REVIEW ARTICLE ADRS

Ann. Disaster Risk Sci. 2019, 1-2, 37-47

THE SECURITY CHALLENGE OF DISRUPTIVE TECHNOLOGIES

Dario Malnar[1], Josip Olujić

[1]Croatian Defence Academy "Dr. Franjo Tuđman"

Abstract

Dynamic changes that characterize the modern security environment have been significantly driven and shaped by the rapid pace of technological development. Of particular importance is the emergence and development of technologies that have caused a revolutionary change to the character of the security environment - disruptive technologies.

The paper analyzes disruptive technologies aimed at the automation, acceleration and autonomy of the data processing process, decision-making abilities, and actions independent of the human factor. These technologies affect all spheres of social life, and subsequently security.

Unlike previous disruptive technologies that influence security driven by the states and their defense sectors, recent technologies are being predominantly developed in the private sector. This fact leads the countries to become dependent on the private sector, and poses significant challenges in identifying threats, their content and possible responses. Technologically less developed countries are particularly vulnerable.

Based on the hypothesis of how disruptive technologies influence the design of security environments, an analysis of strategic security documents of Croatia, the USA, Russia, China, NATO, the EU, and the states from the Croatian neighborhood has been conducted to determine if these countries recognize disruptive technologies as a security threat and how they approach them.

The research has shown that Croatia does not recognize disruptive technologies as a specific threat. The analysis also indicates that, in the case of technologically less developed countries, such as Croatia, security communities such as the EU or NATO provide a platform for responding to those threats.

Keywords: technological development, disruptive technologies, national security, Republic of Croatia

Address for correspondence: Dario Malnar, Croatian Defence Academy "Dr. Franjo Tuđman", e-mail: malnar.zg@gmail.com

1. INTRODUCTION

The general characteristics of the modern world are rapid, dynamic and very diverse changes in all aspects of social life. These are determined primarily by the development of technology that provides the infrastructure for these changes. The dynamics and trends observed at the general social level have a strong impact on the military and security field. A conclusion can be drawn that "the last twenty years have been the period of constant and dynamic changes in the field of security in all aspects, ranging from various threats to participants and referent objects of security at the national and international level." (Tatalović, Malnar, 2016). The military, defense and security sectors are the ones which, have historically generated and encouraged significant technological innovations that were subsequently applied in the civil sector. Besides giving the dynamics and reach to existing threats, technological development multiplies them and generates new threats. It also provides platforms and instruments to counter security threats. Particularly important are the advent of new technologies and the manner in which those technologies are used, such as nuclear technology, which significantly and unexpectedly change the character of the security environment - disruptive technologies - and determine new approaches to the understanding of security and the way in which security policies are defined.

There are, of course, numerous views on the relationship and interdependence between technology and security. American political scientist Bracken

claims that "one common view, particularly in political science and social science departments, is that technology doesn't make much difference at all - we should think more about strategy and be smart, rather than buy technology to gain capabilities we would not otherwise have" (Bracken, 2019). On the other hand, security practitioners from the political sphere have completely opposite views. Vladimir Putin, referring to artificial intelligence, asserted that "artificial intelligence is the future, not only for Russia, but for all humankind. (…) Whoever becomes the leader in this sphere will become the ruler of the world" (CNN, 2017). The European Commission emphasizes another feature of artificial intelligence that other technologies did not have, for instance nuclear technology despite all its significance,which is that "like electricity in the past, artificial intelligence transforms our world" (European Commission, 2018: 1). The potentials and significance of artificial intelligence are also confirmed by the ambitions of China. In its development plan for artificial intelligence, China identifies artificial intelligence as a critical technology due to its military and economic potential. Based on the assessment that "rapid development of artificial intelligence will thoroughly change social life and the world", China defines the development of artificial intelligence as a "national strategic interest" with the goal of "leadership at the international level by 2030" (PR China State Council, 2017a).

