

## GLOBAL SECURITY TRENDS IN EURO-ATLANTIC AREA AND NATO NEW STRATEGIC CONCEPT

Igor Gjoreski<sup>18</sup>

Ministry of Defence of the Republic of North Macedonia

Zoran Nacev<sup>19</sup>

Faculty of Philosophy - Skopje, Institute for Security, Defence and Peace

**Abstract:** The states face complementary with both conventional and non-conventional threats to global security and peace. If yesterday someone thought that conventional conflict in Europe is not possible, today it has to think differently. Contemporary threats are in symbiosis with global security trends that significantly affect resilience and direct the security of countries. Terrorism, hybrid warfare, cyber threats, climate changes, icecaps melt and new transport corridors open, such as the Northern Sea Route in the High North, outer space, Emerging and Disruptive Technologies (EDTs), scarcity of energy the security, threats posed by Russia, a competitive challenge of China as well as EU energy and economic challenges, upgraded by the EU geo-strategic partnership, the current threat of more frequent periodic pandemic presence, are some part of the trends, challenges and threats which countries in the Euro-Atlantic area are faced. The fast changing and rapidly evolving nature is a common feature of modern security trends, challenges and threats. Dealing with indicated security trends and threats requires fundamental changes in the mind set of perception of security by redefining the concepts of security and reorganizing the global security architecture in Euro-Atlantic Area. States often face an invisible adversary who is both their ally and their common enemy. Hybrid warfare and cyber threats are specifics warfare in alternative space, where “the battles” being fought in cyberspace, through disinformation, disintegration and the abuse of Internet through malicious operations on social networks. These clashes are more like battles of narratives in cyberspace than real - time battles on the battlefield. The multitude of information, i.e. disinformation that is placed, confused the public, and no one knows where it is and what the truth is. The challenge of such warfare affects the security of states expressed through the implications of their defence, multiplying the instability that leads to new vulnerabilities and crises. Artificial intelligence, EDTs presents at the same time are both, a new opportunities and risk, and together they are a key element for maintaining the military and technological edge of the states. The control of outer space is becoming increasingly important for the security as well as for the economy, energy and prosperity of states with far-reaching consequences that can have a destructive impact similar as conventional warfare. Consequently, each international organization and institution builds its own concept and strategy to dealing with such security trends, challenges and threats. The report of the reflection group “NATO 2030: United for a New Era” is a NATO’s vision for dealing with such global security trends, challenges and threats in the next decade and beyond. This document

---

<sup>18</sup> Contact address: igor.gjoreski@mod.gov.mk

<sup>19</sup> Contact address: nacevz@fzf.ukim.edu.mk

provides guidance on how the Alliance will adapt to new global security trends, challenges and threats. The practical operationalization of the mechanisms for dealing with them is expected to be formalized with the New Strategic Concept of the Alliance, announced by the NATO Secretary General Stoltenberg to be adopted in mid-2022. The EU, for its part, has developed a Strategic Compass. Only the UN seems to be resistant on the change. However, the efficiency of new concepts and strategies for dealing with contemporary challenges remains to be tested in practice.

**Keywords:** security trends, challenges, hybrid warfare, climate changes.

## Introduction

Today, we face a much broader range of threats than in the past. This threats are asymmetric by its nature and hybrid by its manifestation. Threats are becoming more frequent, complex, destructive and coercive. In order to deal with them properly, it is necessary to make an in-depth analysis and assessment of all characteristic futures of the specificity and unpredictable security situation. One of the steps we need to take is to rethink our understanding not only of security as a concept, but also of an international security environment that is more complex and unpredictable than ever before. It should be born in mind that "the main characteristic of the current security environment is the re-emergence of geopolitical competition" (NATO 2030: United for New Era, 2020:16) between East and West.

The list of security challenges is long, longer than ever. And one threat is not excluding the other, because they are interconnected. Rising cyber and hybrid threats, terrorism, EDTs, climate change, mass migration, spread of weapons of mass destruction, pandemics, cyber – attacks and threats to energy supplies and environmental challenges with security implications are just some of them (What is NATO, 2020). The wide range of threats has forced states and alliances to build their own development strategy in their own way.

