SAFETY&DEFENSE

2021
ISSN: 2450-551X
Volume 7 Issue 1

Centrum Rzeczoznawstwa Budowlanego

ANDARTA
Fundacja Nauka dla Bezpieczeństwa

SAFETY & DEFENSE

Volume 7 Issue 1 (2021)

"Science for Knowledge, Knowledge for Safety & Defense"

ISSN:2450-551X

Table of Contents

Dear Readers,

In 2021, we present you the first issue of “Safety & Defense.” On this occasion, on behalf of the Editorial Board, I would like to thank all the authors for their very interesting papers and the reviewers for the effort put into evaluating the submitted articles. As always, we would like to invite everyone interested in issues related to safety and defense to send their work to our journal. I would also like to emphasize that the efforts devoted so far to the qualitative development of the journal have been recognized and appreciated. In the recent 2021 update of the Polish Ministry of Education and Science journal list, “Safety & Defense” was awarded a high score of 70 points.

Bearing in mind the prospect of further development, we will be grateful for any support for our journal and for sharing your personal opinions, observations, or comments.

In this issue of "Safety & Defense," there are ten peer-reviewed papers that constitute an interesting review of theoretical and empirical research conducted in various areas of military and non-military security.

The opening paper discusses the issues recognized as crucial for information security in the armed forces. In this regard, the main findings indicate that the information security system of the armed forces will play an increasingly important role in shaping the state's security. For this reason, among many others, it should be treated as a priority.

The current issue also includes very interesting considerations describing the methods, techniques, and tools used to manipulate public opinion, including disseminating disinformation, which is seen as one of the severe threats to national security. The paper describes how propaganda can be spread using social media, such as Twitter, Facebook, and other websites.

The next paper focuses on the issues related to identifying trends in the development of Russian precision guidance weapons. The research established that the Russian way of thinking about the strategic use of precision weapons evolved alongside the development of technology, economic opportunities, and changes in Russia's foreign policy. According to the author, the new generation of precision and hypersonic weapon systems will be decisive regarding the outcome of future armed conflicts.

Equally interesting are the results of the research, the scope of which includes the assessment of cooperation between Great Britain and Kenya in the area of defense and security in the second decade of the 21st century. In addition to the theoretical aspects, the article focuses on the conditions of cooperation considering defense and security, restoring peace in Somalia, and strengthening the level of security in Kenya and East Africa.

The next paper focuses on strategic research and its role and importance in shaping the state's security and defense policy. The article emphasizes the unique mission of strategic studies institutes, which are the fundamental entities providing strategic expertise at the request of state authorities. The author, as an example, describes the activities of the *Institut de Recherche Stratégique de l'École Militaire* – IRSEM. The paper concludes with the thesis that the Institute’s activities play a significant role in shaping France's security and defense policy.

The concept of using a swarm of drones in future military operations is the subject of the following article. In the paper, it was emphasized that the use of drones instead of manned planes should be taken into account in the near future. It primarily refers to deep military operations where there is a high risk of losing manned aircraft. Based on the presented research results, it can be concluded that drone swarms have much greater combat capabilities compared to a single use of unmanned aerial vehicles.

The use of unmanned aerial systems was also addressed in the next paper. In this case, considerations focus on the capabilities of air defense means to counter unmanned aerial systems. The article discusses the development of unmanned aerial vehicle systems through the prism of changes in the conceptions of air defense organization for essential state resources.

Threats stemming from the activities of individual terrorists known as the so-called “lone wolves" are the subject of the following paper. The author focuses on several aspects of how lone wolves operate, including tactics and the current and future measures they employ. The final part of the paper is dedicated to the prognosis of the development of this phenomenon in the future.

The following article deals with the issues related to the organization of air defense. However, the paper's primary focus is on Russia's actions to secure the 2014 Sochi Winter Olympics. The research took into account the threats resulting from the geographical location of Sochi and the political situation, as well as the increasing national liberation trends and acts of terror during this period in the region. The research confirmed that the identified threats had a significant impact on the organization of the security system, its costs, and the scale of the forces and military resources used, including air defense systems.

The last paper presented in the current issue of Safety & Defense closes the article, focuses on the political aspects of the development of anti-satellite weapons. The article highlights the space rivalry among the United States and Russia, and China. On the one hand, the United States is struggling to maintain its dominant position as a space power; on the other, its most dangerous opponents are trying to develop technologies that will reduce the American advantage. There is no doubt that there will be numerous objects in outer space designed to destroy enemy satellites in orbit in the near future.

We hope you enjoy this latest issue.

Adam Radomyski
Editor In Chief

SAFETY&DEFENSE
ISSN 2450-551X

The Importance of Military Information Security

Wojciech SŁUGOCKI[1*], Marzena WALKOWIAK[2]

[1] Military University of Technology, Warsaw; slugockywoj@gmail.com,
ORCID: 0000-0003-0275-8096
[2] Military University of Technology, Warsaw; marzena.walkowiak@wat.edu.pl,
ORCID: 0000-0002-3317-562X
* Corresponding author

DOI: https://doi.org/10.37105/sd.93

Abstract

The main goal of the research is to identify the key problems related to information security in the armed forces and to classify the most important factors and aspects necessary to increase security. The implemented research methods include a critical analysis of legal acts, organizational and competence documents, literature on the subject. Synthesis and inference were employed to achieve the formulated goals. The main findings indicate that the armed forces' information security system will play an increasingly important role in shaping the security of modern states and should be treated as a priority. The results of the analyzes indicate that in the coming years, the main challenge of modern armies will be to strengthen the offensive and defensive information capabilities of the state. The general findings of this article present the view that information security is a key task for the armed forces to ensure national security. Therefore, it is necessary to revise, clarify and tighten up the procedures in force for the protection of key information processed in the state - especially in the armed forces – which should have adequate capabilities to conduct complex operations in cyberspace. Moreover, the need for a thorough and comprehensive analysis of this topic is confirmed.

Keywords

information security, national security, military security, safety.

Submited: 26.01.2021. Accepted: 23.02.2021. Published: 11.03.2021.

1. Introduction

The need to ensure the security of important information is becoming a growing challenge for state institutions, mainly due to the emergence of new threats resulting from the progressive computerization, globalization and digitization of the modern world. It could be argued that "for a modern state community, the threats of information crimes, i.e. cybercrime, will be particularly significant. The increase in the importance of information, the development of IT infrastructure and technologies has created a completely new sphere of social activity, and at the same time a platform for competition and possible abuse and crime cyberspace" (Szczurek, Walkowiak & Bryczek-Wróbel, 2020, p. 86). Moreover, there are a number of categories of information whose protection seems particularly important from the point of view of the state's interest. Such data includes messages processed in the armed forces of modern countries.

The concept of state information security began to appear in literature in the second half of the 20th century. However, this does not mean that information was not previously viewed as a security factor. Reliable, accurate and up-to-date information has always been important for state decisions, especially in the field of security – both external and internal. Following the history of this topic, it can be concluded that, traditionally, information security was understood as a conglomerate of several elements. First, it was to ensure access to information about the environment, potential enemies and allies. Secondly, it is the protection of state information, the disclosure of which would violate the interests of a given entity (Aleksandrowicz, 2018).

The main research problem is contained in the following question: What are the challenges in the area of information security in the armed forces of modern countries resulting from the need to ensure the security of the state and its citizens? This main problem was divided into two more specific questions:

- What is the significance of information security for the security of the state and its citizens?
- What are the challenges facing the modern armed forces in the area of information security?

Based on the analyzes conducted so far and after a preliminary study of the literature on the subject related to the research problem formulated above, the following hypothesis was adopted: the information security of the modern armed forces requires further strengthening and improvement with a particular emphasis on classified information and personal data.

The aim of the research was to identify key problems related to the organization of data security in the armed forces and identify the most important elements requiring change or improvement. Therefore, the factors that have an impact on the analyzed issues have been specified, performing conceptual work on improving data protection in the armed forces.

Research methods and techniques used in the research process are mainly based on a critical analysis of the literature on the subject, legal acts, organizational and competence documents, and synthesis and inference.

2. Terminology-related arrangements

The concept of security is understood in many ways. Therefore, when attempting to define and redefine (extend) the contemporary understanding of security (Mathews, 1989), it should be taken into account that it is a social phenomenon that covers many disciplines and scientific specialties. As Koziej (2006, p.7) analyzes: "security in the static sense is a state of no threats to the subject, a state of peace, certainty, an objective and subjective state: conscious and unconscious. Security in the dynamic sense (acting for the benefit of security) [is] the process of achieving and maintaining the state of no threats and freedom of action". The concept of security in the most general terms should be classified into a group of subjective needs and the need for security should be included in existential needs. Zięba (2008a), on the other hand, identified security with the certainty of existence and survival, possession, functioning and development of the subject, which arises as a result of the creative activity of a given subject and is variable over time, i.e. it has the nature of a social process. The concept of security refers to an extremely complex phenomenon, including not only the state of securing the vital interests of society (individuals, social groups, nation) against direct threats but also ensuring conditions conducive to the undisturbed functioning of all the processes ensuring the sustainable development of protected entities or at least ensuring their stability and sovereignty (Nowakowski, 2009).

As Zięba (2008b, pp.17-18) claims, the safety classification can be adapted according to the following criteria:

- "Subjective: national security and international security.
- Subject: political, military, economic, social, cultural, ideological, ecological, information security etc.
- Spatial: personal security (concerning individual people), local (state-national), subregional, regional (coalition), supra-regional and global (global, universal).
- Time: the state of security and the safety process".

From the point of view of this publication, it seems particularly important to define the term 'national security', which has been defined in various ways over the years:

- A nation is secure when it does not have to sacrifice its legitimate interests to avoid war, and is able, if challenged, to maintain them by war (Lippmann, 1943).
- "National security, however, has a more extensive meaning than protection from physical harm; it also implies protection, though a variety of means, of vital economic and political interests, the loss of which could threaten fundamental values and the vitality of the state" (Jordan & Taylor, 1981, p. 3).

J. Marczak described national security as the overall preparation and organization of the state for the continuous creation of national security, including:

- The legal basis of security.
- National security policy and strategy.
- Civil and military protection and national defense organizations.
- Security infrastructure.
- Education for safety.
- Alliances and international cooperation in the field of security (Marczak, 2008, p. 13).

For the scientific considerations outlined in the title of this article, it seems crucial to define the notions of information and information security. The concept of information is defined in many ways:

- "Information: facts, data, or instructions in any medium or form" (Department of Defense, 2011, p. 175).

- "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved" (ISO/IEC 27000:2009).
- "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (CNSS, 2010).
- "Information Security is the process of protecting the intellectual property of an organization" (Pipkin, 2000, p. 53).
- "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business" (McDermott & Geer, 2001, p. 97).
- "A well-informed sense of assurance that information risks and controls are in balance" (Anderson, 2003, p. 309).
- "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties" (Venter & Eloff, 2003, p. 300).
- "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats. Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability" (Cherdantseva & Hilton, 2013, p. 21).

To define the essence of information security, it should be remembered that there is currently no universal general definition of information security and concepts related to it. However, it is important not to lose its essence at individual stages of gathering and verifying knowledge on information security.

The discussion and analysis of the issues are aimed at organizing the basic conceptual apparatus necessary to carry out research covering the broadly defined realm of security related to the activity, which involves information. It includes:

- Information security.
- Information safety.
- Information security policy.
- Information security threats.
- Information struggle (e.g. between organizations)
- Information warfare (Fehler, 2016, p. 25).

In this context, the definition of cyber security is also important. It can be defined as the application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and nonrepudiation (AJP-3.20).

Information security is very often understood as protecting information against undesirable destruction or preventing its processing. According to Allied Joint Doctrine For Information Operations, information security is the protection of information (stored, processed, or transmitted), and the host systems, against a loss of confidentiality, integrity and availability through a variety of procedural, technical and administrative controls (AJP-3.10).

3. The significance of information security

In recent years, we have had the opportunity to observe an extraordinary increase in the importance of computer science. As a result, it becomes a value, which allows for gaining power, money, security, but also when skillfully used, it may pose a threat to opponents. Nowadays, it is evident how much information influences the functioning of the economic, social and cultural life of today's nations. In modern times, which can be called the "electronic age", what decides and ultimately determines the success of people, organizations, states and communities in almost all spheres of their functioning is information and the ability to use it (e.g., to communicate). Communication is the interconnection of spoken and written words or messages (Cutlip, Center & Broom, 2006).

Information itself is obviously nothing new and people have always processed all kinds of messages. It should be noted, however, that the role of information has changed dramatically compared to previous eras – the agrarian and industrial society. It could be said that "with the globalization and dissemination of modern information technologies, the traditional values of many societies began to change gradually" (Górnikiewicz & Szczurek, 2017, p. 472). According to the same authors, in the modern world, the influence of information on human behavior is decisive: "successful information activities are those that will be tailored to the thinking patterns, behaviors, emotional reactions and perceptions of affected people" (Górnikiewicz & Szczurek, 2018, p. 116). Information has become a kind of raw material, i.e. technologies are used to process it, and information is not used to modify technology. Importantly, since information is an integral part of most of the processes taking place in society, it is already possible to speak of the ubiquitous impact of information-based technologies (Castells, 2008).

The development of technology, homogeneous tele-information networks (Internet), the universality of access devices, and the emergence of social networks makes information a key factor determining knowledge, power, and, importantly, the security of citizens, organizations and entire countries (Liderman, 2012). As a consequence, new dangers closely related to the use of information networks and information systems, e.g. related to computer hacking, espionage, sabotage, vandalism have emerged (Liderman, 2012). The growing role of information in the modern world causes an increase in threats to its security (Nowak & Scheffs, 2010). Apart from traditional information threats, such as espionage, the contemporary era has produced new threats resulting from the development of technology, i.e. computer crimes, cyberterrorism, and subsequent challenges related to technological progress may become a source of previously unknown dangers (Bączek, 2006).

In the near future, along with the further development of new technologies and cyberspace, one should expect a progressive increase in threats to information security and personal data. As a result, the extent to which st/ate institutions interfere in the privacy of an individual will continue to increase. This is evidenced by the words of T. Szczurek: "The technological and information revolution caused by artificial intelligence will change our everyday and professional environment to an unimaginable degree. It is possible to imagine that people will start living in interconnected homes and contact each other on a level that is difficult to understand today. Privacy will disappear completely, and the interference of public safety systems in private life will become a generally accepted norm" (Szczurek, 2019, p. 196). In his paper Hatch (2019, p.84) analyzes that: "to prepare for future challenges across the continuum of conflict, the United States must be postured to manage and exploit the effects of information by conducting and defending against strategic information operations. Toward this end, the United States will need to engage in operations through multiple domains to capture data and process intelligence to identify malign actors and understand their intentions...". This indicates the direction threats to

national security may develop. It also shows the importance of information security in modern armies.

In the international aspect, information security issues begin to be regulated in international legal acts. The NIS Directive is the first horizontal legislation undertaken at the EU level to protect network and information systems across the Union. Directive 2016/11481 on security of network and information systems (the "NIS Directive") is the first horizontal legislation that has been undertaken at European Union (EU) level for the protection of network and information systems across the Union. The NIS Directive could be considered a late response to an already exacerbated and well-known problem (Carrapico & Barrinha, 2017). By now, cybersecurity incidents, in the form of cyber-attacks and even cyber warfare, have not only been identified at the expert level but have also frequently captured public attention and been featured on the front pages of the press (Markopouloua, Papakonstantinoua & Hert, 2019).

It is worth mentioning the international organizations responsible for ensuring information security e.g. ENISA - the European Union Agency for Network and Information Security. It is located in Greece (Heraclion Crete) and has an operational office in Athens. ENISA was founded by Regulation (EC) No 460/2004,53 whereas its current regulatory framework consists of Regulation (EU) No 526/2013.54. Since 2004, ENISA has been actively contributing towards warranting a high level of network and information security within the EU (Markopouloua, Papakonstantinoua & Hert, 2019).

4. Information security threats

Information security is often understood as a safe state. The proper identification of threats is now the basis for determining the right strategy not only for survival, but also for the development of each organizational entity. The dangers of information processing are often associated with the development of new technologies. However, threats to information security, cannot be related only to the area of cyberspace and ICT, and thus confuse it with ICT security, which is also referred to as "network security", "network security", "computer security" or "telecommunications security" (Polończyk, 2017, p. 81). The concept of ICT security is narrower than information security, as it only concerns the processing of information in electronic form through computer systems and ICT systems. This concept does not apply to all kinds of data found in the resources of the institution (e.g. library, archives, official collections, etc.).

Information security threats can be divided according to the following criteria:

- Random threats: natural disasters, catastrophes, accidents that affect the information security of the organization (fire in the building where information media are stored).
- Traditional information threats: espionage, subversive or sabotage activities (aimed at obtaining information or offensive disinformation carried out by other people, entities and organizations).
- Technological threats: threats related to the collection, storage and processing of information in ICT networks (e.g. computer crime, cyber terrorism, information warfare).
- Threats related to the civil rights of individuals or social groups (e.g. selling information, providing information to unauthorized entities, violating privacy by the authorities, unlawful interference by secret services, restricting the transparency of public life) (Bączek, 2006, pp. 72-73).

Due to the location of their sources, threats can be divided into:

- Internal (arising within the organization), which include the risk of data loss, damage or modification due to unintentional (erroneous or accidental) or deliberate actions by dishonest users (employees).
- External (generated outside the organization), which include the risk of data loss, data corruption or the inability to be operated by accidental or intentional actions by third parties.
- Physical, where data loss, corruption or the inability to service occurs as a result of an accident, breakdown, catastrophe or other unforeseen event affecting the information system or network device (Żebrowski & Kwiatkowski, 2000, p. 65).

Human activity is the greatest threat to information security. Deliberate threats to the information security system may result from the accumulation of three elements: motive, means of breaking into the system and opportunity, which is access to a computer disk or network. Various methods of hacking into information systems can be used:

- Collusion of several perpetrators.
- Deliberate failure initiation.
- Triggering false alarms.
- Blackmail, corruption.
- Sending surveys, inquiries, proposals to companies.
- Decoding the access password.
- Dictionary attack.
- Network wiretapping.
- Viruses, Trojan horses, logic bombs and other dangerous applications destabilizing the system's efficiency.
- Exploiting security gaps in access to e-mail and information service,
- Security circumvention techniques, e.g. programs that exploit bugs in operating systems and application software.
- Interception of open network connections (Polończyk, 2017, p.83).

These threats will certainly be accompanied with new threats and the methods of breaking into information systems. Therefore, the task of every organization is to constantly monitor threats in the external environment, especially when disseminated data and information can potentially be used to undermine its security. The early identification of potential threats will enable the modification of the existing software so as to eliminate or reduce the likelihood of one of them occurring in the future, thus strengthening the security system of the entire organization.

5. Military information security

Nowadays, in the military sphere, information is seen as a strategic resource. As a consequence, the technologies used for acquiring, processing and protecting important information have become an important part of the potential of the armed forces. It can be concluded that competition for information has become an important part of the armed forces' activities. The advantage gained in this respect may protect against the negative consequences of "information warfare" and, consequently, ensure the security of the state. Therefore, the challenge for the modern armed forces is to ensure the efficiency and security of information systems, to prevent the effects of crimes against information infrastructure and maintain the ability to obtain key information. Thus, it has become a standard to

develop the concept of information operations, create and maintain structures for their implementation. (Nowacki, 2013). Information security is one of the most important military issues of the 21st century. Heavy reliance on computers by the U.S. and its allies for communications, vehicle control, surveillance, and signal processing makes it imperative for U.S. military forces to keep data secure from nations and groups hostile to our national interests (Keller, 2007). The dynamic development of ICT technologies and their effective use on the real battlefield is a highly relevant factor in terms of the functioning of contemporary and future armies (Rybak & Dudczyk, 2019). According to Gerasimov (2019), information technology is in fact becoming one of the most promising weapons. According to Karaman (et al., 2016, p. 6), "the military organizations need to prepare for the worst by establishing resilient and cyber command structure, interoperable and synchronized planning efforts with electronic warfare command. Due to the changing character of wars from conventional to unconventional, symmetric to asymmetric and hybrid wars, cyber operations need to be designed to defense and sustain the military assets".

An important reason for the expansive growth of the importance of information in the armed forces was the change in the nature of contemporary conflicts in the world from a symmetrical asymmetric, i.e., where the parties have different legal and international status and asymmetrical military potential (Górnikiewicz & Szczurek, 2018). Its feature is the recognition of the superior techniques of violence (Ciszewski, 2010). Notably, the armed forces are confronted with an enemy whose goals, organization, means, and combat methods do not fall into conventional categories. The aim of the entity waging an asymmetric fight is to maximize the effects while minimizing costs through spectacular terrorist actions to cause psychological impact on society (Nowacki, 2013). An asymmetric struggle is often waged with clandestine groups that share an ideological and ethnic bond. Their distinguishing feature is the unconventional use of the available means of destructive influence. Apart from the cheapest weapons and ammunition, they can use a different type of means of influence (Bujak, 2005). As Nowacki (2013, p. 118) notes: "In addition to the significant development of electronic means (microprocessors, electromagnetic pulse generators" logical "bombs, computer viruses) and mass media (Internet, television, radio, press), new possibilities of influencing have appeared, such as beam weapons (energy directed), strobe lights inducing nausea or infrasound causing depression, tension, fear, artificial cheerfulness, slower reaction, heart ailments and imbalances. Moreover, various psychotronic techniques can be used, which induce subjective and objective behavior of people under the influence of suggestions or self-suggestions".

Information security and information itself are of particular importance when it comes to conducting of hostilities. The ubiquitous role of the mass media in social life is a factor that could significantly contribute to a greater sense of responsibility for the manner of warfare in the future. Thanks to the inquisitiveness of journalists seeking sensationalism, it is increasingly difficult to hide war crimes or other acts prohibited in hostilities. The media also have a major impact on the assessment of war, both in countries directly involved in a given conflict and among the international community. With the development of the mass media and access to information (satellite TV, Internet), the role of psychological activities in future wars will also increase, fostered by the ever-increasing demand for immediate access to information from the battlefield, often in the form of a live report or near real-time. Live coverage and almost unlimited media access to information do not necessarily entail a lack of censorship and manipulation. An example of manipulating information from the battlefield may be the actions of the American services responsible for contacts with the media during the Gulf War. At that time, journalists had to remain in the background, and they were only taken for short, organized trips to the stations where troops were stationed (often far from the front). Furthermore, only carefully selected information was provided. The contemporary recipient is looking for current and interesting

information. Therefore, in order to meet these expectations, the media present the most spectacular, often shocking images from the battlefield. Therefore, the parties to the conflicts protect and will protect any information that affects their image in the future (Szczurek, 2009).

The modern armed forces must be ready to face new threats in the information sphere, such as penetrating databases or conducting disinformation activities aimed at paralyzing the state security system. Due to the significant increase in security threats in the information sphere, the armed forces are gradually adjusting their structures to new challenges, focusing more and more on the need to protect cyberspace.

In order to ensure the security of key information, from the point of view of the state's interest and national security, the armed forces focus on: creating the information environment, acquiring new technologies (including especially information technologies), expanding the information structure, which should ensure the safe flow of data in almost real time. This may contribute to strengthening one's own potential to influence and protect more effectively against the undesirable influence of external entities. The infrastructure should be composed of systems and subsystems of obtaining source information, management and control of electronic devices.

Currently, in the armed forces, key information that is subject to special protection is classified information and constitutes a state secret. These are data and messages, the loss of which or transfer to the wrong hands would endanger the security of the state. A wide range of forces are commonly used to protect this type of data and measures ranging from specially designed procedures for accessing and processing these data through physical security. The most important security measures used to protect classified information include: security personnel, physical barriers (lockers and lockers), and a system for controlling people and objects. Of course, all kinds of ICT systems are also subject to special protection, the security of which is becoming an increasing challenge in the era of the development of new technologies.

In recent years, another category of data that is specially protected in the armed forces is the personal data of soldiers, whose personal data may be used at any time for purposes incompatible with the interests of a given state. The protection of these data is therefore a task and a challenge for state institutions, which should select the means and methods of strengthening the protection of soldiers' personalities adequately to contemporary threats. However, recent years have proved that in the era of new threats in the areas of ICT and cyberspace and disinformation activities increasingly used by secret services of many countries, improper data protection may pose a threat to the interest of the state. A breakthrough in the perception of the importance of personal data was the adoption in April 2016 of the Regulation of the European Parliament and of the Council (EU) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, commonly referred to as GDPR (Journal of Laws UE L 119 of 4 May 2016, item 1).

With regard to international examples of the use of information in security aspects, Russia should be mentioned. As Szpyra (2020) analyzes: “Studies have revealed that the Russian Federation, aware of the importance of using “information weapons”, is working on concepts of intensive introduction of foreign information technologies into the sphere of activity of the individual, society and the state”. Since Russia has a natural predisposition to playing the role of a superpower in the face of the dynamic growth of globalization and contemporary geopolitical competition, the use of aggressive forms of information warfare is inevitable (Manoylo, 2003). Meanwhile, both theorists and representatives of the Russian authorities are convinced that the modern information war should also be waged in peacetime in all spheres of social life (Rogozin, 2011). According to Frida Ghitis (2020, p. 1): “Russia was engaging in an incendiary and divisive disinformation campaign

in Latin America waged over social media similar to Russia's political interference in the 2016 elections in the US". What is more, Russia has deployed a range of hybrid threats against the energy assets, policies or supplies of NATO allies, and other countries. It has used political and economic leverage, combined with disinformation campaigns, against Bulgaria and Romania to undermine efforts to reduce their dependence on Russian energy sources (Dupuy, et al., 2021).

Therefore, EU countries should strengthen the defense capabilities of information security in times of peace and war.

6. Conclusion

One of the significant consequences of the emergence and dynamic development of modern information technologies is the extension of the objective scope of state security by the category of information security.

In the extensive literature on the subject in the field of security sciences, information security is classified within the subject criterion next to political, military, economic, social, cultural, environmental, ideological and universal security. However, derives directly from public security, perceived as a process involving activities provide protection against prohibited activities. Most often, it is defined as the entirety of activities undertaken to ensure the integrity of the collected, stored and processed information resources, by securing them against unwanted, unauthorized disclosure, modification or destruction (Potejko, 2009).

In today's reality, one of the key challenges facing various states is ensuring information security as one of the most essential elements of national security. Information security plays a special role in the armed forces of modern countries. The protection of important information in military entities has even become a priority. Information began to be treated as a strategic resource of the state; therefore, information resources are a critical element for its functioning. Currently, information is protected at every stage of processing: from obtaining information, through its transmission, storage, analysis and use, to keeping it confidential.

The modern army's dependence on an efficient system of obtaining, processing and distributing information, also in a digitized form, is a fact. The main challenges for the armed forces include expanding the ability to obtain information, analyze it, distribute it, protect its own information resources, as well as the ability to identify and effectively counteract the effects of hostile information operations. The protection of information functioning in cyberspace becomes the greatest challenge. The information security of modern armies is therefore inseparable from information warfare, in which information is both a weapon and a target of attack. It is connected with the armed forces' need to develop their information capabilities in the defensive area (protection of their own information resources and information systems) and in the offensive area (the ability to conduct their own information and disinformation operations).

References

1. AJP-3.10 (2009) Allied Joint Doctrine For Information Operations, Nato Standard, NATO/PfP UNCLASSIFIED publication. The agreement of NATO nations to use this publication is recorded in STANAG 2518.
2. AJP-3.20 (2020) Allied Joint Doctrine for Cyberspace Operations, Nato Standard, AJP-3.20, Edition A, Version 1.
3. Aleksandrowicz, T. R. (2018). Bezpieczeństwo informacyjne państwa. *Studia Politologiczne, Volume 49*, pp. 33-50. http://www.studiapolitologiczne.pl/Teoretyczne-i-praktyczne-aspektybezpieczenstwa-panstwa,115397,0,2.html
4. Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *Volume 22*, pp. 308-313. https://doi.org/10.1016/S0167-4048(03)00407-3
5. Bączek, P. (2006). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek.
6. Bujak, A. (2005). Możliwe kierunki zmian w reagowaniu kryzysowym (part I), *Zeszyty Naukowe WSOWLąd*, Volume 2, pp. 85-93.
7. Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber) Security Actor? *Journal of Common Market Studies, Volume 55* (6), pp. 1254–1272. https://doi.org/10.1111/jcms.12575
8. Castells, M. (2006). The Network Society: From Knowledge to Policy. In M. Castells, & G. Cardoso (Eds.), *The Network Society: From Knowledge to Policy* (pp. 3-22). Center for Transatlantic Relations.
9. Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In F. Almeida, *Organizational, Legal, and Technological Dimensions of Information System Administrator* (pp. 167-169). IGI Global Publishing.
10. Ciszewski, T. (2010). Zarządzanie sytuacją kryzysową w środowisku zagrożonym IED. *Zeszyty Naukowe WSOWLąd*, *Volume 3*, (pp. 205-224).
11. Committee on National Security Systems. (2010). Information value. *In National Information Assurance (IA) Glossary*. (CNSS Instruction No. 4009, p. 38).
12. Cutlip, S. M., Center, A. H., & Broom, G. M. (2006). *Effective Public relation*, Pearson.
13. Department of Defense. (2011). Information. In *Department of Defense Dictionary of Military and Associated Terms* (The Joint Publication 1-02, p. 173).
14. Dupuy, A., Nussbaum, D., Butrimas, V., & Granitsas, A. (2021, January 13). *Energy security in the era of hybrid warfare*. NATO Review. https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html?fbclid=IwAR2rPTR6fzYPOJIshYOo6um9uo1-TBhgk4h3bdfbg_UJhgXG4hdkBHEPxDY
15. Fehler, W. (2016). O pojęciu bezpieczeństwa informacyjnego. In M. Kubiak, & S. Topolewski, *Bezpieczeństwo informacyjne XXI wieku* (pp. 24-43). Pracowania Wydawnicza Wydziału Humanistycznego.
16. Gerasimov, V. (2019, March 04). *Vektory razvitiya voyennoy strategii*. Krasnaya Zvezda. http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1
17. Ghitis, F. (2020, January 23). *Russia's Disinformation War Reaches Latin America, Challenging U.S. Influence*. World Politics Review. https://www.worldpoliticsreview.com/articles/28489/for-putin-venezuela-and-latin-america-are-key-to-challenging-u-s-influence

18. Górnikiewicz, M., & Szczurek, T. (2017). Wschodnioazjatycka, a europejska perspektywa bezpieczeństwa międzynarodowego: wpływ różnic kulturowych na projektowanie polityki bezpieczeństwa ma przykładzie wybranych społeczeństw. In M. Gębska, *Współczesne bezpieczeństwo ekonomiczne i społeczno-kulturowe, Wymiar Międzynarodowy*. Akademia Sztuki Wojennej.
19. Górnikiewicz, M., & Szczurek, T. (2018). *Social Media Wars – The Revolution Has Just Begun*. Military University of Technology.
20. Hatch, B. (2019). The Future of Strategic Information and Cyber-Enabled Information Operations. *Journal of Strategic Security, Volume 12* (4), pp. 69-89. https://doi.org/10.5038/1944-0472.12.4.1735
21. International Organization for Standardization. (2009). *Information technology – Security techniques – Information security management systems* – Overview and vocabulary. ISO Standard No. 27000:2009 (E).
22. Jordan, A. A., & Taylor, W. J. Jr. (1981). *American National Security*, John Hopkins University Press.
23. Karaman, M., Çatalkaya, H., & Aybar, C. (2016). Institutional Cybersecurity from Military Perspective, *International Journal Of Information Security Science, Volume 5* (1), https://www.ijiss.org/ijiss/index.php/ijiss/article/view/174/pdf_33
24. Keller, J. (2007, October 01). *The importance of military information security*. Military Aerospace Electronics. https://www.militaryaerospace.com/communications/article/16706235/the-importance-of-military-information-security
25. Koziej, S. (2006). *Między piekłem a rajem, Szare bezpieczeństwo na progu XXI w*. Wydawnictwo Adam Marszałek.
26. Liderman, K. (2012). *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN.
27. Lippmann, W. (1943). U.S. Foreign Policy: Shield of the Republic. In S.E. Corwin (Ed.), *American Political Science Review* (pp. 259-262). Cambridge University Press. https://doi.org/10.1177/004057364400100211
28. Manoylo, A. (2003). *Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh: Monografiya*. MIFI. http://www.klex.ru/jlj
29. Marczak, J. (2008). Powszechna ochrona i obrona narodowa. In R. Jakubczak (Ed.), *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji* (pp. 37-48). AON.
30. Markopoulou, D., Papakonstantinou, V., & Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, *Computer Law & Security Review, Volume 35* (6). https://doi.org/10.1016/j.clsr.2019.06.007
31. Mathews, J. (1989). Redefining Security. *Foreign Affairs*, *Volume 68* (2), (pp. 167-177).
32. McDermott, E., & Geer, D. (2001). Information security is information risk management. In B. Blakley, McDermott, & D. Geer, *Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 97-104). Association for Computing Machinery. https://doi.org/10.1145/508171.508187
33. NIS Directive - Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union.
34. Nowacki, G. (2013). Znaczenie informacji w obszarze bezpieczeństwa narodowego. *Nierówności społeczne a wzrost gospodarczy*, *Volume 36*, pp. 107-123.
35. Nowak, A., & Scheffs, W. (2010). *Zarządzanie bezpieczeństwem informacyjnym*, AON.
36. Nowakowski, Z. (2009). *Bezpieczeństwo państwa w koncepcjach programowych partii parlamentarnych w Polsce po 1989 roku*. Towarzystwo Naukowe Powszechne.
37. Pipkin, D. (2000). *Information security: Protecting the global enterprise*. Hewlett-Packard Company.

38. Polończyk, A. (2017). Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa. In H. Batorowska, & E. Musiał, *Bezpieczeństwo informacyjne w dyskursie naukowym* (pp. 79-94). Uniwersytet Pedagogiczny w Krakowie.
39. Potejko, P. (2009). Bezpieczeństwo informacyjne. In K. A. Wojtaszczyk, & A. Materska-Sosnowska (eds.), *Bezpieczeństwo państwa* (pp. 209-220). Oficyna Wydawnicza ASPRA-JR.
40. Rogozin, D. (2011*) Voyna i mir v terminakh i opredeleniyakh.* Voyenno-politicheskiy slovar. Veche.
41. Rybak, Ł., & Dudczyk, J. (2019). Increasing the information superiority on the modern battlefield through the use of virtual reality systems. *Security and Defence Quarterly, Volume 25* (3), pp. 86-98. https://doi.org/10.35467/sdq/105998
42. Szczurek, T. (2009). *Konflikty zbrojne.* Wojskowa Akademia Techniczna.
43. Szczurek, T. (2019). *Wyzwania dla bezpieczeństwa – niepewna przyszłość między zagrożeniami a szansami*. Wojskowa Akademia Techniczna.
44. Szczurek, T., Walkowiak, M., & Bryczek-Wróbel, P. (2020). *Military, non-military and paramilitary threats*. Military University of Technology.
45. Szpyra, R. (2020). Russian information offensive in the international relations, *Security and Defence Quarterly, Volume 30* (3), pp. 31–48. https://doi.org/10.35467/sdq/124436
46. Venter, H. S., & Eloff, J. H. P. (2003). A taxonomy for information security technologies. *Computers & Security, Volume 22* (4), pp. 299-307. https://doi.org/10.1016/S0167-4048(03)00406-1
47. Zięba, R. (2008a). *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne.
48. Zięba, R. (2008b). Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego, In R. Zięba, *Bezpieczeństwo międzynarodowe po zimnej wojnie*. Wydawnictwo Akademickie i profesjonalne.
49. Żebrowski, A., & Kwiatkowski, M. (2000). *Bezpieczeństwo informacji* III Rzeczypospolitej. Oficyna Wydawnicza Abrys.

SAFETY&DEFENSE
ISSN 2450-551X

Disinformation and Polarization in the Online Debate During the 2020 Presidential Election in Poland

Dorota DOMALEWSKA

[1] War Studies University, Warsaw; d.domalewska@akademia.mil.pl,
ORCID: 0000-0002-1788-1591

DOI: https://doi.org/10.37105/sd.92

Abstract

The deliberate manipulation of public opinion, the spread of disinformation, and polarization are key social media threats that jeopardize national security. The purpose of this study is to analyze the impact of the content published by social bots and the polarization of the public debate on social media (Twitter, Facebook) during the presidential election campaign in Poland in 2020. This investigation takes the form of a quantitative study for which data was collected from the public domains of Facebook and Twitter (the corpus consisted of over three million posts, tweets and comments). The analysis was carried out using a decision algorithm developed in C# that operated on the basis of criteria that identified social bots. The level of polarization was investigated through sentiment analysis. During the analysis, we could not identify automated accounts that would generate traffic. This is a result of an integrated action addressing disinformation and the proliferation of bots that mobilized governments, cybersecurity and strategic communication communities, and media companies. The level of disinformation distributed via social media dropped and an increasing number of automated accounts were removed. Finally, the study shows that public discourse is not characterized by polarization and antagonistic political preferences. Neutral posts, tweets and comments dominate over extreme positive or negative opinions. Moreover, positive posts and tweets are more popular across social networking sites than neutral or negative ones. Finally, the implications of the study for information security are discussed.

Keywords

disinformation, polarization, fake news, social bots, Facebook, Twitter, information security, hybrid threats

Submited: 05.01.2021 Accepted: 17.02.2021 Published: 12.03.2021

1. Introduction

Hybrid risks pose a threat to the contemporary security environment. They include a combination of conventional and irregular warfare, and political and information threats whose aim is to use hostile "measures that seek to deceive, undermine, subvert, influence and destabilize societies, to coerce or replace sovereign governments and to disrupt or alter an existing regional order" (Monaghan, 2019). The informational dimension of hybrid threats includes massive disinformation, ideological propaganda and using media for political purposes. Disinformation attacks are automatically and aggressively disseminated on a massive scale posing a serious cybersecurity threat and representing a serious hybrid threat to state security. Disinformation campaigns are not an end in itself, but a means for achieving financial or political gains, similarly to cyberattacks which use malware, viruses and social engineering to make a breach to security systems. Therefore, hybrid threats in the form of disinformation or cyberattacks hinder the stability of the security environment (Bajarūnas, 2020; Ivančík, Jurčák and Nečas, 2014).

When living in a network society where information plays a central role, information security should become a priority in the national security policy. The Internet is critical for ensuring state security as both society and economy are increasingly dependent on information technology and computer networks. The growing trends in the consumption of online content prove their increased impact on society, thus creating consumer behavior, political preferences and worldviews (Urych, 2013; Świerszcz, 2017; Benkler, Faris and Roberts, 2018; Colliander, 2019; Żakowska and Domalewska, 2019). The threats associated with social media include increased polarization, the deliberate manipulation of public opinion and the spread of disinformation (Araźna, 2015; Mustonen-Ollila, Lehto and Heikkonen, 2020), which is understood as a set of techniques used deliberately to manipulate people or entire societies for political or economic gains. Disinformation is spread on social media by social bots, that is, programs controlled by algorithms that mimic human behavior on social networks. Numerous studies have confirmed that they were used during the presidential campaign in the United States in 2016 (Bessi and Ferrara, 2016; Klimburg, 2018) and the pre-referendum debate on Brexit in 2016 (Howard and Kollanyi, 2016). However, there is a lack of research analyzing polarization and the use of social bots in public debate on Polish-language social networks. This study aims to fill this gap.