Potentials of new technologies and ambitions of individual states can generate new threats, but at the same time, they open up new opportunities in countering threats, both emerging and traditional. Based on such claims, the NATO sets the goal „ to harness emerging and disruptive technologies at a speed of relevance to thwart adversaries and protect NATO's populations" (NATO Industry Forum, 2018: 1). However, as with all novelties, access to new technologies is neither straightforward nor linear. Even among the NATO Allies, there are disputes and differences. This is confirmed by a dispute between the US and Germany after the Trump administration warned Germany that "if it allows China's tech giant Huawei to enter the German market, security cooperation and even intelligence sharing could be at stake" (VOA, 2019). Dilemmas about new technologies and potential suppliers also exist in the internal politics of states. In the UK, for example, the defense secretary Gavin Williamson was fired by the British Prime Minister Theresa May over the leaking of a key decision from a UK National Security Council meeting related to the Chinese telecommunications company Huawei, which determined that the British prime minister would allow Huawei to build the British telecommunications network (CNN, 2019).

Modern technological development creates complex security relationships in which countries face both the challenges of following technological development and countering threats, especially small and technologically less advanced countries such as Croatia.

In order to define the responses to security threats and challenges triggered by technological developments, the paper analyzes key strategic documents for the security of the US, Russia, China, Croatia and member states of theNATO and the EU to determine whether and how these entities identify disruptive technologies as a security threat and how they approach them.

2. DISRUPTIVE TECHNOLOGIES - CHARACTERISTICS AND HOLDERS

In discussing technologies and their impact on the security paradigm, we distinguish two fundamental technological areas, namelysustaining and disruptive technologies. Certain technologies reinforce the power of the industry leader. Others disrupt that position. Sustaining technologies are those that support the day-to-day processes, products, services, capabilities or power of the industry, the military, etc. They evolve and improve evolutionarily (Bracken, 2019). O the other hand, disruptive technologies are those that bring new technology and / or enable or enhance a product,

service, ability or power in an unexpected way or bring an unexpected change in the use of existing technology (e.g. tactics of using tanks by the German military in World War II). In the business domain, disruptive innovations create a new market and value networks,eventually disrupting an existing market and value networks anddisplacing the leading firms, products, alliances and business models on the established market (NATO, 2018: 18). It is about the "technology that enhances a product or service in a way that the market does not expect"(Bidwell, MacDonald, 2018). Disruptive technologies are therefore technological innovations and ways of using them that significantly change the paradigms of relationships in a particular sphere. Unlike sustaining technologies, disruptive ones have a revolutionary character in their appearance and the effect on the environment. In this way, disruptive technologies significantly change the character of the security environment, the understanding of security, and the manner in which security policies are defined.

It should be emphasized that the disruptive nature of a technology can be seen from a number of levels, those international, regional, and even national ones.

Furthermore, the above-mentioned controversy over the installation and use of technology offered by the Chinese technology company Huawei raises several significant questions regarding technologies, especially disruptive technologies.

The first and very important, which suggests new relations in the sphere of security is that unlike earlier periods when the carriers of technological developments, especially those with security consequences, were in the defense and the state sector, nowadays the holders of development are in the private sphere, "innovation happens in research laboratories, industry and universities" (Mitchell, 2009). This fact produces a very complex relationship between the states (national interest) and the private sector (business interest) with regard to the developments.. Civilian technology has evolved so much and surpassed military that the military sector "since the late 20th century, (...) has been increasingly seeking the development of new technologies by the civilian sector in order to gain technological advantage" (Mitchell, 2009). Private companies, led by high tech companies, play an important role in technological development, and their financial power goes beyond most countries. These companies are international and operate all over the world. It is often very difficult to determine the ownership structure. They provide their services on a commercial supply and demand basis that strengthens the possibility of uncontrolled proliferation of technology. Global companies and organizations have become so powerful that they can even condition states. This reduces the possibility of state control and intervention and sets in motionthe threat of technology proliferation towards individuals and organizations which are the carriers of various threats, such as terrorism or organized crime. In this way, the dependence of states on the private sector is reinforced and competition is transferred to the non-military sector.

The second is that the development of these technologies, and even the leadership in the development of particular technologies, also occurs in countries with questionable democratic potential or countries that are not democratic, such asChina. This opens a new area of threat through the exploitation and misuse of private companies by the state, including intelligence and interests. The confirmation of such concerns can be found in the case of China. Specifically, Article 7 of the Chinese National Law on Intelligence states that "all organizations and citizens shall, in accordance with the law, provide support and assistance, co-operate with the State Intelligence Service, and keep secret national intelligence activities known to them" (PR China National People's Congress, 2017b). China is thus in a comparative advantage over democratic countries that lack such opportunities.