In general, such threats and challenges are too complex for any one country to deal with individually, which is why a collective response is needed to handle them expressed through the strengthening of political dialogue and cooperation among states. In the context of the above, the cooperation of North Macedonia is closely related to NATO member states and partner countries. The common response in dealing with trends, challenges and threats is related "by reinforcing resistance to its deterrence and defence posture, as well as supporting international efforts to project stability and strengthen security outside NATO territory" (What is NATO, 2020).

It is extremely important that the effects of deterrence and defence to be constantly upgraded and exploited. On February 24th, 2022, we witnessed the biggest security crisis since the end of Cold War. Even the most sceptic ones, who believed that war on Europe's soil, in the 21-st century is unthinkable, were proven wrong, unfortunately. Russia proved that the peace, is not for granted, and that rules- based international order can be, and is challenged. It should be borne in mind that although there are numerous mechanisms and tools, as well as open channels for communication, dialogue and diplomacy, unilateral decisions on violence and destruction can still not be sufficiently prevented.

In the interest of a better focus on contemporary trends, challenges and threats in this paper we will focus only on hybrid activities and cyber threats, climate change trends and challenges immanent to the energy-economic implications.

### **Hybrid Activities and Cyber Threats**

“The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a targeted adversaries by combining overt and covert military and non-military means. From one hand hybrid threats combine disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups, and use of regular forces, often over a sustained period of time and in conjunction with one another” (Dupuy and others, 2021). From other hand the Hybrid Warfare is a mixture of conventional and unconventional methods used against a much stronger adversary that aims to achieve political objectives that would not be possible with traditional warfare (Ilbiz & Kaunert, 2021). In fact, “in modern warfare, new technologies and strategies have created an evolution of the manner in which conflict occurs. The terms hybrid warfare, new generation warfare, and others have been used to describe warfare which has more than one facet. These facets include conventional, unconventional, cyber, and influence campaigns—such as disinformation spread on social media and targeted election interference” (Reilly III, 2020:17) and are deadly combination of hybrid warfare.

The potential adversaries use the full spectrum of military, political, economic and other tools to challenge institutions, and economies and to undermine our security. Today, the line between civilians and combatants is being blurred, through the use of proxies\* and private military companies, disinformation, and subversion. Hence, both military and non-military instruments of power take on another seemingly humane form of action. Additionally, the return of geostrategic competition has also brought a proliferation of hybrid attacks and cyber threat from everyone to everyone. Common denominator for hybrid and cyber activities is that they seek to weaken and compromised rule order based values. To counter hybrid activities, it is necessary to invest time in developing political and non-political mechanisms and tools. Those tools and mechanisms include a new approach to understanding, deterrence in the hybrid and cyber domain, and tackling disinformation and fake news. Also, according to NATO Secretary General Stoltenberg “A serious cyber-attack could trigger Article 5, where an attack against one ally is treated as an attack against all” (Stoltenberg, 2021). The serious a cyber-attack would have to be in order to trigger a collective response. Any response could include diplomatic and economic sanctions, cyber measures, or even conventional forces, depending on the nature of the attack (Pearson & Landay, 2022).

Basically, cyber-attacks and hybrid activities are not threat by it selves. They are tools used by hostile actors, undemocratic states and non-state actors. The main goal of such combined activities is weakening the resilience of the state. It is very difficult to find out who exactly is behind these activities because those who undertake such activities often use proxies to cover that kind of activities (Englund & Kathy, 2014).

---

\*A proxy means certain structures that perform certain tasks on behalf of other structures. It is a conflict between two parties or non-state actors, acting on the instigation or on behalf of other parties not directly involved in the specific actions.