The main theoretical goal of this study is to reflect, based on empirical evidence, on the impact of content published by social bots and polarization of the public debate on social media (Twitter, Facebook) during the presidential election campaign in Poland in 2020, and particularly the two months before and a month after the presidential election. The study allows the following research questions to be answered: (1) to what extent were social bots used in the public debate on social media during the 2020 presidential campaign? (2) to what extent did the 2020 presidential election lead to polarization in Polish society? The general assumption of this study was formulated by using the hypothesis that the public debate on candidates running in presidential election would generate increased traffic from a significant number of social bots. We further hypothesize that the 2020 presidential election have led to polarization in Polish society.

2. Disinformation in online debate

Disinformation is "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public" (European Commission, 2018). Disinformation campaigns are carried out to manipulate the information ecosystem for financial and political goals. Economic goals are met when sensational stories and catchy titles are meant to draw readers' attention, increase readership and generate income. Political goals are realized in a variety of ways, such as discrediting a political opponent, undermining their credibility, spreading chaos, and increasing polarization. Disinformation can also lead to a social change by promoting populism, increasing intolerance of various ethnic or cultural groups. It is a serious threat to core values: democratic political and policy-making processes, trust in institutions and the media. Furthermore, disinformation attacks lead to the manipulation of society, influence political behavior and the way of thinking, and cause a number of emotions, such as uncertainty and hostility, which results in social tensions. These goals can be achieved by concealing the source and purpose of the information, distorting the interpretation of facts and one-sided depiction of events, using shocking images, dispersing the facts using a multitude of irrelevant information, or not providing all the facts.

Disinformation content is automatically and aggressively disseminated on a massive scale using social bots, artificial intelligence, trolling and micro-targeted advertising. Social bots are algorithm-controlled programs that share posts and engage in communication with human users (Howard and Kollanyi, 2016). Apart from useful bots used for communication with consumers (e.g., chat bots offer support to individuals in customer help desk situations and telephone answering systems), malicious bots may be employed to generate profit, circulate disinformation, manipulate content, and share spam. Bots can also reply to posts meeting certain criteria and track the activity of users who followed the bot or who publish specific content on the Internet. According to Woolley (2016), American politicians used social bots to increase their follower list, disseminate favorable tweets in order to influence public opinion and flood the hashtag promoted by the opposing party with bot-generated or bot-retweeted content. Automated accounts were also used to generate tweets or retweets around a specific topic to suggest a false sense of consensus around this opinion (astroturfing) (Ratkiewicz *et al.*, 2011; Węglińska, 2018).

Social media accounts that are run by bots can be identified if they exhibit the following features: (1) "a high volume of content in which reposts and retweets prevail over the original output; (2) the user account looks like a default account that has not been personalized by the user; (3) recent account creation date; (4) a random account name that has not been personalized; (5) avoidance of geotagging (social media users usually produce location-specific data); (6) duplicating posts by multiple accounts simultaneously or almost simultaneously; (7) lack of original output; (8) activity is centered on a very narrow thematic scope; (9) rapid reaction to certain articles or posts; and (10) user's demographic information that does not match the style of speech or the subject matter" (Domalewska and Bielawski, 2019).

Automated accounts can be difficult to identify, especially by individual social media users. Bessi and Ferrara (2016) found that bot produced content was retweeted at the same rate as human-generated content. During the 2016 US presidential election, 36,746 Russian bot accounts disseminated 1.4 million tweets that were seen 288 million times (Hudgins and Newcomb, 2017). Bot communication also played a role in generating traffic and misleading social media users during the Brexit debate (Howard and Kollanyi, 2016) and the Ukraine –

Russia conflict in 2014 (Hegelich and Janetzko, 2016). However, studies carried out in Germany (Brachten *et al.*, 2017) have not detected a statistically significant use of social bots in political contexts.

3. Polarization

Polarization takes place when viewpoints and preferences shift from acceptable moderate positions towards the extreme ends of the ideological spectrum. The extreme viewpoints stand in opposition and will always clash with each other. In democratic societies, a certain degree of polarization is expected as political parties differ in their programmatic agendas and seek a loyal electorate. The problem arises when polarization becomes so intense that it poses a threat to democracy. Hence, severe polarization can be defined as "a process whereby the normal multiplicity of differences in the society increasingly align along a single dimension, cross-cutting differences become reinforcing, and people increasingly perceive and describe politics and society in terms of 'us' versus 'them'" (McCoy & Somer 2019).

Kligler-Vilenchik, Baden and Yarchi (2020) distinguish between positional and interpretative polarization. The former refers to people's stance on political issues whereas the latter entails the contextualization or framing of a topic in opposing ways. In the case of strong interpretative polarization, different groups conceptualize the topic in contradictory ways so that reasoned debate between the groups is not feasible. An understanding can only be reached when groups share certain frames and opinions or agree that the arguments put forward by other groups are sound (Risse 2002). Interpretative polarization may strengthen positional polarization (Baden and David, 2018).

Poland has been experiencing growing polarization both among the elites, with two parties dominating the Polish political scene (Law and Justice, PiS, and the Civic Platform, PO), and among the electorate. In fact, as Tworzecki (2019) argues, polarization in Poland is a top-down process that has divided society on such contentious issues as social policy, the legal system and religious issues resulting in escalating tensions. The divide tends to be aligned with political leaning towards one party or the other.

Another significant question related to polarization needs to be considered, namely who drives this process. As McCoy & Somer (2019) argue, some deliberate policies and the discourse of political actors reinforce divides in order to consolidate supporters and weaken opponents. In this case, polarization is on the one hand a tool for power and domination, and on the other hand, a political strategy to realize far-reaching political goals. The mainstream media is another powerful driver of polarization. In fact, the balkanization of the media landscape has been well researched in the USA where the polarization of the media leads to the hardening of viewers' ideological perspectives (Kaylor, 2019). Partisan media outlets provide biased coverage and amplify extreme viewpoints. Using different frames to report the events, biased media coverage manipulates public opinion. As a result, societal trust declines and mutual understanding across partisan divides is increasingly difficult to reach.

Social media also strengthen the cleavage by creating echo chambers, filter bubbles and using microtargeting to promote certain products, ideologies or opinions. What is more, social media users tend to reject information that conflicts with their opinions (cognitive dissonance) and seek information that confirms their beliefs (confirmation bias). Polarization takes place not only through active discussion but also through the mere exposure to the opinions of others (Sunstein, 2017, p. 73). Therefore, social media have become a tool for increasing polarization.

Growing polarization poses a threat to national security for several reasons. First, cyber-balkanization limits the individual's field of vision and focuses their attention on different issues, which hinders mutual understanding and reduces societal trust. Therefore, polarization leads to the decline of social capital, affects state security decision-making and results in political gridlock. Second, it weakens the international position of the country and makes it unable to respond to global challenges (Hawdon *et al.*, 2020, p. 243). As Carothers and O'Donohue (2019) note, polarization "reinforces and entrenches itself, dragging countries into a downward spiral of anger and division for which there are no easy remedies." It threatens democratic norms, undermines the legislature and weakens the apolitical status of the judiciary. Political cleavage also results in increased populism, nationalism, intolerance, and discrimination.

4. Methodology

The posts were collected when monitoring discussions on the public domains of Facebook and Twitter from March 31 to July 31, 2020. The sample consisted of 96 623 tweets with 1 910 154 comments and 103 668 Facebook posts with 937 137 comments (the total corpus was made up of over three million posts, tweets and comments). Both text data (the content of posts and tweets) and metadata (data on the authors of the posts and tweets, their popularity and publication dates) were collected. Then the data was initially processed and cleaned. For example, redundant data and marketing content were removed. The analysis was then carried out using an analytical tool – an algorithm developed in C#. The analysis was carried out in several stages. First, the possibility of using social bots to spread content on social media was analyzed. The analysis was carried out with the use of a decision algorithm that operated on the basis of criteria that identified social bots: the number, time and speed of sending original posts and shares. Twitter or Facebook accounts were selected for further verification if it met the following criteria: the account published multiple posts over a limited span of time and it reposted or retweeted a high volume of non-commercial content. Next, the identified accounts were passed on for further verification to determine whether they were run by algorithms. The verification included the following test: account creation date, degree of the account personalization and its name and the narrow scope of the account activity.

The level of polarization was investigated through sentiment analysis, which allows social media users' opinions, attitude, emotions and appraisal of a particular subject to be analyzed. This popular text-mining method is effective in determining the opinion and emotion of the post or tweet. This method is also effective in measuring the extent of polarization of the debate, as sentiment tends to become more extreme as groups become more polarized (Kligler-Vilenchik, Baden and Yarchi, 2020). Sentiment analysis was used to evaluate moods associated with words and phrases from a data set based on their semantic orientation in vocabularies constructed specifically for this study. Therefore, positive (including words such as effective), neutral (for example, president) and negative (for example, hate) vocabularies were built. Each word in the vocabulary was assigned a score of 1 (positive words), 0 (neutral words) or -1 (negative words). This made it possible to calculate the degree of polarization (highly or moderately positive or negative). Finally, the popularity of tweets or Facebook posts was measured by analyzing the number of users who saw the post or tweet, followed it or liked it, and retweeted or shared it.

5. Results and discussion

As mentioned earlier, the corpus consisted of corpus consisted of 3 060 301 posts and tweets – both main mentions and comments (see Fig. 1): 96 623 tweets with 1 910 154 comments and 103 668 Facebook posts with 937 137 comments.

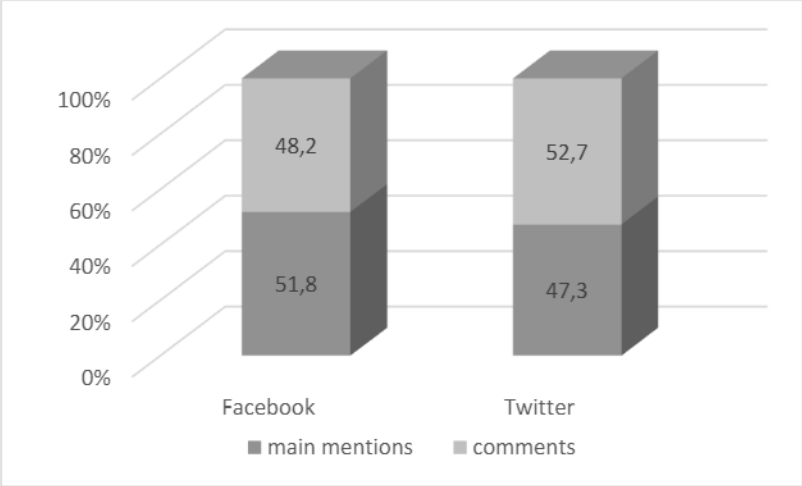

Figure 1. The corpus of the study. Own work.

As can be seen in Figure 1, Facebook contains slightly more main mentions, whereas Twitter is a platform that is used mainly for sharing opinions, which is why it contains more comments than main mentions. The first step of the analysis was processing the data by using two criteria (the account published multiple posts over a limited span of time and it reposted or retweeted a high volume of content) in order to select the accounts that will be passed on for further analysis. Even though a significant amount of duplicate content was found (46.9 %) (retweets and reposts), it was spread by multiple accounts and not individual users. Therefore, none of the accounts were selected for further verification.

The second part of the study concerned the polarization of the debate on social media. A sentiment analysis was performed to determine the viewpoint of social media users (see Fig. 2). Positive and negative sentiment was investigated as the more polarized the group is, the more extreme sentiment it exhibits (people tend to use increasingly positive sentiments to discuss their own viewpoints and increasingly negative sentiments to comment on the stance of other groups).

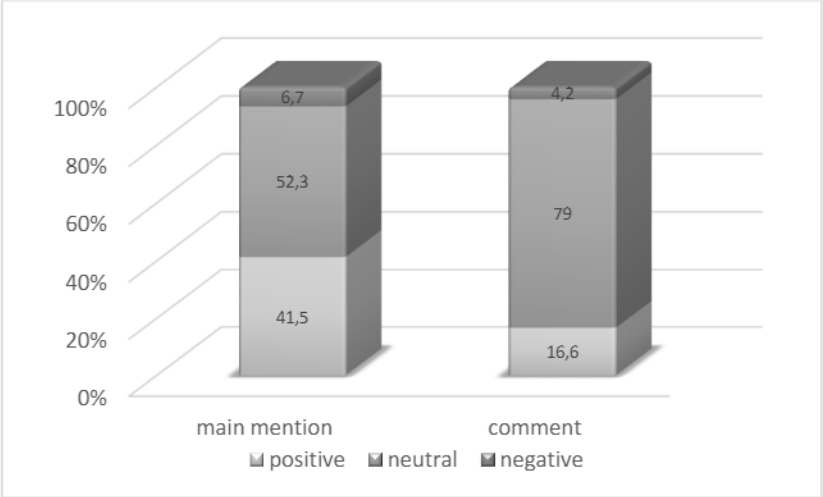

Figure 2. Sentiment analysis of the dataset. Own work.

As is shown in Figure 2, neutral statements dominate the corpus. Negative opinions expressed in both the main mentions and comments are quite rare. One fourth of every main mention was categorized as positive. As far as the comments are concerned, neutral sentiment prevails. As many as 16.6% of all comments are positive. This is in line with Kligler-Vilenchik, Baden and Yarchi (2020) whose study of political discussion on Facebook, Twitter and WhatsApp over time shows the depolarization dynamic, and in particular, a decrease in negative sentiment. The researchers also found an increasing role of shared purposes and mutual respect exhibited by social media users.

The 2020 presidential election in Poland coincided with the first wave of the COVID-19 pandemic, which affected social media discussion. Not only did the quantity of private messages sent via social networking sites increase (by 50% in the case of WhatsApp and Messenger and 30% - Twitter) (biznestrendy.eu, 2020). Other studies (Politechnika Wrocławska, 2020) prove that at the beginning of the pandemic, negative sentiment prevailed, but with time, when schools were closed and a wide-reaching informative campaign was launched by the government, the number of negative posts and tweets decreased and neutral, motivating, or optimistic information grew.

A further analysis was performed to examine the popularity of positive, neutral and negative opinions published as main mentions on social networking sites (see Table 1.).

Table 1.
Popularity of positive, neutral and negative sentiment of main mentions

Sentiment	Popularity measure - mean
Positive	158.68
Neutral	138.50
Negative	121.61

The popularity measure of the posts and tweets was calculated by the number of users who saw the post or tweet, followed it or liked it, and retweeted or shared it. The findings show that positive posts and tweets were read by a greater number of social media users and were liked, shared and retweeted more frequently than neutral or negative posts and tweets. These findings prove that social media discourse does not exhibit traits of increasing polarization, as the sample is not dominated by negativity.

6. Conclusions

The aim of the study was to provide empirical evidence for polarization and the degree of bot-generated content on social media during the 2020 presidential election campaign in Poland. However, the first hypothesis that the public debate during the presidential election would generate traffic from a significant number of social bots has not been supported by evidence. As a result of integrated action addressing disinformation and the proliferation of bots that mobilized governments, cybersecurity and strategic communication communities, and media companies, the level of disinformation distributed via social media dropped. This entails, in particular, the activity of social bots. The representatives of social networking sites and advertising industries endorsed a self-regulatory Code of Practice to tackle the problem

of disinformation and fake news (European Commission, 2019). As a result of this coordinated action, social networking companies such as Facebook and Twitter, intensively scrutinize accounts suspected of being run by algorithms. A great number of fake accounts on social networking sites have been removed. For example, from March 18 to April 1, 2020 (15 days), over 1 100 tweets were removed from Twitter and nearly 1.5 million accounts were deleted as automated accounts spreading spam (biznestrendy.eu, 2020). Many automatic accounts have reduced the traffic they engage in to evade detection.

Furthermore, by analyzing political debate on social media during the 2020 presidential election, the study shows that public discourse is not characterized by polarization and antagonistic political preferences. Therefore, the hypothesis that the 2020 presidential election led to polarization in Polish society has been refuted. Our study demonstrates that neutral posts, tweets and comments dominate over extreme positive or negative opinions. Moreover, positive posts and tweets are more popular across social networking sites than neutral or negative ones. While interpreting the research findings, we need to bear in mind that the 2020 presidential election in Poland took place during the first wave of the pandemic, which affected the quantity and quality of social media consumption. Facebook recorded a 50% increase and Twitter a 30% increase in the number of private messages sent to other users (biznestrendy.eu, 2020). In posts and tweets published in Polish in March – June 2020, topics related to the short-term economic effects of the pandemic and information related to the relief package prevailed (the Anti-Crisis Shield was launched on March 31, April 16 and May 14, 2020). The revised legislation was preceded by a wide-reaching informative campaign, which not only provided a detailed explanation of administrative issues related to the relief package but also calmed down intense negative emotions.

The scope of the study was limited as social media users are not a representative sample of Polish society; studies on the demographic makeup of social networking sites show that both Twitter and Facebook users are mostly professionals with higher education, retirees or students (*Polska szerokopasmowa*). Furthermore, the study has not differentiated between active and passive social media users. Active users, who frequently post, tweet or comment on social media, are overrepresented whereas the passive ones have not been represented in the study. More research, e.g., content analysis, is therefore needed to confirm the findings of the quantitative analysis. A further study could perform a longitudinal analysis of changes in public opinion over a period of time.

The empirical findings in this study contribute to our understanding of information security. Cyberspace plays a pivotal role in ensuring state security. First, our society and economy are increasingly dependent on information technology and computer networks. On the one hand, emerging technologies associated with the Internet of Things, artificial intelligence and sensor networks are used not only to assist in the application and management of security solutions but also to facilitate the decision-making process to meet business goals. On the other hand, information technology may pose a threat to societies. Second, cyberspace is vulnerable to manipulation. Intensive disinformation campaigns lead to economic manipulation and bring major political gains to those who stage the campaigns. In fact, fake content on social media quickly becomes viral: it is disseminated faster and reaches a greater number of users than true content. Given that artificial intelligence systems adapt the content to match the user interaction profile, disinformation campaigns are extremely effective. They are aimed at blocking the exchange of information, marginalization of independent groups and civic movements, limiting public debate, maximizing confusion, and disrupting the other side's decision-making processes. As Liedel (2008) notes, the dissemination of disinformation in the public information system can evoke the mood and political climate intended by the propagandist, which will result in making the decisions that are in line with the expectations of those staging the disinformation campaign.

Apart from disinformation, rising polarization poses a serious threat to state security. A widening divide manipulates the individual's opinion by marginalizing opposing views, focusing their attention on different issues, which results in increased societal distrust and social tensions. Furthermore, pervasive polarization damages democracies, gives rise to populism and nationalism, and weakens the international position of the country making it more vulnerable to global threats.

Acknowledgements – This study was supported by National Science Centre in Poland (NCN) (Grant No. 2019/03/X/HS5/01934)

Declaration of interest – The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Araźna, M. (2015). Conflicts of the 21st century based on multidimensional warfare - "hybrid warfare", disinformation and manipulation. *Security and Defence Quarterly*, *8*(3), 103–129. https://doi.org/10.5604/23008741.1189421
2. Baden, C., & David, Y. (2018). On resonance: a study of culture-dependent reinterpretations of extremist violence in Israeli media discourse. *Media, Culture & Society*, *40*(4), 514–534. https://doi.org/10.1177/0163443717734404
3. Bajarūnas, E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View,* 19(1), 62-70. https://doi.org/10.1177/1781685820912041
4. Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.
5. Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 U.S. Presidential election online discussion. *First Monday*, *21*(11). https://firstmonday.org/article/view/7090/5653
6. Brachten, F., Stieglitz, S., Hofeditz, L., Kloppenborg, K., & Reimann, A. (2017). *Strategies and influence of social bots in a 2017 German state election – A case study on Twitter*. https://arxiv.org/ftp/arxiv/papers/1710/1710.07562.pdf
7. Carothers, T. & O'Donohue, A. (2019). *Democracies divided. The global challenge of political polarization.* Washington, D. C.: The Brookings Institution Press
8. Code of Practice on disinformation, (2019). https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation%0D
9. Colliander, J. (2019). "This is fake news": Investigating the role of conformity to other users' views when commenting on and spreading disinformation in social media. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2019.03.032
10. Domalewska, D., & Bielawski, R. (2019). Social bots as vehicles of spreading disinformation. Implications for state security. Soliman, K. S. (ed.) *Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage. Proceedings of the 34th International Business Information*

Management Association Conference (IBIMA), 3263-3270
11. Hawdon, J., Shyam, R., Leman, S., Bookhultz, S., & Mitra, T. (2020). Social media use, political polarization, and social capital: Is social media tearing the U.S. apart? In G. Meiselwitz (Ed.), *Social computing and social media. Design, ethics, user behavior and social network analysis* (pp. 243–260). Springer. https://doi.org/10.1007/978-3-030-49570_17
12. Hegelich, S., & Janetzko, D. (2016). Are social bots on Twitter political actors? Empirical evidence from a Ukrainian social botnet. *Proceedings of the Tenth International AAAI Conference on Web and Social Media*, 17–20. https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13015
13. Howard, P. N., & Kollanyi, B. (2016). Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2798311
14. Hudgins, J., & Newcomb, A. (2017). Google, Facebook, Twitter and Russia: A timeline on the '16 election. *NBC*. https://www.nbcnews.com/news/us-news/google-facebook-twitter-russia-timeline-16-election-n816036
15. Ivančík, R., Jurčák, V. & Nečas, P. (2014). On some contemporary global security risks and challenges. *Security and Defence Quarterly*, 4(3), 34–49. https//doi.org/10.5604/23008741.1152548
16. Kaylor, B. (2019). Likes, retweets, and polarization. *Review & Expositor*, *116*(2), 183–192. https://doi.org/10.1177/0034637319851508
17. Kligler-Vilenchik, N., Baden, C., & Yarchi, M. (2020). Interpretative Polarization across Platforms: How Political Disagreement Develops Over Time on Facebook, Twitter, and WhatsApp. *Social Media + Society*, *6*(3), 205630512094439. https://doi.org/10.1177/2056305120944393
18. Klimburg, A. (2018). Trolling, hacking and the 2016 US presidential election. *Nature*. https://doi.org/10.1038/d41586-018-06942-9
19. Liedel, K. (2008). Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego, Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego. https://liedel.pl/?p=13
20. McCoy, J. & Somer, M. (eds) (2019). Polarizing Polities: A Global Threat to Democracy. *Special Issue, The ANNALS of the American Academy of Political and Social Science* 681(1). https://doi.org/10.1177/0002716218818058
21. Monaghan, A. (2019). *Dealing with the Russians*. Cambridge: Polity Press
22. Mustonen-Ollila, E. B., Lehto, M., & Heikkonen, J. (2020). Components of defence strategies in society's information environment: a case study based on the grounded theory. *Security and Defence Quarterly*, *28*(1), 19–43. https://doi.org/10.35467/sdq/118186
23. Ratkiewicz, J., Conover, M. D., Meiss, M., Gonçalves, B., Flammini, A., & Menczer, F. (2011). Detecting and Tracking Political Abuse in Social Media. *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*. https://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2850/3274/
24. Sunstein, C. R. (2017). *#Republic. Divided democracy in the age of social media*. Princeton University Press
25. Świerszcz, K. (2017). Systemy informacyjne jako narzędzie bezpieczeństwa - ochrony i monitoringu centrów logistycznych. In J. Żylińska & I. Przychocka (Eds.), *Nauki społeczne i ekonomiczne – węzłowe zagadnienia* (pp. 509–523). UTH
26. Tworzecki, H. (2019). Poland: A Case of Top-Down Polarization. *The ANNALS of the American Academy of Political and Social Science*, *681*(1), 97–119. https://doi.org/10.1177/0002716218809322

27. Urych, I. (2013). Wartości wychowania a bezpieczeństwo młodego człowieka. *Zeszyty Naukowe AON,* 90(1), 227-241.
28. Węglińska, A. (2018). Astroturfing internetowy a zagrożenie bezpieczeństwa - protesty w obronie sądów w Polsce, boty i dezinformacja. *Rocznik Bezpieczeństwa*, 68–81
29. Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday*, *21*(4). https://firstmonday.org/article/view/6161/5300
30. Żakowska, M., & Domalewska, D. (2019). Factors determining polish parliamentarians' tweets on migration: A case study of Poland. *Politologicky Casopis*, *2019*(3). https://doi.org/10.5817/PC2019-3-200

SAFETY&DEFENSE
ISSN 2450-551X

Trends in the Development of Russian Precision-Guided Weapons

Mirosław BANASIK

Jan Kochanowski University, Kielce; miroslaw.banasik@interia.pl,
ORCID 0000-0002-9358-1240

DOI: https://doi.org/10.37105/sd.107

Abstract

This article presents the results of research that set out to identify and diagnose the trends found in the development of Russia's precision-guided weapons. The research process mainly employed the critical assessment of the literature and comparative analyses. As a result of the research, it was established that Russian thought on the strategic use of precision destruction weapons was historically determined and changed with technological progress, economic opportunities and changes in foreign policy objectives. Today, precision-guided weapons are complex strike systems capable of shaping the battlespace. Its high effectiveness makes it a real threat to objects that determine the opposing side's defense capability and can be considered strategic. The new generation of precision-guided weapons and hypersonic weapons will be crucial in achieving victories in armed struggle in the near future. Precision weapons will also be an effective tool of pressure and blackmail used to achieve the goals of international competition without the need for direct military confrontation.

Keywords

precision guided weapons, strategic thinking, Russia, defense

Submited: 01.03.2021 Accepted: 22.03.2021 Published: 01.04.2021

1. Introduction

Trends in the evolution of means of warfare reflect the development of civilization and influence the prevailing principles of the art of war. The machine gun and the massive use of artillery made World War I a positional war. By 1939, the tank, radio, close air support, and the creation of armored divisions restored mobility to the battlefield. In the 1920s and 1930s, Soviet military theorists developed the concept of conducting the so-called deep battle, which emphasized combined arms operations at the tactical, operational, and strategic levels. The principal developers of this concept, including Mikhail Tukhachevsky and Vladimir Triandafilov, envisioned that deep indirect fire would be necessary in such operations at all three levels of armed struggle. They believed that indirect fire would create the conditions necessary to break through the enemy's frontal defenses and penetrate deep into the defenses and prevent the enemy from reconstituting the forward edge of the defenses (Radin et al., 2019, p. 89). This concept was an attempt to incorporate new technology into the traditional Russian strategy of conducting armed combat. The essence of waging a deep battle was to prevent second echelons and reserves from reaching the battlefield and to overwhelm the troops with fire throughout the depth of the battlegroup. In reality, however, it was not until fifty years later that the Soviet armed forces were able to implement the operational concepts begun in the 1920s. Under Warsaw Pact plans, by using coordinated, deep conventional and nuclear strikes against NATO, the intention was to launch a Soviet offensive in Europe with the goal of reaching the English Channel quickly (Ruehl, 1991).

Russian interest in precision-guided weapons (PGW)[1] has evolved with changes in the international security environment, theories of future warfare and strategic deterrence. In the early 1990s, the rapid development of modern technologies enabled the West, and above all the United States of America (USA), to make precision strikes, which revolutionized the way military combat was conducted in the 20th century. In a way, it is paradoxical that Russia appreciated the importance of these weapons only in the second decade of the 21st century, because one of the pioneers of thinking about the revolutionary nature of precision strikes was Marshal Nikolai Ogarkov of the Soviet Union, who died in the mid-1980s. At the time, Soviet engineers were working on designs for the first generation of domestic precision-strike weapons, but the collapse of communism and the Soviet Union caused serious delays in their development. Therefore, the Russian Federation had a limited number of cruise missiles with conventional warheads until 2010. Today, however, precision strike capabilities are prioritized both in military theory and in the development plans of the Russian Federation Armed Forces.

The problematic situation thus identified leads to the formulation of the main research problem: *What trends can be identified in the development of Russia's precision-guided weapons?* The main research problem was fragmented and the following specific problems were identified:

1) How should the concept of precision-guided weapons be understood?

2) How did Russian views on the use of precision-guided weapons change?

This article presents the results of the research which set out to identify and diagnose the trends found in the development of Russia's precision-guided weapons. The point of reference in the research was the combat experience and the directions of development taken by the US strike systems as determined by the application of modern technologies. Against this background, it was possible to analyze the evolution of Russian strategic thought from World

[1] The term precision-guided munition (PGM) is commonly used in American literature. In this paper, the author uses the term precision guided weapon (PGW), which should be understood in the same way as PGM.

War II to present. Moreover, identifying the factors that determined that the development of precision-guided weapons in the Russian Federation was given the highest priority. The research conclusions presented in this article are the result of the application of critical literature assessment and comparative analysis, as well as inductive and deductive reasoning.

2. The essence of precision-guided weapons

Precision has always been recognized as an important feature in the development of weapon systems. The renowned military theorist, strategist, and historian, General J.F.C. Fuller considered accuracy to be one of the five recognizable attributes of a weapon, along with range, firepower, and portability. Of all these attributes, he considered range to be the attribute that is crucial in the conducting of armed combat (Fuller, 1945, p. 7). It is worth noting that modern PGW combine the qualities of accuracy, range, firepower, and fire-carrying capabilities, and this combination makes them a powerful multiplier of combat power in today's era.

The philosophy of military operations that took place during World War II was based on conducting large-scale, imprecise bombing campaigns. As technology advanced, air operations conducted in the late 20th century targeted selective targets that were individual tanks, artillery pieces, or even infantry. After all, there is no logical reason why missiles or bombs should be wasted without achieving operational effects (Meilinger, 1995, pp. 41-47). Viewed from another perspective, the philosophy of warfighting in World War II reflected the opinion that precision was only possible by achieving the operational objective, and not the object of impact. Subsequent air campaigns took advantage of the opportunities afforded by technological advances and focused on both a precisely defined object of impact and the exercise of precise control over the weapons themselves. The quest for precision through accurate identification of the object of impact remains an essential aspect of military power projection. Historical experience suggests that the best results have been achieved by combining strike platforms with intelligent means of delivery and operator experience. However, it is important to remember that precision is a relative concept, relating to the time at which the weapon is used.

The term precision is directly related to accuracy. Accuracy refers to the closeness of a measured value to a standard or known value, while precision refers to the closeness to each other of two or more measurements made. Precision is independent of accuracy. One can be very precise but inaccurate. It is also possible to be precise but imprecise. For example, if the average measurements of a certain quantity are close to a known value but do not coincide, then we have precision without precision. In other words, accuracy describes the difference between the measurement and the actual value, while precision describes the difference that is observed by repeatedly measuring a specific quantity with the same instrument. A good analogy for understanding accuracy and precision is to imagine a basketball player shooting a ball into a hoop. If the player shoots accurately, it means that he attempts to direct the ball into or near the hoop. If a player throws the ball accurately, he aims for the same place, which may be the hoop itself or somewhere nearby. A good player, will be both accurate and precise when shooting the ball in the same way every time in the hoop (Accuracy).

In military literature, the term "precision-guided weapon" refers to a guided weapon that is capable of destroying a target, generally with a single projectile. This definition covers a fairly wide range of means of destruction including both miniaturized and multi-ton guided aerial bombs weighing only a few grams, manually launched small unmanned aerial vehi-

cles, and intercontinental ballistic missiles (Miasnikov, p. 4). What is important in the definition is the wording regarding the weapon's targeting capability, or more specifically, the weapon's targeting capability. Most relevant aspect is the ability to guide in the last phase of flight of the means of destruction (rocket or bomb).

There are several reasons why it is legitimate to use the term "guidance" instead of "precision strike," despite the fact that the latter has gained widespread acceptance. First, precision striking is always associated with accuracy. However, this raises the question of the value of this accuracy, which de facto varies and depends on the type of weapon. Secondly, targeting is associated with the attribute of making aiming corrections in all phases of the flight of the means of destruction. This attribute is crucial and, based on it, weapons and ammunition can be classified as guided or unguided (Watts, 2007, p. 7). Ammunition alone is not sufficient to meet the requirements of the concept of using precision-guided weapons. For guidance, it is necessary to have accurate information about the object of impact.

The term "precision strike," as noted earlier, is related to the attributes of weapon systems that are necessary to successfully paralyze an enemy on the battlefield. Precision-strike weapons include land-, air-, and sea-launched missiles, torpedoes, and guided bombs carried by aircraft. Precision interaction is enabled by systems that locate targets, make strikes, generate desired effects and evaluate them, and maintain the ability to strike again if necessary (Joint, 1996, p. 21). Precision strike weapons are designed to destroy point targets and minimize collateral damage (DOD, 2020, p. 170). At this point, it is important to emphasize again that precision-guided weapons, once activated, can be actively corrected during flight and target guidance, thereby make correcting errors that may have occurred during the initial assignment to destroy targets. Target guidance should be understood as actively conducting corrections during the final phase of flight, virtually up to the point of impact (Watts, 2007, p. 26).

In the late 1970s in the Soviet Union, the terms "precision-guided weapons" and "precision-guided munitions" (Russian: *высокоточное оружие*) were implemented into Russian military terminology by translating its meaning from Western concepts of military success. The correct Russian meaning was broad and referred to systems that allowed precise damage to be inflicted on the enemy from long distances (McDermott, 2017, p. 8). Currently, in the Russian Federation, long-range PGW are ground, air, and sea-based missile complexes designed to selectively and reliably destroy stationary and quasi-stationary land objects, fired from their means of delivery, from a distance of not less than 400 km from the target (Dictionary). When it comes to distance (range of fire), opinions are divided, mainly due to the fact that no qualitative indicators are available. Although the term "long-range" has no specific definition, it is assumed that, in its broadest sense, it encompasses any system that can fire at distances in excess of 1,000 km. Long-range ballistic missiles practically cross both of these thresholds. However, it must be taken into account that they are designed to carry nuclear, not conventional, weapons. Some states use shorter-range ballistic missiles without nuclear warheads. While doing so, one must keep in mind that their accuracy should be up to a few meters to be effective (Borrie et al., 2019, p. 4). It would be more appropriate to consider the definition of long-range as a qualitative characteristic, reflecting the ability of the weapon to strike critical infrastructure located in the entire depth of the adversary's territory (or the bulk of it). In this sense, on European territory, the threshold could be lowered to 500 km due to the relative compactness of the hypothetical theater of operations and the density of critical infrastructure. This may lead to the conclusion that the quantitative definition of long range will vary for different military-strategic situations. One of the possible consequences of such an approach in the future may be the intensification of the trend toward regionalization, that is, clearly defined geographical areas with specific parameters (Arbatov et al., 2019, p. 27).

According to Russian views, PGW are a type of weapon equipped with command-and-control systems that allow the elimination of targets with a single munition with a probability of at least 0.5. The high probability of hitting the target is achieved by conducting periodic correction of the trajectory of the munition (missile, rocket, warhead) after it is fired from the means of delivery until it reaches the target of attack. The correction of the trajectory of the munition to the target is provided by the guidance system (Ènciklopedija). Rather than taking the weapon's range or the missile's airspeed as criteria for qualification, it is the combination of these parameters with maneuverability that distinguishes PGW from ballistic missiles and makes them strategically relevant. Maneuverability can enable a greater precision strike and therefore gives the system the ability to use conventional warheads effectively. At supersonic speeds, it also has an added importance due to the need to evade missile defense systems and also due to the need to miss moving targets (Borrie et al., 2019, p. 5).

Initially in the 1990s, Russia used the term reconnaissance-strike complex (*разведывательно-ударный комплекс*) or reconnaissance-fire complex (*разведывательно-огневой комплекс*). At the beginning of the new millennium, Russian scientists added the word "system" to better reflect the conceptual assumptions of its combat use (McDermott, 2017, p. 8). The terminology used for conventional precision weapons in official documents, statements by political and military leaders, and in military journals varies. For example the Russian military doctrine of 2014 includes the term "precision weapons system" (*систем высокоточного оружия*) and "strategic, non-nuclear precision weapons systems" (*стратегических неядерных систем высокоточного оружия*) (Voyennaya, 2014, p. 5). Other terms used to refer to conventional PGW and conventional long-range precision weapons include: high-precision means of warfare (*высокоточное средсва поражения*), long-range non-nuclear (conventional) precision weapons (*высокоточное неядерное (обычное) оружие для дальнего радиуса действия*), conventional strategic weapons (*конвенциональное стратегическое оружие*), a precision non-nuclear weapon with a large radius of effects (*высокоточное неядерные средства большой радиуса действия*), precision-guided combat complexes (*высокоточнное боевые комплексы*), non-nuclear precision-guided weapon system (*неядерная система высокоточного оружия*), strategic non-nuclear weapons (*стратегическое неядерное оружие*), conventional long-range precision weapons (*обычное высокоточное оружие большой дальности*) and long-range precision weapons (*высокоточное оружие большой дальности*).

According to the Russian perspective, precision strike weapon complexes/systems include the information gathering and battlefield situation assessment subsystems, the command-and-control subsystem, and the missile strike subsystems (Watts, 2007, p. 28). Depending on the military structure that includes a given strike system and the type of munitions possessed, precision strike weapons can be used to accomplish tactical, operational, and strategic tasks. Precision strike systems include air- and sea-launched cruise missiles, certain types of operational-tactical missiles, air and missile defense sets, guided missiles, classic and cassette bombs dropped from aircraft, and selected artillery and missile complexes of anti-ship systems (Ènciklopedija).

The advantage of PGW over unguided weapons is their long-range and reduced need for repeated strikes to achieve desired operational effects. PGW allow shaping the battlespace, increasing the protection of their own troops. The main disadvantage of PGW is their high cost, especially for long-range missiles. Nowadays, to ensure high hit accuracy, a combination of radio signals from the Global Positioning System (GPS), laser guidance and inertial navigation systems with gyroscopes are used for guidance (Hoehn, 2020, p. 2).

Precision weapons are so effective that they can pose a threat to all elements of the strategic nuclear triad: fixed and mobile strategic missile launchers, submarines carrying nuclear missiles, and strategic bombers on airfields and in the air, which makes them currently

treated on par with nuclear weapons. To plan a strike, it is necessary to analyze all operational conditions in terms of expected effects due to the specific vulnerabilities of the target and the characteristics of the means of destruction used (Miasnikov, 2020, p. 4).