We can talk about three groups of threat carriers associated with disruptive technologies: states,

especially those dominant in the development of particular technologies, dominant and leading private corporate entities, non-state actors, organizations and individuals.

2.1. Modern disruptive technologies

Although the term *disruptive technologies* itself is relatively new, first mentioned in 1995 at Harvard by Joseph L. Bower and Clayton M. Christensen, technologies with disruptive characteristics can be observed throughout human history. One of the more prominent historical examples of a disruptive technology is the emergence of nuclear weapons. This technology has been defining the global security environment, security policies, and international relations in general, ever since its first appearance in the mid 20th century.

The technology that has characterized the 21st century is undoubtedly the Internet. With its appearance, the Internet has met the criteria for being a disruptive technology with its accompanying effects. The advent of the Internet has had an enormous disruptive impact. The Internet has enabled global communication connectivity, an unprecedented potential for information transfer, "the Internet enables information to be shared, modified, interpreted and developed by everyone (...)" (Mitchell, 2009). The Internet has ultimately enabled globalization as a process of redefining global international relations, thereby influencing the perception and definition of security policies. The Internet itself is no longer a disruptive technology today. It provides a platform and infrastructure necessary for the development and application and operation of new disruptive technologies.

What in the Cold War was an arms race, in today's world it is certainly a race for the development of an advanced non-military technology that would allow an entity possessing or developing it to dominate the world.

Developing technologies that have the potential to become disruptive technologies, and as such may represent security challenges and threats in the future primarily include: artificial intelligence, 5G networks, quantum computing, 3D printing, the Internet of Things, nanotechnology, hyper velocity, biotechnology, and robotics.

This analysis will primarily focus on data-related technologies that enhance data collection, processing and use through multiplication of quantity, speed, automation and autonomy. Central is the development of artificial intelligence, as a technology that will largely represent the precondition and platform for the development of other technologies. Therefore, the development of artificial intelligence is the basis for gaining dominance on the global level.

Artificial intelligence (AI) refers to systems that exhibit intelligent behavior by analyzing their environment and taking action - with a degree of autonomy - to achieve specific goals (European Commission, 2018).

The scope of application for artificial intelligence is apparent from the Chinese Plan for the Development of Artificial Intelligence. It includes setting up an open and coordinated artificial intelligence science and technology innovation system encompassing big data intelligence theory, cross-media perceptual computing theory, hybrid augmented intelligence theory, group intelligence basic theory, coordinated control and decision-making theory, advanced machine learning theory, brain-like intelligence computing theory, quantum intelligence computing theory. Likewise, knowledge computing engine and knowledge service technology, cross-media analytic reasoning technology, key group intelligence technology, new structure and new technology of hybrid augmented intelligence, autonomous man-less system technology, virtual reality intelligence modeling technology, intelligence computing chip and system and natural language processing technology are all included in the system (PR China State Council, 2017a).

The development of artificial intelligence generates positive and negative consequences. The positive side undoubtedly involves the processing

and derivation of meaning from a large number of unstructured data, accurate identification of processes and phenomena, advanced generalization and visualization of content, links, risks and threats, an increase in the capacity to identify counterfeit and false data, etc. At the same time, from a security standpoint, there are also numerous concerns related to strengthening the ability to influence thedemocratic processes, economic security and social stability,the structure of employment, the breach of privacy or to enable the advanced abuse of autonomous weapons. It could raise the potential for the development of biotechnological threats, cyber threats, creation of virtual reality and virtual identities through the generation of fake news, information, and falsification of media records, and advanced forms of espionage. It could lead to automation of threats.

Artificial intelligence gains its full potential through interconnection with Internet data transmission. Therefore, the development and installation of 5G networks is imposed as a precondition and almost a form of critical infrastructure for the development of the full potential of artificial intelligence. 5G networks are high frequency networks that increase the connectivity of the device by both fifteen times in terms of the number of connected devices, speed and reduction of response time. This creates new opportunities for the development of other technologies such as robotics, laser technologies and finally the Internet of Things that acquire the full scope of disruptiveness through synergy.