The main proponents of hybrid warfare and cyber-attacks are undemocratic and authoritarian countries. This list includes countries such as Russia, China, Iran, Syria and North Korea. In support to its conventional military threat, Russia is deploying a broader hybrid toolkit including offensive cyber, state-sanctioned assassinations, and poisonings – using chemical weapons, political coercion, and other methods to violate the sovereignty of its opponents (NATO 2030: United for New Era, 2020:16). These countries are responsible for multiple hybrid and cyber-attacks not only on NATO member states, but also to other countries across the globe.

### *NATO and Hybrid Threats*

Hybrid activities in the NATO context are an integral part of the concept of deterrence and defence within the core task of collective defence. In order to successfully prevent hybrid activities NATO continuously works on the own capabilities development. Where additional effort is needed is where NATO should invest in building resilience through the development of strategic communication of all member states, strengthen diplomatic efforts and raise public awareness through enhanced education and training through its network of centres of excellence\*. In this context, and in line with the timely and rapid adoption of appropriate decisions, it is desirable to establish a Centre of Excellence for the fight against hybrid and cyber threats, especially in the context of the fight against disinformation and fake news. Another option is to expand the curriculum with new modules to raise awareness of the threat of hybrid warfare within the existing network of Centres of Excellence.

Namely, NATO, through its network of centres of excellence, plays an important role in that respect. NATO Centres of Excellence (COEs) Network as nationally or multi-nationally funded institutions that train and educate leaders and specialists from NATO member and partner countries, should assist in building resilience in society against threats, including hybrid threats and protection of civilians (ACT Centres of Excellence, 2018).

NATO Strategic Communication is a second very important aspect of consolidated action in relation to hybrid threats. STRATCOM means appropriate and coordinated use of NATO communication activities and capabilities in support of Alliance policies, operations and activities, and in order to achieve NATO goals. This requires a clear concept that will operationalize NATO Policy with a particular focus on the implementation through the planning and conduct of operations, training, education and exercises, lessons learned, as well as defence related capacity building activities.

Hybrid threats cannot be effectively suppressed and derogate by conventional means and methods alone. It is necessary to invest more in capacity building in diplomacy and to create mechanisms for cooperation. Defining clear goals and strategies with regard to hybrid warfare is crucial for building resilience and stability of states. Goals and strategies should be closely linked to cooperation in strategic communications and cyber security. This means strengthening Public Affairs, which includes civilian engagement of the Alliance through the media in order to timely, transparently, responsibly and proactively inform citizens about NATO policies, operations and activities against hybrid warfare. Complementary, the next area of activities cover Military Public Affairs, i.e. promoting the military objectives of the Alliance to the citizens in order to strengthen awareness and understanding of the military

---

\*More for Centres of Excellence see on [https://www.nato.int/cps/en/natohq/topics\\_68372.htm](https://www.nato.int/cps/en/natohq/topics_68372.htm)

aspects of the fight against hybrid threats. We cannot forget actions that covers NATO Information Operations, or NATO military advice and co-ordination of military information activities in order to create the desired effect of supporting NATO action against adversaries. The diplomacy is the key element and the key means to re-act against hybrid threats (Nikolov, 2018 p.105-106)

Hybrid and cyber activities there are nothing new for the Western Balkans. They are aimed primarily at hindering the European integration of countries and their destabilization. Also, through these activities, attempts are made to influence the election processes and public information by spreading disinformation and fake news. The aim of these activities is to have negative influence the trust of citizens, to destabilize governments, as well as to undermine Euro - Atlantic perspective and the credibility of both, NATO and EU. On political area, Russia with its hybrid activities and influence to the Western Balkans through proxy's tray to delay European future of the countries.

In order to prevent such activities, it is necessary for Western Balkans countries to establish their own legal framework for dealing with hybrid and cyber threats. There is also a need for enhanced coordination between military and civilian structures and enhanced cooperation with other security actors in the countries. The aim is to create appropriate mechanisms to deal with such malicious threats to the security of states and to ensure an appropriate level of cyber resistance. This implies broad inclusion and inclusiveness and application of a whole - of - society approach in addressing with such activities. Every security actor should know his place, role and responsibilities in the security and defence of the country from such malicious threats.

