, 77 od 31. oktobra 2019.*

Zakon o informacionoj bezbednosti. (2019). *"Službeni glasnik RS", br. 6 od 28. januara 2016, 94 od 19. oktobra 2017, 77 od 31. oktobra 2019.*

Zakonik o krivičnom postupku. (2021). *"Službeni glasnik RS", br. 72 od 28. septembra 2011, 101 od 30. decembra 2011, 121 od 24. decembra 2012, 32 od 8. aprila 2013, 45 od 22. maja 2013, 55 od 23. maja 2014, 35 od 21. maja 2019, 27 od 24. marta 2021 - US, 62 od 17. juna 2021 - US.*

Krivični zakonik. (2019). *"Službeni glasnik RS", br. 85 od 6. oktobra 2005, 88 od 14. oktobra 2005 - ispravka, 107 od 2. decembra 2005 - ispravka, 72 od 3. septembra 2009, 111 od 29. decembra 2009, 121 od 24. decembra 2012, 104 od 27. novembra 2013, 108 od 10. oktobra 2014, 94 od .*

Milošević, M., & Putnik, N. (2017). Sajber bezbednost i zaštita od visokotehnološkog kriminala u Republici Srbiji–strateški i pravni okvir. *Kultura polisa*, 177-191.

Putnik, N. (2022). *Sajber rat i sajber mir.* Beograd: Univerzitet u Beogradu - Inovacioni centar Fakulteta bezbednosti.

Putnik, N., Milošević, M., & Bošković, M. (2017). Strateško planiranje sajber odbrane - ka adekvatnijem pravnom okviru i novoj koncepciji procene rizika, izazova i pretnji. *Vojno delo*, 174-185.

Strategija nacionalne bezbednosti Republike Srbije. (2019). *Službeni glasnik RS, broj 94 od 27. decembra 2019.*

Strategija odbrane R. Srbije. (2019). *Službeni glasnik RS, broj 94 od 27. decembra 2019.*

Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine. (2021). *Službeni glasnik RS broj 86 od 3. septembra 2021.*

Alemzadeh, M. (2023). Iran Protests and Patterns of State Repression. *Iranian Studies, 56*, 557-561. doi:10.1017/irn.2023.16

Babulak, E. (2010a). The 21st century cyberspace. *2010 IEEE 8th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 21-24. doi:10.1109/SAMI.2010.5423748

Babulak, E. (2010b). Keynote Speaker 3. doi:10.1109/AMS.2010.12

Bandura, A. (1999). Moral Disengagement in the Perpetration of Inhumanities. *Personality and Social Psychology Review, 3*, 193-209. doi:10.1207/s15327957pspr0303_3

Bogdanoski, M., & Milkovski, N. (2015). Information as a strategic resource critical to military operations and defence of the nation. Retrieved from https://consensus.app/papers/information-as-a-strategic-resource-critical-to-military-bogdanoski-milkovski/4a4330f794065928911ab7d9a5448944/

Chatinakrob, T. (2024). Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty. *Chinese Journal of International Law*. doi:10.1093/chinesejil/jmae005

Chkhikvishvili, G., & Beridze, S. (2024). Technological Progress in International Armed Conflicts. *Works of Georgian Technical University*. doi:10.36073/1512-0996-2024-2-294-300

Creveld, M. (1992). High technology and the transformation of war part II. *RUSI Journal, 137*, 61-64. doi:10.1080/03071849208445662

Cvetković, V. (2024a). Disaster Resilience: Guide for Prevention, Response and Recovery. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.

Cvetković, V. (2024b). Disaster Risk Management. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.

Cvetković, V. M., & Šišović, V. (2024). Community Disaster Resilience in Serbia. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.

Cyberspace Operations. (2018).

Dexia, W. (2012). On the Effect of Scientific and Technological Progress and Its Applications in the Various Factors of Military Transformation. Retrieved from https://consensus.app/papers/on-the-effect-of-scientific-and-technological-progress-and-dexia/58a435cfd842534ea7ad52fb1d5ed5ca/

Dobash, R., Dobash, R., Cavanagh, K., & Lewis, R. (1996). Changing Violent Men. *Probation Journal, 43*, 217-218. doi:10.1177/026455059604300409

Friedmann, G. (1952). Technological Change and Human Relations. *British Journal of Sociology, 3*, 95. doi:10.2307/587488

Gareev, G. (2001). Problems of maintaining defense security in today's world. *European Security, 10*, 34-44. doi:10.1080/09662830108407503

Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security, 43*, 141-189. doi:10.1162/isec_a_00337

Grozdanić, G., & Cvetković, M. V. (2024). Exploring Multifaceted Factors Influencing Community Resilience to Earthquake-Induced Geohazards: Insights from Montenegro. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.