3. DISRUPTIVE TECHNOLOGIES IN STRATEGIC SECURITY DOCUMENTS

National security strategies as the basic strategic security documents of a given state are the best indicators of how states define threats and how they develop the concept of national security policies based on defined threats.

An analysis of public discourse shows that the major global powers that house the world's leading technology companies are giving greater importance to disruptive threats than smaller, poorer, and technologically less developed countries. The Russian and Chinese President's assessments of the importance of artificial intelligence are an example of this. Another example is also the discussion between the US and European partners about the previously mentioned Huawei company and concerns that their technology could be used for spying by the Chinese government.

3.1. The United States of America

The US national security strategy places technology on an equal footing with political, military, and economic factors, demonstrating the importance given to technology in the context of national security. It starts with the assessment that the US military is still the strongest in the world, while also noting that the US advantage is diminishing as rival countries modernize. It is estimated that "(…) access to technology empowers and emboldens otherwise weak states" (White House, 2017: 3). This is followed by an assessment that "technology is an opportunity for strengthening the leading position that the United States have in the world, but also a threat that other countries will develop and threaten the position of the United States and their national interests. Losing our (US) innovation and technological edge would have far-reaching negative implications for American prosperity and power (White House, 2017: 21)".

The US National Security Strategy mentions and recognizes new technologies that will be of paramount or even crucial importance in the near future for gaining or retaining the leading position in the world, with particular reference to "data science, encryption, autonomous technologies, genetic engineering, new materials, nanotechnology, advanced computing technologies, and artificial intelligence" (White House, 2017: 20). These are potentially disruptive technologies and therefore, given the disruptive nature of these technologies, the measures offered by the strategy should also be considered in that respect: preventing the fall

of sensitive technology into the hands of hostile actors (terrorists and US enemies), capitalizing on new technologies, retaining the ability to produce high technology, overseeing the development of military technologies outside the defense sector in private companies, paying attention to China and the development of Chinese technology.An important tool defined by the strategy for the purpose of preserving security is that the US "will encourage scientists in the government, academia, and in the private sector to achieve advancements across the full spectrum of discovery, from incremental improvements to game-changing breakthroughs" (White House, 2017: 20).

3.2. Russia

Like the US, Russia has recognized the importance of technology as a factor of national security and national interests. The Russian strategy is somewhat different from the United States' one in form, but it mentions technology as an important item in almost all chapters and fields. The strategy starts with an assessment of how technology will affect both the present and the future and emphasizes that the "new forms of unlawful activity are emerging, particularly those involving the utilization of informational, communications and high technologies" (Russian Federation President, 2015: 5). The strategy places science and technology among the primary national interests to be pursued for the advancement of the country. As in the case of the US, Russia's national security strategy mentions technologies that are given the highest regard in the security context, stating that to achieve its goals it is necessary to ensure "the development of promising high technologies (genetic engineering, robotic engineering, biological, information, communications and cognitive technologies, nanotechnologies, and convergent technologies that resemble Nature)."(Russian Federation President, 2015: 17).

As with the US, although not explicitly stated, these are technologies that by definition fall within the scope of those we have defined as disruptive.

Although in its strategy Russia has not fully addressed the potential threats posed by disruptive technologies and the ways they could affect national security and national interests, and thus does have not have fully developed the ways of responding to potential threats, science and technology have been placed as a high priority. Special emphasis is put on "the development of cooperation between educational organizations and scientific research centers and industrial enterprises and the practice of co-founding by the state and by enterpreneurs for long-term (…)" (Russian Federation President, 2015: 17).

3.3. China

As a direct competitor to the US and Russia, China has gradually grown and made significant advances in technology. Due to the specific features of the Chinese system and the high degree of closedness still exhibited by it; it is difficult to reach strategic security documents that would enable the analysis of strategic security views on disruptive technologies. However, by analyzing the public sources, the statements made by the officials and other documents, it is possible to conclude that China has prioritized technology in fulfilling national interests and national security. The Chinese strategy aims to advance the technological sector and reach the leading position in the world and on the markets. China is spending billions of dollars on science and technology, developing research in genomics, quantum computing, robotics, and advanced materials. Beijing's "Made in China 2025" industrial policy seeks to position China as a high-tech global superpower (Forbes, 2019a). It is important to note that President Xi Jinping himself emphasized how China's future lies precisely in technology. Chinese President Xi Jinping said at a Politburo "group study" session about AI that China must develop, control and use artificial intelligence (AI) to secure the country's future in the next technological and industrial revolution. Xi said that China must develop its own AI technology, saying it was important for economic de-