Therefore, by applying of this approach, the Government of Republic of North Macedonia in this domain adopted the National Strategy for Cyber Security of the Republic of Macedonia 2018-2022 and the Strategy for Building Resilience and Counter Hybrid Threats with an action plan in 2018 and in 2021 respectively. In the defence area, the Ministry of Defence adopted the Cyber Defence Strategy in early 2020. The Strategy on building resilience and countering hybrid threats with Action Plan combines the mechanisms for building the resilience of our country with the requirements and recommendations of the both, the EU framework for dealing hybrid threats and the NATO's Seven Baseline Requirements. The Strategy clearly defined the operational areas as well as the stakeholders, and their responsibilities, capabilities, lines of communication, as well as evaluation criteria. For successful implementation of the goals of the Strategy, closer cooperation has been established with both, NATO and the EU in the sharing of information in dealing with hyber and cyber threats (Strategy on building resilience and countering hybrid threats, 2021). Also, there is a plan Public Affairs Regional Centre which is NATO Partnership Training and Education Centre in North Macedonia to be transformed into a Centre for Tackling Disinformation as a NATO Centre of Excellence.

## **Climate Changes**

Climate change is perhaps the most important factor that affects and will increasingly affect future social life. Climate and nature changes will pose key questions for the future from a political, economic, social and environmental point of view. Their impact on the security issues of states is estimated to be exceptional and can be reflected in a number of ways. A

common denominator is that it acts as a risk multiplier. While it does not directly cause conflict but contributes to intensifying geopolitical competition among states and interacts with other pressures to influence security landscapes. Climate changes can also emerge as a security issue when it interacts with other pressures such as population growth, unequal economic development, social inequality, and competitions for resource constraints.

The implications of climate change include drought, extreme hot and dry conditions, soil erosion and marine environmental degradation, deforestation, increasing the frequency and destructive power of hurricanes and tornadoes, polar icecaps melting and rising sea levels and so on. The forecast is that “in a business-as-usual scenario, temperatures of air could rise by 4°C by 2100, with precipitation levels falling by 20-50% and the number of drought days increasing by 20%” (Rüttinger and others, 2021:9). Such extreme weather conditions will be life-threatening not only to the citizens, but also on the military set-up and the need to change the doctrines as well as to the ability to change of military infrastructure, equipment and military to conduct operations in the extreme hot and dry weather conditions.

### *NATO and Climate Changes*

No country is resistant to climate change, nor organization or institution. The effects of climate change are shaping and will continue to shape the geopolitical environment and security environment of countries (NATO 2030: United for a New Era, 2020:14) including the NATO members. If manifested simultaneously and on a larger scale, climate change can affect the behaviour of states and foster contested security and conflict tensions. In order to prevent climate change side effects to security in a timely manner, NATO needs to reflect the influence on the realities in the development of the Alliance’s future strategic documents. This includes building appropriate long-term response mechanisms. Some countries took such steps more than a decade ago. For example, since 2010, official documents, political statements, and actions already taken show that the most of the Nordic countries address the effects of climate change on their region’s security in specific policies and national security concepts. They confirmed that “Climate change is a long-term process that will trigger a range of multi-dimensional demographic, economic, geopolitical, and national security issues with many unknowns and significant uncertainties” (Romig Jr., Backus, and Baker, 2010:3).

Climate change is one of the key elements defining contemporary challenges of our times. It is a threat multiplier and holds serious implications for the security and economic interests of all thirty members of the Alliance (NATO Climate and Security Action Plan, 2021). Climate change worsens existing social, economic and environmental risks that can fuel unrest and potentially result in conflict (Climate Changes and Security, 2017-2021). It is likely to accelerate resource scarcity and global food and water insecurity. Climate change is a reality and it may produce new theatres of competition which will emerge as icecaps melt and new transport corridors open that’s go through North Sea, such as the Northern Sea Route, Northwest Passage, Transport Sea Route, and Arctic Bridge in the High North, which geopolitical rivals are seeking to control and exploit (NATO 2030: United for a New Era, 2020:19). The new sea routes through the Arctic are considerably cheaper, shorter, and faster than the traditional ones. These waters are expected to be open very soon for shipping and for a much longer period of the year than before. On the picture below you can see High North Routes between Asia, North America and Europe.