Hall, W. (2018). The Power of Will in International Conflict. doi:10.5040/9798400699825

Herolf, G. (1988). New technology favors defense. *Bulletin of The Atomic Scientists, 44*, 42-44. doi:10.1080/00963402.1988.11456200

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of The Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Howe, J. (2006). Technology strategy and innovation in the defence context. 51-54. doi:10.1049/IC:20060225

Hubert, P. (2017). Déflagrant Délit. *Leonardo, 30*, 78-80. Retrieved from https://consensus.app/papers/d%C3%A9flagrant-d%C3%A9lit-hubert/2af0092ec4b65fe2a11a22df9b8439b5/

Hybrid Warfare: A New Phenomenon in Europe's Security Environment. (2016). Prague: Jagello 2000 for NATO Information Centre in Prague.

Johnson, J., Davis, R., Wester, R., Exner, F., Cowan, C., Patel, M., . . . Nachenberg, C. (1997). The military impact of information technology. *Communications of The ACM, 40*, 20-22. doi:10.1145/248448.248453

Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms. (2016). Washington, D.C.: Joint Chiefs of Staf.

Kellerman, A. (2010). Mobile Broadband Services and the Availability of Instant Access to Cyberspace. *Environment and Planning A, 42*, 2990-3005. doi:10.1068/a43283

Kier, E. (1995). Culture and Military Doctrine: France between the Wars. *International Security, 19*, 65-93. doi:10.2307/2539120

Kolganov, A. (2022). Fundamental civilizational shifts from the point of view of the method of political economy. *Noonomy and Noosociety. Almanac of Scientific Works of the S.Y. Witte INID*. doi:10.37930/2782-618x-2022-1-3-93-105

Kristoferson, L. (1981). Modern Weapons and the Environment. *Environmental Conservation, 8*, 257-258. doi:10.1017/S0376892900027909

Kupchyn, A., Dykhanovskyi, V., & Kolotukhin, Y. (2020). The war of the future as a strategic guideline for the forming the critical technologies list. *Journal of Scientific Papers "Social development and Security"*. doi:10.33445/sds.2020.10.1.2

Lan, T. (2021). Community of Common Future in Cyberspace. *The Oxford Handbook of Cyber Security*. doi:10.1093/oxfordhb/9780198800682.013.40

Libicki, M., Gompert, D., Frelinger, D., & Smith, R. (2007). Byting Back-Regaining Information Superiority Against 21st-Century Insurgents. Retrieved from https://consensus.app/papers/byting-backregaining-information-superiority-against-libicki-gompert/3f0c43f0090157debf049efb805ac3dd/

López, A. (2020). Necropolitics in the "Compassionate" City: Care/Brutality in San Francisco. *Medical Anthropology, 39*, 751-764. doi:10.1080/01459740.2020.1753046

Mbanaso, P., & Dandaura, P. E. S. (2015). The Cyberspace: Redefining A New World. Retrieved from https://consensus.app/papers/the-cyberspace-redefining-a-new-world-mbanaso-dandaura/12d1701141b65fe38975b33312fd62ab/

Milenković, D., Cvetković, V., & Renner, R. (2024). A Systematic Literary Review on Community Resilience Indicators: Adaptation and Application of the BRIC Method for Measuring Disasters Resilience. *Preprints*, 2024102277.