velopment, social progress and global geopolitics. "AI is a vital driving force (…) and accelerating AI development is a strategic issue (…). Under the plan, China aims to match the world's leading powers in AI by 2020; lead the world in certain aspects of the technology by 2025, and be the world's leading power in AI by 2030" (South China Morning Post, 2018).

China recognizes the potential of modern disruptive technologies and uses them as a platform in an attempt to achieve global domination.

3.4. NATO (North Atlantic Treaty Organization)

The Strategic Concept is an official document that outlines the NATO's enduring purpose and nature, as well as its fundamental security tasks. It also identifies the central features of the new security environment and specifies the elements of the Alliance's approach to security (NATO, 2018a). NATO Strategic Concept is not as comprehensive as national security strategies of individual countries. The current 2010 Strategic Concept titled "Active Engagement, Modern Defense" identifies some disruptive technologies, assessing that "a number of significant technology-related trends – including the development of laser weapons, electronic warfare and technologies that impede access to space – appear poised to have major global effects that will have an impact on NATO military planning and operations" (NATO, 2010: 4).

Disruptive technologies are not explicitly mentioned in this document. The document deals with emerging technologies, defines the concept, but does not single out individual technologies. NATO aims to provide "a full range of capabilities important to deter and defend against any threat". To achieve this, it is necessary to "ensure that the Alliance is at the front edge in assessing the security impact of emerging technologies, and that military planning takes the potential threats into account" (NATO, 2010: 5). The comprehensiveness that NATO attaches to disruptive technologies is evident through the Alliance's various thematic forums. An example of this is the 2018 NATO Industry Forum held in Berlin, which discussed issues related to industry and the economy and where the discussion of disruptive technologies received central attention based on the assessment that "disruptive technologies are moving to the forefront of the modern security environment" (NATO, 2018). The Forum assessed that "in the business domain, disruptive innovations create a new market and value network, which eventually disrupts the existing market and value network, and replaces market leaders, products, alliances and business models". It was accordingly concluded that "disruptive technologies in the military domain enable new concepts and capabilities, alter the operational balance and negate or disrupt existing capabilities" (NATO, 2018).

Through Science and Technology Organization (STO), NATO therefore generates and exploits a cutting edge science and technology operational program, delivering timely results and advice that advance the defence capabilities of individual Allies, partners and the overall organization in support of the core tasks of collective defence, crisis management and cooperative security (NATO, 2019).

3.5. European Union

The European Union did not recognize the issue of disruptive technologies in the 2003 European Security Strategy, a document which istoday somewhat outdated.. However, this does not mean that the European Union as such does not take into account the growing technologies that will be revolutionary in the future and extremely important for security on a global scale. The European Commission's plan on Artificial Intelligence outlines important points for the development and study of artificial intelligence in the European Union, whichis of particular importance as a potential disruptive technology given its widespread use (European Commission, 2018).

The Europe 2020 Strategy places extreme emphasis on technological development, while identifying

technologies that will be highly relevant in the future.. To achieve industrial leadership, the EU will strengthen industrial competitiveness in information and communications technology, space-related technologies and six key technologies that will significantly contribute to the innovation and competitiveness of European products: nanotechnology, microelectronics and nanoelectronics, photonics, advanced materials, biotechnology and advanced manufacturing systems" (Car, 2015: 67).

A 2016 document titled Global Strategy for the European Union's Foreign and Security Policy shows that the European Union is determined to play a greater role in technological advancements and security (European Union, 2016). The document mentions new disruptive technologies and emphasizes that "global rules are also necessary in fields such as biotechnology, artificial intelligence, robotics and remotely piloted systems, to avoid the related security risks and reap their economic benefits" (European Union, 2016: 43). Unlike the US, which takes a confrontational stance towards China, the EU sees increasing security through the development of cooperation, as outlined in the Strategy: "the EU will promote exchanges with relevant multilateral fora to help spearhead the development of rules and build partnerships at the frontiers of global affairs" (European Union, 2016:43). For China as a major competitor of EU, thismeans cooperation based on "the deepening of trade and investment with China, seeking a level playing field, intellectual property rights protection, greater cooperation regarding high-end technology, dialogue on economic reform, human rights and climate action" (European Union, 2016:38). It is important to emphasize that the European Union has a much larger range of tools at its disposal in terms of dealing with disruptive technologies than the NATO.

