Shortage of water resources and cyber – attack are two greatest challenges to contemporary global stability and security

Rashad Tahirov 1,2, Nuran Mahmudov 2, Elnur Gojayev 3, Veselina Aleksandrova 4, Violeta Vasileva 5
Military Scientific Research Institute, Baku, Azerbaijan, rashad_tahirov1975@yahoo.com 1
Military Scientific Research Institute, Baku, Azerbaijan, mahmudovnuran@outlook.com 2
International Military Cooperation Department Baku, Azerbaijan, elnurquca@gmail.com 3
G. S. Rakovski National Defence College, Sofia, Bulgaria, v.gagamova@ndc.bg 4
Artshare, Estarreja, Portugal, violeta.vasileva@artshare.pt 5
rashad_tahirov1975@yahoo.com

Abstract: In response to these global threats, it is essential that nations work together to develop coordinated approaches to ensure global security. This requires building trust, sharing information, and collaborating to develop effective solutions that address the root causes of these threats. One important step in ensuring global security is to focus on the prevention of crises before they occur. This can be achieved by investing in early warning systems, improving communication and cooperation between nations, and addressing the underlying causes of conflict and instability. Another key factor in ensuring global security is to promote sustainable development that prioritizes environmental protection, social justice, and economic progress. This can help to prevent resource scarcity and social inequality, which are often key drivers of conflict and insecurity. In addition, it is important to recognize the central role of technology in shaping global security. While technology can create new threats, it can also be harnessed to develop innovative solutions that promote global security. This includes investing in cybersecurity, developing new technologies to address environmental challenges, and promoting access to education and information to help people around the world build resilience and respond effectively to emerging threats. Global security is a complex and multifaceted issue that requires a coordinated and collaborative approach from nations around the world. By working together to prevent crises, promote sustainable development, and harness the power of technology, we can build a more secure and resilient world for generations to come.

Keywords: GLOBAL SECURITY, TECHNOLOGY, ENVIRONMENTAL PROTECTION, CYBER-ATTACK, CYBERSECURITY

1. Introduction

Throughout the history of world civilization, ensuring security has been one of the main goals of society. In the modern world, the population boom, income inequality and the widespread using of new technologies has significantly changed the aspect of security. The beginning of the XXI century is characterized by the worldwide growth in the number of social, economic, technogenic and environmental threats at different levels. Today numerous, complex and highly interconnected threats affect the lives of millions of men, women and children around the world, as well as global security. In the near future, this trend will continue and we will witness new crises, new conflicts and new victim. In this context, the concept of global security acquires special relevance, since at present the problems that appear in one state immediately spread to the states surrounding it. These processes are accelerated by colossal scientific and technological progress, that has enabled us to travel both vicariously and instantaneously to almost all regions of the world [1]. The development of technologies in the modern world not only allows humanity to solve many problems of its progressive evolution, but at the same time, it creates new challenges and threats to domestic, global security such are water crisis and cyber-attack. In recent years, the world is facing a crisis in the field of water resources. It is obvious that shortage of “water in an arid and semi-arid environment leads to intense political pressures, often referred to as "water stress," and mass migrations of the population. Also in our increasingly interconnected world, threats to our security can come from unexpected new sources and directions such a cyber-attack. This threat, which can paralyze the defense and financial system or infrastructure of an entire country, is becoming more and more real.

2. Definitions

Modern political science considers security as the aspect of identifying and studying, preventing and eliminating factors and conditions that pose threats and dangers to people's existence, society and states stability and prosperity. The simplest way to define security is an absence or preventing threats to key values or “condition where survival of someone or something is not at risk” [2]. Security is interrelated with prosperity and stability. This latter is understood as the ability of a state to provide the safety of law and order, protecting citizens from each other and from foreign foes [3]. The more stable the system, the higher level of prosperity, which simple means improving the standard of living of the average citizen [4]. Therefore, security is largely dependent on the stability of state and society, on the state’s economic growth and thriving and on the military strength.

Concepts of security are identified at national and global level and “referent objects” [5]: homeland (state), human, economic, food, health, environmental, cyber and etc. While national security remains central to peace and stability, there is growing need for recognition an expanded security paradigm. National security, as a multi-level system, is itself one of the elements of a wider system - global security. Today in the context of globalization, national security become closely related to global security and as the result the international dimension of state security has increased many times.