Source: The Geography of Transport Systems. <https://transportgeography.org/contents/chapter1/transportation-and-space/polar-shipping-routes/>

To prevent all this issues and to be prepared for next decade and beyond, NATO is already works on it to include climate change and other non-military threats, such as pandemics, in NATO planning preparations for response and solutions to the new reality, building on resilience and crisis management. Timely inclusion of climate change in these planning processes will allow NATO to adapt more quickly to the future reality. Also the allies will have enough time to prepare, adjust and equip their forces in a timely manner to conduct operations in changing climatic conditions.

In fact, climate change has had the strongest impact on the militaries to carry out their tasks. It is therefore necessary for NATO to ensure that its command and force structure, its installations and deployment are fully prepared to act in a situation of changing and changing conditions. In doing so, NATO has to work on implementation of the Agenda of Climate Change and Security. Implementation of this Agenda provides a 360-degree approach and encompasses measures to increase both NATO's and Allies' awareness of the impact of climate change on security (Environment, climate change and security, 2021). Additionally, is necessary to work on reducing the environmental impact of military activities in order to adapt and become more friendly to the environment and resilient in responding to the security challenges posed by environmental change.

To achieve this, on long – term, NATO should set a standard on how to improve energy efficiency in the armed forces, to reduce emissions from the military sector and contribute to goal of zero carbon emissions by 2050. Also, it is necessary for NATO revision of the 2014 Green Defence framework taking in account growing “challenges and emerging green technologies and make more strategic use of the Science for Peace and Security Programme in order to develop and implement better green military technology” (NATO 2030: United for a New Era, 2020:14). Allies should plan to invest in green technologies for the ultimate purpose of improving military effectiveness and maintaining competitive advantages as well

as to adapt its armed forces to a security environment altered by the effects of climate change.

Although climate change is not NATO's primary area of action, "for better understanding climate change, NATO need to establish Centre of Excellence on Climate and Security or adding climate to the NATO Centre of Excellence on Energy Security. The scientific approach to understanding climate changes will help the Alliance better to understand the implications of climate change, and adapt its strategies and capabilities accordingly, and to remain an effective security provider in the 21st century" (NATO 2030: United for a New Era, 2020:41).

Republic of North Macedonia like all other countries it feels the impacts caused by climate change. North Macedonia is party to the Paris Agreement and has ratified the Convention on Long-range Trans boundary Air Pollution. North Macedonia has also prioritized climate change in the efforts towards implementing the 2030 Agenda for Sustainable Development and the Sustainable Development Goals (SDGs), including SDG13 on Climate Action. At the time of preparing this paper, the Fourth National Climate Change Plan was being prepared by the Government and was expected to be adopted in June 2022

Complementary, North Macedonia is committed to apply EU energy rules and principles. This includes drawing up National Energy and Climate Plan (NECPs), which would help us support long-term energy and climate change targets, as well as transpose the EU Energy acquis into respective legislations. North Macedonia is already aligned with the energy efficiency acquis, and has adopted an Energy Efficiency Law in early 2020.

### **Energy Dependence and Stability, and Economic Security**

Security has always been addictive and a cause for war for territory, resources and energy. The impact of economic security on a national and international level is closely linked to both energy dependence and resource scarcity. The dependence of countries on energy resources from third countries has a long-term impact on security on national and international level. Lack of resources primarily affects economic stability, and then reflects on political, defence, military and other areas of social life. Contemporary economy is based on the use of primary energy resources (gas, oil, hydro, coal and nuclear energy (Diaconu, 2016). The transition from traditional to renewable – green resources is long-term and requires large investments whose return on capital is far lower compared to the use of traditional energy sources. Worldwide consumption of energy resources has seen an upward trend.