3.6. Neighboring countries of the Republic of Croatia

Smaller countries in the vicinity of Croatia, with similar historical, geographical, political and other characteristics such as Slovenia, Hungary and Serbia do not treat disruptive technology at the same level as the analyzed documents of the USA, Russia, China, NATO and the EU.

In its national security strategy, the Republic of Slovenia deals with technology issues at the general level as an important component of national interests and security, mostly in relation to other threats. What is particularly emphasized are thenuclear and rocket technologies, cyber threats, and misuse of information technology and systems (Državni zbor, 2019). Technologies that could cause disruption in the security sector in the future are not mentioned.

The Republic of Serbia in its strategy goes a step further and better recognizes threats and opportunities, even mentioning some new and potentially disruptive technologies. The Serbian strategy thus warns of the possible "(…) misuse of new technologies and scientific advances in the fields of informatics, genetic engineering, medicine, meteorology and other scientific fields" (Republika Srbija, 2009: 13). Serbia sees the response to threats as based on the "full integration in the international communications and information system, with the development of a strategic partnership with countries that are the carriers of modern technologies"(Skupština Republike Srbije, 2009).

Hungary has also recognized the potential of technology to generate new threats. Its strategy warns on "the possibility of certain actors using scientific and technological achievements for non-peaceful purposes" which "poses a strategic threat" (Ministry of Foreign Affairs of Hungary, 2012: 4). However, disruptiveness is not used as a term, nor are technologies having disruptive characteristics defined.

3.7. Republic of Croatia

The National Security Strategy of the Republic of Croatia "is the fundamental strategic document that defines policies and instruments for the realization of the national vision and national interests and the achievement of security conditions

that will enable a balanced and continuous development of the state and society" (Hrvatski sabor, 2017: 1). An insight into the Strategy shows that Croatia is no different from the analyzed countries in its neighborhood. The strategy deals with the general statement that in the future, new technologies will be a security question that will need to be answered, based on the assessment that "new technologies are changing all aspects of life (…)" (Hrvatski sabor, 2017: 2). It states that "the development of information and communication technologies (...) has created new threats and risks." Whereby "the dependence of society and the individual on the Internet and on information technology poses a particular sensitivity (...) increasingly threatening individuals, organizations and countries" (Hrvatski sabor, 2017: 3). The trategy addresses technologies at the supportive level, while specific disruptive technologies are not mentioned.

Another important document for analysis is the Program of the Government of the Republic of Croatia. It mainly deals with technological innovations and new technologies that are important for the development and advancement of society, on the assumption that "investment in research, technological development and innovation will be the key generator for the Croatian economy and factor in raising the added value and increasing the productivity and competitiveness of the Croatian economy in the coming years" (Vlada Republike Hrvatske, 2016a: 8).

Nevertheless, this document also did not identify the potential risk of new disruptive technologies. Moreover, it did not recognize the concept and impact that disruptive technologies could have on national security at any level, whether regional or global.

Based on the initiative of the European Union, Croatia has developed a Smart Specialization Strategy and an Action Plan for implementing the Strategy as a new approach to economic development, based on targeted support for R&D activities and innovation. The aim is to "stimulate research, technological development and innovation (…) through the collaboration and joint efforts of the public, scientific research and business sectors" (Vlada Republike Hrvatske, 2016b: 1). The strategy emphasizes encouraging the development of technologies that come within the scope of defined disruptive technologies such as biomedicine, nanotechnology, semiconductors, photonics, robotics and the Internet of Things (Vlada Republike Hrvatske, 2016b).