National security is identified as the protection of the particular state from external and internal threats, resistance to adverse effects from the outside, ensuring internal and external conditions, which guarantee the possibility of stable progress of society and its citizens. The other definition of the national security is “the requirement to maintain the survival of the state through the use of economic power, diplomacy, power projection and political power” [6]. Ensuring and is not limited only to the elimination of threats, the physical survival of society, the preservation of the sovereignty and integrity of the state, the economic and military power, but also the creation of conditions for the sustainable functioning and development of society. The core of the national security are “state security” and “human security” system and therefore the main priority to ensure state security, stability and prosperity, maintain the quality of life of citizens by focusing “on building human capabilities to confront and overcome poverty, illiteracy, disease, discrimination, restrictions on political freedom, and threat of violent conflict” [7]. National security, as a multi-level system, is itself one of the elements of a wider system - international security. While national security remains central to peace and stability, there is growing need for recognition an expanded security paradigm. Today in the context of globalization, national security become closely related to global security and as the result the international dimension of national security, which has never been challenged by anyone, has increased many times.

40 YEAR VII, ISSUE 2, P.P. 40-43 (2023)
Global security is such a state of international relations that ensures the stability of the development of the world and regional communities, protection from external threats, the right to the free development of all peoples, a guarantee of sovereignty and independence of all officially recognized states. Simply global security is about protecting the global community from global threats. These threats create real challenges to all mankind and all states and if appropriate measures are not taken to eliminate them the unacceptable damage may arise first to the population of a particular state or then to international region. While national defense especially is concerned to provide security against others, global security “is security with others” [8]. Thus, maintaining global security is inextricably associated with the search for solutions or easing the pressure of global problems on humanity. Global problems should be considered as a real factor of modern world development. In modern world, due to urbanization, growing population in poor countries and technological progress, the shortage of fresh water and cyber – attack already have challenged the global security and stability.

3. Fresh water stress and global security

Today, humanity has acutely felt the consequence of all past and present errors associated with the wrong handling of nature. This is due to the fact that our contemporary world has one of the global environmental problems - the acute shortage of fresh water more than ever. Freshwater, in turn, is becoming a significant factor in world politics and remains one of the most important safety components in general, which is tied to three main components: energy, food and water. The lack of fresh water is a phenomenon familiar to mankind since ancient times. More than once, it became the cause of crises and social disasters. In traditional society, water shortages occurred on a local scale, and the crises caused by them remained local. Violent tensions over water are certainly nothing new, but because of overpopulation, climate change and rapid technological progress, they are on the rise. Anxiety about the growing shortage of drinking water is associated both with the effects of climate change and with human activities leading to a reduction in available water resources due to pollution and degradation of freshwater ecosystems, as well as the consequences of industrial production, uncontrolled urbanization and land use changes.

The desire to control natural resources, mainly hydrocarbon, may lead to military conflicts in the future. If until recently the states focused on the lack of fresh water for the needs of the population, agriculture and industry, now there is a growing interest in getting access to the vital waterways of the border states, which in the future will be able to ensure the security of the country and establish control over the neighbors and regions in general. In modern conditions access to international fresh water resources turn into a powerful tool of foreign policy of states, and international relations. Simple fresh water has become one of the most valuable resources in the world, for which regional or even global wars may erupt in the future. For these reasons in modern world the fresh water crisis is becoming global and its lack poses a serious threat to global security, equating to such problems as the rapid growth of weapons of mass destruction, terrorism, cyber-attacks on important infrastructure facilities, etc. [26]. “Stories of water shortages in Israel, India, China, Bolivia, Canada, Mexico, Ghana, and the United States are making headlines in major newspapers, magazines, and academic journals” [9].