Milinovic, M., & Ivaniš, Ž. (2015). Advanced military concepts and organizations determined by technology requirements. 429-450. doi:10.2298/zmsdn1552429m

Muller, L. (2015). Cyber Security Capacity Building in Developing Countries. Retrieved from https://consensus.app/papers/cyber-security-capacity-building-in-developing-countries-muller/4e1728e1f9ee518b8d2663fea59c3248/

Neculcea, C.-A. (2021a). Information Operations. The Adequate Communication Response to Contemporary Threats. *Romanian Military Thinking*. doi:10.55535/rmt.2021.4.05

Neculcea, C.-A. (2021b). Operaţiile informaţionale – răspunsul comunicaţional adecvat la ameninţările contemporane. *Gândirea Militară Românească*. doi:10.55535/gmr.2021.4.05

Pysarenko, T., Kvasha, T., Bohomazova, V., Paladchenko, O., Molchanova, I., & Shabranska, N. (2024). Defense-industrial complex: scientific and technological trends. doi:10.35668/978-966-479-140-0

Reese. (2020). Operations in the Information Environment Application of the direct and indirect approach for by LtCol C. Retrieved from https://consensus.app/papers/operations-in-the-information-environment-application-of-reese/473f67141c1c596d9dceccd2a046461e/

Santala, R. (2004). Don't Start the Revolution Without Me: A Review of the Army Transformation. Retrieved from https://consensus.app/papers/dont-start-the-revolution-without-me-a-review-of-the-army-santala/5a46ed75c23a580a81e2a754ec9741c5/

Schinkel, W. (2004). The Will to Violence. *Theoretical Criminology, 8*, 31-35. doi:10.1177/1362480604039739

Serrano, Y., & López, W. (2008). Estrategias de comunicación militar y dinámicas mediáticas ¿dos lógicas contradictorias? , *4*, 269-277. doi:10.15332/S1794-9998.2008.0002.04

Sim, S. (2023). The Development of Digital Technologies and Cyber Security Threats. *Sungshin Women's University Center for East Asian Studies*. doi:10.56022/ceas.2023.29.1.197

Stepanyants, M. (2022). Problems of Civilizational Development in the Leading Countries of the Asian Region. *Voprosy Filosofii*. doi:10.21146/0042-8744-2022-7-5-14

Tanasić, J., & Cvetković, V. (2024). The Efficiency of Disaster and Crisis Management Policy at the Local Level: Lessons from Serbia. In: Scientific-Professional Society for Disaster Risk Management, Belgrade.

Toroi, G.-I. (2021). Information activities – essential warfighting function in today's military operations. Retrieved from https://consensus.app/papers/information-activities-%E2%80%93-essential-warfighting-function/86c0c34fb67552999a305200b7fd80df/

Townsend, T., Dillard-Wright, J., Prestwich, K., Alapatt, V.-A., Kouame, G., Kubicki, J., . . . Williams, C. (2023). Public safety redefined: Mitigating trauma by centering the community in community mental health. *The American psychologist, 78 2*, 227-243. doi:10.1037/amp0001081

Urbatsch, R. (2021). Physical formidability and acceptance of police violence. *Evolution and Human Behavior*. doi:10.1016/J.EVOLHUMBEHAV.2021.03.008

Van Swol, L., Prahl, A., MacGeorge, E., & Branch, S. (2019). Imposing Advice on Powerful People. *Communication Reports, 32*, 173-187. doi:10.1080/08934215.2019.1655082

Westing, A. (1988). The Military Sector vis-à-vis the Environment. *Journal of Peace Research, 25*, 257-264. doi:10.1177/002234338802500305

Wilén, N., & Strömbom, L. (2021). A versatile organisation: Mapping the military's core roles in a changing security environment. *European Journal of International Security, 7*, 18-37. doi:10.1017/eis.2021.27

Zgirovskaya, E. V. (2023). Providing scientific and technological progress as a function of the modern state. *Proceedings of the 6th International Conference "Futurity designing. Digital reality problems"*. doi:10.20948/future-2023-12

Ноономика, Б. С. Д., Альманах, Н., С.Ю, И. И., Том, В., Бодрунов, С. Д., Нообщество, Н., 新兴工业发展研究所，俄罗斯圣彼得堡，博. (2022). Scientific and technological progress and transformation of society: noonomy and noosociety. Part 1. *Noonomy and Noosociety. Almanac of Scientific Works of the S.Y. Witte INID*. doi:10.37930/2782-618x-2022-1-1-24-42

Putnik, N. (2022). *Sajber rat i sajber mir*. Beograd: Univerzitet u Beogradu - Inovacioni centar Fakulteta bezbednosti.