4. CONCLUSION

Modern technological development and the characteristics of new technologies, especially those that have the potential to bedisruptive, significantly affect all aspects of life, and thus the character of threats and the security paradigm as a whole. A specific feature of development is the transition of threats from the physical to the cybernetic sphere with the accompanying growth of the potential to affect all aspects of the social and individual spectrum, control all aspects of life and consequently influence both the general and the individual level. Threats can almost be tailor-made for each individual. Past experience shows that defense against cyber threats is very complex. In the event of such threats security systems face the challenges of detecting threats or attacks, identifying the carrier of the threat/attack, and defining the protection and countermeasures.

Another significant aspect is the transition of the development of technologies that can be disruptive security-wise, as well as their use in a variety of areas, ranging from the military and security fields to private business enterprises– often multinational corporations -as the main carriers that make states dependent on the private sector.

Finally, the development of the analyzed technologies is directed towards capacities that will be able to act automatically and autonomously, which is another significant feature of the security threats of the future. This increasingly strengthens the role of those civilian aspects of the state system,

which until now have been largely separate from the security sphere; and reinforces the need to strengthen the coordination of many public and private entities, subsequently complicating the planning and operation of the security system. This poses serious challenges to security systems to redefine the very basics of their conceptual definition, planning and action.

Analyzed strategic security documents show that countries see the response to the threat of modern and potential disruptive technologies as going in several directions, primarily by encouraging investment in science and scientific and technological development, then by controlling the development of these technologies and preventing them from falling into the wrong hands, and finally by encouraging public - private partnerships. This imposes the need to enhance co-operation and the exchange of information, build trust and strengthen the interoperability of allies, industry and the R&D and other partners.

The specific properties of the disruptive threats analyzed and the shift of the response focus to the civilian sections of society confront traditional military alliances such as NATO with problems that can hardly be given a comprehensive answer. Given the nature of the threat and the EU's security role an EU-NATO cooperation based on common security interests can be expected.

In such complex conditions, the importance of ensuring a coherent and coordinated action of the security system based on the defined security policies and the legal regulations keeps growing. As those are completely new threats according to their content and character, a change in the mindset and the approach to innovation is necessary for the successful planning and operation of the system.

A new approach to contemporary disruptive technologies requires a significant scientific and technological potential, as well as human and financial resources, which can be a problem for smaller and less developed countries in particular. It is precisely in the case of such countries that cooperation becomes a prerequisite for activity. In the case of Croatia, this certainly means cooperation that is achieved through the EU and the NATO.

4. LITERATURE

Bidwell C. A. JD & MacDonald B. W. (2018) Emerging Disruptive Technologies and Theri Potential Threat to Strategic Stability and National Security, FAS

Bracken, P. (2019) Technological innovation, national security, ETH Zurich, Center for Security Studies, Retrieved from http://www.css.ethz.ch/en/services/digital-library/articles/article.html/88467/pdf (19.7.2019.)

Car S. (2015.) Značaj nanotehnologije za gospodarstvo, Polytechnic and design, Vol. 3 No. 1, 2015. Tehničko veleučilište u Zagrebu, str. 66-73

CNN, Putin and Musk are right: Whoever masters AI will run the world, September 5, 2017, Retrieved from https://edition.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-9allen/index.html (19.7.2019.)

CNN, UK Defense Secretary Gavin Williamson fired over Huawei leak, May 1, 2019, Retrieved from https://edition.cnn.com/2019/05/01/uk/defense-secretary-fired-huawei-leak-gbr-intl/index.html (19.7.2019.)

European Commision (2018) Communication from the Commission to the European parliament, the European council, the Council, the European economic and social committee and the Committee of the regions, Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final

European Union (2003) European Security Strategy, A Secure Europe in a Better World Brussels, 12 December 2003. Retrieved from https://www.cvce.eu/content/publication/2004/10/11/1df262f2-260c-486f-b414-dbf8dc112b6b/publishable_en.pdf (19.7.2019.)

European Union (2016) Global Strategy for the European Unions Foreign and Security Po-licy- Shared Vision, Common Action: A Stronger Europe, Bruxelles. Retrieved from https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf (19.7.2019.)

Forbes (2019a) China's Grand Strategy, Jan 14, Retrieved from https://www.forbes.com/sites/danielaraya/2019/01/14/chinas-grand-strategy/#7d18dc961f18 (14.7.2019.)