Fresh resource such are rivers, lake, and ground water are often cross several national boundaries, or located between several countries. In a time of fresh water scarcity, misused transboundary water resources cause to spark conflict between countries. One of the critical, non-substitutable resources are transboundary rivers, which flow and fluctuate across time and space, for which legal problems and property problems should be considered vague and contradictory” [10]. Most of the major rivers on Earth are international and it should be recognized that majority continental countries share river basins. There are 261 international river basins in the world, which account for 60% of the global freshwater flow and “covering almost half of total the land surface of the globe” [11] with 145 countries and “about 40% of the world’s populations live in regions that directly compete for shared transboundary water resources” [12]. However, many of the most difficult problems are related to transboundary waters. The situation is complicated by the fact that several states which share the vital water arteries are not always able to find a common language in solving water problems. The main problem that the states located in the upper part of the watercourse consider water, like other natural resources, their own property and want to dispose of it at their own discretion, including as a commodity traded on international markets. The states located below tend to regard water as a natural gift of nature, to which they have a “natural” right and accuse upper countries for abusing fresh water usage. Therefore, the disagreement over using fresh water resources creates tension between more than 50 countries on five continents [13], which can lead to conflict. Such regions are the Nile River Basin, which is shared by 10 African states, the Jordan River Basin, the Aral Sea basin countries, Senegal River Basin, Juba River and Shebelle River Basins the Indus, the Gang and the Brahmaputra-Meghna Rivers Basins. The main big challenge to global security is that amount of fresh water remains or decrease due to climate change, but demand will raise as result of significantly raising of population and economic growth in mentioned area. It is estimated that by 2025 the number of people living in countries with water stress would rise to 3.3 billion [14]. This tension will be augmented by already existing political turbulence between Arabs and Israelis’, India and Pakistan, India and China, Egypt and Sudan. As example of a worst-case scenario, can be shown the arid and hostile Middle East, where armies have in fact been mobilized and shots fired over this scarce and precious resource [15].

4. Cyber - attack

The development of technologies in the modern world not only allows humanity to solve many problems of its progressive evolution, but at the same time, it creates new challenges and threats to domestic and global security. Today, the national infrastructure of any state is closely connected with the use of modern computer technologies and now “we are living in a society that is increasingly dependent upon information technology”[16]. The major infrastructures, which maintain security and stability of state, such are bank and air traffic systems, power station, transportation network, army and even defense systems connected to network. However, putting global information networks in its service, humanity did not foresee what possibilities for abuse such a rapid development of information infrastructure and technologies carries with it. The growth of information technology throughout the world has led to not only the rapid development and effective use of information networks in business and everyday life, but also the growth of new threats. Therefore, faced with a qualitatively new threat - this time in the global cyberspace - the world community was not ready to confront it. In this case, the safety of thousands of people, or countries may be dependent on several or even one criminals. One of this threat is a cyber - attacks, which nowadays considered as a main threat to security.

Cyber-attack is the consequence of emergence of a fundamentally new digital environment, cyberspace, which is not geographical in the generally accepted sense of the word, but nevertheless is fully international. The lack of borders in this so-called cyberspace has led to a dramatic increase in the number of threats, acts of cyber-terrorism and cyber-crime throughout the world. Today, victims of criminals operating in the information space can be not only people, but also vital structure of states. The boundaries of cyberspace are not reducible to the boundaries of the physical space; they are mobile and changeable, easily overcome physical barriers and geographical distance. It is united and scattered everywhere, at the same time it is not displayed on any world map and is indivisible by the borders of national states [17]. Therefore, anyone who possesses the necessary knowledge can
penetrate into any point of this space. At the same time, cyberspace represents endless possibilities for communication, due to the fact that communication in it is almost instantaneous. The possibilities of expanding the authorized access of cyber systems were not known before in any other point of cyberspace, they have not always good purposes. These opportunities are viewed as threats to the disruption of the normal functioning of cyberspace and, accordingly, all national infrastructure facilities that use its potential for ensuring work.

At the present stage, a cyber – attack should be qualified not only as an action against information resources, but also as a modern form of committing an act of aggression. Incidents in cyberspace already gone beyond the ordinary crimes and already became tool of war. This type of war focuses on the use of various forms and methods of disabling the state information infrastructure or on the use of information infrastructure to create an environment that leads to disastrous consequences for society and the state. Carrying out cyber-attack, information constituting state secrets can be stolen, the state’s livelihood system is compromised, and such serious sabotage as the destruction of the missile defence system “without having to bomb an adversary’s air defence system”[18] can be committed. The primary objectives of offensive cyber-attacks include the command and control systems of the armed forces, as well as critical infrastructure, which include the energy, banking and industrial sectors. Cyber-attacks on critical infrastructures are increasingly common today and have become a significant problem for various countries and organizations around the world. Critical infrastructure the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public’s health or safety and the failure of which in any case affects the welfare of the country’s citizens, defence and economic security [18]. Cyber-attacks by Shamoon, Stuxnet, and others have shown how vulnerable systems of critical infrastructures. In 2012, Saudi Aramco, the world’s largest oil company, fell victim to a targeted attack by Shamoon malware. Hackers gained access to the network through one the company’s computer and managed to prevent approximately 30,000 computers from starting.