3. The evolution of precision-guided weapons

Prior to 1943, most ammunition used on the battlefield missed its target because initial aiming errors could not be corrected. Unguided ammunition was used, and its lack of accuracy was compensated for by its quantity. The earliest instances of combat success with precision-guided munitions occurred in March 1943. The German Navy introduced the first G7e/T4 Falcon acoustic torpedo on four submarines. Its use probably led to the sinking of four merchant ships, which was considered the first successful use of guided munitions. In May 1943, an American Mark-24 acoustic torpedo fired from a patrol plane sank the German submarine U-640, and by the end of the war, 37 German and Japanese submarines, damaging 18 others (Watts, 2007, p. 3).

Aerial munitions meeting the guidance criterion were first developed in the 1940s when the U.S. Army Air Corps tested the feasibility of using radio to guide bombs dropped from aircraft. At that time, an accuracy of 1,200 feet was achieved, and 16% of the munitions dropped by the crews landed within 1,000 feet of the established target (Correll, 2008). While the system showed promise in terms of accuracy, it was not fully utilized during World War II. This was likely due to technological limitations and the high cost per munition used. By the 1950s, guidance systems used television signals and required a companion aircraft to provide command and control of the bombs being dropped (Hoehn, 2020, p. 2). During the 1960s and early 1970s, progress in the evolution of PGW was rather limited. The weapons were too inaccurate and susceptible to anti-aircraft defenses, so no breakthrough could be made with them in terms of the way armed struggle was conducted. The development of anti-aircraft means, especially short- and medium-range missile sets, forced such changes in the American combat systems that made it possible to defeat it (Watts, 2007, p. 6). The breakthrough appears to have been made in Vietnam with the introduction of laser-guided aerial bomb guidance capabilities. Based on wartime experience, it was determined that the U.S. military used more than 10,500 laser-guided bombs in 1973, with 5,107 weapons achieving a direct hit and another 4,000 coming within 26 feet of the target (Hoehn, 2020, p. 2).

The Soviet Union's investment in increasingly sophisticated weapons in the 1970s, along with the rapid expansion of the Soviet naval fleet, stimulated U.S. countermeasures, which turned out to be increasingly precise weapons. One of these was the acquisition of the F-14 Tomcat supersonic airborne fighter with variable wing geometry, armed with six Phoenix long-range guided air-to-air missiles, as well as advanced early warning radars and guidance systems. In addition, new precision airborne and missile defense weapons have been acquired, notably the Phalanx and Sea Sparrow, and the Harpoon (Hallion, 1995) short-range anti-ship cruise missile, launched from the surface, underwater, and airborne platforms, has been fielded.

Until the Persian Gulf War, aircraft capabilities permitted low-altitude placement of unguided munitions within 30 feet of the target. However, Iraqi air defenses, with their large numbers of man-portable and artillery anti-aircraft sets, did not permit such routine performance. On the other hand, operations above 5,000 meters were very complicated in terms of bombing accuracy, especially against targets requiring direct hits, such as hangars, bunkers, tanks, and artillery assets (Hallion, 1995).

Unlike the United States, the Soviet Union began to invest in traditional types of conventional forces, i.e., tanks, infantry fighting vehicles, and tactical aircraft from the late 1960s onward. By the late 1970s, the authorities concluded that the threat of aggression from the North Atlantic Alliance had been greatly reduced (Trulock, 1988, p. 97). Looking ahead, however, it did not appear that this favorable situation was going to last forever. The advent of U.S. precision strike capabilities began to shift the European balance in NATO's favor, prompting the abandonment of the investment the Soviets had made in traditional conventional forces during the previous decade. By the early 1980s, Soviet military authorities and military theorists were increasingly concerned that emerging military technologies, specifically a new family of highly accurate, precision-guided non-nuclear munitions systems, would lead to a revolution in military affairs by the end of the twentieth century that would change the picture of warfare (Trulock, 1988, p. 97).

In the early 1980s, Russian military theorists wrote extensively about the likely implications of using reconnaissance and strike systems for future warfare. Systems with long-range precision strike capabilities enhanced the ability to inflict losses deep within enemy groupings, more than 10 times farther than was possible during World War II on the Eastern Front. Moreover, the probability of eliminating a target with a single shot of a precision weapon ranged from 0.6 to 0.9, for both stationary and mobile targets (Trulock, 1988, p. 107). As Marshal Nikolai Ogarkov wrote in May 1984, the development of non-nuclear means of striking, which included everything from precision munitions to fuel-air bombs, made it possible to significantly increase, the destructive potential of conventional weapons by at least an order of magnitude, thus bringing them closer in effectiveness to weapons of mass destruction (Watts, 2011).

U.S. tests conducted in 1982 confirmed that precision-guided missiles could be used to attack Soviet forces approaching from deep within a battle grouping, i.e., virtually from outside the front lines. In the case of the Warsaw Pact's attempt to overrun Western Europe, both the program codenamed Assault Breaker and the development of stealth aircraft such as the F-117 were intended to use U.S. technological capabilities to offset the three-to-one quantitative advantage the Warsaw Pact had in Central Europe at the time, which could eliminate the need for nuclear weapons (Watts, 2013).

The tests confirmed that nuclear munitions could be replaced by conventional precision-guided munitions in many cases and thus achieve the required level of destruction without incurring their own losses and raising the risk of nuclear escalation (Trulock, 1988, p. 110). This idea was not new. In fact, American defense specialists thought of it in the aftermath of the Vietnam War. In 1975, the final report of the research program on the development of long-range means of destruction concluded that precision conventional munitions could substitute for nuclear weapons in a variety of operational situations (Paolucci, 1975, p. 45), which was conceptually implemented in both the United States and the Russian Federation at the beginning of the new millennium.

In 1986, Russian concerns about the balance of power in Central Europe intensified when NATO decided to implement the concept of cutting-off second echelons and reserves (FOFA).[2] The essence of this concept was to increase the deep strike capability of conventional forces in the theater of operations, which was intended to eliminate the need for the Alliance to use nuclear weapons to deter Warsaw Pact aggression (Shaw, 1986, p. 1). Verification of the feasibility of U.S. air operations using PGW occurred in 1991 during the Gulf War. For the first time in the history of operational warfare, reconnaissance, radio warfare, communications, and command were integrated with precision strike systems, making it

[2] The FOFA concept was developed by Gen. Bernard W. Roders in 1984. It was designed as a complement to the NATO concept of the advanced forward deployment and air-to-ground battle strategy (Canan, 1984).

possible, virtually in real-time, to conduct the air campaign of Operation Desert Storm. Modern technologies made it possible not only for strike aircraft to remain invisible but also to integrate space with combat systems, as emphasized by prominent Russian experts in their assessments (Blank, 1991, p. 10). As the head of the Operational and Strategic Center of the General Staff, Sergei Bogdanov, recognized, the use of the reconnaissance capabilities provided by space for the needs of intellectualized precision strike complexes made it possible to achieve incredible operational effectivity (Blank, 1991, p. 10). In the opinion of Russian General Ivan N. Vorobyev, the effectiveness of PGW changes the picture of the armed struggle and deeply imprints on the strategy of its use in the future (Lambeth, 1992, p. 68). Andreev F. Krepinevich, compared Operation Desert Storm to the use of tanks, for the first time in history on a large scale, by the British at the Battle of Cambrai, France, in November 1917. He posited that the use of PGW leads to a whole new picture of the theater of operations and gives rise to another revolution in the conducting of armed struggle (Krepinevich, 2002, p. 3 & 9).

According to the Russian point of view, a high-precision weapon that is not subject to any quantitative, qualitative, or territorial restrictions, but is well camouflaged, makes it eligible for "anti-terrorist" treatment. It is also a weapon that can target strategic facilities. Furthermore, due to its minimal flight time and high targeting accuracy, it provides a surprise attack and significantly reduces the possibility of retaliation (Antonov, 2012, p. 65). Russian experts estimate that the another major trend in the development of high-precision, non-nuclear strike missile systems will be the use of space-deployed basing control systems (Arbatov & Dvorkin, 2012, p. 357). An orbital or semi-orbital high-precision missile strike system is likely to emerge in the foreseeable future, with implications for the future arms race. Over the next decade, nuclear deterrence is likely to remain an element of international security guarantees, but its importance can be expected to diminish. It is estimated that non-nuclear precision-guided systems are likely to play an increasingly important role in mutual deterrence and strategic stability. It is in the interest of the international community that this process takes place in a coordinated manner and is regulated by mutual agreements (Arbatov & Dvorkin, 2012, p. 357).

Today, the technological revolution is accelerating with the use of optoelectronics and satellite navigation systems. Work is also underway to make the weapon independent of weather conditions, and ammunition with optional warheads is being procured, enabling a variety of missions, from penetrating hard point targets to the ability to destroy superficially distributed single combat objects on the battlefield with a single salvo (Hallion). However, one should be aware that the acquisition of new weapons is not a simple procedure. There are a number of difficulties arising from the enormous complexity of integrating different types of munitions into a single weapon system. It is also necessary, for example, to skillfully use the information obtained from long-range reconnaissance systems. This information can be used to overcome the difficulties of positioning striking objects and tracking them, navigate the means of destruction, precise timing, and have an appropriate means of communication. Above all, it is essential in order to network the entire process of destruction, which would allow to exercise the command process in combat conditions and to destroy objects of strategic and operational importance in real-time (Watts, 2013).

Secondly, although modern precision-guided missile systems have made accuracy independent of the distance to the target and the location from which the munition was fired, they still have not made unit costs independent of the distance to the target. For example, the most expensive missiles today are U.S. Tomahawk missiles, which are several times more expensive than guided aerial bombs. Thus, unit costs are a major reason why the United States currently holds a monopoly on long-range PGW (Watts, 2013). Among the various

weapons, the future is likely to include networked precision-guided weapons, which will allow them to communicate with other systems on the battlefield. The exchange of information between the platforms delivering the means of destruction and the means of reconnaissance, including satellite, and command and combat management posts, will be crucial for accurate and precise mission execution (Esposito, 2019). In turn, the development of hypersonic systems of the Russian Federation may raise the risk of causing an unintended nuclear war, as it will deprive ground-based radars of the ability to determine in a timely manner the trajectory of enemy missiles and the area of their impact, which means that in response to this type of attack, a decision on the type of response will have to be validated immediately after the satellites generate a (probably false) nuclear alert (Arbatov, 2019). Given scientific and technological advances, it is reasonable to expect that deploying precision weapons systems in space could pose an even greater risk to international security (Dvorkin, 2019, p. 4).

It is estimated that future Russian high-tech precision-guided missile systems, mounted on a variety of platforms, are likely to have comprehensive destruction characteristics. In the Russian Federation, it is assumed that the conflict will not be confined to a single operational domain. Actors involved in the fight will likely move between domains, attempting to exploit those that will allow them to achieve the greatest advantage or those in which the likelihood of gaining an advantage will increase (Kepe, 2018, p. 16). In fact, the next generation of Russian PGW will likely be carried and operated by both conventional manned platforms and autonomous, unmanned aircraft. These weapons will have both highly lethal and nonlethal missile effectiveness. It will also likely be capable of operating in a physical environment while being controlled in a virtual. It will be able to be used alone or be integrated with other missile systems. It is likely that its range, maneuverability, and precision of strikes will be increased. Considering the arguments presented, it can be concluded that the directions of development of PGW will be set by hypersonic and laser weapons (Esposito, 2019).

4. Conclusion

Russia's interest in developing conventional precision-guided weapons is not new. In the transformation of the armed forces, acquiring new precision-guided capabilities is a top priority, as evidenced by the successful testing in 2018 of hypersonic weapon systems. They are also evidence of the evolution of Russian thought on conflict resolution in a strategic context. Understanding this trend requires taking into account historical circumstances, advances in Soviet and Russian military theory, addressing doctrinal assumptions and, above all, understanding the Russian Federation's foreign policy objectives.

As this article demonstrates, Russia has long regarded precision-guided weapons as an essential component of modern warfare. Marshal Nikolai Ogarkov is considered the father of this school of thought, but later Russian military theorists such as General Vladimir Slipchenko and others have also made significant contributions to its development. The economic collapse of the 1990s, combined with warming relations with the West, made indigenous development of precision-guided weapons both financially difficult and less politically necessary. However, this situation changed dramatically after Vladimir Putin came to power, the annexation of Crimea, and the Russian Federation's involvement in Syria.

As a result of the research, it was determined that there are terminological differences in understanding precision-guided weapon systems between the Russian Federation and the U.S. and NATO. Moreover, the Russian Federation uses a variety of nomenclatures to describe precision-guided weapons. According to the Russian perspective, precision-guided

weapons should be considered in terms of complex systems and should not be limited to means of destruction. Precision-guided weapons make it possible to shape the battlespace, which proves their high effectiveness. Therefore, they can pose a real threat to all of the elements of the adversary's defense system, and first and foremost the strategic nuclear triad. In the Russian Federation, precision-guided weapons are treated on par with nuclear weapons. It is believed that the rapid technological progress made in the last decade will make it possible to exploit space and make hypersonic weapons decisive for achieving victory in future armed struggle. It is estimated that hypersonic weapons, due to their attributes, will be used as a tool to apply pressure and aggression, and to achieve foreign policy objectives without the need for direct armed confrontation. The large-scale acquisition of hypersonic capabilities and the high effectiveness of the PGW will undoubtedly influence doctrinal changes and the strategy of its use in the future.

The author believes that the opinions and conclusions presented in this article may serve as a starting point for considering the utility of the PGW in the strategic context; and, in particular, their role in achieving the objectives of the rivalry that the Russian Federation is currently conducting on the international arena.

Declaration of interest - The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Accuracy vs. Precision. https://www.diffen.com/difference/Accuracy_vs_Precision
2. Antonov, A.I., (2012). *Контроль над вооружениями: история, состояние, перспективы* [Arms Control: History, Status, Prospects]. ПИР–Центр. http://mil.ru/files/morf/A_Antonov__monografia.pdf
3. Arbatov, A. (2019). *Роль ядерного сдерживания в стратегической стабильности. Гарантия или угроза* [Nuclear Deterrence: A Guarantee or Threat to Strategic Stability?]. Carnegie. https://carnegie.ru/2019/01/28/ru-pub-78209
4. Arbatov, A. & Dvorkin, V. (Ed.) (2012). *Противоракетная Оборона: Противостояние Или Сотрудничество?* [Missile Defense: Confrontation or Cooperation?]. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/PRO_Book_rus20121.pdf
5. Arbatov, A., Oznobishchev, S., & Bubnova, N. (Ed.). (2019). *Russia: Arms Control. Disarmament and International Security*. Primakov national research institute of world economy and international relations Russian academy of sciences.
6. Blank, S. (1991). *Soviet Military Views Operation Desert Storm: A Preliminary Assessment*. Strategic Studies Institute. https://www.researchgate.net/publication/279439030_The_Soviet_Military_Views_Operation_Desert_Storm_A_Preliminary_Assessment
7. Borrie, J., Dowler, A., & Podvig, P. (2019). *Hypersonic Weapons. A Challenge and Opportunity for Strategic Arms Control*. United Nations Office for Disarmament Affairs.

8. Canan, J.W., (1984.09.01). NATO On the Upbeat. *Airforce magazine*. https://www.airforcemag.com/article/0984nato/
9. Correll, J.T., (2008). *Daylight Precision Bombing*, Air Force Magazine. https://www.airforcemag.com/article/1008daylight/
10. *Defense Primer: U.S. Precision-Guided Munitions*. (2020). The Congressional Research Service.
11. *Dictionary military terms of the Russian Federation*. http://dictionary.mil.ru/folder/123102/item/129202/
12. *DOD Dictionary of Military and Associated Terms*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf
13. Dvorkin, V., (2019). *Стратегическая стабильность: сохранить или разрушить* [Preserving Strategic Stability Amid U.S.-Russian Confrontation]. Carnegie. https://carnegie.ru/2018/11/28/ru-pub-77809
14. *Ènciklopedija Minoborony Rossii*. https://desecuritate.uph.edu.pl/images/De_Securitate_NUMER_2_2019.pdf
http://энциклопедия.минобороны.рф/encyclopedia/dictionary/details_rvsn.htm?id=12896@morfDictionary
15. Esposito, F., (2019). *Precision-Guided Munitions of the Future and the Related Challenges to NATO*, JAPCC. https://www.japcc.org/precision-guided-munitions-of-the-future/
16. Fuller, J.F.C. (1945). *Armament and History: A Study of the Influence of Armament on History: From the Dawn of Classical Warfare to the Second World War*. New York: Charles Scribner's Sons. DOI: https://doi.org/10.1017/S003467050004050X
17. Hallion, R.P. (1995) *Precision Guided Munitions and the New Era of Warfare*, APSC Paper Number 53. Commonwealth of Australia. https://fas.org/man/dod-101/sys/smart/docs/paper53.htm
18. Hoehn, J.R. (2020). *Precision-Guided Munitions: Background and Issues for Congress*. Congressional Research Service.
19. *Joint Vision 2010*. (1996). Center for Counterproliferation Research National Defense University Washington.
20. Kepe, M. (2018). *Exploring Europe's Capability Requirements for 2035 and Beyond*. European Defence Agency.
21. Krepinevich, Jr, A.F. (2002). *The Military-Technical Revolution: A Preliminary Assessment*. Center for Strategic and Budgetary Assessments.
22. Lambeth, B.S. (1992). *Desert Storm and its meaning. The View from Moscow*. Rand Corporation.
23. McDermott, R.N., & Bukkvoll, T. (2018). Tools of Future Wars — Russia is Entering the Precision-Strike Regime, *Journal of Slavic Military Studies*, NO. 2, pp. 191-213. https://doi.org/10.1080/13518046.2018.1451097
24. Meilinger, P.S. (1995). *10 Propositions Regarding Air Power, Air Force History and Museums Program*. Air Force Historian.
25. Miasnikov, E. *Long-Range Precision-Guided Conventional Weapons: Implications For Strategic Balance, Arms Control And Non-Proliferation*. https://www.armscontrol.ru/pubs/en/em090918.pdf
26. Paolucci, D.A. (1975). *Summary Report of the Long Range Research and Development Planning Program (LRRDPP)*. Skyline Center.

27. Radin, A., Davis, L.E., Geist, E., Han, E., Massicot, D., Povlock, M., Reach, C., Boston, S., Charap, S., Mackenzie, W., Migacheva, K., Johnston, T., & Long, A. (2019). *The Future of the Russian Military Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition*. Appendixes. Rand Corporation.
28. Ruehl, L. (1991). Offensive defense in the Warsaw Pact, *Survival. Global Politics and Strategy*, Issue 5, pp. 442–450. https://doi.org/10.1080/00396339108442611
29. Shaw, A. (1986). *Technologies for NATO's Follow-on Forces Attack Concept*. Congress of the United State. https://ota.fas.org/reports/8630.pdf
30. Trulock, N. (1988). *Emerging Technologies and Future War: A Soviet View*. In Marshall, A.W. & Wolf, C., Jr. (Ed.), *The Future Security Environment*. US Government Printing Office. http://albertwohlstetter.com/CILTS/FSE/19881000-CILTS-FutureSecurityEnvironment.pdf
31. Watts, B.D. (2013). *Precision Strike: An Evolution. The world once thought guided munitions were the future of warfare. The truth has been more complicated*, The National Interest 02.11.2013. https://nationalinterest.org/commentary/precision-strike-evolution-9347
32. Watts, B.D. (2011). *The Maturing Revolution in Military Affairs*, Center for Security Studies. https://ethz.ch/content/specialinterest/gess/cis/center-for-securities-studies/en/services/digital-library/articles/article.html/162685
33. Watts, B.D. (2007). *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects*, Center for Strategicand Budgetary Assessments.
34. *Voyennaya doktrina Rossijskoj Fiedieracyi* (2014). Moscow.

SAFETY&DEFENSE
ISSN 2450-551X

British-Kenyan Cooperation in the Areas of Defense and Security – A Postcolonial Perspective

Łukasz JUREŃCZYK

Kazimierz Wielki University, Bydgoszcz, Poland,
lukaszjurenczyk@ukw.edu.pl, ORCID: 0000-0003-1149-925X

DOI: https://doi.org/10.37105/sd.104

Abstract

This paper aims to analyze and evaluate the cooperation between the United Kingdom and Kenya in the areas of defense and security in the second decade of the 21st century. The analysis is conducted in the light of the theory of postcolonialism. The research uses the method of analyzing text sources. This paper begins with an introduction synthetically describing the transition of British-Kenyan relations from colonial to postcolonial and the main methodological assumptions of the paper. Then the theoretical assumptions of postcolonialism are presented. The next three sections include: the circumstances of cooperation in the fields of defense and security; Military cooperation to restore peace in Somalia; and The United Kingdom programs to enhance peace and security in Kenya and East Africa. The paper ends with a conclusion.
The main research questions are: Was the defense and security cooperation during the recent decade a continuation of the status quo or was there something different about it? If there was something different, what caused the change? Are there prospects for strengthening the cooperation in the future?
Over the past decade, the United Kingdom has strengthened cooperation with Kenya in the areas of defense and security. The actions of the British were aimed at strengthening Kenya's military potential and its ability to influence the international environment. The United Kingdom's increased involvement in Kenya was driven by internal, bilateral and international factors. Kenya also expressed its readiness to strengthen this cooperation, guided by its own interests.

Keywords:

defense cooperation, foreign policy, Kenya, security cooperation the United Kingdom.

Submited: 22.02.2021 Accepted: 03.04.2021 Published: 15.04.2021

1. Introduction

After the Second World War, the decolonization of the British Empire began, starting with the Indian subcontinent. As a result, the UK's influence on the international security environment diminished. Outside Europe, it retained significant importance in the Middle East and parts of Africa, including Kenya (Bell, 2013). Due to the abuses of the British against the Kenyans, in 1952 the Mau Mau organization led by Jomo Kenyatta launched a rebellion against the colonial authorities, which deepened hostility between countries and societies (Callaghan, 2007). In 1955, the British managed to suppress the rebellion at the cost of about 3,000 members of the Kikuyu tribe and several hundred British citizens. The British used brutal methods, including the placement of persons suspected of insurgent activity in concentration camps and the use of torture, slave labor and murder in them (Elkins, 2013). At that time, the United Kingdom forged its counter-insurgency policy in Kenya. Even then, the British knew that gathering intelligence from captured insurgents was the key to success. Forcing information to protect British soldiers and civilians led to the ill-treatment of detainees (Rowe, 2016). Despite the British brutal attempt to maintain the colonial empire, the rebellion led to Kenya's autonomy in 1958 and independence in 1963 (Nasong'o, 2007).

Independent Kenya was of less importance in the United Kingdom's foreign and security policy (Cullen, 2017). In the following decades, the involvement of the Soviet Union in the former British colonies in Africa increased, which was a cause of concern for Great Britain (White, 2002). However, the risk of Kenya entering the zone of Soviet influence was limited. One of the reasons was Kenya's dependence on trade with the United Kingdom, including imports of British weapons, which lasted until the end of the Cold War (Kaplan, 1982).

After the Cold War, Kenya and the UK cooperated mainly in the area of international security. They undertook joint efforts to resolve conflicts in Central and Eastern Africa, including the civil war in Rwanda (Kameron, 2013). Counteracting international terrorism was systematically becoming an increasingly important area of cooperation between the states. In 1998, Al-Qaida bombed US embassies in the Kenyan capital Nairobi and the city of Dar es Salaam in neighboring Tanzania. They were just one of a series of attacks carried out by this terrorist organization in the 1990s (Brown, 2013). As we know, the group carried out the most spectacular attack on September 11, 2001, in the United States. At the beginning of the 21st century, both the UK and Kenya have engaged in the global war on terror led by the US. Even so, British influence in Kenya has been diminishing, partly being superseded by rising Chinese influence (Branch, 2011). This has been a consequence of the adoption of the "Look East Policy" by the Kenyan Government.

The aim of this paper is to analyze and evaluate cooperation between the United Kingdom and Kenya in the area of defense and security in the last decade. The analysis is conducted in the perspective of the theory of postcolonialism. The research uses the method of analyzing text sources. The main research questions are: Was the defense and security cooperation during the recent decade a continuation of the status quo or was there something different about it? If there was something different, what caused the change? Are there prospects for strengthening the cooperation in the future?

Over the past decade, the United Kingdom has strengthened cooperation with Kenya in the areas of defense and security. The increased involvement in Kenya was driven by internal, bilateral and international factors. This mainly concerned Great Britain's search for a new international role due to Brexit, its benefit from cooperation with rapidly developing

Kenya, attempts to rebuild its position in East Africa, the need to stabilize the region, preventing the spread of China's influence, using its advantage over other powers resulting from postcolonial ties, and the redemption of complicated colonial history. For Kenya, cooperation with the United Kingdom in the areas of defense and security offers the opportunity to strengthen its security forces, increase the possibility of stabilizing neighboring countries, including Somalia, counter the spread of terrorism and extremism more effectively, increase its position in East Africa, and benefit from development cooperation. Over the last decade, the convergence of goals, the possibility of achieving mutual benefits, historical and cultural ties, and the readiness to overcome the negative consequences of colonialism have favored efforts to strengthen cooperation between the United Kingdom and Kenya in the areas of defense and security. This trend should continue throughout the current decade.

2. Theoretical assumptions

In the 21st century, Kenya's foreign and security policy has undergone a major paradigmatic shift. Kenya's orientation has been defined as moving further away from traditional Western allies, i.e. Great Britain and the United States. Kenya has strengthened its relations with the emerging global powers, mainly with China, and has also focused more on the region of East Africa. However, Kenya's relations with the West may turn out to be deeper than it seemed in recent years, and its future policy direction is not certain. It is because Western states, especially the United Kingdom, are trying to warm up tarnished relations with Kenya (Nzau, 2016). This is especially true in the area of security and defense, where the states have many common interests.

Contemporary relations between the United Kingdom and Kenya in the fields of security and defense can be seen from the perspective of postcolonial theory. Jean-Paul Sartre, Franz Fanon and Edward Said, who defined themselves as representatives of the postcolonial school of thought, should be considered the pioneers of postcolonial studies. The postcolonial current was established as an independent research approach in the mid-1980s. Part of the literature of anti-colonial movement leaders, including Mahatma Gandhi, Leopold Senghor and Kwame Nkrumah, is also included in the postcolonial canon. In the 21st century, Gayatri Spivak, Homi Bhabha and Walter D. Mignolo may be recognized as the best-known representatives of the academic community participating in the postcolonial discourse (Polus, 2014).

The theory of postcolonialism primarily criticizes the one-sided view of the period of colonialism and neo-colonialism from a Western perspective. This perspective may lead to the belief that the West was an active player expanding its influence, ideas and values, and that the rest of the world was a passive, irrational witness of its development, acting like a victim or subject to external authority (Gawrycki, 2013). Such an attitude entails binary categorizations (master-slave, colonizer-colonized, civilized-uncivilized, white-black), being a derivative of triumphalist European historiography, justifying the imperial political benefits of the West, its legal system and morality (Grovogui, 2007). Proponents of the postcolonial current tend to redefine the period of colonialism, supplementing the discourse with the perspective of colonized entities, taking into account the contemporary impact and effects of colonialism on political, social and cultural issues (Gawrycki, 2013).

The concept of postcolonialism is most often understood as the history of former colonies after the process of decolonization. According to some authors, the prefix "post" is

supposed to suggest that colonialism is over. However, it is a falsification of reality (Domańska, 2008). Many postcolonial scholars emphasize the considerable degree of continuity and durability of colonial forms of power in contemporary world politics. The degree of protection of economic and military interests by world powers in the southern countries sometimes seems to be higher than in the period of direct domination, i.e. colonialism. Most often, this phenomenon is called neo-colonialism. The starting point of postcolonialism are issues of global inequalities, forms of power that enable them, and persistent forms of the dominance of rich over poor (Smith & Owens, 2008). Postcolonialism should rather be considered as an international system after the formal political process of decolonization, but with the consequences of the colonial period and some of its remains. In this sense, postcolonialism is a form of colonialism that can last forever. The possibility of overcoming it depends on both postcolonial governments and societies and former colonial empires (Mazurczak, 2016).

Postcolonialism has specifically drawn attention to the international relations theory's neglect of the critical intersections of an empire, race/ethnicity, gender and class in the workings of global power that reproduce a hierarchical system. This hierarchy focuses on the concentration of power. The central theme of postcolonialism is that Western perceptions of the non-West are a result of the legacies of European colonization and imperialism. Non-Western states and peoples are presented most often as "others", usually in such a way that it can be understood as "inferior". This approach helped the West to justify its domination over other peoples in the name of bringing the civilization or progress (Nair, 2017).

According to representatives of postcolonialism, identities do not have a permanent and inherent character but arise during social processes and practices. Cultural hybrids arise as a result of the mutual co-existence of the colonizer and colonized identity. Nevertheless, socially constructed racial, gender and class differences are understood as factors enabling the emergence and duration of global subordination and control hierarchies. Racism, in turn, partly contributed to humanitarian norms sanctioning certain obligations as a type of colonial mission (Smith & Owens, 2008).

Postcolonialism interrogates and somehow challenges a world order dominated by major state actors and their domineering interests and ways of looking at the world (Nair, 2017). Representatives of postcolonialism not only criticize reality but also explore possible forms of resistance to colonial ideologies and formulate strategies for assuming real power (Smith & Owens, 2008).

3. The circumstances of cooperation in the areas of defense and security

The historic British involvement in Africa has had a significant impact on Kenya, where modern legal, institutional and cultural patterns have spread. However, some of the actions of the colonial power led to tensions with Africans, including Kenyans, which the British government has to deal with (International Relations and Defence Committee, 2020). The United Kingdom and Kenya have a long tradition of bilateral relations. They have mainly cooperated in areas such as trade, investments, tourism, defense and security, anti-piracy, counter-terrorism, and climate change (Kenya High Commission UK). From a postcolonial perspective, we can say that British-Kenyan relations were projected by a period of colonialism, the consequences of which significantly influence contemporary relations and facilitate cooperation. Prime Minister Theresa May said "Kenya holds a special

place in the hearts of the British people and our countries share a long history that has left us deeply connected to one another" (GOV.UK, 2018d).

As part of the redemption of difficult moments in common history, in the summer of 2013 Secretary of State for Foreign and Commonwealth Affairs William Hague acknowledged and apologized for British crimes against the Kikuyu ethnic group during the Mau Mau rebellion. He announced reparation payments for elderly Kikuyu survivors who filed a lawsuit against the British Government for colonial abuses (Carotenuto & Luongo, 2016). On 11 October 2016, the new Defence Cooperation Agreement (DCA) entered into force which allowed British troops to continue their military training in Kenya for another five years (GOV.UK, 2015a). There were also many conciliatory gestures during a visit to Nairobi by Theresa May in August 2018, which was the first visit to Kenya by the British Prime Minister in three decades. In the perspective of Brexit, Prime Minister May promoted in Africa the concept of "Global Britain", which assumed closer relations with former colonies. As part of the concept, Kenya was to become the UK's model partner in East Africa, which concerned both economic and other issues. The visit provided an opportunity to sign additional agreements, including in the fields of defense and security. In turn, in January 2020 in London, Prime Minister Boris Johnson and President Uhuru Kenyatta agreed on a new strategic partnership for the years 2020-2025. The second pillar of the partnership assumes joint efforts to tackle global terrorism, violent extremism, organized crime and corruption. Furthermore, it involves closer defense cooperation, promoting security in East Africa, and improving the cyber resilience (GOV.UK, 2020). Although the British authorities do not admit it, the tightening of relations with Kenya is also expected to limit the spread of Chinese influence in East Africa.

Great Britain actively cooperates with Kenya in defense and security. The cooperation basically aims at improving the defense capabilities of Kenya and the safety of citizens, tourists and investors. In turn, Great Britain has the opportunity to train its expeditionary forces in Kenya. Cooperation for conflict resolution in Somalia and South Sudan is also an important issue. It is worth mentioning that Ethiopia, which competes with Kenya for a dominant position in East Africa, also plays a vital role in this respect. So far, none of the two states has come close to achieving hegemonic status in the sub-region (Hartmann, 2016). However, close cooperation with the United Kingdom is vital for Kenya in this competition.

Relations with Great Britain in defense and security were severely strained after the December 2007 elections in Kenya, which resulted in the outbreak of violence. Under these circumstances, Prime Minister Gordon Brown even made inquiries about the possibility of military involvement in Kenya. However, he received information that this option could not be realized due to the British forces' involvement in Iraq, Afghanistan, and other countries. Thus, there were no available military units (Dorman, 2016). Along with the stabilization of the internal situation in Kenya, traditional military relations with Great Britain normalized. Relations could be rebuilt quickly thanks to the long-standing historical connections and Kenya's open door policy (International Relations and Defence Committee, 2020).

Kenya and the United Kingdom are engaged in an enduring defense cooperation that has been going on for four decades. This allows British troops to be present in Kenya mainly for training purposes. According to the official position of the British Government, the United Kingdom has "an excellent, long-standing relationship with the Kenyan armed forces and the local communities surrounding the training areas" (Kamau, 2013). British Army Training Unit Kenya (BATUK), which stations in Kenya, is a permanent training support unit. BATUK is located mainly in Nanyuki, 200 km north of Nairobi. A small element is placed in Kahawa, Nairobi. BATUK fulfils advanced training of units preparing to participate in peacekeeping and stabilization missions or assume high-readiness tasks.

BATUK consists of around 100 permanent staff and reinforcement of about 280 personnel on a short-term basis. Every year, up to six British infantry battalions carry out eight-week training in Kenya. Three Royal Engineer Squadrons carry out exercises, too. Two medical company groups of the Royal Army Medical Corps also station in Kenya. They provide primary health care assistance to the civilian community (The British Army). Overall, the British Army trains up to 10,000 British soldiers in Kenya every year (Kamau, 2013). However, this is usually a slightly smaller number, oscillating around 7.5 thousand (GOV.UK, 2018b). British soldiers participating in military missions in Afghanistan and Iraq and earlier, for example, in Sierra Leone trained in Kenya.

The British Peace Support Team East Africa (BPSTEA) stations in Kenya, too. Its main aim is to coordinate British military assistance to armed forces in Eastern Africa, especially to contribute to Security Sector Reform and to increase peacekeeping capacity (Tossini, 2017). The British Army is involved in various initiatives implemented in Kenya. It trains locals, including local rangers in the fight against poachers killing elephants and rhinos (Vaughan, 2013).

4. Military cooperation to restore peace in Somalia

British soldiers regularly participate in military exercises together with troops of the Kenyan army (Dorman, 2016). The purpose of joint exercises is "to promote stability in East Africa and beyond and to build the continent's capacity to overcome its own challenges and deliver its own security" (GOV.UK, 2018d). Kenya is adjacent to countries where the security is precarious, like Somalia and South Sudan. Both Kenya and the United Kingdom want to stabilize the situation in these countries. They regularly consult each other regarding peace initiatives in Somalia and South Sudan. Moreover, Kenya participates in the Intergovernmental Authority on Development (IGAD), a regional grouping to promote peace, cooperation and development in East Asia.

Cooperation between Great Britain and Kenya in resolving the conflict in Somalia is particularly advanced. In mid-October 2011, Kenya declared war on terrorist organization Al-Shabaab militia operating from Somalia. Kenya Defence Forces (KDF) were ordered to pursue and combat its fighters along the border between Kenya and Somalia. Military operations were also carried out in Somalia. The government in Nairobi justified the operations with the right to self-defense. In response, Al-Shabaab made several terror incursions into Kenya and threatened to carry out major terrorist attacks in Kenyan cities. During the London Conference in Somalia in May 2013, President Kenyatta was a distinguished guest, despite a dislike of his political past, including his involvement in the 2007 electoral violence. The constructive approach to the new president of Kenya resulted from the British authorities' awareness of the state's position in East Africa, its contribution to the fight against international terrorism and its resistance to instability arising from war-threatened Somalia (Nzau, 2016). It was also due to concerns about the China's increasing involvement in Kenya (Kamau, 2013).

Since 2015, the United Kingdom has been supporting Kenya in anti-terrorist activities in Somalia through the deployment of personnel to Somalia to offer logistical support to the Kenya Defence Forces and anti-terrorist training for the police and border guards of Kenya (Tossini, 2017). Kenya is also involved in the African Union Mission to Somalia (AMISOM). Great Britain actively participates in the UN Security Council works to strengthen the AMISOM and to support the engagement of KDF in the mission (Kenya

High Commission UK). The UK provides financial and training support to the African Union (AU) in carrying out the mission in Somalia. The British army gives support to Kenyan soldiers participating in AMISOM, including those training Somali security forces (GOV.UK, 2018d). Most observers recognized military intervention in Somalia and involvement in AMISOM as Kenya's involvement in the global war on terror led by its key Western allies - the United States and Great Britain (Nzau, 2016). In May 2019, Secretary of State Jeremy Hunt described Kenya's mission in the Horn of Africa as vital to global peace (Wakaya, 2019).

The United Kingdom also supports Kenya in dealing with the refugee crisis resulting from the civil war in Somalia. Kenya hosts more than 450,000 refugees from the region. Thanks to the Kenyan Government's consent and the support of international donors, including the UK Government, they can be in a safe environment close to their homeland (GOV.UK, 2018b). On 25 March 2017, the IGAD Extraordinary Summit on Somali Refugees took place in Nairobi. Countries participating in the summit, including Great Britain, declared their continued support for Kenya in helping refugees from Somalia and other countries of the region.

5. The United Kingdom programs to enhance peace and security in Kenya and East Africa

The United Kingdom has been implementing several programs aimed at strengthening security in East Africa, including Kenya. The East Africa Security Program was to be implemented by the Ministry of Defence (MoD) with £0.47 million in funding from Official Development Assistance (ODA) and £ 2 million from Non-ODA between April 2015 and November 2020. The program included two goals - developing a counter Improvised Explosive Devices (IED) training wing of the International Peace and Security Training Centre (IPSTC) and supporting the British Peace Support Team (Africa). The program was directed at increasing local troops' capacity, including Kenyan soldiers participating in peacekeeping missions, mainly in AMISOM, in protecting and counteracting IED (GOV.UK, 2015c).

The Foreign and Commonwealth Office (FCO) and the MoD implemented Africa Peace and Security Program (APS) in the period between April 2018 and March 2021. As much as £4 million from ODA and £4.5 million from Non-ODA had been mobilized for the program. These funds were intended for three purposes – the African Union Support Program (AUSP), the British Peace Support Team Africa (BPST) and Other Costs – Delivery, Monitoring and Evaluation. Meanwhile, APS "focused on improving the African Union's capacity to prevent, manage and respond to conflicts in Africa, and to enhance the capability of Troop Contributing Countries participating either in AU or UN missions". In practice, this included technical assistance in the form of advisors for protection of civilians, gender and international humanitarian law, as well as conflict support prevention, diplomacy aid, early warning systems and mediation. Support for regional peacekeeping training centers which train staff to assist AMISOM was one of the specific tasks (GOV.UK, 2018a).

Between April 2015 and March 2020, the FCO was implementing the East Africa Crime and Justice Program for the amount of £1.85 million from ODA. The goal of the program was to support "Kenya and Tanzania to strengthen their law enforcement and criminal justice capability to tackle serious organized crime more effectively, from investigation to prosecution". In practice, support included assisting the development of key institutions

and criminal justice systems and mentoring for police officers and prosecutors (GOV.UK, 2015b).