Forbes (2019b) The Largest Technology Companies In 2019: Apple Reigns As Smartphones Slip And Cloud Services Thrive May 15, Retrieved from https://www.forbes.com/sites/jonathanponciano/2019/05/15/worlds-largest-tech-companies-2019/#7691c708734f (14.7.2019.)

Hrvatski sabor (2017) Strategija nacionalne sigurnosti Republike Hrvatske, NN 73/2017. Retrieved from https://www.uvns.hr/UserDocsImages/dokumenti/nacionalna-sigurnost/Strategija%20nacionalne%20sigurnosti%20RH.pdf (14.7.2019.)

Ministry of Foreign Affairs of Hungary (2012.) Hungary's national security strategy, Budapest. Retrieved from

https://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf (28.7.2019.)

Mitchell II S. T. (2009.) Identifying Disruptive Technologies Facing the United States in Next 20 Years, West Point, Kansas

NATO (2010.) Strategic Concept - Active Engagement, Modern Defence, Bruxelles. Retrieved from https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (28.7.2019.)

NATO (2018a) Strategic Concepts, 12 Jun. 2018. Retrieved from https://www.nato.int/cps/en/natohq/topics_56626.htm (28.7.2019.)

NATO (2018b) NATO Industry Forum, Berlin November 12-13, Retrieved from file:///C:/Users/User/Desktop/Disruptive%20technology/NATO%20DT%20super.pdf (28.7.2019.)

NATO (2019) NATO Science and Technology Organization. Retrieved from https://www.nato.int/cps/en/natohq/topics_88745.htm (28.7.2019.)

PR China State Council (2017a) Next Generation Artificial Intelligence Development Plan, China Science and Technology Newsletter, Department of International Cooperation Ministry of Science and Technology (MOST), P.R.China, No.17, September, 15 2017.

PR China National People's Congress (2017b) National Intelligence Law of the People's Republic, National People's Congres, June 27, 2017.

Russian Federation President (2015) Russian Federation's National Security Strategy, 31 December 2015. Retrieved from https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf (28.7.2019.)

Republika Srbija (2009.) Strategija nacionalne bezbednosti Republike Srbije, Beograd. Retrieved from http://www.mod.gov.rs/multimedia/file/staticki_sadrzaj/dokumenta/strategije/Strategija%20nacionalne%20bezbednosti%20Republike%20Srbije.pdf (28.7.2019.)

South China Morning Post (2018) Develop and control: Xi Jinping urges China to use artificial intelligence in race for tech future, 31 Oct, 2018.

Tatalović, S. i Malnar, D. (2016) New Security Paradigm and Crisis Management, Sarajevo Social Science Review, Godište V, Broj 1-2, Fakultet političkih nauka, Sarajevo, 2016. str. 53-70.

The World Bank (2019). Military expenditure (current USD), Retrieved from

https://data.worldbank.org/indicator/MS.MIL.XPND.CD uvid 14.7.2019. (14.7.2019.)

Vlada Republike Hrvatske (2016.a) Program vlade Republike Hrvatske za mandat 2016 - 2020, Zagreb. Retrieved from

https://vlada.gov.hr/UserDocsImages/ZPPI/Dokumenti%20Vlada/Program_Vlada_RH_2016_2020.pdf (14.7.2019.)

Vlada Republike Hrvatske (2016b) Strategija pametne specijalizacije Republike Hrvatske za razdoblje od 2016. do 2020. godine i akcijski plan za provedbu Strategije pametne specijalizacije Republike Hrvatske za razdoblje od 2016. do 2017. godine, Retrieved from https://www.mingo.hr/page/vlada-usvojila-strategiju-pametne-specijalizacije-rh-za-razdoblje-2016-2020 (14.7.2019.)

Vlada Republike Slovenije (2019.) Resoulucija i strategiji nacionalne varnosti Republike Slovenije, Ljubljana. Retrieved from https://imss.dz-rs.si/imis/557792390bcd5987fd14.pdf (19.7.2019.)

VOA, US Warns Germany a Huawei Deal Could Hurt Intelligence Sharing, March 12, 2019, Retrieved from https://www.voa.news.com/europe/us-warns-germany-huawei-deal-could-hurt-intelligence-sharing (19.7.2019.)

White House (2017) National Security Strategy of the United States of America, December 2017.