Energy dependence was strongly felt in 2021 when countries began to recover from the COVID 19 pandemic. Increased demand for resources has led to rising prices for raw materials and commodity prices. The entry of Russian troops into Ukrainian territory in February 2022 has increased this trend of resource and products prices rising, but also endangered the economic security of Western European countries. In order to reduce the effect of energy dependence on Russia, European countries have begun to invest intensively in alternative sources of energy supply and especially in renewable - green sources. Unequal access and uneven energy supplies have made them the same instrument of power of states. The past and the present have confirmed that it can generate negative effects, i.e. tensions, economic and financial crises, and even military conflicts on medium and long term. Adverse



effects can jeopardize not only the security of states but also the security of a rule-based international order.

Energy, water or food, once they become insufficient for some countries, the stakes will be possible disputes and therefore can challenge governments and can generate risks and threats to the security of the states (Diaconu, 2016). Economic and technological development determines progress globally as well as economic power of the states. In these circumstances, the strategic raw materials depend on import, supply security threat can challenge national security of the state. Economic security of the states can be challenged by uncontrolled mass migrations followed by tensions and conflicts on the regional or global level.

### *NATO and Energy Security*

Perhaps in the NATO context, we can talk more about energy stability than energy security. However, if this is seen from the perspective of using energy as a means of hybrid warfare, energy becomes a key factor in security. Energy security has been a key strategic factor particularly pronounced since the start of the 20th century. The events from the past years show that it has become a major and growing challenge for the Alliance in an era increasingly dominated by hybrid warfare (Dupuy, and others, 2021). Energy security plays an important role in the overall and common security of NATO Allies. The importance of energy security was noticed at the NATO Summit in Brussels in 2018: “A stable and reliable energy supply, the diversification of routes, suppliers and energy resources, and the interconnectivity of energy networks are of critical importance and increase our resilience against political and economic pressure. While these issues are primarily the responsibility of national authorities, energy developments can have significant political and security implications for Allies and also affect our partners” (Brussels Summit Declaration, 2018:78).

For NATO Energy security is a vital element of building resilience and more important due to the emerging security challenges, such as cyber and hybrid threats to infrastructure. It means that cyber threats, with a focus on the energy sector as the main goal, have been growing, with the energy sector a major target (Grubliauskas and Rühle, 2018). Given that disruption of energy supply can affect the security of states, this is one of the most emphasized issues of primary importance to the governments of states. Power outages could also affect the security of NATO countries, and have an impact on NATO’s military operations. That is why NATO regularly holds consultations on this topic, especially related to enhance Allied awareness and resilience (NATO’s role in energy security, 2021).

NATO seeks to enhance its strategic awareness of energy developments with security implications; develop its capacity to support the protection of critical energy infrastructure; and ensure reliable energy supplies to the military. In times of the global energy transition, energy efficiency and innovative energy solutions help the military to become more sustainable, while maintaining operational effectiveness (NATO’s role in energy security, 2021). Since 2014, NATO has prioritized enhancing energy efficiency in the military. The realization of this priority is also related to the efforts for improvement of the technological and the process of energy use, by reducing the energy consumption of military vehicles and camps, allies hope to make the energy sector not only resilient but also sustainable (Bartuška, Lang, And Nosko, 2019).

Energy dependency is a key challenge for Western Balkans including North Macedonia. Countries in this region have low energy production that does not meet their needs and are dependent on imports. On a positive note, the energy dependence of the countries of this part of Europe is only 1% of Russia's exports and they are not of strategic interest to Moscow. This means that Russia cannot further destabilize them by using energy as a security policy tool. However, all countries have to work closely to minimize this dependency as soon as possible, and to reduce the impact of this challenge and threat to our countries.