East Africa Preventing Violent Extremism for the period between April 2019 and March 2022 is another program to be implement by FCO for the amount of £4 million from ODA. The program is targeted to "strengthen the evidence base for preventing violent extremism and reduce the drivers and enablers of violent extremism in East Africa". Specific objectives include supporting the Kenyan Government in implementing national action plans to prevent extremism. In addition, they include actions to identify the primary sources of extremism, sharing best practices of tackling the extremism and supporting the most vulnerable groups to reintegrate into local communities (GOV.UK, 2019).

The FCO, in cooperation with the National Crime Agency (NCA) and the Crown Prosecution Service (CPS), implemented East Africa Migration Program between April 2018 and March 2020 for the amount of £1.5 million from ODA. This program primarily intended to limit the activity of regional criminal groups involved in the illegal transfer of people to Europe, including Great Britain, but also to East Africa, including Kenya. The activities consisted in the identification, arrest, investigation and prosecution of the traffickers (GOV.UK, 2018c).

Great Britain and Kenya also cooperate to counteract child sex abuse, which made it possible to arrest many pedophiles in the UK. During the visit to Kenya in August 2018, Prime Minister Theresa May announced plans for Britain to set up a cyber-center in Nairobi to help authorities fight online child sex abuse (Webber, 2018). In 2019 Kenya has become the first African country to connect to International Criminal Police Organization's (INTERPOL) International Child Sexual Exploitation (ICSE) database.

Over the last decade in Kenya, there has been a radicalization of Islamic moods, which is particularly visible in the north of the country and coastal areas (Porteous, 2008). This phenomenon is treated by both Kenyan and British authorities as a serious threat. At the beginning of 2019, Nairobi benefited from a British security funding pledge worth Sh3 billion to fight violent extremism and poaching, and boost trade (Mutambo, 2019). These activities are to contribute to the improvement of social mood in Kenya and thus strengthening stability and security.

5. Conclusion

The colonial period significantly influences contemporary relations between the United Kingdom and Kenya. This is due to historical, cultural and economic dependencies. In order to maintain and deepen postcolonial relations, states had to adapt to new circumstances. This required dealing with the difficult experiences of the colonial period, as well as treating oneself as equal partners. States have made efforts to reduce the inequalities resulting from colonialism and to solve contemporary problems together.

Over the last decade, the United Kingdom has undertaken intensified efforts to improve relations with Kenya, including strengthening cooperation in the areas of defense and security. These actions were conditioned by both internal, bilateral and external factors. In supporting Kenya, the United Kingdom counts primarily on the benefits of cooperation with the country. The ties established during the colonial period make it easier for Great Britain to develop closer relations with Kenya. Building a genuine partnership is helped by London's assumption of responsibility for difficult moments in the history of bilateral relations. In the context of Brexit, the United Kingdom had to reevaluate its role in the world,

returning to the concept of "Global Britain". In order to rebuild its influence in East Africa, it focused on cooperation with the relatively stable and rapidly developing Kenya. Increasing influence in the region is possible with its stabilization, including limiting the threat from Somalia. The British are keen to train and support the Kenyan armed forces in these activities so that they themselves do not have to become significantly involved in regional conflicts. At the same time, strengthening cooperation with Kenya and supporting the peace process in East Africa increases Britain's ability to limit China's influence.

Thanks to the United Kingdom's support, Kenya is strengthening its security forces, which is especially important due to the infiltration of extremism and terrorism from destabilized Somalia. In addition, Kenya has ambitions to gain a dominant position in East Africa, which would give it a greater ability to influence its neighbors. Close cooperation with Great Britain increases Kenya's prestige and creates greater development opportunities. The convergence of goals implies that cooperation between the United Kingdom and Kenya in the areas of defense and security should be further tightened.

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Bell, C. (2013). The 'Special Relationship'. In M. Leifer (ed.), *Constraints and Adjustments in British Foreign Policy* (pp. 103-119), London-New York: Taylor & Francis. https://doi.org/10.4324/9781315884936.
2. Branch, D. (2011). *Kenya. Between Hope and Despair, 1963-2011.* New Haven-London: Yale University Press.
3. Brown, D. (2013), Britain and the Politics of Counter-Terrorism: The 2002 New Chapter and Beyond. In D. Brown (Ed.), *The Development of British Defence Policy. Blair, Brown and Beyond* (pp. 81-106). London: Ashgate Publishing.
4. Callaghan J. (2007). *The Labour Party and Foreign Policy. A history*. London-New York: Routledge. https://doi.org/10.4324/9780203647127.
5. Carotenuto, M., & Luongo K. (2016). *Obama and Kenya. Contested Histories and the Politics of Belonging*. Athens: Ohio University Press.
6. Cullen, P. (2017). *Kenya and Britain after Independence: Beyond Neo-Colonialism.* Cambridge: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-56276-6.
7. Domańska, E. (2008), Badania postkolonialne, In L. Gandhi (Ed.), *Teoria postkolonialna. Wprowadzenie krytyczne* (pp. 157-165). Poznań: Wydawnictwo Poznańskie.
8. Dorman, A. M. (2016). *Blair's Successful War. British Military Intervention in Sierra Leone*. London-New York: Routledge. https://doi.org/10.4324/9781315569529.
9. Elkins, C. (2013), *Rozliczenie z imperium. Przemilczana historia brytyjskich obozów w Kenii.* Warszawa: Świat Książki.

10. Gawrycki, M. F. (2013). Postkolonializm jako perspektywa badawcza w nauce o stosunkach międzynarodowych. *Stosunki Międzynarodowe – International Relations,* 47(1), pp. 35-54.
11. GOV.UK. (2015a). *Agreement between the Government of the Republic of Kenya and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defence Cooperation.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/569346/TS_34.2016_Cm_9359_Kenya_Defence_WEB.pdf.
12. GOV.UK. (2015b). East Africa Crime and Justice Programme, https://www.gov.uk/government/publications/conflict-stability-and-security-fund-programme-summaries-for-africa-2019-to-2020.
13. GOV.UK. (2015c). *East Africa Security Programme,* https://www.gov.uk/government/publications/conflict-stability-and-security-fund-programme-summaries-for-africa-2019-to-2020.
14. GOV.UK. (2018a). *Africa Peace and Security (APS) Programme.* https://www.gov.uk/government/publications/conflict-stability-and-security-fund-programme-summaries-for-africa-2019-to-2020.
15. GOV.UK. (2018b). DFID Kenya. Gov.uk. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/723198/Kenya-July-2018.pdf.
16. GOV.UK. (2018c). East Africa Migration Programme, https://www.gov.uk/government/publications/conflict-stability-and-security-fund-programme-summaries-for-africa-2019-to-2020.
17. GOV.UK. (2018d). *Prime Minister's press statement in Nairobi: 30 August 2018.* https://www.gov.uk/government/speeches/prime-ministers-press-statement-in-nairobi-30-august-2018.
18. GOV.UK. (2019). East Africa Preventing Violent Extremism, https://www.gov.uk/government/publications/conflict-stability-and-security-fund-programme-summaries-for-africa-2019-to-2020.
19. GOV.UK. (2020). *UK-Kenya Strategic Partnership 2020 to 2025: joint statement.* https://www.gov.uk/government/news/uk-kenya-strategic-partnership-2020-2025.
20. Grovogui, S. N. (2007). Postcolonialism. In T. Dunne, M. Kurki, and S. Smith (Eds.), *International Relations Theories: Discipline and Diversity* (pp. 229-246). Oxford: Oxford University Press.
21. Hartmann, Ch. (2016). Leverage and linkage: how regionalism shapes regime dynamics in Africa. In M. Bogaards, and S. Elischer (Eds.), *Democratization and Competitive Authoritarianism in Africa* (pp. 79-98). Wisebaden: Springer. https://doi.org/10.1007/978-3-658-09216-0.
22. International Relations and Defence Committee (2020, July, 10*). The UK and Sub-Saharan Africa: prosperity, peace and development co-operation.* House of Lords. https://publications.parliament.uk/pa/ld5801/ldselect/ldintrel/88/8802.htm
23. Kamau, J. (2013, March, 21). *China threat forces UK rethink of Kenya policy.* Business Daily. https://www.businessdailyafrica.com/news/China-threat-forces-UK-rethink-of-Kenya-policy/539546-1726968-kvfj9d/index.html.
24. Kameron, H. (2013). *Britain's Hidden Role in the Rwandan Genocide.* London-New York: Routledge. https://doi.org/10.4324/9780203113592.
25. Kaplan, I. (1982). *Kenya. A country study. Second Edition.* Washington: U.S. Government Printing Office.
26. Kenya High Commission UK. *Kenya-UK Relations.* https://kenyahighcom.org.uk/kenya-uk-relations.html.

27. Mazurczak, W. (2016). Kolonializm – Dekolonizacja – Postkolonializm. Rozważania o istocie i periodyzacji. *Przegląd Politologiczny,* 3, pp. 131-143. https://doi.org/10.14746/pp.2016.21.3.9.
28. Mutambo, A. (2019, March, 26). *Kenya to bolster UK ties despite Brexit challenges: Esipisu.* Daily Nation. https://nation.africa/kenya/news/kenya-to-bolster-uk-ties-despite-brexit-challenges-esipisu-152250.
29. Nair, S. (2017, December, 8). *Introducing Postcolonialism in International Relations Theory.* E-International Relations. https://www.e-ir.info/2017/12/08/postcolonialism-in-international-relations-theory/.
30. Nasong'o, & S. W., Ayot, T. O. (2007). Women in Kenya's Politics of Transition and Democratisation. In G. R. Murunga, and S. W. Nasong'o (Eds.), *Kenya. The Struggle for Democracy* (pp. 164-198). Dakar: Cordesia Books.
31. Nzau, M. (2016). The Strategic Art of Appeasing Old Lovers while Courting New Friends: Kanya's Foreign Relations in Retrospect. In M. M. Kithinji, M. M. Koster, and J. P. Rotich (Eds.). *Kenya After 50. Reconfiguring Historical, Political, and Policy Milestones* (pp. 135-164). London-New York: Palgrave Macmillan.
32. Polus, A. (2014). Postkolonialna teoria stosunków międzynarodowych. In K. Kącka (Ed.), *Stosunki Międzynarodowe. Wokół zagadnień teoretycznych* (pp. 113-128). Toruń: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.
33. Porteous, T. (2008). *Britain in Africa.* London-New York: Zed Books.
34. Rowe, P. (2016). *Legal Accountability and Britain's Wars 2000–2015.* London-New York: Routledge. https://doi.org/10.4324/9781315727578.
35. Smith, S., & Owens, P. (2008), Teorie stosunków międzynarodowych – podejścia alternatywne (transl. M. Staszkiewicz). In J. Baylis, and S. Smith (Eds.), *Globalizacja polityki światowej. Wprowadzenie do stosunków międzynarodowych* (pp. 337-372). Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.
36. The British Army. *The British Army in Africa,* https://www.army.mod.uk/deployments/africa/.
37. Tossini, J. V. (2017, March, 30). *The British Forces in Africa – The Training Unit in Kenya.* UK Defence Journal. https://ukdefencejournal.org.uk/the-british-forces-in-africa-the-training-unit-in-kenya/.
38. Vaughan, A. (2013, November, 1). *British army joins fight against elephant and rhino poaching.* The Guardian. https://www.theguardian.com/environment/2013/nov/01/british-army-elephant-rhino-poaching-kenya.
39. Wakaya, J. (2019, May, 3). *UK pledges stronger ties with Kenya, denies counter-checking China.* Capital FM. https://www.capitalfm.co.ke/business/2019/05/uk-pledges-stronger-ties-with-kenya-denies-counter-checking-china/.
40. Webber, E. (2018, August, 30). *President Kenyatta criticises Theresa May's 'rushed and belated' Africa visit.* The Times. https://www.thetimes.co.uk/article/president-kenyatta-criticises-theresa-may-s-rushed-and-belated-africa-visit-7cp8nfw6x.
41. White, B. (2002), *Britain, détente and changing East-West relations.* London-New York: Routledge. https://doi.org/10.4324/9780203194591.

SAFETY&DEFENSE
ISSN 2450-551X

Strategic Research and the State Security and Defense Policy: The Case of IRSEM

Grzegorz ROSŁAN

Rzeszow University of Technology, Rzeszów, Poland;
g.roslan@prz.edu.pl, ORCID: https://orcid.org/0000-0002-2566-5004

DOI: https://doi.org/10.37105/sd.115

Abstract

As strategic research plays an important role in shaping and implementing the state's security and defense policy, there is a need for institutionalized capability in this field. Institutes of strategic studies serve as primary institutions providing states' authorities with expertise related to strategic problems. This article discusses the mission, organization and activities of the Institute for Strategic Research of the Military School (Institut de Recherche Stratégique de l'École Militaire – IRSEM). This article attempts to assess the role of the institute with regards to France's security and defense policy. The research has been based on the critical qualitative analysis of publicly available sources on IRSEM mission, organization and activities. The analysis was reinforced by a short term internship of the author to the Institute in 2020. The results of research suggest that the scope of the Institute's activities is broader than its research activities. The important of the IRSEM French security and defense policy also stems from its support to professional military education, outreach activities and so called "strategic succession".

Keywords

defense, France, Institut de Recherche Stratégique de l'École Militaire (IRSEM), security, strategic research

Submited: 06.04.2021. Accepted: 06.05.2021. Published: 18.05.2021.

1. Introduction

Strategic research is of critical importance to the development and implementation of the security and defense policy of any state. The evolution of the security environment and the complexity of conditions influencing the activities of states on the international arena make it necessary to systematically conduct research focused on problems of strategic importance. This task is usually performed by specialized research centers and governmental analytical agencies. Strategic research seeks to maintain a broad research perspective and an interdisciplinary approach to avoid bias caused by the organizational culture of specific organizations or institutions. Most countries with a global and regional security and defense policy have developed institutionalized strategic research capabilities. Strategic studies focused on war are an essential component of strategic research, complementing more general studies. These studies contribute directly to shaping the foundations and then the implementation of the security and defense policies of states (Hasselbladh & Ydén, 2020). Depending on national approaches, institutions tasked with strategic military research may be established as separate entities directly subordinated to the ministry of defense, be a division of defense research agency or function within national institutions of professional military education. Some of such institutions are recognized regionally and globally, such as the Institute for National Strategic Studies at the National Defense University or the Strategic Studies Institute at the U.S. Air War College, mainly because of the scope of their research. Some research institutions conduct strategic military research to support national defense and therefore are recognized in the national and regional context. The Defense Analysis Division of the Swedish Defense Research Agency or the Center for Security and Strategic Research at the National Defense Academy of Latvia may serve as examples. Typically, military strategic research institutions combine research activities with education and outreach programs.

Institutes researching military aspects of strategic studies have been established in most of the ministries of defense of the states that pursue security and defense policy on a global and regional scale. Locating such think tanks at military universities allows them to combine their advisory functions for political and military decision makers in the field of security and defense with the support to the professional military education (Little, 2016). The military strategic study centers complement the activities of the civilian centers dealing with broadly defined security and strategy issues by offering military strategic expertise (Urrutia, 2013). The French IRSEM can be a model example of supporting the state's security and defense policy through targeted military strategic research. For the above reason, this may be an inspiration to implement similar solutions in Poland and other countries that do not have well-established institutional solutions in the field of strategic military studies.

The case of the Institute for Strategic Research of the Military School proves the direct link between security and defense policy and the requirement for institutionalized capability for strategic military studies. The need for in-depth strategic military studies result, inter alia, from a comprehensive perception of challenges and threats by France, mainly caused by its geographical location in the south of the European area of stability (Jurczyszyn & Terlikowski, 2018). A marginal threat to France posed by an armed attack by another state has shifted the focus of its strategic research to more universal challenges and threats, such as uncontrolled migration, social radicalization or organized terrorism resulting from the disintegration of states, civil wars, regional crises and conflicts or natural disasters. The incen-

tive for a broader scope of strategic military studies has stemmed from the fact that geographically distant threats more and more often have materialized on the territory of France (Ministère de la Défense, 2017).

The need for in-depth strategic military studies may be result of a dual nature of French security and defense policy. Although France remained primarily a regional power for years, its security and defense policy has been frequently global in the context of political, social and economic changes in the security environment. Strategic military studies are necessary for the development and implementation of its national security strategy. France needs its strategic assessment capability to assert its role as a world power. Independent strategic military research also supports France's full independence and its ability to defend its own interests globally. The scope of the requirements with regard to the spectrum of strategic military studies is influenced by such attributes of the French superpower as permanent membership in the UN Security Council allowing to France decide on many global and regional security issues or the arsenal of nuclear weapons. French contributions to the security of Africa and its good relations with the Arab world require strategic reflection as well (Williams, 2010).

The security interests of the Fifth Republic are global. At the same time French foreign and security policy is characterized by independence, the idea of universalism and rationalism. France takes an active part in the fight against the spread of Islamic extremists in the Mediterranean and helps resolve conflicts in Africa. Such a broad security policy requires proper preparation and training of personnel for the defense of the state in all conditions and for all types of threats and crises. This clearly translates into the need for national capabilities to conduct strategic military studies and provide military expertise that would complement the broader strategic studies conducted by civilian centers (Holeindre & Vilmer, 2015).

IRSEM's contribution to the development of French military strategic thought is unquestionable. By conducting innovative research, it contributes directly to current and future activities within the security and defense policy of France.

The objective of this article is to provide a brief assessment of the role the Institute for Strategic Research of the Military School plays for France's security and defense policy. The article starts with an introduction to the security and defense policy of France. It then discusses the mission, organization and activities of the Institute. The research has been based on a critical qualitative analysis of publicly available sources on the IRSEM's mission, organization and activities. The analysis of those sources has been reinforced by a short term internship of the author to the Institute and library query at the Military School in 2020.

2. Developing France's security policy

In order to understand the importance of the Military School's Strategic Research Institute for the security and defense policy of France, one should explore in more detail this policy of the Fifth Republic. The definition of France's national interests is primarily influenced by its history, geography, culture, internal political order, economy, social system and religion. It should be emphasized that these factors influence, but do not determine the national security interests (Dufourcq, 2010). Their choice has been always of a political nature and depended on their own capabilities and external influences created by other actors of the international relations. The national interests of the Fifth Republic concern not only tangible aspects, such as security. They call also for the external projection of values typical of

French culture. French security policy also supports the concept of organizing the international system so that it best suits France's interests and principles (Claeys, 2004). For this reason, it is difficult to find a more interesting case to study the value of strategic research and its relations to security policy than France. There are few countries in the world that have consistently pursued an ambitious security policy aimed at gaining the position of superpower in international relations for several hundred years (Cholewa, 2015). The end of the Cold War, when France re-evaluated its security policy, was a turning point. The country was forced to develop a new security and defense policy adapted to the new balance of power (Młynarski, 2010). Ultimately, it returned to the integrated structures of the North Atlantic Alliance (NATO), fundamentally changing its attitude towards the alliance's policy, and also professionalizing the armed forces. At the same time, the new development of the armed forces was realigned with emerging threats that France expected to be exposed to in the short and long term. Moreover, the Armed Forces of the Fifth Republic were to carry out tasks resulting from the ambition and role that France wanted to play in the new international reality (Kozicki, 2011).

Strategic research plays important role in the development of French security and defense policy. The model of the approach to developing security policy, currently in use in France, is the result of a process that has been used for many years and is subject to systematic development and modification. For France as a country that faces diverse spectrum types of threats, efficient mechanisms for security management are crucial, both from the perspective of the state and its citizens (Ministère de l'Éducation Nationale et de la Jeunesse, 2019). Moreover, the characteristic feature of the French solutions related to development and implementation of security and defense policy is the adoption of formalized processes that are subject to constant control and constructive evaluation (Furgała, Szlachter, Tulej & Chomentowski, 2010).

This approach has been frequently observed with the process of modeling the security environment. It has been conducted using multidimensional perspectives of different internal and external stakeholders. It has allowed for an assessment of the security environment that provides a more precise representation of reality. The need for comprehensive strategic research seems more evident as the same information signals result in different solutions for different recipients. Comprehensive strategic research helps in limiting the cultural and educational biases of analysts representing different stakeholders and facilitates improvements in conceptualizing the security environment, as well as ways and means of security strategy and policy.

Thus, the idea of the involvement of various organizations and institutions in developing French security and defense strategy and policy finds verification in the real world. With a closer look at the strategic documents defining security and defense policy of France, one may clearly observe that the synergy of sectoral modeling and understanding the security environment of France has its roots in various perspectives (Ministère de la Défense, 2013, 2017). The perception of French sovereignty and independence is also significantly influenced by the division of competences between various levels of government, which is subject to changes with subsequent revisions of the security policy (Rytel-Baniak, 2018). Such a collaborative approach to development of security and defense policy requires institutionalized capabilities in the field of strategic research. Moreover, these capabilities should be decentralized to avoid cultural bias and provide the state authorities with a spectrum of strategic perspectives and sectoral assessments (Tvaronavičienė, 2018).

3. The Mission of the Institute

The creation of the Military School's Institute for Strategic Research (IRSEM) in 2010 may be directly linked to the comprehensive approach to the development of the security and defense policy that was adopted in France more than a decade ago (Dalichau, 2009; Kozicki, 2011). The establishment of the IRSEM was largely a result of disappointment with the previous formulas for assessing the security environment of France, and especially reducing these assessments only to military threats (Vilmer, 2017). The creation of the ISREM contributed to expanding the scope of strategic studies conducted by French military and opened it to new directions of scientific activity, including new areas of academic solutions (Vilmer, 2016).

In order to define the role of the IRSEM in France's security and defense policy, it is necessary to present its mission, which is directly linked to the implementation of tasks within four problem areas. The first part of the ISREM mission is broadly understood research. The researchers of the Institute are supposed to conduct security related strategic research in various regions of the world. These research activities are conducted to satisfy the so-called internal needs, which means meeting the expectations of the French Ministry of Defense. At the same time, the Institute is supposed to conduct research to participate in academic debate with external institutions. This part of research is intended for the scientific community, and its results are readily available to international community (Ministère de la Défense, 2016).

An important part of the Institute's mission is referred to as strategic succession. The ISREM is involved in nurturing a new generation of researchers dealing with defense and security issues. This part of the mission relates to searching for young talented reseracher and providing them with various support at the Military School. This care may be in the form of financial support (e.g. doctoral scholarships) and broadly understood promotion in the military and civilian environment. Another part of the IRSEM's mission is its contribution to higher military education by conducting classes with students of the Military School and the Center for Advanced Military Studies (CHEM), as well as substantive care for interns from these universities. Finally, the IRSEM is supposed to be involved in the public debate related to security and defense strategy and policy of France (Vilmer, 2016). In this area, the Institute is supposed to the organize national and international scientific conferences, publish research papers, and participate and promote its scientific potential in the media. Thus, the Institute contributes to the revival of public debate in France on issues related to defense and security (Holeindre & Vilmer, 2017).

4. Organization of ISREM

The Institute was established by combining elements of four different research institutes of French Ministry of Defense in September 2009 and started its activities formally in 2010 (Ministère de la Défense, 2010). Until 2015, it was subordinated to the Staff of the Armed Forces, and then reassigned as an external body of the General Directorate for International Relations and Strategy (DGRIS) of the Ministry of Defense. The Institute is organized into three core teams dealing with management, science (research or academic) and support. The IRSEM is headed by a civilian director, whose military deputy is also the secretary general responsible for the administrative management of the Institute. The secretary general is also

responsible for implementing the budget and all non-scientific reports. The director responsible for science and the research support manager also report directly to the director of the IRSEM. The former is responsible at the Institute for scientific research, annual research program and scientific validation of publications. It is worth mentioning that both the director of the IRSEM and his subordinate responsible for science are also extramural university professors (Vilmer, 2016). The research support manager is responsible for administrative assistance and the promotion of the Institute's research in the form of publications, cooperation with the media, and scholarship assistance (Institute de Recherche Stratégique de l'Ecole Militaire, 2021).

This structure of the Institute transparently delineates the responsibilities of its teams, rules of operations and cooperation, and instruments to secure the operation of the IRSEM. In addition, it should be emphasized that, in accordance with the legal regulations on the organization of the Institute for Strategic Research of the Military School adopted in 2010 and 2015, the organization of the IRSEM has to ensure so-called hybrid identity, which is meant to connect two types of expertise (called also "worlds"): the scientific (academic) with operational (military) (IRSEM, 2021).

The academic community is represented primarily by the director of the Institute, who has to be a university professor and hold an academic degree. In addition, the potential of the world of science is created by civilian researchers who must hold at least a doctoral degree and be authorized to conduct independent scientific research. Moreover, the management of the IRSEM endeavors to ensure that each of the scientists involved is an active academic lecturer. This academic part of the Institute community is also created by young researchers who stay at the Institute for the purpose of writing their own scientific dissertations. As of 2020 almost all researchers teach at universities, publish scientific articles in peer-reviewed journals in French and English, and organize and participate in international scientific conferences (Vilmer, 2020). In addition, the IRSEM conducts monthly doctoral seminars with approximately thirty doctoral students, funds annual fellowships, and publishes specialized scientific journals. According to experts, this solution ensures that in many respects, the IRSEM is closer to the academic environment and various research centers than to non-profit research and analysis organizations. It should be added that the current Director of the IRSEM, Philippe Boulanger, is also a university professor at the Sorbonne (IRSEM, 2021).

The other part of the community of the Institute, which is called operational staff, is represented by experienced military personnel and civilian employees who are former soldiers. Their knowledge is very valuable to the French Ministry of Defense. This human potential is responsible for the preparation of studies and notes, which are derived from the work of a team of scientists, and then forwarded to the General Directorate for International Relations and Strategy (DGRIS) and the French Armed Forces Defense Staff (EMA). These studies are also sent to other institutions and units related to French foreign and internal policy. It is worth noting that the IRSEM also organizes closed seminars and workshops attended by both civilian and military experts related to French security issues (Holeindre & Vilmer, 2017).

5. Research of the Institute

To understand the importance of strategic military studies for the state security and defense policy, it is worth getting acquainted with the research conducted at the Institute, which is of key importance to the subject matter presented. And so, people representing the

scientific potential conduct research in six problem areas – teams (IRSEM, 2021). The research focus of Institute encompasses four broad fields of study related to security and defense. The largest portion of the research is tied to "regional studies", which are focused on the vaguely defined regions of the North and the South. Regional studies of the North research security and defense problems of Europe, the United States, Russia, the post-Soviet space, China, Japan and the Korean Peninsula. At the same time, regional studies of the South research in detail the security and defense of the Arab world, Africa and South Asia. Aside from geographic focus, the northern part of the regional research also deals with cross-cutting issues, such as the evolution of power, the strategies of influence, the manipulation of information, and the role of the armed forces and conflicts in the evolution of power. The southern part of regional research covers problems related to political authoritarianism and economic liberalization in emerging countries and the influence of armed forces and security services on the states' in the contemporary Arab world (Vilmer, 2016).

Research in the field of "economic and environmental approaches to conflicts" covers two themes: quantitative approaches to armed conflicts and interrelationships between environment and conflicts. Economic research methods and statistical tools are used to explore the dynamics of armed conflicts. These interdependences of environment and conflict are analyzed using two approaches. This part of research seeks to explore the impact of changes in the environment as a contributing factor to conflicts, and the influence of conflicts on the environment. The field of research described as "technological challenges of armed conflicts" focuses on technology developments and its impact on armed conflict. This part of the Institute's research explores what new threats the technology brings, how new technologies influence the conduct of armed conflicts, and their implications for defense industry. The research field described as "defense social sciences, military sociology" explores a set of issues relating to the sociology of the military, including civil-military relations and societal changes that may impact armed forces (Vilmer, Escorcia, Guillaume & Herrera 2018). One of the research themes within this particular field of study are the links between the armed forces and political decision-making, the values and problems of socialization (Vilmer, 2018).

6. Other activities of the Institute

The Institute has actively pursued a number of activities, that focus on strategic military research. Internships and support for young researchers make the Institute research community stronger and more diverse. The IRSEM activities have been supported by several associate researchers, who make a contribution by publishing research papers or studies, and participating in organization of scientific events. The status of associate researcher may be granted to researchers affiliated with a French or international university or research organization, as well as to the military personnel with a doctorate or preparing a doctoral thesis. The status of associate researcher is granted for a renewable period of one year and attracts up to twenty researchers a year, with some of them staying longer at the Institute (Holeindre & Vilmer, 2017). Since its establishment in 2009, the IRSEM has devoted a lot of efforts to support a new generation of young researchers in human and social sciences, willing to deal with security and defense problems. The program of "strategic succession" has been offering young researchers a system of aid and scientific support. Up to March 2021, around a hundred young researchers have benefitted from support within the framework of IRSEM's Strategic Succession. The young researchers have been granted financial and academic support. The financial support include grants and scholarships for theses,

post-doctoral contracts, and mobility aids. Academic support is centered around doctoral seminars and research groups. Academic support also consists among others of so-called accompanying measures, such as information exchange, incentives to mobility for international conferences, and support for publication (IRSEM, 2021).

One of the important missions carried out by the Institute is its contribution to public debate on security and defense issues. The IRSEM has organized up to four scientific events a month in recent years, including conferences in France and abroad. Support for public debate is offered by numerous research works in French and English, most of them available online. The IRSEM makes its research results available to the public in various formats. The Institute has been publishing since a peer-reviewed scientific journal of strategic studies since 1996. Research results are published as in-depth research reports of at least forty pages, research notes up to fifteen pages and strategic news providing strategic analysis of current issues in a two-page format. The Institute also publishes a monthly newsletter summarizing the research and activities conducted by IRSEM. To expand its reach to target audiences, the IRSEM publishes a podcast *Le Collimateur* online, and maintains its YouTube channel. The Institute also maintains a documentary portal ARES, which stores 3957 different documents and sources related to strategic research. Social media like Twitter, and publishing interviews in various media outlets are the tools to promote the research carried out in the Institute in the cyberspace (IRSEM, 2021).

7. Conclusion

When assessing the importance of the Institute for Strategic Research of the Military School for French security and defense policy, several conclusions can be drawn. The need for institutionalized capability in the field of strategic military study that become evident a decade ago was one of the major factors that prompted creation of the Institute. The Institute is an integral part of the French Ministry of Defense and facilitates development of strategic military assessments that translates into national security and defense documents. The academic and operational staff synergy within the Institute, its organization and methodology of conducting research has allowed for an unbiased strategic military expertise that supports France's security and defense policy. The strategic research conducted by the IRSEM has proved its interdisciplinary nature exploring the political, social, military, cultural and economic subjects. It can be argued that the research policy of the Institute for Strategic Research of the Military School allow researchers to go beyond the boundaries of inherited culture, transgress it, learn and use other values, enriching them in the shaped spaces of political and military life in France. With its hybrid academic and military nature, the Institute may serve as a role model for other countries in how to develop and maintain credible institutionalized capability in the field of strategic military studies necessary for development and implementation of national security and defense strategy.

Declaration of interest – The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. *Arrêté du 15 octobre 2010 portant organization de l'institut de recherche stratégique de l'Ecole militaire*, JORF n°0242 du 17 octobre 2010. Ministère de la Défense, pp. 1-3. https://www.legifrance.gouv.fr/eli/arrete/2010/10/15/DEFD1021948A/jo/texte.
2. *Arrêté du 22 décembre 2015 portant organization de l'institut de recherche stratégique de l'Ecole militaire*, JORF n°0025 du 30 Janvier 2016. Ministère de la Défense, pp. 1-3. https://www.legifrance.gouv.fr/eli/arrete/2015/12/22/DEFD1532666A/jo/texte
3. Cholewa, M. (2015). Zmiany w kulturze strategicznej Francji po zimnej wojnie. *Zeszyty Naukowe Uniwersytetu Jagiellońskiego*, *Prace Historyczne* 142, z. 4, pp. 725–740. https://www.ejournals.eu/Prace-Historyczne/2015/Numer-4/art/6184/
4. Claeys, A.-S. (2004). Sense and sensibility': the role of France and French interests in European development policy since 1957. In K. Arts, and A.K. Dickson (Eds.), *EU development cooperation from model to symbols* (pp. 113–132). Manchester University Press. https://www.manchesteropenhive.com/view/9781526137340/9781526137340.00012.xml
5. Dalichau, O. (2009). Sécurité et Défense: Nouveaux Défis, Nouveaux Acteurs. Friedrich-Ebert-Stiftung, Antananarivo, pp. 1–40. http://library.fes.de/pdf-files/bueros/madagaskar/06889.pdf
6. Dufourcq, J. (janvier 2010). French Strategic Interests. *Diploweb.com: la revue géopolitique*, pp. 1-6. https://www.diploweb.com/French-strategic-interests.html
7. *Enseignement moral et civique, La Défense et la sécurité nationale en France: les transformations de l'outil militaire, les stratégies de la défense, les espaces de l'exercice de la défense et de la sécurité*. (2019). Ministère de l'Éducation Nationale et de la Jeunesse, pp. 1-5. https://cache.media.eduscol.education.fr/file/Defense/51/2/EMC-Defenseetsecuritenationale_1159512.pdf
8. Furgała, A., Szlachter, D., Tulej, A., & Chomentowski, P. (2010). System antyterrorystyczny Republiki Francuskiej. *Przegląd Bezpieczeństwa Wewnętrznego nr* 3, pp. 29–36. https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstw-3/702,Przeglad-Bezpieczenstwa-Wewnetrznego-3-2010.html
9. Hasselbladh, H., Ydén, K. (july 2020). Why Military Organizations Are Cautious About Learning? *Armed Forces & Society*, *Volume* 46 *Issue* 3, pp. 475–494. https://doi.org/10.1177/0095327X19832058
10. Holeindre, J.-V., & Vilmer, J.-B. (2017). La revue des études sur la guerre et la paix. *Les Champs de Mars. Revue d'études sur la guerre et la paix, n°* 29, pp. 5–12. https://doi.org/10.3917/lcdm.029.0005
11. Holeindre, J.-V., & Vilmer, J.-B. (décembre 2015). Pour des War Studies en France: un diagnostic et des propositions. *Revue Défense Nationale*, *n°* 785, pp. 1-7. https://www.jbjv.com/IMG/pdf/Pour_des_War_Studies_en_France.pdf
12. Institut de Recherche Stratégique de l'Ecole Militaire. (2021, 02, 17). *L'équipe de l'IRSEM*. https://www.irsem.fr/
13. Institut de Recherche Stratégique de l'Ecole Militaire. (2021, 02, 17). *Présentation de l'IRSEM*. https://www.irsem.fr/
14. Institut de Recherche Stratégique de l'Ecole Militaire. (2021, 02, 17). *Offres d'emploi/stages*. https://www.irsem.fr/
15. Institut de Recherche Stratégique de l'Ecole Militaire. (2021, 02, 17). *L'équipe de recherche est répartie en six domaines*. https://www.irsem.fr/

16. Institut de Recherche Stratégique de l'Ecole Militaire. (2021, 02, 17). *Offres d'emploi/stages*. https://www.irsem.fr/
17. Institut de Recherche Stratégique de l'Ecole Militaire. (2021, 02, 17). *Les collections de l'IRSEM*. https://www.irsem.fr/
18. Jurczyszyn, Ł., & Terlikowski, M. (luty 2018). Przyszłość polityki obronnej Francji. *Polski Instytut Spraw Międzynarodowych* (PISM), *Nr* 20 (1593), pp. 1-2. https://pism.pl/publikacje/Przysz_o___polityki_obronnej_Francji
19. Kozicki, W. (2011). Reforma Sił Zbrojnych Francji. *Bezpieczeństwo Narodowe nr* 19, III, pp. 241–263. https://www.bbn.gov.pl/pl/prace-biura/publikacje/kwartalnik-bezpieczens/wydania-archiwalne/192011/3506,Zagrozenia-asymetryczne.html
20. *Le Livre Blanc sur la Défense et la Sécurité Nationale 2013*. Ministère de la Défense, pp. 1-160. https://www.defense.gouv.fr/actualites/memoire-et-culture/livre-blanc-2013
21. Little, P.M. (2016). *Think Tanks and Influence on US Foreign Policy: The People and the Ideas*. School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas, pp. 1-58. https://apps.dtic.mil/dtic/tr/fulltext/u2/1039265.pdf
22. Młynarski, T. (2010). Strategia i koncepcje bezpieczeństwa Francji w XXI w. In K. Budzowski (Ed.), *Europejska Polityka Bezpieczeństwa i Integracji* (pp. 161–176). AFM. https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/75226/mlynarski_strategia_i_koncepcje_bezpieczenstwa_2010.pdf?sequence=1&isAllowed=y
23. *Revue stratégique de défense et de sécurité nationale 2017*. Ministère de la Défense. The Strategic Review Committee, pp. 1-100. https://franceintheus.org/IMG/pdf/defense_and_national_security_strategic_review_2017.pdf
24. Rytel-Baniak, I. (2018). Redefinicja strategii bezpieczeństwa Francji, In K. Sówka, and D. Jarnicki (Eds.), *Istota i perspektywy bezpieczeństwa w drugiej dekadzie XXI wieku* (pp. 15–24). Wydawnictwo Naukowe Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce. https://repozytorium.uph.edu.pl/bitstream/handle/11331/2259/Rytel-Baniak%20I.%20Redefinicja_strategii_bezpieczenstwa_Francji.pdf?sequence=1
25. Tvaronavičienė, M. (2018). Towards efficient policy making: forecasts of vulnerability to external global threats. *Journal of Security and Sustainability Issues* 7(3), pp. 591-601. http://doi.org/10.9770/jssi.2018.7.3(18)
26. Urrutia, O. (2013). The Role of Think Tanks in the Definition and Application of Defence Policies and Strategies. *Revista del Instituto Español de Estudios Estratégicos, Núm.* 2, pp. 1-33. https://www.scribd.com/document/486100828/Dialnet-ElPapelDeLosThinkTanksEnLaDefinicionYAplicacionDeL-4537281-2
27. Vilmer, J.-B. (2018). *La réforme de l'irsem. Deux ans d'action (2016-2018)*. IRSEM, pp. 1-15. https://www.irsem.fr/media/3-a-la-une/2018/la-reforme-de-lirsem-deux-ans-daction-2016-2018.pdf
28. Vilmer, J.-B. (janvier 2020). La relève stratégique: les jeunes chercheurs de l'IRSEM, *Revue Défense Nationale, n°* 826, pp. 13-20. https://www.defnat.com/e-RDN/vue-article.php?carticle=22238
29. Vilmer, J.-B. (mai 2017). Le tournant des études sur la guerre en France. *Revue Défense Nationale, n°* 800, pp. 51-61. https://www.defnat.com/e-RDN/vue-article.php?carticle=21432
30. Vilmer, J.-B. (septembre 2016). *La Lettre Édition spéciale*. IRSEM, pp. 1-9. https://www.irsem.fr/data/files/irsem/documents/document/file/2387/Lettre_Edition_speciale_2016v2.pdf
31. Vilmer, J.-B., Escorcia, A., Guillaume, M., & Herrera, J. (2018). *Les Manipulations de L'information: un défi pour nos démocraties*. Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du Ministère de l'Europe et des Affaires étrangères et de

l'Institut de Recherche Stratégique de l'École Militaire (IRSEM) du Ministère des Armées, Paris, pp. 1-214. https://www.diplomatie.gouv.fr/IMG/pdf/les_manipulations_de_l_information_2__cle04b2b6.pdf

32. Williams, R. (1999). Beyond old borders: Challenges to Franco-South African security relations in the new millennium. *African Security Review*, *Volume* 8 *Issue* 4, pp. 3-19. https://doi.org/10.1080/10246029.1999.9627902

SAFETY&DEFENSE
ISSN 2450-551X

Factors Determining a Drone Swarm Employment in Military Operations

Tadeusz ZIELIŃSKI

War Studies University, Warsaw; t-zielinski@akademia.mil.pl,
ORCID: 0000-0003-0605-7684

DOI: https://doi.org/10.37105/sd.112

Abstract

The aim of this study is to identify a drone swarm's capabilities and the key factors influencing its employment in military operations. The research takes the quantitative analysis of scientific literature related to the technical and operational utilization of drones. The use of drones for military purposes in contemporary world is widespread. They conduct dull, dirty, dangerous and deep military operations replacing manned aviation in many areas. Progressive technological development including artificial intelligence and machine learning allows for the use of military drones in the form of a swarm. It is a quite new technology at the beginning of development. The study indicates that the capabilities of a drone swarm based on communication within the group and autonomy differentiate it from the typical use of unmanned aircraft. Size, diversity, self-configurability and self-perfection amongst the others indicated in literature are attributes of a drone swarm which may give advantage in military operation comparing to the classic use of unmanned aircraft. Emergent coordination as a command and control model of a drone swarm is a future way of utilizing that technology in military operations. In the future, a drone swarm will be a cheaper equivalent of advanced and much more expensive weapon systems conducting combat operations.