Cyber-attacks, unlike other types of aggression, begin without prior announcement and come as a complete surprise while attacks on important objects can be carried out both from the territory of the attacker and from other territories. Moreover, the affected country may not even guess about it, because attack can take a long time to be destructive. In addition, could be said that the isolation of the object of attack from the Internet does not guarantee its security. An example, the Stuxnet the first worm designed to attack industrial control systems, discovered in June 2010 at the uranium enrichment complex in Iran’s Natanz. Using the SCADA system software to regulate the work of nuclear centrifuges, the Iranians mistakenly believed that the isolation from the Internet would provide the security of their plant. However, through this particular system the virus penetrated into the computer control centre of nuclear reactor, even though they were disconnected from Internet and cause the abnormal acceleration of centrifuge rotations, which eventually bring them down.

Attack on internet infrastructure Estonia in 2007 and Georgia information and communication systems during the Russian aggression in 2008 disconnected two countries from the Internet, led to the isolation of the Georgian government and Georgian people from the rest of the world. However, neither the events of the past, nor the real scandals associated with the intervention of Russian hackers in the American elections, fortunately, have not lead to the real cyber war. Potentially, the consequences of conducting aggressive actions on the Internet will be much more serious. A strike at the Bushehr nuclear power plant knocked out uranium centrifuges, and if his goal was a working nuclear reactor? Each state has countless vulnerabilities in its critical infrastructures, including nuclear power plants, gas and oil pipelines, chemical plants, power grids. To protect them all is very difficult and due to military, economic and political interconnections between countries, cyber-attacks will create big challenge not only to national, but global security as well. Because the allies’ responses to the attacks on Estonia demonstrated, “those countries would not remain detached and complacent as states or nonstate actors threatened the sovereignty of their allies by using the Internet as a weapon” [19, 24]. Today many countries understand to take necessary steps for the further development and improvement of their own cyber-warfare capabilities [19, 25] and have already included them to the national defence strategy [23].

5. Conclusion

“New concepts of security that addressed not only the military realities of the contemporary world but also the political, economic and social realities were developed” [21]. Many modern threats have a global, cross-border scale and threaten the security system, which previously was primarily focused on one state. The present life is characterized by the inhibition of all mankind in world processes, “whose course is accelerated by unprecedented scientific and technical progress, that has enabled us to travel both vicariously and instantaneously to almost all regions of the world” [22].

It is clear that disagreements over the distribution of water resources can be resolved exclusively through cooperation, as mentioned in numerous works of prominent scientists and politicians who call on the warring parties to embark on a peaceful path. Despite the complexity of the fresh waters problems, the available data suggest that disputes over water can be resolved through diplomatic means. Over the past 50 years, only 37 violent disputes over water have resulted in the use of violence and 21 use of military actions, whereas during the same period 150 contracts were signed with these resources. It is important that states realize that cooperation is much more profitable than conflict.

The danger of cyber-attack is that it does not have national borders and terrorist actions can be carried out from anywhere in the world. As a rule, it is very difficult to find an offender in the cyber space, since he acts through one or several dummy computers, which makes it difficult to identify and locate him. Although identifying an attacker in cyberspace is very difficult, revealing him should weaken other intents to attack. However, it is necessary to emphasize that due to large number of cyber-attacks and with the fact that these attacks can occur anywhere in the world and quickly, the most reliable way to protect is active cyber defence. The goals of this action are to destroy, nullify, or reduce the effectiveness of cyber threats. These include patrolling within networks, filtering known attacking IP addresses, and actively blocking malicious activity on the Internet. Therefore, the government should invest in technologies aimed at raising cyber security standards as well as in programs for the development of qualified personnel.

In addition, international legal activities aimed at combating cyber-attacks and conflicts over fresh water, has many obstacles due to insufficiently developed legislative framework in these areas. The whole world community should recognize the danger of cybercrime and fresh water stress, theirs cross-border nature and the impossibility of solving these issues by the forces of one state. The solution of these problems is possible only with active cooperation in taking the necessary technical measures and the development of uniform legislation. It is important to develop a dialogue between the state, the private sector and civil society, the outcome of which is likely to be ideas and options for defining technical and political solutions to the problem of increasing the resiliency of information systems and appropriate use of fresh water.
Acknowledgements

This publication was financed by the Ministry of Education and Science in implementation of the National Scientific Program – Security and Defence that is funded by Ministry of Education and Science of the Republic of Bulgaria in implementation of National Strategy for the Development of Scientific Research 2017-2030 and was adopted by Decision of the Council of Ministers No. 731 of October 21, 2021.

5. References