## Conclusion

Dealing with contemporary security challenges is an ongoing process that requires a jointly coordinated response through appropriate mechanisms and activities. Hybrid warfare and cyber threats are complex challenges to which the Alliance pays significant attention and invests in the development of tools to tackle them. The importance is so great that NATO believes that cyber-attacks may be a trigger of Article 5 of the Washington Treaty. That means collective defence and a synchronized response at the diplomatic, intelligence and military levels. Tackling hybrid threats is not possible without a strengthened role of diplomacy, strengthened strategic communications and strong Public Affairs. The Alliance's response should be in line to strengthen its capabilities for respond, defence and deterrence for collective defence, cooperative security and crisis management. NATO needs to build close relations and partnerships not only in the transatlantic area but also beyond with other democracies to protect its interests. In such an approach, the Allies should take into account the threats and challenges that are not geographically restricted or limited by state borders, such as hybrid and cyber threats, emerging and destructive technologies, climate change, but also new security issues that strongly affect the security of countries such as energy dependence, production of food and others.

It is also necessary to monitor the integrated approach to crisis management as well as enhanced cooperation with other international organizations and institutions, in particular with the UN, the EU the OSCE and other organizations. NATO needs to pay attention of the training, and investment in its forces and in building capacity which will help in dealing with hybrid warfare and cyber-attacks. This will increase resilience and increase the ability to intercept, confront, deal with and overcome the consequences.

North Macedonia's contribution to the fight against hybrid threats and cyber-attacks should move in the direction of developing Strategic Communications networked in all government institutions and state bodies, which will simultaneously be synchronized with those of NATO and will build national capacities for appropriate response and resilience. One development could be the transformation of the current Regional Public Relations Centre into a NATO Centre for Excellence in Combating Hybrid Warfare and Disinformation.

Climate change and global warming are a growing global security trend that countries cannot tackle individually. They are a growing trend that affects all countries without exception and in dealing with them a collective response is necessary. This means adhering to the signed conventions on climate change and adopting them by those countries that have not adopted them, but also commitment in their implementation. NATO as an interesting side needs to review the 2014 Green Defence Framework and step up the application of green technologies in the production of military equipment and to increase the energy efficiency of

military infrastructure. Climate change is affecting all, the states and collectivises and all of us has to contribute in preventing it and reducing its effects to enable decent for the future of our generations.

Energy dependence is a trend on which affects all countries without exception. There is no state that can provide all energy and products independently. The growing demand for energy also causes competition between countries and an increase in the price of energy and products. Fewer countries control certain energy sources such as oil, natural gas and coal and they dictate the price. The dependence of countries on these energy sources allows countries that control energy, and in some situations they try to extort strategic priorities and concessions from countries that depend on these energy sources. There are still areas that have not been explored, and which are known to be rich in natural energy, such as the Arctic. With the melting of the Arctic polar caps, a new opportunity opens up for geopolitical competition between states and a struggle for control of those resources. But let us not forget that the struggle for energy control, whether in the Arctic or elsewhere in history, has caused conflicts and could lead to serious conflict between nations in the future.

## References

- Allied Command Transformation, "Centres of Excellence," 2018. Accessed April 5, 2018, <http://www.act.nato.int/centres-of-excellence>.
- Brussels Summit Declaration, 2018. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018. [https://www.nato.int/cps/en/natohq/official\\_texts\\_156624.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en)
- Climate Change and Security Strengthening Resilience to Climate-Fragility Risks, UN Environment. [https://postconflict.unep.ch/publications/ClimateChange\\_Security\\_twopager.pdf](https://postconflict.unep.ch/publications/ClimateChange_Security_twopager.pdf)
- Diaconu, Bebe I. (2016). Risks, Threats and Vulnerabilities to the Security of the Euro-Atlantic, International Scientific Conference "Strategies XXI"; Bucharest Vol. 2: 193-205. Bucharest: "Carol I" National Defence University. (2016)
- Dupuy, C. Arnold, Nussbaum, Dan, Butrimas, Vytautas, Granitsas, Alkman. 2021, Energy security in the era of hybrid warfare. NATO Review, 13 January 2021, <https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html>
- Englund, Will & Kathy Lally. 2014. Ukraine, Under Pressure from Russia, Puts Brakes on E.U. Deal," The Washington Post, Nov. 21, 2013;
- Environment, climate change and security, 2021. NATO, Last updated: 03 Dec. 2021, [https://www.nato.int/cps/en/natohq/topics\\_91048.htm#:~:text=In%20March%202021%2C%20NATO%20Foreign,of%20climate%20change%20on%20security](https://www.nato.int/cps/en/natohq/topics_91048.htm#:~:text=In%20March%202021%2C%20NATO%20Foreign,of%20climate%20change%20on%20security).