Keywords

autonomy, capabilities of drone swarm, command and control models, defense, drone swarm, military operations, unmanned aerial vehicle

Submited: 28.03.2021 Accepted: 30.04.2021 Published: 23.05.2021

1. Introduction

Progress in two critical technologies – artificial intelligence and machine autonomy – leads to the transformation of combat operations, in which the concept of a "drone swarm", consisting of cooperating autonomous robots that react over the battlefield as one organism, appears more and more often. Non-state actors have already demonstrated the effectiveness of mass attacks against conventional military and economic targets using drones. The first such an attack took place on the Russian air and naval bases in Hmeimim and Tartus in western Syria on the night of January 5/6, 2018. Thirteen GPS-guided drones participated in the attack. It was the first time that terrorists had organized a massive attack with unmanned aircraft sent over 50 km with the use of modern GPS satellite navigation system receivers. The application of this concept was further confirmed when around ten drones were used on September 14, 2019 to set fire to two Saudi Arabian "Aramco" oil processing plants in Abqarq and Khurais. The concept of a drone swarm was also applied in the recent conflict between Azerbaijan and Armenia in Nagorno-Karabakh. Leading military powers such as the United States, China, Russia and the United Kingdom are already involved in the development of this technology and have carried out numerous trials of drone swarm over the last 3–4 years. The United States has been conducting drone swarm tests since 2015. In January 2017, the US Strategic Capabilities Office and Air Force conducted trials with 103 Perdix Quadcopter Drones as swarm. The US Defense Advanced Research Projects Agency (DARPA) is also working on a program called "Gremlins," which includes microdrones with size and shape of missiles to be dropped from aircraft. Meanwhile, the US Navy is conducting an entire research program towards the development of autonomous swarms known as "Low Cost Unmanned Aerial Vehicle Swarm Technology" (LOCUST). Russia is also working on the concept of a drone swarm and is possibly trying to integrate drones into its "sixth generation fighters". The Chinese have also repeatedly demonstrated their capabilities and progress in this field.

The aim of the research is to identify drone swarm's capabilities and the key factors influencing its employment in military operations. The study allows the following research question to be answered: (1) what kind of capabilities describe a drone swarm? (2) what key factors determining the employment of a drone swarm in military operations? In order to answer these questions, a quantitative analysis of literature have been used. The first group of analyzed literature was related to the technological aspects of a drone swarm. Conclusions from the research allowed us to define a drone swarm and then identify and describe its capabilities and command and control models. The second group of literature was connected with the utilization of drones in military operations. By analogy, the scope of employment a drone swarm in military operations and dilemmas related to its autonomy have been identified.

2. Defining a drone swarm and describing its capabilities

SWARM stands for "Smart War-Fighting Array of Reconfigured Modules." John Arquilla and David Ronfeldt (2000, p. 8), authors of one of the first scientific studies on swarm technology in military applications, defined a swarm as "systematic pulsing of force and / or fire by dispersed, interneted units, so as to strike the adversary from all directions simultaneously". Paul Scharre (2014, p. 26), on the other hand, defines the swarm as "large numbers of dispersed individuals or small groups coordinating together and fighting as a coherent

whole". Robotics swarm can be thought of as a hybrid cooperative robotics that encompasses swarm and multiagent systems. It can consist of either homogenous or heterogeneous agents, which operate in different domains with varying system capabilities and complexity. Each agent is also capable of conducting a useful task, but at limited capabilities when compared to the entire swarm. The swarm's size varies but is large enough to cater redundancies to increase robustness. Its software also allows for scalability to increase the flexibility and dynamism (Tan & Zheng, 2013).

A drone swarm consists of multiple unmanned aerial platforms and / or weapon systems deployed to achieve a common goal. Air platforms and / or weapon systems autonomously change their behavior by communicating with each other. A drone swarm exhibit more complex behaviors than individual drones. This may include attack-capable platforms or existing weapon systems suitably modified to communicate and operate autonomously. The drones in a swarm may be in close or very close proximity to each other or be distant from each other for many kilometers. The key fact is the ability to communicate and share information affecting the execution of a task. The current limitation as to the number of drones in a swarm is the ability to manage information exchange, which will probably be eliminated in the coming years. A drone swarm may consist of many drones of similar or identical size and capabilities, or heterogeneous set of platforms with different weapon and sensor systems. Currently, drone swarms are designed primarily as platforms with sensors, intended mainly for observation and reconnaissance missions (Suzuki, 2018). They are usually composed of small platforms with limited reach. Nevertheless, the dynamic technological progress causes a drone swarm to include much larger platforms with a greater range of use and the possibility of carrying a large amount of weapons. In other words, a drone swarm will become more and more advanced (thanks to improved control algorithms, increased payload, range and flight duration). The differentiation of roles in heterogeneous a drone swarm brings many benefits. Combat drones carry weapon, reconnaissance drones use advanced sensors to track potential targets and detect threats. In turn, communication drones provide stable communication links inside the swarm and in the chain of command. Dummy drones can focus enemy fire on themselves, generating a false radar image. The composition of a drone swarm will depend on the specifics of a given mission and may be modified depending on the nature of the operating environment. The distinction of roles in a drone swarm allows for more complex behavior of the swarm as a whole. As a part of the swarm, multi-task teams can be created cooperating with each other, ensuring the implementation of a wide range of reconnaissance and combat missions (Ekelhof & Paoli, 2020).

The individual drones in a swarm are typically: autonomous, situated in the environment which can act to modify it, capable of sensing their local environment and other nearby drones, able to communicate (locally) with other drones, unaware of the global state of the environment (and other drones), able to cooperate with other robot to perform a given task (s). Based on a study conducted by Arkin (2009), we can distinguish some of the advantages of multi-robotic systems (such as drone swarms) comparing to single robot systems (a single drone) Firstly, improved performance – if tasks are decomposed and execute in parallel, groups will achieve tasks more efficiently. Then, task enablement: just like in nature, a group of drones (swarm) will enable the implementation of tasks that cannot be performed by individual drones. Next, as a part of distributed sensing, a drone swarm will form a "sensor grid" more effectively, which will allow for more information than in the case of a single drone (Kallenborn, 2020). In turn, a distributed action, through parallel, coordinated actions of a large number of drones, will enable conducting of tasks in different places at the same time. What is more, fault tolerance is much greater in a drone swarm than in the case of single unmanned aerial vehicles. The failure of a single drone does not affect the implementation of a task throughout the swarm (Johnson, 2020). On the other hand, Arkin (2009) describes some disadvantages or challenges related to multi-robotic systems as well.

In the case of imperfect technology, the operation of individual drones may disrupt the functioning of the entire swarm (e.g. collisions, loss of communication), which may affect accomplishing a mission. In assumptions, the operation of a drone swarm is autonomous. However, there are concerns about the lack of cooperation and coordination, which may result in competition instead of cooperation in the implementation of specific tasks. These actions may result in uncertainty concerning other robots' intentions.

A large number of unmanned aerial vehicles carrying out a joint mission does not mean that they use swarm tactics. One should distinguish the operation of unmanned aerial platforms used on massive scale (in large numbers), which do not use communication within the group and are not autonomous. Their actions are coordinated by one or more operators (decision makers) in real time or in advance based on programmed behaviors (Ilachinski, 2017). The tactics of using a drone swarm distinguishes it from the massive use of unmanned aerial vehicles as well. John Arquilla and David Ronfeldt (2000, p. 45) define tactical swarming as "seemingly amorphous, but it is a deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points, by means of a sustainable pulsing of force and / or fire, close-in as well as from standoff positions". Drone swarms are highly suited for employing swarming tactics, but do not necessarily need to do so. The members of a drone swarm rapidly share information and coordinate their actions, enabling them to attack from all directions. The ability of drones within a swarm to act either individually or collectively also enables drones to concentrate or disperse as needed.

A drone swarm owns specific attributes distinguishing it from the typical use of unmanned aerial vehicles. To begin with, drone swarms should be self-directed and self-governed. This is achieved through complex behavior, which is the result of combining a few simple behaviors and their interaction with the environment. The natural conclusion is that a drone swarm with planned mission goals must also possess autonomy. Amongst many attributes indicated in literature (See: Sterritt & Hinchey, 2005; Truszkowski et al., 2006), such as self-optimizing, self-healing and self-protecting, development of a future drone swarm capabilities should focus on four issues. First, the size of the swarm. As a rule, the more drones in a swarm, the greater its capabilities. For example, they can search and identify objects over a larger area. Huge number of drones in a swarm increases its survivability in the event of an attack, as losing parts of it will not significantly affect the tasks conduct throughout the whole swarm. On the other hand, building a large drone swarm requires, above all, the ability to handle huge amounts of information. More drones mean more inputs that can influence swarm behavior and decisions. And on a basic level, more drones mean a greater risk of one drone colliding with another. Of course, the size of a drone swarm will depend on the nature of the mission. Stealth missions do not require thousands of drones. In certain cases, a large number of drones can unnecessarily attract the attention of defenders.

Second, diversity. A drone swarm does not have to be of the same type and size of unmanned aerial vehicles, but it can contain both large and small drones equipped with different capabilities. The combination of various sets of drones creates an echelon that is more effective than the individual parts, contributing to synergy effect. Currently, drone swarms mainly consist of small, identical drones, but in the future there will be multi-domain swarms working with other systems in the air, on the water and on the ground. For example, a flying drone will map the area and the ground drone will use this information to plan its operations. A drone swarm can play different roles depending on their various capabilities. Some drones will attack the target, while sensor-based drones will collect battle damage assessment and forward this information to the command post. In turn, communication drones ensure the integrity of communication within a swarm. Small drones with sensors can provide reconnaissance for larger unmanned aerial vehicles by gathering information

about targets and transmitting it to the drone for air strike. A drone swarm can contain unmanned aerial vehicles of various sizes, optimized for different types of targets. A swarm aimed at suppressing enemy air defenses could include drones equipped with anti-missile kits to defeat ground defense, while other drones could be armed with air-to-air missiles to counter enemy aircraft. Cheap dummy drones may turn out to be an extremely valuable complement to a swarm mission, focusing the enemy's defense on themselves and providing freedom of action for more advanced drones. The key, however, is that diversity enables more complex behaviors.

Third, self-configurability. Customizable swarms offer commanders flexibility by allowing them to add or remove drones as needed, and it also allows the swarm to be tailored to the needs of a specific situation or mission. The commander can also change the capabilities of the swarm by adding drones equipped with various sensors, weapon or other capabilities. In extreme cases, a customizable drone swarm could merge into one large unit. This would enable a quick and decisive response to the changing dynamics of combat operations. For example, a small group of drones could draw apart from the larger mass to investigate a possible enemy aircraft. If the new target poses a serious threat, the full swarm may reconfigure itself to attack the identified enemy.

Fourth, self-perfection. A drone swarm is prone to electronic disturbances due to the need for continuous communication between individual units – on which the capabilities of the entire swarm depend. The inability to share information due to disruptions means that a drone swarm cannot function as a coherent whole. The vulnerability to electronic impact depends on the composition of a drone swarm. The swarm may contain drones specifically designed to counteract disruptions. Communication drones can serve as relays to share information, provide alternative communication channels, or simply detect possible jamming and issue withdrawal commands. A drone swarm could also include drones equipped with anti-jamming systems.

3. Key factors influencing a drone swarm employment in military operations

3.1. Operational factor: the scope of drones (swarm) employment in military operations

Basically, drones can be utilized (Figure 1) in an adaptable way in conducting tasks such as intelligence, surveillance, target acquisition, and reconnaissance missions. More specifically, they are used in strikes against surface targets, relaying of information over-the-horizon, Electronic Warfare, Combat Search and Rescue operations, Chemical, Biological, Radiological and Nuclear Warfare threats motoring, payloads and logistics transportation. Drones are presumed to provide their services at any time, be reliable, automated and autonomous. They may store a wide range of information from troop movements to environmental data and strategic operations.

From doctrinal point of view, based on NATO solutions, unmanned aircraft may be categorized into three classes, and the division criterion is the maximum take-off weight of the unmanned aircraft (NATO Standardization Office, 2020). The first class includes unmanned aerial vehicles up to 150 kg, class II 150–600 kg, class III over 600 kg. The adopted classification adjusts individual classes to command levels and assigns them specific tasks. Drones can be also divided as strategic, operational, and tactical. Strategic drones are used for long-range reconnaissance over hostile territory. They include systems like the Global Hawk, which can cruise at 20,000 meters above sea level for 40 hours and travel 3,000 nautical miles. Operational drones include the Predator and Reaper systems, which can fly at 7,500

and 15,000 meters respectively. They are deployed at the theatre level of combat and can be used for both reconnaissance and attack purposes. Lastly, tactical drones are low altitude, short range aircraft (20 miles or less). An example is the Dragon Eye system. Unlike strategic and operational drones, which can be either remotely piloted or preprogrammed to fly autonomously, tactical drones are fully operator-controlled (Willis et al., 2021).

Cass I of unmanned aircraft (micro, mini, small) are primarily used by land forces and special forces. Land forces use them to conduct reconnaissance in the close tactical area, in order to improve situational awareness of a given subunit. Additional tasks from this class may be mark a target and support artillery operations by airborne adjustment of fire. Class I mainly supports operations conducted by ground forces from the platoon level to the battalion. Similar tasks will be carried out by special forces subunits. However, most unmanned aircraft are micro and mini class – highly mobile and simple to use, suitable for use in combat environment.

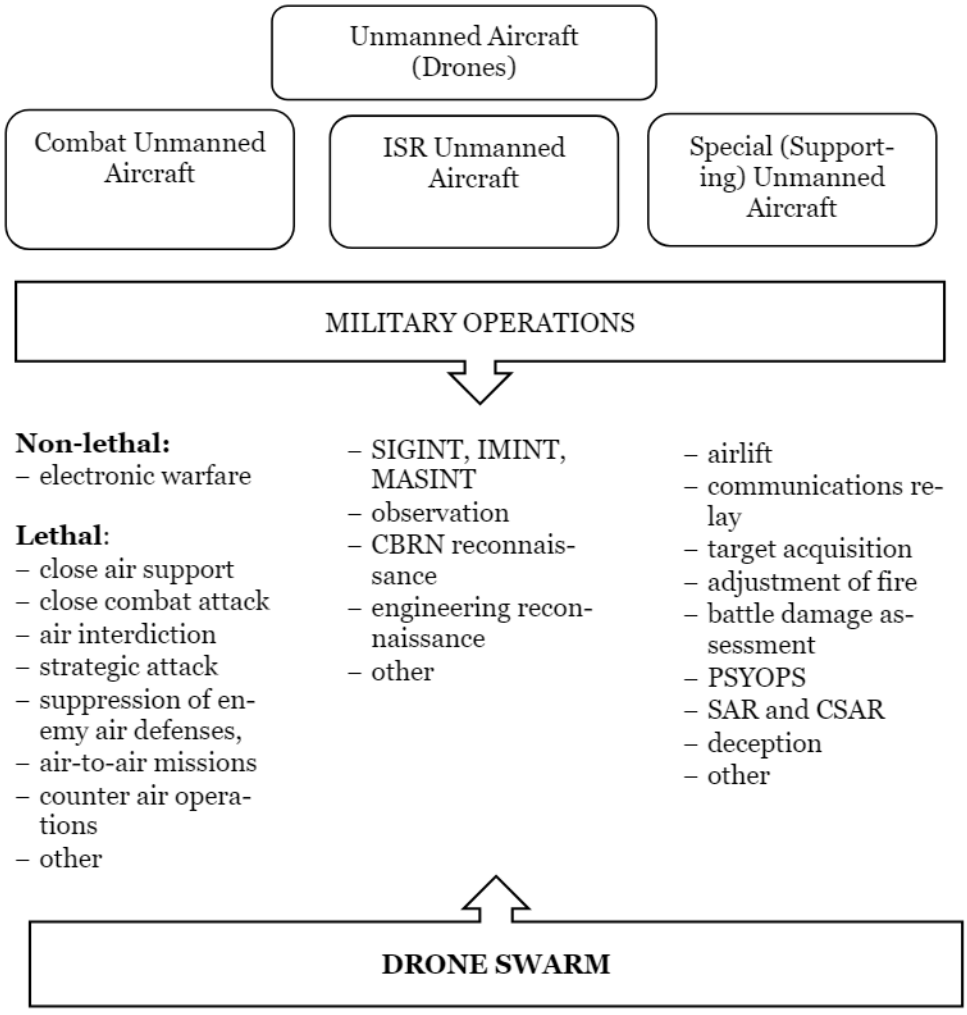

Figure 1. Unmanned Aircraft Systems employment in military operations. Own work.

Naval forces use mini and small unmanned aircraft of Class I, mainly VTOL (Vertical Take Off and Landing). They are capable of operating from the decks of ships. Their main task is to supervise and control sea areas as well as participate in searching and identifying of enemy submarines and surface ships. The naval force may also be equipped with land-based Class I (small) of unmanned aircraft that are part of the maritime reconnaissance

squadron. Their tasks is similar to those presented above, including the protection of sea bases (ports).

Class II of unmanned aircraft are mainly short- and medium-range tactical aircraft conducting tasks at the brigade and division level. They carry out reconnaissance and observation missions at distances ensuring a given level of command in decision-making of. The prospective development of dedicated devices (sensors) does not exclude their use for other tasks, e.g. close combat attack. Tactical unmanned aircraft can also be used by naval forces from land based airfields to conduct reconnaissance of sea basins.

Class III of unmanned aircraft is used mainly by the Air Force. Their size and maximum take-off weight force them to operate from air bases (airports) with prepared infrastructure. These are MALE (Medium Altitude Long Endurance) and HALE (High Altitude Long Endurance) systems, which may be armed. These platforms carry out tasks over theater of operations supporting land, sea, special and air forces. The main task conducted by class III of unmanned aircraft is airspace surveillance and early warning. The information (data) obtained has an impact on decision making at the Joint Forces Command level. Like manned aviation, they can also conduct air strikes against targets selected in targeting process or close air support and air interdiction.

One can assume that in the next decade, leading military powers as well as non-state actors will be equipped with a drone swarm. A drone swarm will be a cheaper equivalent of advanced and much more expensive weapon systems including typical unmanned aircraft. They will be used to destroy ground targets, but their effectiveness will probably also be proven in air-to-air operations – against enemy aircraft or its drone swarms. New means of transporting and launching them will be implemented, based on both ground vehicles, aircraft (manned and unmanned), as well as individual soldiers' equipment.

From a doctrinal point of view, a drone swarm can be used for several types of military operations. First, it will ensure a dispersed distribution of sensors responsible for reconnaissance, observation, tracking, precise location and tracing. This can be done both actively and passively. For instance, multiple widely distributed sensors can locate emitters by comparing the differences in time of arrival and frequency due to the Doppler shift from relative movement. For active detection, distributed sensors can operate like a multi-static radar, with one sensor emitting a radar pulse and multiple sensors detecting the reflection, allowing stealthier and higher-quality radar detection (Martinic, 2020).

Second, a drone swarm will provide offensive actions in the form of kinetic attack or an attack using electronic warfare kits. It will be able to affect many enemy targets, attacking them with their weakest defense. Acting in a distracted manner it will hinder the defender's reaction. If ten drones attack a target simultaneously and seven are shot down, three will still be able to accomplish their mission. Presumably, in the future even a large drone swarm will be more effective and less costly to use compared to single manned or unmanned aerial vehicles.

Third, a drone swarm will be used for defensive operations, misleading (deception) the opponent as to the size and number of the combat group in the air and counteracting his attack. Scharre (2014) describes how miniature air-launched decoys can be used to fool enemy radars. He also notes that large numbers of drones could swarm over an enemy's airfield to prevent aircraft from taking off. A similar tactic could be used to protect a piece of territory from overflights by enemy helicopters or airplanes, though the difficulty of such a mission would increase with the size of the area that needed protecting.

Drone swarms in combat operations can be directed against targets that require a small amount of explosives: helicopters at landing areas, planes at airports, fuel tanks or elements of transmission and communication systems. Hundreds or even thousands of drones in the area of operations may engage enemy combat systems, blocking the ability to conduct their

tasks (Rossiter, 2018). Moreover, electronic interference by the enemy with a large number of drones in the swarm will not bring the desired effects.

3.2. Technical factor: Command and Control models of a drone swarm

As Scharre (2014) notes, in recent years the concept of coordination of activities between multiple vehicles (objects) has been tested in simulations and experiments all over the world. Hence, it can be concluded by analogy that the use of a drone swarm to a certain extent is technically possible today.

Referring to command and control (C2) models, Scharre (2014) believes that the implementation of effective command and control over a swarm is a relatively new research area in which the concept of decentralized swarm management is considered to be the essence of its functioning.

Scharre's (2014) model includes four distinctly different C2 swarm architectures (Figure 2):

- Centralized control model: the swarm elements feed information back to a central planner which then tasks each element individually.
- Hierarchical control model: the individual swarm elements are controlled by "squad" level agents, which are in turn controlled by higher level controllers, and so on.
- Coordination by consensus model: the swarm elements communicate to one another and converge on a solution through voting or auction-based methods.
- Emergent coordination model: the coordination arises naturally by individual swarm elements reacting to others, like in animal swarms.

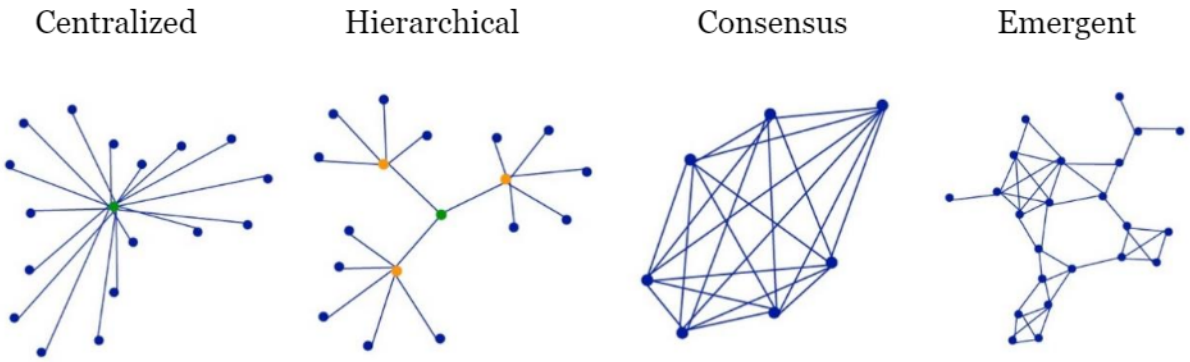

Figure 2. C2 swarm architectures. Adopted from: "Robotics on the Battlefield, Part II: The Coming Swarm" by P. Scharre. Copyright 2014 by Center for a New American Security.

As far as practice is concerned, the presented models can be applied to command a squadron of combat aircraft. The centralized control model imitates a fighter squadron. Pilots can communicate with each other, but their mission is coordinated centrally by a command post on the ground. Therefore, the degree of autonomy of individual pilots is limited. In line with the hierarchical control model, the squadron commander's superiors set the overall directions for the mission, but the squadron commander retains a certain degree of autonomy to actually carry it out (Grimal & Sundaram, 2018). There is a noticeable difference related to coordination by consensus model. The drones would have autonomy in making decisions among themselves within the swarm, while the squadron of manned aviation would be dependent on the final decisions of the ground control, even though pilots may of course communicate with each other during the mission. Finally, the emergent coordination model which is unique in terms of intuitiveness because there is no need to communicate

with ground control. This model indicates that the drone swarm is much more complex than the fighter squadron. It is likely that highly trained manned air squadron pilots may act in a similar way, but the level of intuition about how a squadron works as a group during a mission is definitely lower than in a drone swarm.

Specifying the presented C2 models of a drone swarm, in a centralized control model the chain of command is relatively simple, comparable to a uncomplicated command system. According to Burdick (2015), the lead drone assigns tasks to the drones in the swarm, and all nodes are identical. The choices of the leading drone, treated as a commander, depend on its current position, combat situation and other current factors affecting the execution of the task. If the lead drone cannot assign the accomplishment of tasks, it may be replaced by another node so that the mission can continue.

The hierarchical control model is based on a system of nodal points. Each node in turn controls multiple subsets in the swarm, which in turn can also be nodes. This model replicates the traditional C2 military structure. If any node is eliminated, the next one takes over, maintaining continuity of command and situational awareness. The commanding node is responsible for creating a big picture plan which is transmitted hierarchically and tactical details are added by subordinate nodes. This means that at the beginning of each operation, the main (lead) drone determines the battle plan and search pattern, including the number of drones necessary to accomplish the mission. Moreover, it entrusts each drone with a specific task to conduct (Grimal & Sundaram, 2018).

The coordination by consensus model, referred to as a distributed drone swarm, allows the swarm to operate without a perceptible constant linkage command-individual drones in the swarm. In certain situations, the drones in the swarm can independently decide on the way of conducting the mission. They can stick to the original plan or change it to successfully complete their mission. In other words, all decisions are made by consensus (Chen, Tang & Lao, 2020).

The fourth, emergent coordination model is a conceptual challenge. As with coordination by consensus model, there is no apparent chain of command. The swarm operates “organically” adjusting to the current situation shaped by external elements, not a predetermined course of action. The operation of a drone swarm is intuitive, focused on independent decision making, reliant on changes in the environment in which they operate (Grimal & Sundaram, 2018). The value of the emergent C2 model is that it extends range, decreases bandwidth, and allows the swarm to dynamically scale in size. This means that the geographic coverage area of a swarm weapon using an emergent C2 model is significantly larger than either a consensus or a centralized model (McLaughlan & Hexmoor, 2011).

3.3. Human factor: dilemmas of a drone swarm autonomy

The use of an appropriate C2 model in drone swarm operations is directly related to the level of autonomy of the entire system. In the case of defining autonomous systems, the most common approach includes the criterion of the degree of human control over a machine (human-machine relation). This categorization distinguishes semiautomatic systems ("human in the loop"), in which the automatic operation is possible until a certain moment and then human intervention is necessary. The second group covers supervised systems ("human on the loop"), in which there is a possibility of uninterrupted autonomous operation, but with the possibility of human intervention at any given moment. Weapon systems from this group are able to select and combat targets on their own, from the moment they were activated. However, the operator of such weapon system has the knowledge about what kind of objects can be targeted and the operator may intervene at any time by interrupting the process. In practice, these types of weapon systems (supervised) are used in defensive operations and in undemanding operational environment. They react directly to the defined

threats, where the reaction of a human (operator) could be too slow, and in the case of doubtful situations the operator may react at any time. The third group consists of fully autonomous systems ("human out of the loop"), without the possibility of human intervention. They refer to weapon systems that independently, without human participation, are able to select and combat targets in a previously defined geographical region, time interval and according to the adopted rules. The operator does not know what targets will be selected for combating, but it should be remembered that the types of combated objects have been previously defined by a human according to the specific criteria. In other words, a man decides earlier in what manner the autonomous combat system will carry out its tasks (OUSD(A&S), 2018).

In the case of using a drone swarm in military operations, it is desirable to employ the emergent coordination model based on full autonomy. However, while full autonomy offers clear benefits for drone swarms, clear risks exist too.

More autonomous drone swarms are easier to control. Autonomy can allow multiple drones in a swarm to follow a single leader, maintain constant distances from each other, avoid obstacles, and launch attacks against targets. Each function automized is one less function requiring operator attention. Larger, more complex swarms of drones place greater cognitive demands on human operators. Large swarms have greater operational requirements and more sensors to send information to operators. Overworked operators may react slower. Heterogeneous swarms of drones of various sizes and payloads require even more attention. Operators must coordinate complex activities, such as deploying one drone to search for targets and the other to conduct attacks (U.S. Department of Defense, 2017).

Even assigning humans alone to make decisions about the use of force would be a challenge as the size of the swarm grows due to the large amount of inputs. An operator must be aware of input signals from multiple sensors in the remote area. While many operators could be used to control a swarm of drones, this would offset any cost benefits. In a military context, an operator must also detect, avoid and counter potential enemies. Any delays in communication between drones and an operator increase the risk of enemies overcoming the swarm. Since drone swarms are essentially information-dependent weapons, enemies can attack the communication systems between drones, and between drones and the operator (Scharre, 2016).

Greater autonomy can ensure greater survivability. A swarm of human-controlled drones would be at risk of losing the operator. In the case of a swarm of human-controlled drones, the human is the weakest point as killing or incapacitating the operator would deactivate the swarm. A human operator may also become sick or injured unrelated to an enemy attack. A fully autonomous drone swarm does not face such threats. Greater autonomy also allows a drone swarm to make decisions faster. In the case of a remotely controlled drone swarm, an operator must receive information from drones in the field, interpret this information, decide to use sensors or weapons, and issue the command to fire against targets. Delay can cause the enemy to open fire first, change position, or take any other defensive action. Delay will be even greater when there are more drones in the swarm as the operator can focus on a different location. Delegating decision making to artificial intelligence in the field can shorten the decision-making loop and thus increase the swarm's survivability and ability to cause harm. Greater autonomy also enables innovative use of a drone swarm. It can be programmed to carry out multiple attacks over a longer period, dispersed between attacks (Defense Science Board, 2016).

On the other hand, concerns about losing control of a drone swarm must be taken into account. An uncontrolled a drone swarm has the potential to kill friendly civilians or military personnel simply because of an algorithm error. There are concerns about possible violations of international law of armed conflict in places where it is planned to use of autonomous systems, including a drone swarm. Giving full control to artificial intelligence could

create new security gaps that undermine the reliability of a drone swarm. By its nature, full autonomy requires software and / or hardware to assist in making more sophisticated decision making. It is software and / or hardware that can make mistakes or adversaries can introduce errors through a cyber-attack. The complexity of the system can make it difficult to identify intentional or random errors. Lack of human control can exacerbate these fears into the belief that they are unexpected or uncontrollable (Wallach, 2017). There are also more mundane concerns. Military services may have cultural inhibitions before granting full autonomy to drone swarms. Long-term bans are especially likely if systems are unreliable. Full autonomy may just not be worth it. Nevertheless, due to the potential benefits, it is certainly possible for the state or the military to recognize that the benefits of using autonomous drone swarms outweigh the costs.

4. Conclusions

The architecture of a drone swarm should be based on artificial intelligence and machine learning algorithms. Drone's ability to communicate with each other within a swarm is a feature that distinguishes them from typical use of unmanned aerial vehicles. A drone swarm should be built from as many unmanned aerial vehicles as possible with comparable qualities. The utilization of artificial intelligence will allow to assign tasks inside the swarm to individual drones, which will increase the probability of conducting missions. In the future, an emergent coordination model will be optimal for a drone swarm command and control. It will be based on natural behaviors of swarms occurring in nature, such as a swarm of bees, birds or a school of fish. In this model, there will be no classic chain of command, and a drone swarm will be adaptive and intuitive, making decisions depending on a given tactical situation. The specific attributes of a drone swarm that distinguish it from typical use of unmanned aerial vehicles include size, diversity, self-configurability and self-perfection.

Currently, it is difficult to predict new types of military operations unique to a drone swarm. It should be assumed that these will be typical operations conducted today by unmanned aerial vehicles. These contain: intelligence, surveillance and reconnaissance operations, distributed offensive operations and defensive operations. However, attributes of a drone swarm suggest that these operations will be carried out more safely and faster with minimal (human on the loop) or without human intervention (human out of the loop).

There is a need for further research on the autonomy of a drone swarm. Despite the undoubted advantages associated with the use of full autonomy in conducting tasks by a drone swarm, there are also concerns about some uncontrolled, independent carry out of tasks by them without human intervention in a manner that is illegal. Research into artificial intelligence and machine learning may partially solve these issues. However, the decision to employ a drone swarm for a specific task should be left to humans, and should also be exercised constantly during the mission.

All in all, despite the dynamic development of drone technologies, an expectancy of application a drone swarm in combat operations seems to be distant so far. Public shows are not swarms, as they perform a programmed procedure based on a defined algorithm. Likewise, the aforementioned attacks on the Russian airbases, the Syrian military convoy and the Saudi oil fields were not drone swarms. These were coordinated strikes involving a large number of drones which did not communicate or cooperate in carrying out the mission. They can currently be defined as a drone proto-swarm. However, technology is constantly evolving and software is available on the market. At this stage, no state or non-state entity is able to operate a drone swarm in combat operations. In turn, military experiments in this field

are carried out in simplified environments, with the use of relatively small swarms and limited communication equipment (sensors) on board. The main limitation is the equipment that determines the size, weight, battery power and on-board computers, which in turn translates into the communication capacity between the swarm and its operator.

Declaration of interest – The author declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article

References

1. Arkin, R. (2009). *Governing Lethal Behavior in Autonomous Robots.* Taylor and Francis Group Publishing.
2. Arquilla, J., & Ronfeldt, D. (2000). *Swarming and the Future of Conflict*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/RAND_DB311.pdf
3. Burdick, J.E. (2015). *Instantly Basing Locust Swarms. New Options for Future Air Operations (Drew Paper No. 20)*. AU Press. https://media.defense.gov/2017/Nov/21/2001847261/-1/-1/0/DP_0020_BURDICK_INSTANT_BASING_LOCUST_SWARMS.PDF
4. Chen, X., Tang, J., & Lao, S. (2020). Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols. *Applied Sciences, 10*(10:3661). https://doi.org/10.3390/app10103661
5. Defense Science Board (2016). *Report of the Defense Science Board Summer Study on Autonomy*. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. https://www.hsdl.org/?view&did=794641
6. Ekelhof, M., & Paoli, G.P. (2020). *Swarm Robotics. Technical and Operational Overview of The Next Generation of Autonomous Systems*. United Nations Institute for Disarmament Research. https://unidir.org/sites/default/files/2020-04/UNIDIR%20Swarm%20Robotics%20-%202020.pdf
7. Grimal, F., & Sundaram, J. (2018). Combat Drones: Hives, Swarms, and Autonomous Action? *Journal of Conflict & Security Law*, *23*(1), 105–135. https://doi.org/10.1093/jcsl/kry008
8. Ilachinski, A. (2017). *AI, Robots, and Swarms. Issues, Questions, and Recommended Studies*. CAN Corporation. https://www.cna.org/cna_files/pdf/DRM-2017-U-014796-Final.pdf
9. Johnson, J. (2020). Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare. *The RUSI Journal, 165*(2), 1–11. https://doi.org/10.1080/03071847.2020.1752026
10. Kallenborn, Z. (2020). *Are Drone Swarms Weapons of Mass Destruction? (Future Warfare Series No. 60)*. AU Press. https://media.defense.gov/2020/Jun/29/2002331131/-1/-1/0/60DRONESWARMS-MONOGRAPH.PDF

11. Martinic, G. (2020). Swarming, Expendable, Unmanned Aerial Vehicles as a Warfighting Capability. *Canadian Military Journal*, *20*(4), 43–49. http://www.journal.forces.gc.ca/vol20/no4/PDF/CMJ204Ep43.pdf
12. McLaughlan, B. & Hexmoor, H. (2011). Emergent command and control architecture for dynamic agent communities. *Journal of Experimental & Theoretical Artificial Intelligence*, 23(4), 363–387. https://doi.org/10.1080/09528130701664608
13. NATO Standardization Office (2020). *ATP-3.3.8.2 Unmanned Aircraft System Tactics, Techniques And Procedures*. NATO Standardization Office. https://nso.nato.int/nso/
14. OUSD(A&S) (2018). *Unmanned Systems Integrated Roadmap 2017–2042*. United States. Office of the Under Secretary of Defense for Acquisition and Sustainment. https://www.defensedaily.com/wp-content/uploads/post_attachment/206477.pdf
15. Rossiter, R. (2018). Drone usage by militant groups: exploring variation in adoption. *Defense & Security Analysis,* 34(2), 113–126. https://doi.org/10.1080/14751798.2018.1478183
16. Scharre, P. (2014). *Robotics on the Battlefield, Part II: The Coming Swarm*. Center for a New American Security. https://www.files.ethz.ch/isn/184587/CNAS_TheComingSwarm_Scharre.pdf
17. Scharre, P. (2016). *Autonomous Weapon and Operational Risk*. Center for a New American Security. https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf
18. Sterritt R., & Hinchey, M. G.(2005). Apoptosis and self-destruct: A contribution to autonomic agents? In Hinchey, M.G., Rash, J.L., Truszkowski, W.F. & Rouff, C.A. (Eds.), Formal Approaches to Agent-Based Systems (pp. 269–278). Springer. https://www.springer.com/gp/book/9783540244226
19. Suzuki, S. (2018). Recent researches on innovative drone technologies in robotics field. *Advanced Robotics, 32*(19), 1008–1022. https://doi.org/10.1080/01691864.2018.1515660
20. Tan Y., & Zheng, Z. (2013). Research Advance in Swarm Robotics. *Defence Technology*, *9*(1), 18–39. https://doi.org/10.1016/j.dt.2013.03.001
21. Truszkowski, W. F., Hinchey, M. G., Rash, J.L. & Rouff, C. A. (2006). Autonomous and autonomic systems: a paradigm for future space exploration missions. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* 36(3),279–291.https://doi.org/10.1109/TSMCC.2006.871600
22. U.S. Department of Defense (2017). *Directive 3000.09: Autonomy in Weapon Systems*. U.S. Department of Defense. www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.
23. Wallach, W. (2017). Toward a Ban on Lethal Autonomous Weapons: Surmounting the Obstacles. *Communications of the ACM*, *60*(5), 28–34. https://doi.org/10.1145/2998579
24. Willis, M., Haider, A., Teletin, D.C., Wagner, D. (2021). *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Joint Air Power Competence Centre. https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf

SAFETY&DEFENSE
ISSN 2450-551X

Unnamed Aircraft Systems: Challenges to Air Defense

Eugeniusz CIEŚLAK

University of Natural Sciences and Humanities, Siedlce, Poland;
eugeniusz.cieslak@uph.edu.pl, ORCID: https://orcid.org/0000-0002-6476-3643

DOI: https://doi.org/10.37105/sd.110

Abstract

The 2019 attacks on the oil processing facilities in Saudi Arabia and the effectiveness of combating Armenian long-range anti-aircraft systems have highlighted the nature and scale of the challenges for air defense posed by unmanned aircraft systems. The aim of this article is to summarize the lessons learned from the use of unmanned systems in recent conflicts, to assess the development of trends in such systems, and to discuss the implications of those developments for air defense. This article discusses the impact of the development of unmanned aircraft systems on air defense concepts, their organization, and the effectiveness of this defense for the defended assets. It also tries to highlight how unmanned aircraft systems may reduce the survivability of air defense systems. This research is based on publicly available documents related to air defense and unmanned aircraft systems as well as selected analytical studies on the implications of the development and use of unmanned aircraft systems for air defense. As such, this research identifies the possible challenges related to ensuring effective air defense against attacks by unmanned aircraft systems, resulting from the costs of defense despite the availability of technological solutions. It also raises the issue of survivability of air defense systems if attacked by unmanned aircraft systems.

Keywords

air defense, challenges, threats, unmanned aircraft systems

1. Introduction

Submited: 13.03.2021. Accepted: 13.04.2021. Published: 25.05.2021.

Although unmanned aircraft systems have been used in combat operations for a long period of time, the last two decades have witnessed their widespread deployment in a wide range of reconnaissance, surveillance, and strike tasks. The dynamic development and proliferation of technologies that enable the development and use of unmanned aircraft systems has increased their availability not only to major military powers but also to smaller countries and non-state actors. Currently, unmanned aerial vehicles provide a wide spectrum of platforms, having different endurance, altitude and flight speed, or being multi-role or optimized for specific tasks. A significant part of them – especially those smaller and cheaper unmanned aircraft systems – became available to a wide group of countries, substituting manned aviation. The weaponization of small, unmanned aircraft systems increased the combat capabilities of light infantry in several countries but also provided non-state actors with a new offensive weapon. The employment of unmanned aircraft systems in Syria by ISIS and anti-government forces as well as attacks on oil processing facilities in Saudi Arabia have proved the potential of unmanned aircraft systems to conduct not only tactical but strategic attacks. The unmanned swarm attack against the terminal highlighted the potential challenges for air defense resulting from the skillful use of unmanned swarms as part of an air and missile attack by a state opponent or an attack on critical infrastructure elements by non-state actors. The unmanned aircraft systems proved effective in the destruction of ground-based air defenses in Syria, Libya, and the Nagorno-Karabakh conflict between Armenia and Azerbaijan. Therefore, recent conflicts have highlighted the direct threat to air defenses posed by unmanned systems. Both of these trends observed in recent years can be considered a harbinger of challenges for air defense in the coming decade.

The aim of this article is to make a preliminary assessment of the challenges and threats to air defense posed by unmanned aircraft systems. Based on the analysis of selected attacks with the use of unmanned aircraft systems in recent years, the possible consequences for air defense were assessed in two aspects. First, this article explores how the development of unmanned aircraft systems affects the effectiveness of air defense. Then, the article addresses the issue of how unmanned aircraft systems influence the survivability of the components of the air defense system.

This research uses publicly available documents related to air defense and unmanned aircraft systems as well as selected analytical studies on the implications of the development and use of unmanned aircraft systems for air defense. While quantitative analysis of the subject has been hard to conduct due to a lack of verifiable information, this article focuses on the qualitative aspects of the challenges that unmanned aircraft systems pose to air defense. Therefore, new concepts for employment, tactics and impact on warfare and air defense are researched in more detail.

The introductory part of this article discusses the main trends in the development of unmanned aircraft systems in the context of the challenges and threats they may pose to air defense. Then, the article presents a preliminary assessment of unmanned aircraft systems' attacks in the context of the requirements for air defense related to the protection of defended assets. The next part of the article focuses on the assessment of the impact of the use of unmanned aircraft systems on the survivability of the air defense system and its individual components. The final part of the article addresses future trends related to the use of unmanned aircraft systems and analyzes the possible impact on air defense.

2. The evolving threat of unmanned aircraft systems

The threat posed by unmanned aircraft systems is broad and comprehensive, which results, inter alia, from the existing diversity of their design, purpose, and availability. For air defense, the tactical and technical parameters of unmanned aircraft systems are more important than their military or civilian affiliation. Therefore, in assessing the trends related to the proliferation of such systems, military, civil, and commercial off the shelf systems should be considered. The upper tier of military unmanned aircraft systems, such as High-Altitude Long Endurance (HALE) systems and dedicated Unmanned Combat Aircraft Systems (UCAS), will most likely remain available to a relatively small group of states with an advanced technological base. At the same time, Medium Altitude Long Endurance (MALE) unmanned aircraft systems will proliferate around the world at modest pace either produced by growing number of states or procured. The most disruptive proliferation will be witnessed for smaller unmanned aircraft systems, as they are becoming available virtually to any state or non-state actor. According to available Joint Air Power Competence Centre (JAPCC) estimates, at least ninety-five countries in the world maintain active unmanned aircraft systems programs, and armed forces have used at least twenty-one thousand drones (JAPCC, 2020). The US Department of Defense itself has operated more than eleven thousand unmanned aircraft systems of different classes. At least twenty countries have produced military-grade unmanned aircraft systems, which creates favorable conditions for the proliferation of this type of weapon system. The number of non-state actors with drone capability is increasing. Such actors tend to weaponize commercially available drones or are provided with military grade systems by sponsoring states (Patterson, 2017).

Commercially available unmanned aircraft systems weighing from 100 grams to 150 kilograms dominate in civil applications. The scale of unmanned aircraft system proliferation can be assessed through the prism of data available for several countries. In 2019, 1.3 million recreational unmanned aircraft systems were registered in the United States. However, it is estimated that several hundred thousand more remain unregistered. In Germany, the number of unmanned aircraft systems increased from 162,000 in 2015 to over 600,000 in 2020 (JAPCC, 2020). Such trends may be probably observed for several other states around the world.

Unlike the conventional air threats of manned aircraft and missiles, which are predominantly used in times of war, the unmanned aircraft systems must be considered a threat in times of peace, crisis, and war. To some extent, HALE and MALE unmanned systems may be considered conventional air threats, as they are easily attributable to their state operators. This does not hold true for a range of smaller aircraft systems, which may be hardly attributable to specific state actors. Therefore, in peacetime, small, unmanned aircraft systems that may be used as a means of air attacks will most likely be commercial civil systems used by non-state or state actors willing to conceal the origin of the attack. The threat in peacetime cannot be considered through the lens of possible kinetic attacks as unmanned aircraft systems may be employed for obtaining the information necessary for further terrorist or criminal activities. There is no doubt that the ad hoc weaponization of the civilian unmanned aircraft systems may allow their use in kinetic attacks as well. Due to the limited payload offered by most of commercial unmanned aircraft systems, they might be used primarily for attacks on soft targets, such as civilian or military infrastructure facilities and mass events (Zieliński, 2018a).

The use of dedicated military unmanned aircraft systems will dominate during major combat and crisis response operations. The threat posed by unmanned aircraft systems during such operations will be a consequence of their employment for both information acquisition and as a means for strike missions (Cieślak, 2018). Unmanned aircraft systems have traditionally provided target acquisition data for land, air, and sea fire support systems. The conflict in Eastern Ukraine saw three Ukrainian mechanized battalions destroyed by rocked artillery fire in several minutes due to surveillance and target acquisition provided by drones

(IISS, 2019). Armed unmanned aircraft systems can pose a threat to point targets and soft area targets. Unmanned aircraft systems platforms employed in electronic warfare may disrupt the enemy's command, control, and communications systems, preventing the enemy from achieving and maintaining information superiority.

The relatively low costs of acquiring small, unmanned aircraft systems mean that they are specifically designed for expandability. Although there are dedicated loitering munitions or 'kamikaze' drones, low costs facilitate decisions to turn regular small, unmanned aircraft systems into munitions. Low costs and advances in the field of system automation and autonomy will change the tactics of unmanned aircraft systems. One may expect more frequent use of swarming tactics by the drones in the execution of their attacks on both defended assets and air defenses. For unmanned aircraft systems optimized for Suppression of Enemy Air Defenses (SEAD), one should consider that the unmanned aircraft systems will be able to perform increased tasks in autonomous mode. Unmanned aircraft systems provide clear advantage over manned aircraft in regard to operational threshold, and therefore they constitute new challenges for air defense. The JAPCC report on comprehensive approach to countering unmanned aircraft systems lists three principal advantages related to reduced risk, expendability and less potential for escalation (JAPCC, 2020). This may mean that, unlike manned unmanned aircraft systems, unmanned aircraft can be widely used already during a developing crisis.

Another factor that changes traditional air defense calculus relates to space and time considerations. Traditionally, effective air defense benefited from early warning that allowed multiple engagement of fighters and ground-based air defenses against air threats. That may not be the case for attacks by small, unmanned aircraft systems. Such attacks may be executed from the proximity of intended targets, and the means of attack may be assembled from commercially available components in the last minutes prior to the attack. Such a scenario limits the warning period for traditional air defense air surveillance and control systems and limits kinetic defense to the terminal phase of attack. The possibility of conducting an attack from within the enemy air defense system also offers several other advantages. It may increase chances for plausible deniability. This may encourage possible attacker and increase the risk of false flag attacks. Availability of small, unmanned aircraft systems may also enable lone wolf attacks.

3. Defending against unmanned aircraft systems

The last two decades have been a period of unmanned aircraft systems proliferation in military applications. The most common trend has been the use of unmanned aircraft systems for reconnaissance and observation, but a growing number of strike missions have been performed as well. Unmanned aircraft systems have started to be used for transport missions. As the post 11 September 2001 period has seen the so-called 'Global War on Terrorism,' the drone attacks during last two decades focused on key leaders of terrorist organizations. The use of Medium Altitude Long Endurance (MALE) unmanned aircraft systems in Afghanistan, Iraq, Syria, and North Africa was part of military operations, and these systems were used by various types of armed forces and government institutions. The use of unmanned aircraft systems by non-state actors in the first decade of the 21st century was incidental. Attempts to use unmanned aerial vehicles were made by Hezbollah in 2004 but were mostly unsuccessful (IISS, 2019).

The situation began to change after 2011, when unmanned aircraft systems began to be used more often by non-state actors. The first successful use of an UAS for a strike mission

by a non-state actor took place in 2013, when Hezbollah attacked a camp of anti-government forces in Syria (Uracosta, 2020). The most prolific user of unmanned aircraft systems turned out to be the so-called Islamic State of Iraq and the Levant. It proved competent in using such systems against Iraqi and Coalition forces in Iraq between 2013 and 2017. This terrorist organization developed its own "Jihadi drone air arm" and was able to conduct large number of attacks against battlefield targets (Urcosta, 2020). As Gen. Raymond Thomas observed jihadi drones were most daunting threat to U.S. and coalition forces fighting in Mosul in 2016. The adaptive use of drones allowed Islamic State group militants to enjoy tactical superiority under coalition forces' conventional air superiority. And the only available response at that time was small arms fire (Larter, 2017).

The attacks by unmanned aircraft systems that have influenced the perception of threats from such systems in recent years include the attack on oil installations in Saudi Arabia in September 2019. A swarm of twenty-five drones and cruise missiles hit oil-processing facilities at Abqaiq and Khurais, cutting Saudi daily production of oil by 50 percent and global supply by 5 percent. The Houthi movement of Yemen claimed responsibility for the attacks while the United States and Saudi Arabia believed that Iran was behind them. Iranian involvement was however not proven despite a three-years long investigation conducted by the United Nations. The economic consequences of the attack and the defenselessness of the Saudi air defense system highlighted the possibility of using unmanned aircraft systems to carry out strategic air attacks (Frantzman, 2019). Difficulty in attributing this aggressive act to any state or non-state actor may be considered another worrying factor describing unmanned aircraft systems attacks against Saudi Arabia in 2019. This might in turn be seen as a possible incentive for future use of unmanned aircraft systems by rouge states. Anthony H. Cordesman of the Center for Strategic and International Studies observed (2019), the use of unmanned aircraft systems against Saudi Arabia oil installations provided a clear strategic warning that the era of air supremacy of the United States and the near US monopoly on precision strike capability is rapidly fading. This lesson will be learnt by other global and regional powers, as unmanned aircraft systems are becoming one of the most prominent weapons of choice in hybrid and gray area warfare.

The unmanned aircraft systems attack on Russian air and naval bases in Syria, most likely carried out by Syrian opposition forces, should also be noted. While the attack of thirteen drones on 6 January 2018 has been most publicized, there were many more such attacks in recent years. The Khmeimim air base alone was attacked by hundreds of drones between 2018 and 2020 along with separate mortar and rocket attacks. In 2019, there were around sixty drone attacks against this base alone (Urcosta, 2020). The drone threat was persistent and affected air base operations for extended periods of time. The military significance of these drone attacks against Russian bases in Syria goes beyond the arithmetic of losses inflicted to equipment and manpower. Rather, they have shown the new opportunities of attacking military infrastructure by an enemy without advanced weapon systems and traditional airpower. Attacks against Russian air bases in Syria have also demonstrated the necessity to consider defense against unmanned aircraft systems as a vital part of the force protection measures. Based on Russian experience in Syria, one may argue that in the future, other leading militaries may be subjected to similar attacks. What is more, the threat of drone attacks against air bases may be present not only during expeditionary operations but extend also to air bases in home countries (Vick et al., 2020).

The use of unmanned aircraft systems by Turkish forces in Syria in spring 2020 is a good example of the effective use of these systems in conventional warfare. Turkey proved to be competent in using a domestically produced medium altitude long endurance unmanned aircraft systems fleet, marking the integration of unmanned systems in combined arms operations. The Turkish military was able to mount hundreds of unmanned aircraft system attacks against Syrian ground troops, allegedly destroying more than a hundred targets and

effectively halting their offensive. Both direct drone strikes and unmanned aircraft systems' support to indirect fires were integrated with combined arms operations (Urcosta, 2020). On the contrary, despite the short duration of military confrontation, notable losses to Turkish unmanned aircraft systems force could have been observed, which puts into question the sustainability of their tactics in future scenarios, especially in a contested air environment and against an integrated air defense system typical for a conflict with a peer adversary (Parahini, 2020).

Some experts have touted the Libyan Civil War as the largest drone war in the world (Defenceworld.net, 2020). The conflict has seen more than one thousand strikes by unmanned aircraft systems since its beginning of conflict, with the Libyan National Army forces alone conducting around 850 drone strikes before the beginning of 2020 (United Nations Support Mission in Libya, 2020). All parties to the conflict in Libya have been using low-endurance commercial drones for intelligence, surveillance, and reconnaissance tasks at the tactical level (Panel of Experts, 2019). In 2016, external support by the United Arab Emirates to the Libyan National Army (LNA) allowed it employing Chinese medium altitude long endurance systems and gain advantage over the UN-recognized Government of National Accord (GNA). Since mid-2019, Turkey buttressed its support to the GNA forces with medium altitude long endurance unmanned aircraft systems, and the balance of power shifted again. Turkish armed drones attacked LNA's ground targets, conducted air interdiction against its supply lines, and were able to conduct effective strikes against its forward airbases, destroying several aircraft and surface to air missile systems there. Skillful use of ground-based air defenses along with jamming systems by the Turkish forces increased the survivability of the GNA drone force and disrupted drone operations by the LNA, thus depriving it from achieving initial air supremacy. High intensity drone operations resulted in a significant rate of attrition. During the first half of 2020 alone, seven-teen Turkish and eight Chinese-made medium altitude long endurance unmanned aircraft systems belonging to the two warring parties were destroyed (Defence-world.net, 2020). It testifies that there are notable costs of drone warfare, even if they are lower than those of conventional war.

The conflict for Nagorno-Karabakh in autumn 2020 has sparked an intense discussion on emerging importance of unmanned aircraft systems in future warfare. The widely discussed effectiveness of Azerbaijani UAS deployment in the conflict with Armenia sparked several comments related to the decline of tanks and advent of drone warfare. Such claims seem premature. While air defense systems are only partly effective against emerging threat of unmanned aircraft systems, several other factors might have contributed to the Armenian defeat. The Armenian military was not prepared for a limited conflict both in terms of its hardware and in terms of tactics. On the other hand, the Azerbaijani military heavily invested in advanced weapon systems in recent decade and prepared for using those (Flannelly, 2020). The Armenian military failed to meet the basic requirements of combined arms operations, which ultimately allowed freedom of deployment for Azerbaijani unmanned aircraft systems and contributed to their effectiveness (Clancy, 2020). Live video footage from unmanned aircraft systems and loitering munitions heavily influenced the public perception of the conflict. Azerbaijan was able to use live footage to reinforce its propaganda and shape perceptions of not only the Armenian population and military, but also that of the international community as well.

When assessing the threat posed by unmanned aircraft systems, attention should be paid to their use by criminal groups, including terrorist organizations, and to the risks related to commercial and hobby activities. Unmanned aircraft systems are used for criminal surveillance purposes, including tracking police activities, transporting drugs and other goods, delivering weapons, and prison contraband drops. Attacks on rival groups as well as intimidating police have been observed in recent years. Attacks against high-level politicians and military have also been conducted, but it has been difficult to attribute them immediately to

specific actors (IISS, 2019). Unidentified unmanned aircraft systems have been recently observed around critical infrastructure, such as nuclear plants, which raises concerns related to their vulnerability to drone attacks (Solodov et al., 2018). A growing number of civilian airports have suffered disruption of air operations because of unmanned aircraft systems in their vicinity. Pyrgies (2019) identified 139 serious UAV incidents in the vicinity of worldwide airports between 2014 and May 2018 alone. Stray unmanned aircraft systems have ended up near governmental buildings such as the White House or the Japanese Prime minister's office, just to name a few examples. The limited scope of the criminal use of unmanned aircraft systems so far results in a situation in which they remain in the focus of police and civilian investigative services but do not raise public interest or concerns. However, with the growing potential of unmanned aircraft systems, the military air defense community cannot neglect it.

4. Surviving Unmanned Aircraft Systems attacks

The challenge of unmanned aircraft systems to air defense is twofold. With challenges related to the effective protection of defended assets discussed in the previous part of the article, more attention should be given to the threat that unmanned aircraft systems pose to air defense systems themselves. The development of advanced ground-based surface to air missile systems, termed sometimes as "double digit SAMs," pushed for a more effective means of suppression of enemy air defenses (SEAD). As a single combat air defense vehicle was able to pose a threat to air operations, there was a growing requirement for means capable to hunt for such targets. Anti-radar missiles that revolutionized SEAD operations after the Vietnam War lacked the capability to remain over battlefield for an extended time. It meant that to provide effective suppression for longer time, one needed to fire preemptive salvos of expensive missiles.

Unmanned aircraft systems have changed this calculus. Traditionally, unmanned aircraft systems were used as decoys to deceive enemy air defenses, to saturate them or bait so that they would become easier targets for anti-radiation missiles. Since the end of 1990s, 'kamikaze' drones entered the service, with IAI Harpy as the most prominent example and unmanned aircraft systems started to be used more frequently for assisting SEAD attacks by other weapon systems.

The last few years saw highly publicized cases of effective attacks by unmanned aircraft systems against ground-based air defenses. In Syria, Turkish unmanned aircraft systems were able to destroy several advanced Russian SA-22 systems in early 2020 and that was also the case in Libya (United Nations Support Mission in Libya, 2020). The Armenian-Azerbaijani conflict later in autumn 2020 saw successful unmanned aircraft systems attacks against S-300 launcher vehicles. Live footage of attacks supported Turkish and Azerbaijani claims about the effectiveness of unmanned aircraft systems attacks and grabbed the attention of international community, which started heralding a new era of drone wars (Clancy, 2020). SA-22 performance against unmanned aircraft systems seems disappointing, although they were able to shoot down several medium altitude long endurance unmanned aircraft systems both in Syria and in Libya. The anti-government forces of General Haftar, which operated the SA-22 systems in Libya, may have lacked proper training with this specific weapon system. It is hard to accept such an explanation for the actions of the Syrian armed forces. The disparity of the quality of weapon systems and deficient training may have also contributed to the defeat of Armenian air defenses in the Nagorno-Karabakh conflict.

Predominantly Soviet-era surface-to-air missile systems failed to stand up to the coordinated use of strike and 'kamikaze' drones supported by surveillance and command and control unmanned aircraft systems and indirect fires (Shaikh & Rumbaugh, 2020).

What recent analyses miss is the fact that successful unmanned aircraft systems attack in Libya, Syria, and Armenia were not conducted against integrated air defense systems combining ground-based air defenses with fighters, early warning systems, and electronic warfare systems. To simplify this description to some extent, unmanned aircraft systems proved effective against stand-alone SAMs fighting in the open. It is hard to believe that this is going to be the most likely scenario in the future.

While there is no publicly available data regarding unmanned aircraft systems strikes against air defense's fighter force, the attacks against Khmeimim in Syria may offer some lessons about vulnerabilities of air defense fighters while on the ground. A non-state opponent without conventional manned air assets was able to disrupt airfield operations and cast doubt on the survivability of air assets outside reinforced shelters. With potential for follow-on strikes, such use of unmanned aircraft systems would effectively deny air defense to employ its fighters for at least a limited time. This in turn may be sufficient to create conditions for successful air and missile attacks against other targets. In a broader sense, unmanned aircraft systems attack against Russian airbases in Syria have emphasized the urgent need for improvements in the survivability of air defense systems in relation to both active and passive air defense.

5. Future challenges related to unmanned aircraft systems

The discussion on future challenges for air defense posed by unmanned aircraft systems needs to be seen within a broader context and not merely concentrate on its tools. Such unmanned aircraft systems will proliferate and become available to a growing number of both state and non-state actors. While unmanned combat aircraft systems and high altitude long endurance and medium altitude long endurance systems will most likely remain in state arsenals, smaller unmanned aircraft systems may be used increasingly frequently by both state and non-state actors. Such smaller systems offer the capability to attack beneath adversary air supremacy and allow for plausible deniability, which both are worrying trends for international peace and security. Small, unmanned aircraft systems may become a weapon of choice in proxy wars but may be more often used in local and regional interstate conflicts. Due to relatively low costs small, unmanned aircraft systems may facilitate the "democratization of technology," which means that leading militaries will not only take advantage of having them as a new capability but will have to see them as a ubiquitous threat to themselves.

Unmanned aircraft systems will pose a challenge to air defense as both strike and surveillance assets. They will provide precision strike capability in lieu of close air support, but at the same time, they may contribute to counter air operations and strategic air attack. Persistent surveillance capability offered by unmanned aircraft systems may shorten the so-called "kill-chain" and increase effectiveness of missile and artillery strikes (Cieślak, 2020). Limited unmanned aircraft systems strike may originate from inside of the adversary territory and even from vicinity of their intended targets, diminishing warning time, and denying traditional layered air defense concepts. Unmanned aircraft systems may conduct stand-alone attacks, but most likely they will be used by state actors as a part of saturation attacks, supporting more complex air and missile strikes. The number of possible targets that may be attacked with unmanned aircraft systems precludes the viability of permanent air defense

of all protected assets in peacetime, crisis, and war. It will have to be decided which assets need dedicated drone defense, and which may be left without it.

The affordability of small unmanned aircraft systems and advances in information technologies will increase the probability of swarming tactics combining kamikaze drones with traditional unmanned aircraft systems. Swarms of 'kamikaze' drones will increase the demands for the point or terminal air defense of protected assets. Recent developments suggest that one may see swarms of hundreds drones in near future in comparison with the current coordinated attacks of swarms of tens. The largest difference will lie in the emerging capability of swarms to conduct autonomous attacks and last-minute coordination (Zieliński, 2018a, b). As a result, future swarm attacks will pose a much greater challenge to air defenses compared to those mostly deconflicted ones as of now (Sprenger, 2019). The lessons learned in recent years suggest an increasing need for both hard and soft defenses, combining affordable kinetic defense with electronic warfare.

The future drone threat demands reactive and proactive developments in air defense systems. Although one may argue that drones caught air defense by surprise, this period has now ended. Air defense systems will remain largely relevant in countering the threat posed by high altitude long endurance and medium altitude long endurance unmanned aircraft systems. The most problematic threat will be posed by those smaller unmanned aircraft systems that are becoming ubiquitous and have become cheaper than most of air defense effectors. There is a widely recognized need for low-cost anti-drone systems, and they are starting to be fielded by several states and their militaries (Patterson, 2017). Most of those systems combine several surveillance techniques with electronic interference and kinetic defenses. So far, the available anti-drone systems are short and very short-range systems that may be exclusively used for point defense. Due to the drone threat, several militaries are rethinking the role of anti-aircraft artillery while some leading militaries opt for anti-drone lasers (IISS, 2019). There is no doubt that air defenses are getting more vulnerable to attacks by unmanned aircraft systems. Therefore, currently deployed air defense assets need better protection against drone attacks. For long and medium range surface to air missile systems, the static elements of air surveillance, control assets and airbases, and additional layers of terminal kinetic and electronic effectors are needed.

6. Conclusions

While recent years have witnessed spectacular examples of the effectiveness of attacks by unmanned aircraft systems, it may be argued that it is only a preview of what will occur in the nearest future. The proliferation of unmanned aircraft systems and the democratization of access to this capability means that drones may become a weapon of choice for a wide range of state and non-state actors. Defending against drone attacks has proved problematic as current air defenses are optimized for conventional manned air threats. Unmanned aircraft systems have been successfully employed in attacks against strategic targets, displaying their potential in suppression of enemy air defenses and in the handling battlefield targets. Swarming has started to become standard tactics of drone employment, which adds another layer of complexity to the process of defense against them. Unmanned aircraft systems have revealed the vulnerabilities of existing air defenses against drone attacks. Although recent conflicts have provided most of the examples of successful attacks against ground-based air defenses, unmanned aircraft systems may also attack airbases and air surveillance and control systems. This underpins the importance of the survivability of air defense systems

against this emerging threat and the potential role of unmanned aircraft systems in the counter air operations.

A large portion of current air defenses will remain relevant if the conventional threat of manned aircraft and missile attacks continue to exist in their current form. However, air defense systems will need additional surveillance assets and effectors dedicated to counter the threat of unmanned aircraft systems in nearest future. The affordability of anti-drone defense will be crucial as the costs of prospective small, unmanned aircraft systems will be quite low. With the growing potential to launch drone attacks from within a territory protected by air defense system, there is a need to reinforce point and terminal air defenses, which combine both hard and soft techniques to address the drone threat. The opening of the confrontation between unmanned aircraft systems and air defenses has seemed to favor the attacking side in recent decades. However, there is no doubt that air defenses will adapt to the situation, shifting the balance back to an equilibrium, getting more effective against drone attacks, and becoming less vulnerable to their attacks.

Declaration of interest - The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Cieślak, E. (2020). The Development of Poland's Air Defense System: The Operational Context. *Safety & Defense, 6(1), 1-10*. https://doi.org/10.37105/sd.44
2. Clancy, J. P. (2020, November 18). *Suicide drones – the threat from above in Nagorno-Karabakh conflict*. https://www.esjnews.com/suicide-drones-the-threat-from-above-in-the-nagorno-karabakh-conflict
3. Cordesman, A. H. (2019, September 2019). *The Strategic Implications of the Strikes on Saudi Arabia*. https://www.csis.org/analysis/strategic-implications-strikes-saudi-arabia
4. Defenceworld.net, (2020, July 2). *Libyan War Claimed 25 Large military Drones in 2020*. https://www.defenseworld.net/news/27332/Libyan_War_Claimed_25_Large_military_Drones_in_2020#.YEStJpozZPY
5. Flannelly J. (2020, December 7). *Drone Effectiveness Against Air Defenses, Not Tanks, Is the Real Concern*. https://www.thedefensepost.com/2020/12/07/drone-effectiveness-air-defense/
6. Frantzman S. J. (2019, September 26). Are air defense systems ready to confront drone swarms?. https://www.defensenews.com/global/mideast-africa/2019/09/26/are-air-defense-systems-ready-to-confront-drone-swarms/
7. Ho, B. (2020, May 14). Air Defence Challenges in the New Decade. *Asian Military Review, 2020, Issue 2*. https://asianmilitaryreview.com/2020/05/air-defence-challenges-in-the-new-decade/
8. International Institute for Strategic Studies (2019). *The Military Balance 2019, Bonus Military Balance 2019 content. Emerging air-defence challenges*. https://www.iiss.org/publications/the-military-balance/the-military-balance-2019/xmb2019-bonus-content

9. Joint Air Power Competence Centre (2020). A Comprehensive Approach to Countering Unmanned Aircraft Systems. https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf
10. Larter D.B. (2017, May, 16). *SOCOM commander: Armed ISIS drones were 2016's 'most daunting problem'*. https://www.defensenews.com/digital-show-dailies/socfic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/
11. Panel of Experts on Libya established pursuant to resolution 1973 (2019, December). *Letter dated 29 November 2019 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council. United Nations Security Council S/2019/914*. https://digitallibrary.un.org/record/3838591/files/S_2019_914-EN.pdf
12. Parachini J. V. (2020, July 2). Drone-Era Warfare Shows the Operational Limits of Air Defense Systems. https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html
13. Patterson, D. R. (2017). Defeating the Threat of Small Unmanned Aerial Systems. *Air & Space Power Journal,* Issue 2/2017, 15-25. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-2/2017_2_03_patterson_s_eng.pdf
14. Pyrgies, J. (2019). The UAVs threat to airport security: risk analysis and mitigation. *Journal of Airline and Airport Management, 9*(2), 63-96. doi: http://dx.doi.org/10.3926/jairm.12
15. Shaikh S., & Rumbaugh W. (2020, December, 8). *The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense*. https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense
16. Solodov, A., Williams, A.; Al Hanaei, S., & Goddard, B. (2018), Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities, *Security Journal*, pp. 305–324. https://doi.org/10.1057/s41284-017-0102-5
17. Sprenger S. (2019, October 22). *Europeans propose siccing self-learning drone swarms on air defences*. https://www.defensenews.com/global/europe/2019/10/22/europeans-propose-siccing-self-learning-drone-swarms-on-air-defenses/
18. United Nations Support Mission in Libya (2020, January, 15). *Report of the Secretary-General. United Nations Security Council S/2020/41*.
19. https://digitallibrary.un.org/record/3847369/files/S_2020_41-EN.pdf
20. Urcosta R. B. (2020, August, 31). *The Revolution in Drone Warfare. The Lessons from the Idlib De-Escalation Zone*. https://media.defense.gov/2020/Aug/31/2002487583/-1/-1/1/URCOSTA.PDF
21. Vick A. J., Zeigler S. M., Brackup J., & Meyers J.S. (2020). *Air Base Defense. Rethinking Army and Air Force Roles and Functions*. RAND.
22. Zieliński T. (2018a). Małe bezzałogowe systemy powietrzne w działaniach bojowych: zdolności, zagrożenia, przeciwdziałanie. In Dobija K., Maślanka S., Żyłka D. (Eds), *Wyzwania i rozwój obrony powietrznej Rzeczypospolitej Polskiej: obronność RP XXI wieku* (pp. 55-69). Wydawnictwo Akademii Sztuki Wojennej.
23. Zieliński, T. (2018b). Discussion about preemptive ban on lethal autonomous weapon systems. *Journal of Security and Sustainability Issues 7*(4): pp. 807-816. https://doi.org/10.9770/jssi.2018.7.4(1)

SAFETY&DEFENSE
ISSN 2450-551X

Lone Wolves as a Threat to Aviation Security: Typology, Tactics, Development Prospects

Elżbieta POSŁUSZNA

Military University of Aviation, Dęblin, Poland; e.posluszna@law.mil.pl,
ORCID: 0000-0001-8652-5729

DOI: https://doi.org/10.37105/sd.127

Abstract

This paper discusses the threats related to the development of the phenomenon known as lone wolf violence. Its main goal is to analyze lone wolves' activities, particularly their tactics in carrying out actions that pose a threat to aviation safety. The primary method used for the main argument of the paper, interdisciplinary modeling of the determinants of violence, allows for formulating forecasts on the development of lone wolves phenomenon in the most important context for those predictions, i.e., changeability of used means. This inventiveness comes down to disorganized forms of functioning (leaderless resistance) and the methods used in fighting, both of which stem from considerable power disproportions between lone wolves (terrorists) and states. The development of violence among lone wolves is analyzed from the perspective of this constantly changing tactical and technological means. This paper is of both explanatory and prognostic nature. It consists of five parts. The first is dedicated to providing theoretical background and depicting case studies that serve as a starting point for the following analyses. The second section is dedicated to a brief description of used methods. Next, the types of lone wolves' activities are characterized and examined. In section four, the current and potential tactics employed by terrorists are analyzed. This paper concludes with the author's prognosis regarding the future development of this phenomenon.

Keywords

aviation security, leaderless resistance, lone wolf violence, single issue terrorism

Submitted: 18.05.2021 Accepted: 24.05.2021 Published: 13.06.2021

1. Introduction and historical background

The aim of this article is to analyze the phenomenon referred to as "lone wolf violence" in the aspect of threats to air safety. This form of violence has always been a hazard, despite the fact that its real dimension (measured by the number of victims) can be described as very modest. Of course, there are arguments over data, which are not always properly collected and interpreted. However, the data is not the only indicator of risk. It should be remembered that the strength of the impact of terrorism (in particular lone wolf terrorism) is measured not only by the number of attacks and their greater or lesser lethality, but by the fear-based media interaction – a human reaction that translates into specific social behaviors (usually expected by terrorists) (Gill, 2015). The popularity of the lone wolf ideology was also contributed to by the far-right theorists (supremacists, anti-abortionists and supporters of racial divisions), such as: Joseph Tommasi, Luis Beam, William Luther Pierce, Tom Metzger and Alex Curtis (Kaplan, 1997), as well as many attacks on public institutions and large corporations.

Lone actors also do not shy away from the so-called air terrorism. An example of this can be the attack of the probably most famous lone actor, namely Theodore Kaczynski. The attack he carried out was the third in his terrorist career. It took place on November 15, 1979. The subject of the attack was an American Airlines passenger plane, and the tool was an explosive placed in an air shipment that Kaczynski sent from Chicago to Washington. The explosive charge with an installed altimeter exploded in a shipping container when the plane reached an altitude of 2,000 feet. As a result of the explosion, the pressure inside the aircraft dropped and the cabin filled with smoke. None of the passengers were badly hurt (only 12 people were hospitalized due to smoke inhalation), but the plane had to make an emergency landing. After this incident, the FBI nicknamed him Unabomber (based on the words "UNiversity", "Airlines", and BOMbings), and Kaczynski noted: "In some of my notes I have mentioned revenge against society. I planned to blow up a plane during flight. Unfortunately, the plane was not destroyed, the bomb was too weak" (Chase, 2003, p. 52). The Unabomber's motivation was based on the belief that the technological advances we are constantly experiencing have a negative impact on human life, which has become barren, apathetic, devoid of fulfillment and dignity. Continuing the technological progress will only worsen this situation, because "it will further humiliate man and will expose the natural world to greater degradation, possibly leading to further social destabilization and psychological suffering" (Kaczynski, 2003, p. 29). Man can return to the world of freedom. However, to do so, the technological system must be destroyed and be turned to what is counter-ideal for this system, namely wildlife.

Another interesting case of a lone actor conducting attacks on airlines was Muharem Kurbegović, born in 1943, also known as The Alphabet Bomber. This lonely Yugoslav engineer (working in the aviation industry) emigrated to the USA in 1967, where he planted an 11-pound bomb at the Pan American World Airways terminal at the Los Angeles International Airport on August 6, 1974. As a result of the explosion, three people died and eight were injured. Most likely, he was motivated by accusations of masturbating in the dance hall. Although found not guilty, the arrest made him unable to apply for the US citizenship. This led to frustration that turned into a personal vengeance against the judge and commissioners. There was also an ideological motivation. This was a demand for changes to immigration and naturalization laws in the United States, as well as lifting all restrictions relating to sex-

ual activity. He also called for the rejection of all forms of racism, nationalism, fascism, communism, or religion. He particularly condemned the United States Supreme Court for the criminal nature of his actions. His declared aim was also to "undermine the foundations of the Western civilization, which is the Scriptures". Although Kurbegovich did not belong to any organization and he did not have any external support, he claimed to be Isak Rasim, the military commander of the group ("Chief Military Officer of Aliens of America") he called Aliens of America. Two years after his arrest, police found 25 pounds of potassium cyanide and nitric acid in his apartment.

Is the activity of lone actor terrorists a real security threat? The figures on the number of attacks are not particularly frightening. The data collected between 1968 and 2010 in the 15 surveyed countries recorded only 88 lone actors who carried out 198 attacks - out of 11,235 attacks recorded in the Global Terrorism Database (Global Terrorism Database, 2021). These countries include the United Kingdom, Germany, France, Spain, Italy, Poland, Netherlands, Denmark, Sweden, Czech Republic, Portugal, Russia, Australia, Canada and the United States. As Ramon Spaaij wrote, this number of attacks represents only 1.8 percent of all attacks carried out in those years, indicating that lone actor attacks are rather marginal (Spaaij, 2012). The lethality of lone actor attacks is also not very impressive. A lone actor has an average death toll of 0.62 per incident. This number is even less impressive if it is compared with all the terrorist attacks in these 15 countries – the death rate in these 15 countries is 1.6 (Spaaij, 2012, p. 27). When it comes to ideological motivation, Spaaij assesses it as unknown in over 30% of cases. The remaining ones can be described as extreme-right – 17%, jihadist – 15%, anti-abortion – 8%, nationalist-separatist – 7% (Spaaij, 2012, pp. 29-31). According to Petter Nesser, those presented by Spaaij do not reflect the gravity of the threats, as the data covers only successful attacks. In fact, there are many more. And so, according to him, in Europe alone in the years 1995 – 2012, as many as 14% of all attack plots were prepared by lone actors (Nesser, 2012).

However, the impact of terrorism is measured not only by the number of attacks and their greater or lesser lethality, but by the fear-based interaction through the media – human fear that translates into specific social behaviors (usually expected by terrorists). The act behind which there is an organized group has a different "emotional rank" for the society than the act of a lone wolf. It probably happens as a result of the subconscious assumption that a group, as an entity composed of individuals with comparatively different personalities and with varying interests (despite strong ideological unification), is something rational to some extent, at least it is an environment where a certain, though sometimes an unstable "balance of interests" is worked out, which in turn must lead to toning down in terms of activities and goals. On the other hand, an individual (in the opinion of the potential addressees of a terrorist act) is a closed world. If they act on their own, without any hints and suggestions from other terrorists, they are influenced only by their own impulses. Since they are not subject to external orders and restrictions (resulting from the intersection of the interests of other members of the ideological community), and if they are not countered by other internal impulses (e.g. fear of the consequences of the act), their terrorist activity may take an extremely radical form. Such fears seem to have some justification in the mental reality of a lone actor.

2. Research methodology, research tools and procedures

The basis of the entire research process will be analysis and synthesis. Original source texts and all types of publications will be analyzed. The purpose of this analysis in relation

to the source texts is to extract the truth about a given document and to conclude on its basis and on the basis of the previously acquired knowledge what really happened and what phenomena accompanied the event. The use of synthesis is intended to go beyond the simple merging of the reconstructed fragments of the phenomenon studied in the research process in order to create a complete picture.

The radicalism of lone wolves is an extremely complex phenomenon and therefore the research perspectives cannot be homogeneous, but must complement and interpenetrate each other. For example, it is impossible to understand and thus properly grasp the political aspects of their activities without a thorough analysis of the ideological foundations of their activities, which in turn requires a closer look at the social and political changes. On the sociological level, the methods of media studies have been applied. All available source materials, as well as scientific studies (presented from an axiologically neutral point of view) were collected, ordered, categorized and criticized. At the political science level (especially with regard to organizational structures and action strategies), a decisive role is played by comparative analysis, concerning both classic hierarchical organizations (comparing individual organizations and their types) and new types of organizations (based on the idea of network warfare and leaderless resistance).

3. Types of activities

Lone wolves are not monolithic, neither ideologically nor strategically. Although definitions are always of foundationalist nature, their shape is undoubtedly connected to some extent with the social habit of classifying items into a given group or groups. In the methodology of sciences, a practice of this kind is referred to as an empirical generalization. The researchers of the phenomenon of lone wolves do not deviate from this pattern, distinguishing several different types of these.

Thus, Raffaello Pantucci distinguishes three categories in his typology: loner, lone wolf, and lone wolf pack (Pantucci, 2011). "Loner" is an individual who carries out terrorist attacks without having virtual or real connections with other extremists. However, they can draw inspiration from foreign sources for their deeds. According to Pantucci, there are few individuals that fit into this standard. These exceptions include, for example, Roshonara Choundhry, who, apart from the passive "consumption of materials" on the Internet (these were mainly lectures by the radical Islamic clergyman, the leader of Al-Qaeda in the Arabian Peninsula, Anwar al-Awlaki) most likely had no contact with other extremists. According to Pantucci, a "lone wolf" is someone who, while committing terrorist acts without anyone's command, maintains certain contact with other extremists. The contact may be carried out both online and in person. An example of such a lone wolf is Nidal Malik Hasan, who, a year before the attack on Fort Hood, Texas, contacted the aforementioned Anwar al-Awlaki by e-mail. In January 2009, al-Awlaki published an essay entitled *44 Ways to Support Jihad*, which is a collection of tips for the proponents of the jihad movement. Contrary to the name "lone wolf", Raffaello Pantucci suggests it is also to attribute the activity of lone wolves not only to individuals, but also to isolated couples and even groups. In his typology, in addition to the category of the loner or the lonely wolf, he also distinguishes a group of lone wolves, defined as an autonomous unit that, acting on its own and using extremist ideology as its justification, tries to commit terrorist acts. Such a group, as Pantucci puts it, "may or may not have ties with acting terrorists, but presents a lack of subordination in terms of control and orders", and "just like lone actors it activates itself and sets tasks" (Pantucci, 2011, p. 19). An example of such a group can be the brothers Tamerlan and Dzhokhar Tsarnaev.

A different categorization is given by Jeffrey D. Simon in his book *Lone Wolf Terrorism. Understanding the Growing Threats*. Taking into account the criterion of the source and nature of the motivation, he distinguished five categories of lone wolves. These are secular lone wolf, religious lone wolf, single-issue lone wolf, criminal lone wolf, and idiosyncratic lone wolf. I will try to briefly characterize these categories (Simon, 2013). A secular lone wolf is an individual who carries out violent attacks, driven by political, ethnic-nationalist or separatist motivations. This category includes Simon Timothy McVeigh and Andreas Breivik. The second type is a religious lone wolf. They perform acts motivated by a specific religious doctrine – whether it be Islam, Christianity, Judaism, Buddhism or any other metaphysically rooted philosophy of life. Simon also includes American white supremacists or neo-Nazis in this group, because many of them are supporters of the Christian Identity Movement (or are inspired by this religious view of the world), whose anti-Semitic and racist ideology justifies their violence. This category includes: Nidal Malik Hasan and James von Brunn. The third type is "single-issue lone wolf". They do not pursue broad socio-political changes, but rather deal with certain specific matters. Simon lists radical anti-abortionists, animal defenders, and environmentalists within this type of lone wolf. Eric Rudolf and Volkert van der Graaf are representatives of this category. Another type of lone wolves Simon identifies as "criminal". This type of lone wolf is mainly motivated by the desire of profit. According to Jeffrey Simon, John Gilbert Graham and Panos Koupparis are the representatives of this category. The fifth and the last type of lone wolves – in Simon's nomenclature called "idiosyncratic" wolves, motivated primarily by their own mental problems. Their very expression is irrational. Usually they are diagnosed with paranoid schizophrenia. According to Simon, Theodore Kaczynski and Muharem Kurbegovic belong to this category.

Another classification is presented by Khaled A. Beydoun in the article *Lone Wolf Terrorism: Types, Stripes, and Double Standards*, in which he distinguishes: lone soldiers, lone vanguards, loners, lone followers, and lone killers (Beydoun, 2018). "Lone soldiers" are those who formally belong to a given terrorist organization, accept their ideology, but commit violent acts on their own, albeit with the consent and support of this organization. A typical representative of this category would be Mark Stroman, who in 2001 killed three men (who he considered Muslims) in Dallas, Texas in retaliation for the September 9, 2001 attack. Stroman was closely associated with the Aryan Brotherhood and carried out the assassination with the approval and support of that organization. Another example of a lone soldier given by Beydoun is Syed Rizwan Farook who, together with his wife Tashfeen Malik, shot 14 people and injured another 21. "Lone vanguards" are people who willfully decide to act independently. They can, of course, be externally inspired in terms of ideology to some extent (stimulated by various currents of thought), but the entire ideological message that is the source of violent actions is their own original creation. This category includes Andreas Breivik who, although loosely inspired by various supremacist and nativist groups, based his actions on his own ideological construct. "Loners", just like "lone vanguards", operate independently and under the influence of their own ideology, which is more or less their own ideological construct. Unlike the latter, however, their solitary action is not a conscious choice, but results from social rejection. According to Khaled Beydoun, Theodore Kaczynski (Unabomber) is an example of a "loner", whose terrorist activity for Beydoun was the result of social alienation, and not a consequence of a chosen strategy or ideology. "Lone followers" are those who wish to act as members of a given grouping, but due to their lack of competence, cannot formally become a part of it. However, they fit into the ideological profile of a given grouping, hoping that they will become its rank and file members. One of the lone followers is Dylan Roof, who, motivated by racist ideology, killed 9 African Americans in 2015. As Beydoun suggests, the perpetrator's manifesto shows the ideological influences of the radical organization called Council of Conservative Citizens, which he did not aspire to "due to lack of competence". "Lone killers" is the last of the proposed categories. According

to Beydoun this group includes killers (usually mass killers) who have not been recognized by law enforcement as terrorists. It is also difficult to attribute greed as the main motive for their criminal activity. Beydoun does not provide examples to illustrate this type of lone wolves, but he would most likely be inclined to include those who have committed the so-called hate crimes, such as the perpetrators of school massacres.

Of course, the basis of any definition is the terminological decision of the author who defines the term in the way they deem valid. However, in my opinion, too much conceptual blur, which occurs when a phenomenon is defined too broadly, is bad for scientific pragmatics. Such imprecision prevents us from distinguishing the specific features of the phenomenon in question, and, consequently, to efficiently use the given term. I mean, for example, Pantucci's typology, which extended the category of lone wolves to include groups as well, which in my opinion leads to a lot of confusion, especially if we allow, as Pantucci himself does, that these groups may have had "ties to acting terrorists". The only restriction made by Pantucci is that there should be no "subordination in terms of control and orders" between lone wolves (a group of lone wolves) and some organization, which is not a particularly significant restriction here, as the concept of "organization" today does not mean a hierarchical structure, but a decentralized movement. There is also no reason why this "group of lone wolves" should not be treated simply as a small organization.

Jeffrey Simon's typology also raises methodological doubts in my opinion. I mean the "idiosyncratic" type, which, according to him, is primarily motivated by one's "own mental problems". To my mind, there is no practical application for this category, because it is impossible to simply determine the exact motivation of each perpetrator. Simon himself does not make it easier, including Andreas Breivik in the secular lone wolf category, and categorizing Theodore Kaczynski as an idiosyncratic lone wolf. Against this background, distinguishing the category of criminal lone wolves seems slightly more understandable (the source of motivation in this case is easier to verify), but it is not known whether this category can be considered cognitively interesting. If we consider the desire to obtain material goods as the source of terrorists' motivation, we should consider each criminal working on their own as a lone wolf. I am not sure whether this is the conclusion the researcher aimed to reach.

I have considerable doubts about Khaled Beydoun's typology, in particular with regard to the "lone soldiers" he has distinguished, who supposedly formally belong to a given terrorist organization and accept their ideology, but carry out violent acts on their own, albeit with the consent and support of the organization. Here, in my opinion, the "conceptual blur" is evident. It is not entirely clear to me why these individuals should not be considered members of the organization. It is also not known how, in accordance with this typology, the verification of "independence" in the field of activities can be carried out. In short, in this case excessive "conceptual subtlety" leads to conceptual blur.

4. Tactics

Lone actors' activity is usually viewed as the progressive stage (and sometimes even the highest stage) of leaderless resistance. It is a tactic, the basis of which is to give up all (especially hierarchical) organizational structures and replace them with a decentralized structure, based on a common ideology and common goals that result from it.

The sources of the lone wolf concept can be found, as specified before, in the concept of "leaderless resistance", whose foundations can be found in the ideas of two political activists – the founder of the International Service of Information, Colonel Ulius Louis Amoss and

the radical activist of the American Right, Louis Beam. This strategy assumes abandoning any hierarchical organizational structures that would be replaced by a loose configuration of small, autonomous cells that are not managed by any central unit. These cells act independently, following their own tactics and strategy, not agreed with other individuals or groups (Posluszna & Mares, 2016).

Leaderless resistance has many advantages. First of all, organizations based on this model are actually not exposed to police surveillance at all. In a pyramidal structure, a potential agent, even if they manage to penetrate to a certain level of the hierarchical pyramid, they can easily destroy all levels below their own level, as well as threaten the levels above. The danger of infiltration is much smaller for "organizations" in which individual actors or small groups not only do not have any organizational hub, but also operate without any structural connection with each other. In organizations of this type, the basic unifying element becomes the ideology from which members of the movement will learn about the appropriate methods of fighting. This ideology has had its vital source since the beginning of the 1990's. This source is the Internet.

On the Internet, network connections can take many different shapes (Arquilla & Ronfeldt, 2001). They can take the form of chains ("chain network", "line network"). In such a case, the communication between individual links (information exchange) will run along the lines of links connected only by neighboring elements. Another type is a nodal network ("star network", "hub network", "wheel network"). Here, the communication between centers and the coordination of activities depends on the central element, which is an intermediary node that acts as a transmitter of information and goods. Another type of network is the omnichannel network ("all-channel network", "full-matrix network"). In an omnichannel network, all centers are connected with each other. There are no distinguished nodes and the communication between the selected elements in the network can take place independently from any other connection.

Regardless of the kind of the intra-organizational operation model of we consider, whether it is the one based on the model of "leaderless resistance" or the one based on the model of the omnichannel network, the problem of internal communication between all activists of the movement deserves attention in this context. Here, the central place (though probably not the only one) is occupied by websites. These sites are in fact intermediary nodes in the exchange of information, and at the same time centers of ideological influence. Activists operating under the banner of the given organization provide information about their activity by means of anonymous, often encrypted messages, which are then placed on websites. These websites also provide detailed instructions on security rules and data encrypting methods. A particularly rich set of tips can be found on the ELF website (The Nord American Earth Liberation Front Press Office, 2009). The website owners usually deny that they have anything to do with leading or encouraging direct action, claiming that they are merely advocating freedom of expression, freedom of information, and the public good (No Compromise, 2009).

5. Conclusion

Will the future bring a dynamic development of the activity of "lone wolves"? It seems that such a scenario is highly probable for at least two reasons. The first is the emergence (and continuous development) of new information and communication technologies allowing for relatively unrestricted and to a large extent anonymous information exchange. The Internet, of course, plays a special role among these technologies. As Southern Poverty Law

Center analyst Mark Potok correctly points out, “The Internet is an important part of a leaderless resistance strategy. It allows lone wolves to obtain up-to-date information on events, to follow changes in ideology, and to discuss tactics – all this influences the choice of the target of an attack. To a much larger extent than printed publications, the Internet allows lone wolves to be part of a wide movement, even though they do not attend meetings, subscribe to any mailing list, and generally try to remain invisible” (Levin, 2002, p. 965). I do not think it is a matter of coincidence that a significant increase in the number of terrorist actions involving lone actors took place in the 1990s, i.e. at a time when the Internet began to develop dynamically. Another likely reason for the future dynamic development of activities based on the lone wolf strategy is their positive evaluation in the so-called "terrorist movement". For many ideological radicals, undertaking independent activity (both legal and illegal) is a testimony to the highest commitment an individual can make. It is no wonder that radical literature is full of calls to "not look at others" and to take action on your own. Such action, according to many, is not only "something extremely noble", but also relatively safe (mainly due to the difficulty of surveillance). Also in the "Declaration of War", considered one of the most radical texts referring to the “single issue” model, an incentive for this type of action can be found. The term "single issue" refers to the terrorism of one issue, which is usually defined as an individual or group activity based on violence, the purpose of which is not so much to induce deeper (revolutionary) social or political changes, but to solve one problem ("settling" one specific issue) (Posluszna, 2016). "Declaration of War": "We must remember that this is the time of war. Each of us is a potential enemy. Moving on, we must work alone or in the company of a trusted person. However, when choosing your comrades, remember that people do not always remain faithful to each other. Liberators do not have a leader, because their organization does not create any structures. We are independent people who feel responsible for our family" (Wyjący Wilk, 1998, p. 71).

It is difficult to imagine the law enforcement bodies to be able to effectively prevent actions of an individual nature, especially when their perpetrators do not inform about their intentions in advance, and do not send any forecasting signals. When such individuals decide to launch an attack that threatens air safety, the consequences must necessarily be dire. These difficulties are also exacerbated by the fact that these are usually highly fanatical individuals who resort to the "lone wolf" strategies and they do not withdraw due to failures or due to lack of support from other participants of the movement. It happens that such people create an all-channel virtual network in the area of information flow or they settle for a star network or a multi-node network. In the former case, there is a certain chance that their activity in the network will be tracked and recognized, in the latter (much more frequent) such possibility does not exist in practice. Then, their capture only becomes a matter of chance.

Declaration of interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Arquilla, J., & Ronfeldt, D. (2001). The Advent of Netwar (Revised). In: J. Arquilla, and D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation, 1-29.
2. Beydoun, K. A. (2018). *Lone Wolf Terrorism: Types, Stripes, and Double Standards*. 112 (5), 1213-1244, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1333&context=nulr
3. Chase, A. (2003). *Harvard and the Unabomber. The Education of an American Terrorist*. Norton&Company, https://doi.org/10.1007/s12129-003-1067-x
4. Gill, P. (2015). Lone-Actor Terrorists: A Behavioural Analysis. Routledge.
5. Global Terrorism Database, A Department of Homeland Security Emeritus Center of Excellence led by the University of Maryland, https://www.start.umd.edu/research-projects/global-terrorism-database-gtd
6. Kaczynski, T. (2003). *Społeczeństwo przemysłowe i jego przyszłość. Manifest Wojownika*. Wydawnictwo Inny Świat.
7. Kaplan, J. (1997). "Leaderless Resistance", *Terrorism and Political Violence*, 9 (3), 80-95, https://doi.org/10.1080/09546559708427417
8. Levin B. (2002), "Cyberhate. A Legal and Historical Analysis of Extremists' Use of Computer Networks in America", *American Behavioral Scientist*, 45 (6), 958-988, https://doi.org/10.1177/0002764202045006004
9. Nesser, P. (2012) Research Note: Single Actor Terrorism: Scope, Characteristics and Explanation. *Perspectives on Terrorism,* 6(6), 61-73.
10. No Compromise, (4 January 2009), "Disclaimer", http://www.nocompromise.org/index.html
11. Pantucci, R. (2011 March). *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorist*. International Centre for the Study of Radicalization and Political Violence – ICSR, 1-40. https://icsr.info/wp-content/uploads/2011/04/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf
12. Posłuszna, E. (2015). Environmental and Animal Rights: Extremism, Terrorism, And National Security, Amsterdam: Elsevier.
13. Posłuszna, E., & Mares, M. (2016). Environmental-extremist and Animal Rights Single Issue Perpetrators. In M. Fredholm (Ed.), Understanding Lone Wolf Terrorism. Past Experience, Future Outlook, and Response Strategies, 77 (pp. 87-106). Routledge.
14. Potok, M. (2002). Statement of September 6, 2001. In B. Levin, Cyberhate. A Legal and Historical Analysis of Extremists' Use of Computer Networks in America. *American Behavioral Scientist*, 45(6), 958-988 .
15. Simon, J. D. (2013). *Lone Wolf Terrorism. Understanding the Growing Threats*. Prometheus Books.
16. Spaaij, R. (2012). *Understanding Lone Wolf Terrorism. Global Patterns, Motivation and Prevention*. Springer, https://link.springer.com/book/10.1007%2F978-94-007-2981-0
17. The Nord American Earth Liberation Front Press Office, "Security", http://www.elfpressoffice.org/security.html
18. Wyjący Wilk. (1998). *Deklaracja wojny*. Bleeding Earth.

SAFETY&DEFENSE
ISSN 2450-551X

Security of the 2014 Winter Olympics in Sochi

Adam RADOMYSKI

Military University of Aviation, Deblin, Poland; a.radomyski@law.mil.pl,
ORCID: 0000-0001-7522-308X

DOI: https://doi.org/10.37105/sd.117

Abstract

Given the fact that major sporting events such as the Olympic Games attract attention all over the world, the aspect of their security has become even more important, especially after the terrorist attacks of September 11, 2001. Organizers of this type of mass sports event treat the issue of safety as top priority.
The paper examines the empirical data from scientific publications, press releases and formal government documents that pertain to Russia's preparation to properly secure the 2014 Sochi Winter Olympics in terms of security.
The aim of this article was to identify the threats to the Winter Olympics in Sochi and to characterize the security system organized by Russia against this background.
The conducted research confirmed that the greatest threat in Russia was the high activity of national liberation groups, fighters and terrorists from the Sochi area, which clearly intensified in the period preceding the Olympics. In addition, the security system created by Russia involved many different state bodies, including agencies, police and law enforcement services, and the army.
Based on the research, it can be concluded that the security system created in Sochi may be a good example for other countries that will try to organize the Olympic Games in the future.

Keywords

air defense system, air safety, restricted areas, security system, terrorist attack

Submitted: 15.04.2021 Accepted: 03.06.2021 Published: 13.06.2021

Introduction

Terrorism is a systematically recurring phenomenon that generates threats of various scale, form and scope. In this regard, the global reach that accompanies sporting events such as the Olympic Games makes them attractive to terrorists. By carrying out attacks during the Olympic Games, they can ensure a wide publicity and disturb the sense of security among the international community. Analyzing various aspects of terrorist attacks in relation to this type of mass sporting events, it can be noticed that the potential perpetrators commit these acts not because they have any particular claims against the Olympic movement, but because of its powerful symbolism – associated with the peaceful dimension of this type of sporting events. In addition, terrorist attacks are sometimes also part of a campaign against an enemy, e.g. the government of the state or its representatives participating in the Olympic Games (Silke**,** 2010). At this point, it should also be noted that terrorist threats at the Olympic Games have their tragic history, which have been outlined, among others, by the events of 1972 in Munich, where extremists from the Black September organization killed five Israeli athletes and six coaches, and a German policeman. This tragic event became a specific impulse to intensify the counter-terrorism activities in the world, also during subsequent mass sports events such as the Olympics. Security gained even greater importance after the terrorist attacks of September 11, 2001 in the United States (Spaaij, 2016). This made the Olympic Games a serious challenge for the host countries. One of the researchers of terrorism, Ronald Crelinsten, refers to the issues related to the safety of the Olympic Games, and considers terrorism to be a new form of war, in which all far-reaching means should be used. In practice, this way of thinking translates into a systematic increase in security costs (Boyle, 2012). This is also confirmed by the words of a security expert Neil Fergus, who, in relation to the 2004 Summer Olympics in Athens, stated that it was "the largest security operation since the time of Alexander the Great marching through Persia" (Fergus, 2010). Concerning the 2008 Beijing Olympics, a political scientist Ying Yu described it as "the largest peace security operation in the history of the country" (Yu et al., 2009, p. 390). A dozen or so years ago, sociologists John Horne and Wolfram Manzenreiter also commented on this issue, and predicted that security issues "are likely to be of the utmost importance during the organization of the subsequent great sports events" (Horne & Manzenreiter, 2006, p. 19). Bearing in mind the above opinions, one should not be surprised that ensuring safety at the 2014 Winter Olympics in Sochi has become a priority for the Russian authorities.

Taking into account the problem situation outlined, it was assumed that the aim of the article will be: *to identify the threats to the Winter Olympics in Sochi and, against this background, to characterize the security system organized by Russia*. It has been assumed that this goal will be achieved as a result of theoretical research. In order to obtain the most reliable information about the subject of the research, a critical analysis of factual documents was carried out, mainly reports on the preparation and conduct of international sports events. In addition, scientific publications and documents relating to the threats of mass sports events, the organizational measures used by Russia and the technical solutions implemented into the security system of the Olympics in Sochi were also included in the analysis. Comparisons and analogies with the organizers of the Olympic Games before 2014 were also used.

2. An assessment of the threats to the Sochi Winter Olympics

The security concerns were fully justified as they had their historical background. The time of two wars in Chechnya in 1994–1996 and 1999–2003 was a period of particularly intensified violence in this region. Despite their termination, various types of local military operations continued throughout the North Caucasus. The Krasnoyarsk Krai, in which Sochi is located, was not a battlefield during the years of the wars in Chechnya, but it fell victim to several terrorist attacks. According to the US warnings issued on January 24, 2014 to travelers from the United States to Sochi, there were reports of terrorist acts that had taken place in this region over the past 15 years. Most commonly terrorist attacks targeted Russian government buildings, airfields, hotels, tourist spots, markets, entertainment venues, schools and housing facilities. There have also been large-scale attacks on public transport, including the underground, buses, trains and regular commercial flights.

Russian experts themselves confirmed that in the North Caucasus there are about 500-1000 terrorists operating mainly in small groups of several dozen people, which were associated with the Chechen terrorist Doku Umarov, the head of the self-appointed group, the Caucasus Emirate (Radomyski et al., 2012).

Despite these difficulties, it should be emphasized that the Russian security forces managed to frustrate terrorists' plans to attack the Black Sea resort of Sochi. However, concerns over terrorism during the Olympic Games intensified in July 2013. This was related to the call for attacks on civilian targets across Russia, announced online by Umarov himself. The leader of the Caucasus Emirate called on his supporters to make attacks during the Winter Olympics in Sochi. In a four-minute video posted on an independent website kavkazcenter.com, Umarov called on all Muslims and his followers to use any methods, including brutal ones. On May 10, 2012, the Russian National Antiterrorism Committee announced that the Russian and Abkhazian security agents had confirmed that Umarov indeed planned large-scale attacks during the Winter Olympics in Sochi. This was evidenced, among others, by the hiding places with a large number of grenade launchers, surface-to-air missiles, mines and other weapons discovered in Abkhazia (a detached region of Georgia bordering with the north of the Caucasus and declared independent by Russia) (Lovelace, 2017). These actions, however, sparked off terrorist activities. On October 21, 2013, a suicide bomber blew up a bus in Volgograd in the Southern Federal District, which includes Sochi. It was the first bomb attack since the attack at Moscow's Domodedovo Airport in January 2011. On December 27, 2013, as a result of a car bomb explosion in front of the police building in Pyatigorsk, Stavropol Krai, the administrative center of the North Caucasian Federal District, three people died. Following this attack, six alleged terrorists were arrested in Kabardino-Balkaria. On December 29-30, 2013, two suicide bombings took place in Volgograd, the first at a railway station and the second in a trolleybus. As a result, over thirty people died and over 100 were seriously injured. On January 12, 2014, a Fatwa justifying the attacks in Volgograd was published on a website related to the Caucasus Emirate. Quoting Osama bin Laden, the Fatwa argued that such attacks were "necessary" as they "enraged the infidels" who were responsible for the deaths of Muslims in the North Caucasus and Syria (related to Russia's support for the Syrian government) (Lovelace, 2017, p. 71).

Bearing in mind the real threats, several analysts outlined different scenarios of the possible terrorist incidents before and during the Games, including attacks on the Olympic venues or attacks elsewhere in Russia. They were to consist of taking hostages, carrying out suicide attacks and other bombings or armed violence. In addition, they warned that the attacks could also be targeted at Russian embassies abroad and even at the embassies of other countries' sending athletes to the Olympics in Sochi.

3. Characteristics of the security system of the Winter Olympic Games in Sochi

After Russia was granted the right to host the Olympic Games in Sochi, many domestic and foreign analysts and media outlets drew attention to the high cost of the Olympics and the potential organizational problems and security threats. Particular attention was paid to the very high costs of building the Olympic venues and the entire infrastructure, often recalling the total cost of the preceding Summer Olympics (a much larger event than the Winter Olympics) and all previous Winter Olympics. This is also confirmed by the data in Table 1 (Müller, 2014, pp. 628–655).

Table 1.

Tabulation of resources spent for the organization of the Olympic Games

Year	Host city	Budget
1996	Atlanta	USD 3.6 billion
2000	Sydney	USD 6.9 billion
2002	Salt Lake City	USD 2.5 billion
2004	Athens	USD 16.0 billion
2006	Turin	USD 4.5 billion
2008	Beijing	USD 45.0 billion
2010	Vancouver	USD 7.6 billion
2012	London	USD 18.0 billion
2014	Sochi	USD 51.0 billion

Adapted from: *The Economics of Hosting the Olympic Games* by J. McBride Council on Foreign Relations Copyright 2018 January 19 by Publisher; *Security Requirements at the Olympic Games, by* V. Šiljak, V. Vukašinović, D. Đurović, Copyright 2016 by Publisher.

It has been confirmed by hard financial data that show that the budget proposed by Russia as part of the offer has been significantly exceeded. The budget initially planned for 2007 was USD 12 billion (RUB 314 billion). By 2010, this figure had risen to about RUB 950 billion, about USD 30.6 billion, and official estimates for 2013 were USD 51 billion (Dean, 2014, p. 5).

Despite the rising costs for the Russian authorities, the safety of the participants of the Olympics was a matter of the utmost importance. Pursuant to the Act of December 2007 and the Presidential Decree of August 2013, a special safety zone was created around the Olympic venues. Additional controls and other restrictions were introduced for people and vehicles entering and leaving this zone. From January 7, 2014, a special security regime was introduced in Sochi (Nichol et. al. 2014). It provided for the introduction of increased security measures during the Winter Olympics, including the establishment of a restricted zone. Apart from that, the Ministry of the Interior of the Russian Federation has created an unprecedented security cordon around the venues for sports competitions. The boundaries of the area were defined in detail: part of its territory lay on the Karachay-Cherkessia border and it extended to the Russian border with Abkhazia. Security measures were also increased in the area that encompassed some 100 km of the coast in the Sochi region and extended deep into the city to a depth of 20-40 km (Luccacioni & Cohen, 2014). It also included a ski resort in Krasnaya Polyana, opened before the Olympics, located 39 km from Sochi. Starting in January 2014, a more stringent air traffic safety control system has been introduced. Shipments and luggage have also been subject to detailed control. In addition to the Olympic venues, controlling bridges, railway tunnels, power grid facilities, schools, hospitals, hotels, restaurants and shops have also been reinforced. What is more, the sale of firearms, dual-

use chemicals and other prohibited items has been banned. A restriction on the entry of vehicles into the security area has also been adopted. Only vehicles with special license plates were authorized to enter. Local car owners had to leave their cars in parking lots that were located 50 miles from Sochi. Even more rigorous security measures applied to checks on Olympic visitors and support staff at Olympic venues. A decision was also made to introduce a "forbidden zone" on the border with Abkhazia. Restrictions also applied to the air space and water in the vicinity of the Olympic Games and national parks. In total, the safety zones extended approximately 60 miles along the Black Sea coast and up to 24 miles on land (Figure 1). In addition, on March 21, restrictions on the entry, permanent or temporary stay of visitors came into force under a special regime.

Figure 1. The Sochi Area. Adopted from: *The 2014 Sochi Winter Olympics: Security and Human Rights Issues, Report*, Congressional Research Service by J. Nichol, E. Halchin, J. W. Rollins, A. Tiersky, S. Woehrel. Copyright 2014 by Publisher.

Starting on February 4, 2014, ships from the Russian fleet were on duty at the seaside of Sochi. These forces included a group of small tactical submarines "Aleksandrovets" and "Muromets" (the best ship of the Black Sea fleet in 2013). They were prepared to combat submarines, surface ships and carry out air defense tasks. The naval forces also included the tactical minesweepers "Kovrovets" and "Turbinist". The naval force was complemented by the missile cruiser and patrol ships "Pytliviy", which departed from the naval base from Sevastopol. Their task was to protect sea waters and air space in the area of the Olympic Games 2014. Other fleet units were also ready to go to sea.

The security system described above was in force during the Games in Sochi, which took place from February 7 to 23, and during the Paralympic Games, which were held from March 7 to 16. An important stage in the preparation of the military forces to protect sports facilities in Sochi was the Kavkaz-2012 exercise, which ended in southern Russia in the second half of September. It was a kind of war game aimed at ensuring internal security. The maneuvers were carried out taking into account the volatility of the situation in the North Caucasus during the Winter Olympics in Sochi. The exercises took place from September 17 to 23 and

covered a large theater of operations that enclosed a large part of the area of responsibility of the Russian joint strategic command "South", which corresponds to an area of operation extending from the Black Sea in the west to the Caspian Sea in the east. The exercise was carried out in November 2013, and 7,000 soldiers, officers of the Ministry of the Interior and the Federal Security Service participated in it.

In order to coordinate the activities of the forces responsible for the security of Sochi, an inter-agency operational center was created, which also included the Federal Security Service, as the leading agency, and the Ministry of the Interior, the Ministry of Defense and other bodies. According to official reports, the size of the security forces was estimated differently, from several tens of thousands to even 100,000 people. Around 22,000 soldiers, 2,000 military vehicles, 72 planes, 40,000 police officers and 8,900 medical workers with 1,600 vehicles were involved in securing the Olympic Games in Sochi. These forces were supported by uncertain number of Federal Security Service functionaries. According to some estimates, the number of the Russian security personnel deployed to the Games was significantly greater than that of the 2012 London Summer Olympics.

International cooperation was an important element from the point of view of security. In November 2013, a Russian general Oleg Syromolotov, the head of the operational command, announced that representatives of intelligence services from several dozen countries were invited to help, and they were to send their national delegates to Sochi. He also pointed out that this type of cooperation had been being prepared since 2011, when the Operations Center initiated the creation of a group of experts that met several times in Sochi. The cooperation included exercises at sports facilities in Sochi. In addition, President Putin announced in early September 2013 that Russia had concluded agreements with the United States and several European countries on cooperation in the field of security at the Sochi Olympics (Interview to Russian and Foreign Media, 2014). In order to discuss the military cooperation and resolve the most important issues related to ensuring the security of the American delegation, on January 21, 2014, General Martin Dempsey, the Chairman of the Joint Chiefs of Staff, and the Chief of the Russian General Staff, General Valery Gerasimov, met in Brussels (Garamone, 2014). The US Department of Defense announced that General Gerasimov had confirmed that the armed forces would support the Olympic Games by providing air and sea defense, defense against chemical and biological weapons, as well as providing medical support and electronic protection. The Department of Defense also said Gerasimov had expressed an interest in the US technology of counteracting improvised explosives (IED). In addition, according to the information provided by the Press Secretary of the Department of Defense John Kirby, General Philip Breedlove, the commander of the European command of the US forces, was to be responsible for preparing an emergency military operation in the event that the State Department needed US military forces to support Russia during the Olympic Games in Sochi (US Department of Defense, 2014). Two US Navy ships were also directed to the Black Sea region. Apparently, some American planes stationed at military bases in Germany were also ready to carry out a possible evacuation of the members of the American delegation from Sochi (U.S. Department of Defense, 2014). Private companies were also involved in the protection of the American athletes in Sochi, e.g. Global Rescue (Global Rescue, 2013), whose employees protected members of the U.S. Ski & Snowboard Association (USSA) during the Games in Turin, Italy (2006) and Vancouver, Canada (2010).

The large-scale US action was principally due to both the safety of the athletes and other US citizens who were to take part in the Sochi Winter Olympics. These fears were also expressed by conducted surveys. They indicated that more than half of the American population were unsure that Sochi would be safe from terrorist attacks, but most people still wanted the United States to participate in it. A recent Economist/YouGov poll showed that most

Americans were unsure that the Olympics in Russia would be well protected against terrorism (see Figure 2).

Figure 2. The results of a survey presenting Americans' opinions on the threat of terrorism during the Winter Olympics in Sochi. Adopted from: More than half of Americans have little to no confidence that Sochi will be safe from terrorist attacks, but most people still want the US to participate by K. Frankovic, Copyright 2014 by Publisher.

To sum up, all activities related to ensuring safety and security during the Olympic Games in Sochi were implemented in accordance with the concept approved by the President of the Russian Federation in 2009. The concept defined the main goals, tasks, the scope of activities and measures that were necessary to ensure safety and security at the Olympic and Paralympic Games. The main threats include (Demidov, 2015): the possibility of seizing (hijacking) civil aircraft flying on domestic and international routes, both in the air and on the ground. They were considered means that could be used to launch attacks on the Olympic venues. This group of measures also includes small and ultra-light aircrafts, and radio-controlled models (Radomyski & Bernat, 2018).

4. Securing the airspace over Sochi

Bearing in mind the forecasted threat, it is hardly surprising that the airspace safety was one of the most important areas for the Russian authorities during the organization of the 2014 Winter Olympics in Sochi. This was also clearly demonstrated by the words of General Viktor Gumenny, the commander of the air defense forces of the Russian air force, spoken during one of the press conferences: “We will do anything possible to perform the task of protecting the Russian airspace along the southern borders and ensuring safety during the Winter Olympics” (Demidov, 2015).

With regard to the identified threats, it was decided that the forces and means of air defense will be the pillar of the airspace security system. Their use was to prevent unauthorized entry into the Olympic area airspace by unidentified aircraft (Radomyski, 2019). Therefore, all facilities in the Sochi region (the seaport, the Adler airport, the Olympic venues and the Olympic Village in the Lower Imereti Plain). Krasnaya Polyana was also to be protected, as

well as the roads between the individual amenities. After analyzing the location of these places, two groups of them were distinguished, which were concentrated in two clusters (coastal and mountain), as shown in Figure 3.

Figure 3. Facilities under special protection during the Olympic Games in Sochi. The 2014 Sochi Winter Olympics: Security and Human Rights Issues, Report, Adopted from: Congressional Research Service by J. Nichol, E. Halchin, J. W. Rollins, A. Tiersky, S. Woehrel, Copyright 2015 by Publisher.

The first of them included the Olympic venues that were located on the Black Sea coast in the immediate vicinity of the state border of the Russian Federation with the Republic of Abkhazia. The sports facilities and the Olympic Village were considered as one facility (Figure 4).

Figure. 4. Facilities included in the coastal cluster. Adopted from: Sky over Sochi at the castle Organization of air defense of facilities for the XXII Winter Olympic Games and XI Winter Paralympic Games 2014, Aerospace Defense, by D. D. B. Demidov, Copyright 2015 by Publisher.

In turn, the facilities located in the Krasnaya Polyana and Estosadok areas were located on the slopes of the Aibga and Psekhako ridges and formed the mountain cluster. In order to organize an airspace protection system in Sochi, a special working group was established in 2011, composed of representatives of the military command and control bodies from the

Southern Military District, research institutes and industrial enterprises. As a result of the work of this group, an air defense group was organized in Sochi to secure the air defense of the XXII Winter Olympic Games and the XI Winter Paralympic Games in 2014. Its fundamental element was the Sochi anti-aircraft missile regiment, which was reinforced with additional forces. The supporting units included squadrons armed with Pantsir-S sets and the anti-aircraft battery of the Tor-M2 missile sets as shown in photo 1. On the left side of the photo a passive reconnaissance radar is visible, very similar to the Ukrainian Kolchuga. Two masked Tor-M2 anti-aircraft missile sets with new air target detection radars (Figure 5) are visible on the next photo.

Figure. 5. The Tor-M2 missile system deployed to protect the Olympic venues in Sochi. Adopted from: *Meanwhile, air defense is being deployed in Sochi*, Military Review, Copyright 2013 by Publisher http://karelmilitary.livejournal.com

It is a weapon designed to detect, track and destroy ballistic and cruise missiles, unmanned aerial vehicles and possibly also stealth airplanes. In addition, the airspace over Sochi was also protected by other anti-aircraft missile systems, such as: Buk-M1, S-300PS, S-300PM, three S-300V4 missile batteries with a greater range, which were ordered by the Ministry of Defense in 2012. The air zone was controlled by squadrons of Su-24 bombers, Su-25 attack aircraft, Su-27 and MiG-29 interceptors, MiG-31 and Mi-8, Mi-24 and Mi-28 military helicopters located near the city of Krymsk.

The most problematic zone was the heavily forested mountainous area with a large number of ravines stretching for tens of kilometers into the territory of neighboring countries. Such topography created favorable conditions for hidden penetration of saboteurs, terrorist groups, and unmanned aerial vehicles. Thus, in order to control these critical areas, the reconnaissance unmanned helicopter "Horizon Air S-100", which was produced by the company from Rostov-on-Don, was used. It was designed for vertical take-off and landing, which meant that it did not require any runway or special ground equipment. It could also take off from decks of ships and sea platforms (Figure 6).

Figure 6. The air reconnaissance kit – unmanned helicopter „Horizon Air S-100”**.** Winter Olympics in Sochi: Potential Threats and Security Measures That Are Being Taken Adopted from: Independent Analytical Center For Geopolitical Studies Borysfen Intel, Copyright 2013 by Publisher. http://bintel.com.ua/uploads/spravka/spravka_vvs.html#s100

Moreover, such difficult terrain conditions seriously hindered the proper distribution of radar reconnaissance means. After a detailed reconnaissance in the field, a solution was adopted which consisted in placing the air defense systems at different altitudes, which allowed to provide the facilities with multi-layer cover at different heights. In addition to the serious terrain limitations, additional difficulties arose related to the dense layout of the built-up area, the lack of roads and the need to organize a location in the Sochi National Park. One of the units with air defense means was located in the area of the Adler Sanatorium, under construction, which made it possible to obtain very good conditions for the protection of facilities located in the coastal cluster from the sea (see photo 1). It became more difficult to organize the locations for air defense means for the facilities located in the mountain cluster. An example was the position "Rosa Khutor", which was located in the immediate vicinity of the ski resort of the same name (Figure 7). This location was the only possible place to deploy air defense systems to cover the Olympic venues from the east, where the longest gorges extended further southeast. These are just some examples illustrating the difficulties in organizing the combat positions for the air defense assets (Demidov, 2015).

Figure 7. Rosa Khutor From the left: the Pantsir-S system at the "Sanatorium Adler" position; the Pantsir-S system at the Rosa Khutor position. Adopted from: Sky over Sochi at the castle Organization of air defense of facilities for the XXII Winter Olympic Games and XI Winter Paralympic Games 2014, Aerospace Defense, by D. D. B. Demidov, Copyright 2015 by Publisher.

As a result of the deployment of air defense assets in the selected regions, all facilities of the Olympic and Paralympic Games were in the air-defense zones and were protected against air threats from all directions, as shown in Figure 8. The restrictions on the use of airspace in the Sochi area in the form of no-fly zones and zones restricting the movement of aircraft were also introduced.

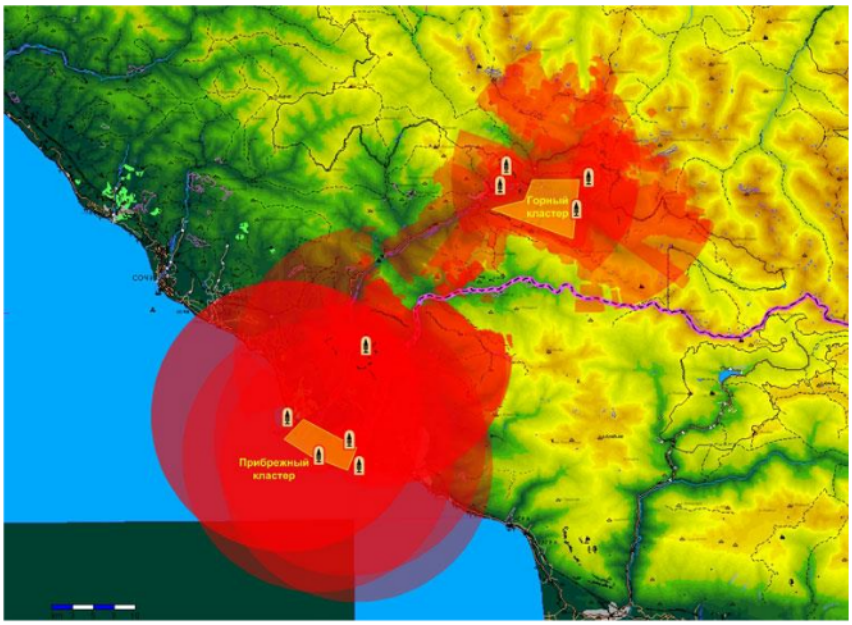

Figure 8. The layout of zones for the protection of the Olympic venues in Sochi against air threats at very low altitudes. Adopted from: Sky over Sochi at the castle Organization of air defense of facilities for the XXII Winter Olympic Games and XI Winter Paralympic Games 2014, Aerospace Defense, by D. D. B. Demidov, Copyright 2015 by Publisher.

The forces and resources deployed to protect the Olympic venues were managed by the Safety Management Center, created especially for the Olympic and Paralympic Games. In addition, it should be emphasized that the air defense system also included the air defense forces of the Black Sea Fleet.

4. Conclusions

Analyzing the threats of the Olympic Games in Sochi, one can risk making the statement that the experience gathered in the organization of the safety system in the case of such large and spectacular international sports events indicates that as early as at the planning stage, the threats that may occur during the event should be identified.

The Russian security forces were directly responsible for ensuring the safety of the guests, fans and participants of the Olympics. However, a very important role was also played by the specialized forces and means of air defense assigned by the Russian Armed Forces, which fully fulfilled the task of securing the airspace over the Olympic facilities. The operations carried out at sea by the separated forces from the Black Sea Fleet looked equally efficient.

The need to effectively counter the diagnosed threats also forced the search for new procedural, organizational and technical solutions. One such solutions was the introduction

of temporary No-Fly Zones, the use of unmanned reconnaissance systems around the potential Olympic facilities threatened by an air attack. The implementation of such restrictions is now becoming a global standard. This is confirmed by the security of subsequent mass sports events, e.g. the Summer Olympics in Rio de Janeiro, Brazil (2016), PyeongChang 2018 Olympic Winter Games in South Korea and other important international events, i.e. the G-8 economic summits, G -20, NATO summits, important national and religious celebrations and anniversaries. In the case of the organization of the security system of the Winter Olympic Games in Sochi, it should be emphasized that it took into account the use of a wide range of civil and military means. Moreover, the practice of Sochi confirmed that the effective use of the forces and resources subordinate to various governmental institutions requires an enormous effort to coordinate and prepare for joint operations.

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Boyle, Ph. (2012). *Securing the Olympic Games: Exemplifications of Global Governance,* in Helen Jefferson Lenskyj and Stephen Wagg (eds.), *The Palgrave Handbook of Olympic Studies,* Basingstoke: Palgrave Macmillan, p. 394.
2. Dean, K. (2014). *Winter Olympic Games: Long-term Lessons for Sochi, Colliers International, Ester Europe, I* Q, February, p. 5. file:///C:/Users/ADAMRA~1/AppData/Local/Temp/colsochi.pdf
3. Demidov, D.D.B. (2015). Sky over Sochi at the castle organization of air defense of facilities for the XXII Winter Olympic Games and XI Winter Paralympic Games 2014, Aerospace Defense, No 3.
4. Department of State (2014). Office of the Spokesperson, *Special Briefing: Senior Administration Officials Teleconference*, January 24.
5. Horne, J. Manzenreiter, W. (2006). *An Introduction to the Sociology of Sports Mega-Events*, *Sociological Review* 54, No. 2, p. 19.
6. Lovelace, D. C. Jr. (2017). Terrorism: Commentary on Security Documents: Russia's Resurgence, Oxford University Press, Volume 146, p.71.
7. Luccacioni, C. Cohen, A. (2014). *Sochi: Security and Counterterrorism at the 2014 Winter Olympics*, Issue Brief, No 4116, January 06, p.1.
8. Müller, M. (2014).*After Sochi 2014: costs and impacts of Russia's Olympic Games*, Eurasian Geography and Economics , Vol. 55, No. 6, p. 628–655.
9. Nichol J. Halchin E. J. W. Rollins, A. Tiersky, S. Woehrel (2014, January, 26), The 2014 Sochi Winter Olympics: Security and Human Rights Issues, Report, Congressional Research Service. file:///C:/Users/ADAMRA~1/AppData/Local/Temp/R43383.pdf
10. Radomyski, A. (2019). *Contemporary aspects of civil aviation security against aviation terrorism*, Transport Means - Proceedings of the International Conference, October 2-4, Palanga, Lithuania, file:///C:/Users/ADAMRA~1/AppData/Local/Temp/Transport-means-2019-Part-3.pdf

11. Radomyski, A. Bernat, P. (2018). *Contemporary Determinants of Organising Effective Protection of Civil Aviation Against Terrorism*, Transportation Research Procedia, Volume 35. https://www.sciencedirect.com/science/article/pii/S2352146518303612
12. Radomyski, A. Dobija, K., Michalak, A. (2012). *Determinanty użycia wojsk OPL w osłonie imprez sportowych o wymiarze międzynarodowym*, Akademia Obrony Narodwej, Warszawa.
13. Šiljak, V. Vukašinović, V. Đurovi, D. (2016). *Security Requirements at the Olympic Games*, Sportlogia, No 12 (1), p. 38.
14. Silke, A. (2010). *Understanding Terrorist Target Selection*, A. Richards, P. Fussey, and A. Silke (Eds), *Terrorism and the Olympics: Major Event Security and Lessons for the Future,* London, Routledge, p. 58.
15. Spaaij, R. (2016). *Terrorism and Security at the Olympics: Empirical Trends and Evolving Research Agendas*, The International Journal of the History of Sport, Vol. 33, No. 4, p. 452.
16. The Kremlin (2014). *President of Russia, Interview to Russian and Foreign Media*, January 19. http://www.en.kremlin.ru/events/president/transcripts/interviews/20080
17. U.S. Department of Defense (2014). *Press Briefing with Rear Admiral Kirby from the Pentagon*, January 23. https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/606940/department-of-defense-press-briefing-by-rear-adm-kirby-in-the-pentagon-briefing/
18. Yu. Y, Klauser, F., Chan, G. (2009). Governing Security at the 2008 Beijing Olympics', *The International Journal of the History of Sport* 26, No 3, p. 390.
19. Russian Secret Service (2012, May, 10). *Sochi 2014 Olympics Terror Attack Foiled in Breakaway Republic of Abkhazia,* CBS News. http://www.cbsnews.com/news/russian-secret-service-sochi-2014-olympics-terror-attack-foiled-in-breakaway-republic-of-abkhazia/
20. Parfitt, T. (2013, July, 3), *Doku Umarov Calls for Islamists to Disrupt Sochi Winter Olympics*, *Telegraph*. http://www.telegraph.co.uk/news/worldnews/europe/russia/10157474/Doku- Umarov-calls-for-Islamists-to-disrupt-Sochi-Winter-Olympics.html
21. Frolov, V. (2013, October, 28). *A Global Power Can't Have Porous Borders*, *The Moscow Times*, http://www.themoscowtimes.com/opinion/article/a-global-power-cant-have-porous-borders/488532.html
22. Global Rescue (2013, November, 25). *Global Rescue to Support U.S. Ski and Snowboard Association at 2014 Sochi Winter Olympic Games*, news release. https://www.globalrescue.com/about.cfm?view=news&article=116.
23. Garamone, J. (2014, January, 21). U.S., Russian Leaders Discuss Afghanistan, Sochi, History," *News, American Forces Press Service. https://www.jcs.mil/Media/News/News-Display/Article/571636/us-russian-leaders-discuss-afghanistan-sochi-history/*
24. Frankovic, K. (2014, January, 29). More than half of Americans have little to no confidence that Sochi will be safe from terrorist attacks, but most people still want the US to participate, Politics & current affairs. https://today.yougov.com/topics/politics/articles-reports/2014/01/29/olympic-interest-olympic-fears
25. Fergus, N. (2014, June, 26). *A former Australian intelligence agent whose consulting firm Intelligent Risks worked on the Athens Olympics, quoted in Andrew Chang*, 'Fearing Olympic Terror, Athens Gears Up', *ABC News* http://abcnews.go.com/International/story?id=79466

26. J. McBride (2018, January,19). *The Economics of Hosting the Olympic Games*, Council on Foreign Relations. https://www.cfr.org/backgrounder/economics-hosting-olympic-games
27. Colarusso, J. (2019, August, 1). RUSSI: *The Circassians and the Sochi Olympics*. John Colarusso. Retrived http://www.johncolarusso.net. Russia: New Harassment of Olympic Critics.

SAFETY&DEFENSE
ISSN 2450-551X

Anti-Satellite Weapons: A Political Dimension

Marek CZAJKOWSKI

Jagiellonian University, Kraków, Poland; marek.czajkowski@uj.edu.pl, ORCID: 0000-000304276-4984

DOI: https://doi.org/10.37105/sd.129

Abstract

This article tackles the political dimension of the development of anti-satellite weapons. The main goal is to assess their significance from the American, Russian, and Chinese perspective to understand the emerging balance of power in space. While the U.S. is struggling to maintain its position of dominant space power, its main adversaries are developing technologies that can diminish American dominance. It is, therefore, widely believed that outer space is poised to be weaponized by multiple systems designed to destroy satellites in-orbit, both ground- and space-based. On the other hand, the United States is executing multiple fast-track research& development programs aimed at increasing the resilience of the U.S. space systems.

Keywords

international security, safety in space, space systems defense, space security, space weapons.

Submitted: 20.05.2021 Accepted: 15.06.2021 Published: 29.06.2021

1. Introduction

There is no need to discuss at length the utility of satellite systems and their significance for nation-states' economy, security and social sphere. Suffice it to say that the global satellite industry revenues reached 366 billion USD in 2019 (Satellite Industry Association, 2020), and security-related satellite applications are indispensable for every country, providing communications, earth observation and positioning. Satellites are also present in social life as they are a vital part of cyberspace, enabling many socially significant activities like multi-domain communications, social networks, and entertainment. However, these benefits are not absolute because many technologies designed to hinder space operations have been perfected within the last decade or so. Others are under development with a good prospect for entering operational service in the coming years.

This article tackles the political dimension of the development of anti-satellite (ASAT) weapons. The main goal is to assess their significance from the perspective of the United States, Russia, and China to understand the emerging balance of power in space. It will be argued that a slowdown or even freeze of the development of this kind of armaments is going to occur in the coming years.

As a military competition, strategic considerations and the global power struggle are referred to in this article; naturally, the realist paradigm has been adopted for the purpose of the research. This kind of approach will allow us to underline the basic characteristics of the relations among main global competitors, as our goal is to provide the most general answer to the question referring to their strategies. Qualitative methods will be performed with regard to open-source information and analyses available on the issue of ASAT weapons.

2. Anti-Satellite Weapons – a short summary

There are many ways to negate satellite capabilities, either partially or in full. Spacecraft may be dazzled or blinded, their signals may be jammed, spoofed or otherwise distorted. Antagonistic forces may also take orbiters over, physically or through cyber intrusion. Certainly, satellites may also be destroyed or damaged by hostile entities using various forms of physical or non-physical attack. These means are usually referred to as counterspace capabilities or counterspace weapons (Harrison et al., 2021).

This research directly tackles only one category of counterspace capabilities, which we refer to as anti-satellite weapons. We define them as ground- or space-based systems designed to damage or destroy satellites in orbit. However, other means of disrupting the operations of satellite systems are also considered in this paper as they are an indispensable context for the main argument. The following presents shortest possible summary of the ASAT capabilities of the United States, China and Russia.

The United States adamantly holds that it does not possess and is not developing any dedicated ASAT system. However, the Ballistic Missile Defense System (BMDS) consists of several weapons systems designed to attack ballistic missiles in space. This means that it possesses intrinsic ASAT capabilities (Grego, 2011). The most capable of the systems belonging to the BMDS is the Aegis/SM-3, installed onboard 48 U.S. Navy cruisers and destroyers (O'Rourke, 2020). According to the FY 2019 budget submission, the inventory of SM-3 interceptors reached 464 in 2021 (O'Rourke, 2019). The system may be scaled up relatively quickly, as BMD-capable ships can carry from 90-to-122 missiles each; therefore, the matter

is only one of the production rates of missiles. Grego (2011) calculates that the SM-3IA/B variant can attack satellites at a distance of up to 600 km, and the SM-3IIA up to 1450-2350 km. Note that according to the Union of Concerned Scientists (2021), of the 3372 satellites active as of January 1st, 2021, roughly 2500 orbited below 1000 km.

As the Office of the Secretary of Defense (2020, p. 65) believes, the Chinese military "has an operational ground-based Anti-Satellite (ASAT) missile intended to target low-Earth orbit satellites". However, publicly available sources of reliable information provide no clue as to the nature of the system dubbed SC-19 (Harrison et al., 2021). There is also no open-source indication of whether this weapon has been adopted for operational use or put into combat service. Additionally, it is thought that China is pursuing other ASAT capabilities, including direct-ascent (DA) systems able to threaten geosynchronous orbit (GEO), co-orbital (CO) systems, and lasers with the potential to damage or destroy satellites (Harrison et al., 2021). However, the operational deployment of these advanced capabilities is the somewhat distant future.

Weeden and Samson (2021) argue that "Russia is almost certainly capable of some limited DA-ASAT operations, but likely not yet on a sufficient scale or at sufficient altitude to pose a critical threat to space assets." Current Russian anti-satellite development programs refer to both direct-ascent and co-orbital systems. The PL-19/Nudol missile represents the former tested several times in recent years (Podvig, 2020). It is, however, unknown whether any decision regarding the production or deployment of the operational units of this system has been made. It is frequently repeated that the S-400 air defense system, deployed in large quantities throughout Russia and abroad, is capable of conducting ASAT missions. We do not share this conviction, and we agree with Weeden and Samson (2021,) who do not list the S-400 as an anti-satellite weapon. However, the next-generation Russian air defense system, the S-500, will most probably be able to intercept medium-range ballistic missiles in space (Weeden & Samson, 2021). This feature would render the S-500 capable of ASAT operations, but it is not known if such a mission is envisaged for it. According to current estimates, the S-500 is slated to be deployed in significant numbers by 2025 (McDermott, 2021). Additionally, a noteworthy number of rendezvous proximity operations (RPOs) executed by Russian satellites have been observed in recent years, which might suggest that work on co-orbital ASAT weapons is in progress. Laser weapons are also being tested in Russia, and they may have some limited ASAT capabilities (Cooper, 2019).

Finally, it is necessary to point to the important context in which ASAT weapons must be considered, as they are just a part of a vast arsenal of counterspace capabilities. Other means of space warfare, even though non-destructive, present formidable opportunities to harm an enemy's systems and negate their capabilities. All three leading space powers have perfected electronic and cyber warfare against adversaries' space systems. China and Russia (Defense Information Agency, 2019), in particular, have developed the capabilities to negate missions of the American satellites. According to Harrison et al. (2020, p. 25), there is "overwhelming evidence that Russia has employed the use of mobile, ground-based electronic counterspace weapons on a regular basis both within its borders and abroad". The United States also possesses extensive electronic warfare counterspace capabilities (Weeden & Samson, 2021), although it is not known if they have actually been used.

3. Trends in the Development of Military Satellite Systems

The development of ASAT weapons must be placed within the context that relates to satellite systems' evolution. Indeed, current military constellations pose relatively easy targets

because they consist of a relatively small number of huge and expensive satellites, which are difficult to replace quickly. This feature makes ASAT weapons such a tempting remedy for the U.S. military preponderance; the "high ground" space systems occupy for executing their missions turn out to be a weak position as far as defense is concerned, as they are exposed, easily targetable and fragile. As Harrison, Johnson and Young (2021, p. 12) observed, "[w]hile U.S. space capabilities remain far ahead of other nations, some adversaries, namely China and Russia, are arguably making advances in counterspace weapons faster than the United States is making advances in protections against these threats."

On the other hand, however, in the last several years, we have witnessed a surge of concepts, ideas, and developmental works regarding increasing space systems' resilience to offset the development of anti-satellite weapons and other counterspace measures. This development must be mentioned within this paper because it forms one of the most important contexts for analyzing an emerging strategic balance in space. We will, therefore, briefly review these ideas below.

There are many possible ways to ensure the uninhibited operation of satellite systems that may be considered in designing the next-generation constellations. The first category of passive defense contains propositions for changes in the architecture of space systems. In general, this idea embodies the drive to create military constellations in such a way that they would represent a much larger target. Simply speaking, the multiplication of systems and elements within systems will make adversaries commit to more information gathering on assets, targeting devices and interceptors to harm a constellation. It will also take more time to accomplish these things, as the attacked system will not instantly lose its capabilities and would degrade gradually.

The second group of passive methods for protecting satellite systems are of a technical nature. It encompasses sophisticated prospective means that are difficult to explain without delving into technicalities, such as increasing space situational awareness (Bielawski, 2019), strengthening electronic warfare capabilities, installing technical means of protection of satellite lenses and electronics, increasing the jamming-resistance capacities of radio frequencies, using advanced encryption protocols, and so on. These means are mostly suited to confronting non-destructive, electronic or cyber counterspace weapons, but they can also contribute to defense against ASAT systems.

Finally, there are operational ways to complicate counterspace activities, particularly ASAT missions. For example, satellite constellations may be kept in-store and rapidly deployed if necessary. In this case, the adversary will be suddenly confronted with previously unknown systems it may not be prepared for. Similarly, the existing space systems may be backed up by components stored on the ground to reconstruct compromised constellations quickly. Additionally, the maneuverability of spacecraft may be somewhat augmented; stealth technologies may be employed in their construction, and they also may be equipped with countermeasures such as decoys or chaff.

Furthermore, we should mention possible forms of active defense, ranging from jamming, spoofing, dazzling, and blinding interceptors or ground components of ASAT systems to equipping spacecraft with defensive weapons. Co-orbital anti-satellite systems may also be pre-emptively seized or destroyed, and numerous actions against ground-based ASAT infrastructure may be taken, including electronic, cyber and kinetic pre-emptive attacks. It is safe to assume that in the case of hostilities, the adversary's anti-satellite infrastructure will be the first priority of the U.S. forces.

Many aerospace companies, scientific institutions, and military organizations in the United States are currently working on concepts for the next generation of space systems to make them more resilient. It is impossible to list them all within this article's framework, and suffice it to say that fast-tracked research and development works aimed at countering the effect of counterspace weapons (Strout, 2021), with particular attention to ASAT, are

underway in the U.S. and allied countries. The scope of these activities suggests that a sort of revolution in military space system operations has begun. Within the next decade, we will probably witness the advent of a new generation of military constellations substantially more resistant to adversaries' actions.

It should also be mentioned that many of the most promising technologies or operational concepts for strengthening space systems are very expensive. However, since the United States decided it was crucial to increase its space systems' resilience dramatically, we may expect that billions of dollars will be spent to reach the desired level of resilience. On the contrary, it is doubtful whether China or Russia are ready to do the same with their own satellite systems, which may remain vulnerable in the foreseeable future while the American will gradually become safer.

4. The Emerging Strategic Equation in Outer Space

It is frequently argued that outer space is poised to be quickly weaponized due to research and development works in progress in many countries, most notably in Russia and China (Raymond, 2020). Some even argue that, due to the dual-use nature of satellite systems, the weaponization of the Earth's orbit is a natural development as almost every satellite invokes a security dilemma (Lubojemski, 2019). Consequently, this purportedly unavoidable process will add to the already existing and widely used non-destructive counterspace capabilities. All in all, as the argument goes, the times of actual "star wars" in which lasers, microwave weapons, EMP pulses, and missiles will be used to damage and destroy satellites are about to come in the not-so-far future.

However, other factors should also be taken into consideration. More than a simple drive to offset the American strength governs Russian and, especially, Chinese actions. Both countries must consider many other issues regarding their own use of satellite systems, ranging from the general goals and aims of the respective states' strategies, through technical and operational considerations, to economic constraints. Furthermore, this is not to mention the so-called Kessler effect (Kessler & Cour-Palais, 1978), which looms over all human space activities. In essence, it means that the destruction of even a small number of satellites would lead to the obliteration of at least a significant portion of the whole space architecture. This would happen because destroyed spacecraft would, in most cases, be reduced to a great amount of fragmented debris, which, in turn, would hit other satellites, producing a potentially massive cascade effect. Furthermore, vital orbits would be rendered inaccessible for decades.

Therefore, we believe that the decision to deploy dedicated ASAT weapons systems in quantities significant enough to alter the existing military balance will not be based only on the sheer technical capabilities demonstrated during laboratory and field tests. The most important question revolves around the security dilemma (or trilemma): whether the deployment of a novel weapon would bring more benefits than costs. Every leg of the arms race has its own dynamics, and, contrary to the common view, not every weapon which has been developed must be deployed or used. For example, during the Cold War both sides considered fractional orbit bombardment systems (FOBS); the Soviet Union even managed to design an operationally capable model of such a weapon. Nevertheless, it was never deployed in significant quantities because both sides decided that it was impractical, extremely costly, and would add dangerous volatility to the strategic balance without offering many advantages. The same happened to strategic missile defense, which was designed, developed and deployed but in strategically insignificant quantities. In simple terms, before a novel

and costly weapon is put into full operational capacity, the user must decide whether the potential costs and dangers do not exceed gains. We believe that it is the case with ASAT weapons as well.

The "benefit side" of the security dilemma (trilemma) associated with ASAT weapons that China and Russia face is apparent. If Moscow or Beijing has a significant number of ASAT weapons deployed today, it would mean that the U.S. vital satellite systems are held hostage. This would represent political leverage in peacetime and a critically important advantage in case of a crisis and conflict. This is undoubtedly true, but five important contexts of various kinds should be considered at the "cost side" of the security dilemma (trilemma). Firstly, the United States already possesses significant ASAT capabilities, which hold the space assets of China and Russia hostage. Thus, in the case of a conflict, the U.S. could quickly retaliate if confronted with an act of aggression in space. The U.S. Navy BMD-capable cruisers and destroyers scattered throughout the world can "clear" the LEO of enemy's satellites using their independent detection, tracking and targeting capabilities. Therefore, the retaliation would happen even during an unlikely but possible scenario in which the instant and total annihilation of the American space systems would occur. Of course, the United States is more dependent on satellite systems than its main competitors, so one might say that such a space Armageddon would harm the U.S. side more. However, others, China or Russia, would also lose their vital assets, and the balance that would emerge out of such an event would still favor the U.S. even if some capabilities had been nullified. China, particularly, would lose the assets indispensable for its most cherished strategy of expanding global reach and strengthening its military's power projection capability (Biddle & Oerlich, 2016). The American intelligence community (Office of the Director of National Intelligence, 2021, p. 7) underline that "Beijing is working to match or exceed US capabilities in space to gain the military, economic, and prestige benefits."

Secondly, the scenario mentioned above assumes that China or Russia do have significant ASAT capability at the moment. We have made this assumption to illustrate the consequences of the exchange of strikes against the space infrastructure. However, the reality is different. Neither China nor Russia have significant ASAT capabilities. On the other hand, the United States already has formidable anti-satellite weapons systems, even though it is not officially acknowledged. This means that any anti-satellite arms race initiated by China or Russia would be doomed to be lost by them, simply because the U.S. already has a huge numerical and technological advantage in DA anti-satellite systems, which will surely grow once the race is on. The same goes with future co-orbital ASAT weapons or lasers powerful enough to damage or destroy a satellite. The U.S. retains so great an economic and technological advantage that even if surprised by the rapid deployment of first units procured by adversaries, it would certainly be able to quickly catch up and overtake competitors in every aspect of the race. This is the most important reason that makes the whole idea of the ASAT arms race an impractical and futile effort from the point of view of the Russian or Chinese interest.

Thirdly, if, despite the above-mentioned facts, China or Russia decide to design and deploy a significant number of combat ASAT units, it will take not only a lot of financial and organizational effort but also much time. This very time will be used by the United States not only to speed up its own weapons deployment; the reconfiguration of the American space capabilities will also be quickened, first of all by changing their architecture and modes of operational use. And so, by the second half of the decade, the emerging ASAT force of China or Russia would be confronted with an increasingly complex and quickly evolving target, rendering any attack calculus very difficult. In other words, an anti-satellite force ready to be fielded within several years will operate alongside today's principles. Still, it will a face space architecture which, at least in significant part, will operate according to tomorrow's

principles. Of course, this prediction is valid only if some unexpected technological breakthrough in anti-satellite weapons does not occur. Absent such a "black swan" event, the U.S. would remain well ahead of its competitors both in its offensive ASAT capabilities and measures aimed at increasing the resilience of space systems in the foreseeable future.

Fourthly, the above-mentioned Kessler effect must be seriously taken into consideration. This means that even a minor exchange of blows in space may lead to serious and uncontrollable consequences. Therefore, there is no room for an escalation-de-escalation strategy in space warfare. This renders ASAT weapons clumsy and inflexible as nuclear deterrents, and impractical as tools of everyday policies, though extremely expensive ones.

And finally, all three countries, most notably China and Russia, but we may safely assume that the U.S. as well, are engaged in day-to-day non-destructive combat in electronic and cyber realms. Laser blinding and dazzling is also commonplace. This ongoing activity carries much less political weight than the use of destructive systems, but it brings benefits and advantages without the risk of a space Armageddon.

5. Current Realities of the ASAT Race

Let us reiterate the point that if an ASAT arms race is triggered, the U.S. will most probably retain their decisive advantage. This means that the ability of America's competitors to inflict significant damage on U.S. systems will bring inevitable risks for their own vital capabilities. Even if a successful "space Pearl Harbor" occurs, the likely Kessler effect will negate it by destroying most of the attackers' satellites even without American action. The loss of its satellite systems would surely cripple the U.S. military, but America would remain the most powerful military in the world, even if its capabilities are diminished. Additionally, the economic consequences of damage to space architecture would be tremendous, not only for the parties to the conflict but also for the whole world, because all countries and commercial entities will have their space assets at least badly damaged. Furthermore, many orbits may be rendered unusable for a long time, which would degrade the world's space capabilities for years or decades to come.

The risk/benefit equation should also be analyzed in light of the obvious and well-known advantages of the unhindered use of space systems. Even if they are somewhat compromised by non-destructive means of space combat, they are still indispensable in peacetime, in the case of crisis or heightened tensions, or during armed conflicts of various natures. Putting these advantages in jeopardy by initiating an anti-satellite arms race seems unreasonable.

Furthermore, it should be noticed that the development of ASAT weapons into a politically significant instrument requires much investment in technology, organization, training, and infrastructure. In addition, a doctrine of the implementation of a novel weapon must be developed in which the overall task, terms of use, and decision-making process must be operationalized. The next step is the formation of combat units and their final training and certification for operational use. Finally, hardware must be procured, and a number of units deployed to fulfill the ASAT mission envisaged for them. In the case of direct-ascent ASAT, a force that may be called significant would probably comprise of tens of combat units, dozens of launchers, hundreds of missiles, and thousands of personnel scattered across numerous installations. This might prove prohibitively expensive even for China, which already carries a burden of multi-domain military modernization.

Taking all of the above-mentioned arguments into consideration, we can easily notice that the anti-satellite arms race is not inevitable because no one would actually benefit from it. ASAT weapons are costly and impracticable, and also add to the inherent volatility of the

strategic balance. Therefore, it is our assessment that no side in the emerging space deterrence equation will decide to deploy significant ASAT force. Thus, a full-blown anti-satellite arms race will not be started in the foreseeable future absent a sudden technological breakthrough would instantly nullify all of the capabilities of one side of the equation.

However, the question still arises as to why China and Russia continue developing ASAT weapons, even though they are so obviously impractical. We assume that these works are not intended to lead to the deployment of significant ASAT forces. This means that, in our opinion, the decision to weaponize outer space is not going to be made either in Moscow or in Beijing. However, this does not preclude the conduct of research and development activities that may be deemed practical for at least several reasons.

Firstly, both countries may intend to accumulate knowledge and expertise as a hedge against possible future changes in the strategic balance, especially should the U.S. decide, and paradoxically it is not unlikely to trigger an ASAT arms race sometime in the future. Secondly, it is possible that China and Russia count on some technological breakthrough that could rapidly change the balance in their favor. Thirdly, the development of anti-satellite weapons may be continued in order to retain a bargaining chip in possible future strategic arms limitation/reduction talks, be they two- or three-sided. Finally, both countries might strive to use their ASAT development to gain international prestige. This would especially be the case of Russia, as Vladimir Putin frequently boasts about novel Russian superweapons. They are surely formidable, but they do not change the strategic balance within current strategic realities, especially considering the shrinking Russian military budget. The same goes with China's ongoing drive to display its technological prowess. A small, experimental in nature, ASAT force, even if undeclared, would have a similar propaganda effect.

In this way, research and development work on anti-satellite weapons may continue, and the deployment of a small ASAT force may even occur, but the strategic equation of the space MAD will hold anyway. All sides of the new strategic balance will refrain from deploying a full-blown anti-satellite force. This will make their vital space capabilities relatively reliable, and satellite war will continue with non-destructive methods. It will also spare military budgets the burden of a new arms race. Finally, rudimentary anti-satellite capabilities will be retained as a hedge against future developments and as a kind of hidden deterrent.

6. Conclusion

In conclusion, we reiterate that considering the current state of affairs, especially with regard to technical and organizational issues, anti-satellite weapons will not materialize in the quantities significant enough to influence the strategic balance. Most probably, they will not be deployed at all. It is, however, unclear whether this is going to happen only with a tacit acknowledgement of the existing balance or perhaps along the lines of some legally binding international agreement. We assume that, in the foreseeable future, the former will be the case. However, we cannot exclude some regulations in the more distant future, probably as a part of some wider strategic balance-imposing treaty. Surely, concluding such a treaty will not be easy, especially since three sides are involved, which dramatically complicates the negotiation process. Nevertheless, reaching such an agreement is not impossible, provided the world powers will understand their interests and recognize the threats and risks. It is also possible that after several years or maybe a decade or so of uncertainties caused by the multi-dimensional crisis of the international system, some new system will emerge. This would make the main powers more susceptible to compromise, and the regulation of ASAT weapons might become part of the strategic realities of a new international

system. However, more detailed consideration with regard to this is rather premature at the moment.

The realist perspective that we have adopted assumes that nation states act more or less rationally regarding realistically defined interests. The analysis above is based on this premise. However, for the sake of comprehensiveness, we should add that it is also possible that leaders or elites within the countries will indeed act irrationally and contrary to their own best interests. It may also occur within the sphere we have just described. For example, the Chinese leadership may relentlessly push for the deployment of a significant number of direct-ascent ASAT systems to offset the U.S. military advantage at any cost. Furthermore, the Russian leadership may decide that the deployment of anti-satellite capabilities would serve in favor of Russia's image as a world power despite the financial burden that it would bring. Moreover, in the United States, the military or industrial lobbies may feed on popular fears and push through the weaponization of space for their own sake, regardless of the state's interest. The American Department of Defense (2020) has already identified outer space as a warfighting domain. However, these possible outcomes require a more detailed and nuanced approach and implementation of a different theoretical paradigm.

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

References

1. Biddle, S., Oelrich, I. (2016). Future Warfare in the Western Pacific: Chinese Antiaccess/Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia. *International Security*, Volume 41, Issue 1, Summer, pp. 7-48, doi:10.1162/ISEC_a_00249.
2. Bielawski, R. (2019). Space as a New Category of Threats to National Security. *Safety & Defense*, 5(2),(2019), pp. 1-7. https://doi.org/10.37105/sd.48
3. Cooper, J. (2019). *Russia's 'Invincible' Weapons: An Update*. University of Oxford. https://static1.squarespace.com/static/55faab67e4b0914105347194/t/5c9b6bd8085229887babeb2c/1553689562006/Cooper+Invincible+Weapons+update.pdf
4. Defense Information Agency. (2019). *Challenges to Security in Space*. Defense Information Agency. https://fas.org/spp/military/program/asat/dia-challenges.pdf
5. Department of Defense. (2020). *Defense Space Strategy*. U.S. Department of Defense. https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF
6. Grego, L. (2011). *The Anti-Satellite Capability of the Phased Adaptive Approach Missile Defense System*. Public Interest Report, Winter, Federation of American Scientists. https://fas.org/pubs/pir/2011winter/2011Winter-Anti-Satellite.pdf
7. Harrison, T., Johnson, K., Roberts, T.G., Way, T., Young, M. (2020). *Space Threat Assessment 2020*. Center for Strategic & International Studies. https://www.csis.org/analysis/space-threat-assessment-2020

8. Harrison, T., Johnson, K., Moye, J., Young, M. (2021). *Space Threat Assessment 2021*. Center for Strategic & International Studies. https://www.csis.org/analysis/space-threat-assessment-2021.
9. Harrison, T., Johnson, K., Young, M. (2021). *Defense Against the Dark Arts in Space. Protecting Space Systems from Counterspace Weapons*. Center for Strategic & International Studies. https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons
10. Kessler, D.J., Cour-Palais, B.G. (1978). Collision frequency of artificial satellites: The creation of a debris belt. *Journal of Geophysical Research*, Vol. 86, no. A6, pp. 2637-2646, https://doi.org/10.1029/JA083iA06p02637
11. Lubojemski, A. M. (2019). Satellites and the Security Dilemma. *Astropolitics*, vol. 17, no. 2, pp. 127-140, https://doi.org/10.1080/14777622.2019.1641689
12. McDermott, R. (2021). Moscow Weighs Options to Procure S-500 Air-Defense Systems, *Eurasia Daily Monitor*, Volume: 18 Issue: 48, Jamestown Foundation. https://jamestown.org/program/moscow-weighs-options-to-procure-s-500-air-defense-systems/
13. O'Rourke, R. (2019). *Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/RL/RL33745/190
14. O'Rourke, R. (2020). *Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress*. Congressional Research Service. https://www.hsdl.org/?view&did=848440
15. Office of the Director of National Intelligence. (2021). *Annual Threat Assessment*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
16. Office of the Secretary of Defense. (2020). *Military and Security Developments Involving the People's Republic of China 2020. Annual Report to Congress*. Office of the Secretary of Defense. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF
17. Podvig, P. (2020). *Nudol ASAT system tested from Plesetsk*. Russian Strategic Nuclear Forces. http://russianforces.org/blog/2020/12/nudol_asat_system_tested_from.shtml
18. Raymond, J.W. (2020, 12, 20). *How We're Building a 21st-Century Space Force*. The Atlantic. https://www.theatlantic.com/ideas/archive/2020/12/building-21st-century-space-force/617434/.
19. Satellite Industry Association. (2020). *2019 Top-Level Global Satellite Industry Findings*. Satellite Industry Association. https://sia.org/news-resources/state-of-the-satellite-industry-report/
20. Strout, N. (2021, 02, 11). *SDA to launch several demonstration satellites in 2021*. C4ISRnet. https://www.c4isrnet.com/battlefield-tech/space/2021/02/11/sda-to-launch-several-demonstration-satellites-in-2021/
21. Union of Concerned Scientists. (2021). *USC Satellite Database*. Union of Concerned Scientists. https://www.ucsusa.org/resources/satellite-database
22. Weeden, B., Samson, V. (Eds.). (2021). *Global Counterspace Capabilities*. Secure World Foundation. https://swfound.org/media/207162/swf_global_counterspace_capabilities_2021.pdf