- Ethem Ilbiz&Christian Kaunert, 2021. Cyber-attacks: what is hybrid warfare and why is it such a threat? Published: July 21, 2021 in <https://theconversation.com/cyber-attacks-what-is-hybrid-warfare-and-why-is-it-such-a-threat-164091>.
- Grubliauskas, Julijus and Michael Rühle (2018). Energy security: a critical concern for Allies and partners. *NATO Review*, 26 July 2018, <https://www.nato.int/docu/review/articles/2018/07/26/energy-security-a-critical-concern-for-allies-and-partners/index.html>
- Marson, James et al. 2014. Ukraine President Viktor Yanukovich Driven From Power," *The Wall Street Journal*, Feb. 23, 2014.
- NATO 2030: United for a New Era. (2020). "NATO 2030: United for a New Era, Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General" Brussels: NATO, 25 November 2020.
- NATO Climate Change and Security Action Plan 2021. NATO Last updated: 14 Jun. 2021. [https://www.nato.int/cps/en/natohq/official\\_texts\\_185174.htm](https://www.nato.int/cps/en/natohq/official_texts_185174.htm)
- NATO's role in energy security, 2021. Last updated: 23 Jun. 2021. [https://www.nato.int/cps/en/natohq/topics\\_49208.htm](https://www.nato.int/cps/en/natohq/topics_49208.htm)
- Nikolov Orlin.2018. Building Societal Resilience against Hybrid Threats, *Information & Security: An International Journal*, Volume 39, Issue 1, p.91-109 (2018)
- Pearson, James & Landay, Jonhatan. 2022. Cyber-attack on NATO could trigger collective defence clause – official. Reuters, February 28, 2022, [https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/#:~:text=LONDON%2FWASHINGTON%2C%20Feb%2028%20\(spill%20over%20into%20other%20territories](https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/#:~:text=LONDON%2FWASHINGTON%2C%20Feb%2028%20(spill%20over%20into%20other%20territories).
- Reilly III, Raymond L. 2020. Strategic Competition and Escalation Management in the 21st Century: Russian Hybrid Warfare and China's Rise. (PhD). Advisor: Dr. David Goldfischer Degree Date: June 2020, the Faculty of the Josef Korbel School of International Studies University of Denver.
- Romig Jr. A. D., George A. Backus, and Arnold B. Baker, (2010). A Deeper Look at Climate Change and National Security. SANDIA REPORT, March 2010, <https://www.osti.gov/servlets/purl/1010413>
- Rüttinger, Lukas; van Ackern, Pia; Gordon, Noah; and Adrian Foong. Regional Assessment for South-Eastern Europe. Security implications of climate change. (Berlin: adelphi; Vienna: OSCE, 2021)
- Stoltenberg, Jens, 2019. NATO will defend itself, Article by NATO Secretary General Jens Stoltenberg published in Prospect's new cyber resilience supplement, 27 Aug. 2019, [https://www.nato.int/cps/en/natohq/news\\_168435.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en)

- Václav Bartuška, Petr Lang, Andrej Nosko, 2019. The Geopolitics of Energy Security in Europe. Carnegie Europe, November 28, 2019. <https://carnegieeurope.eu/2019/11/28/geopolitics-of-energy-security-in-europe-pub-80423>
- What is NATO, why does it still exist, and how does it work? (2020). Premiered April 8th, 2020. <https://www.youtube.com/watch?v=snXhtOpSXtl&t=239s>
- Strategy for Building Resilience in Dealing with Hybrid Threats, 2021, Government of the Republic of North Macedonia, <https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf>