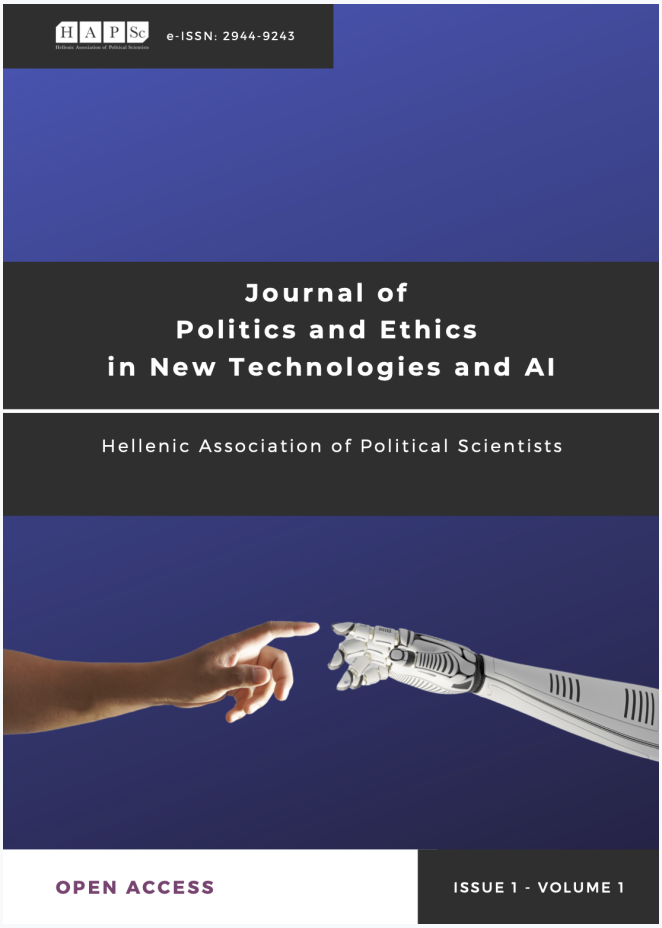
Journal of Politics and Ethics in New Technologies and AI

Vol 1, No 1 (2022)

Journal of Politics and Ethics in New Technologies and AI



Cutting-Edge Warfare: The Cases of Russia, China and Israel

Panagiota Tzanetou

doi: 10.12681/jpentai.31243

Journal of Politics and Ethics in New Technologies and AI
Volume 1, Issue 1 (2022)
e-ISSN: 2944-9243

https://doi.org/10.12681/jpentai.31243

RESEARCH ARTICLE

Cutting-Edge Warfare:
The Cases of Russia, China and Israel

Panagiota Tzanetou
Department of International and European Studies, University of Piraeus, Greece.

Abstract
According to political realism, countries are in a constant state of competition with each other. This competition ranges from markets to weapons causing the ones that wish to change the balance of power to opt for innovation in all fields. Although the concept of innovation is not new, current conditions demand that this innovation is connected to technology. The incorporation of new technologies gives states the chance to rise to the top of the power competition, while middle powers have the ability to tackle their state and non-state enemies using them. This paper focuses on what these new technologies are and what Russia, China and Israel are doing with them, providing insight regarding the way these technologies can be used to serve national interest in a security dilemma environment.

Keywords: Modern Warfare, New Technologies, Russia, China, Israel, Cyber Warfare, 5th Generation Networks

Introduction

National security is the number one priority for a state, based on political realism. It is defined as the ability of a nation to protect its citizens and its values from threats of any type, other states or non-state actors. It is ensuring a state's survival and protecting its vital interests. It is the lack of violence, threats and hostility, so that the citizens are able to live decently and create civilization. Under this scope, national security can be acquired by state power, in which the main element in global politics is military power (Heywood, 2013). A rising power is threatening to displace the hegemonic one, thus a security dilemma or else a "Thucydides' Trap" (Alisson, 2012) is created and the never-ending cycle of arms race that comes with it.

Political realism suggests that each state is responsible for its national security since self-help is the only reliable pathway to follow to ensure state survival. Self-help is translated into internal and external balancing with military, economic, diplomatic and technological means. States that realise the

Tzanetou, P. (2022). Cutting-Edge Warfare: The Cases of Russia, China and Israel. *Journal of Politics and Ethics in New Technologies and AI, 1*(1), e31243. https://doi.org/10.12681/jpentai.31243

importance of self-help due the anarchical nature of the international system have stopped relying on external forces to ensure their survival. They acknowledge the contribution of innovation and technology for increasing their relative economic and military power. Technological means can bridge the gap of power between adversaries and could give a comparative advantage to the conventionally weaker one. That's why states that are involved in an asymmetrical competition or warfare opt for the incorporation of new technologies in their capabilities.

Nowadays, emerging technologies are the new "hot topic" and are present in our daily lives more than ever. This commercial use of new tech has made it widely accessible and has given research the boost it needed, so that all possible applications of new technologies are found, including ones in defence. According to the US Congress Office of Technology Assessment (1998), dual-use technologies that are being produced commercially are necessary for the development of weapon systems. In the past, military necessities promoted general technological development. Today, synergies between the private and the public sector are notable for technological innovation.[1]

In this paper, the most important new and emerging technologies will be examined as well as their defence applications. Furthermore, the cases of Russia, China and Israel will be presented, since they are states that are actively involved in the development and deployment of such technologies in a way that serves their national defence doctrine.

New Technologies in Warfare

Disruptive technologies have the ability to disrupt the current environment and work in favour of those using them. In this chapter, cyber warfare, Big Data, 5G and Artificial Intelligence are being examined in relation to how they work and their current and possible applications for defence purposes.

Cyber Warfare

Hybrid warfare is a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts and criminal disorder (Hoffman, 2007). Cyber warfare, as a form of hybrid warfare, refers to offensive and defensive operations conducted in cyberspace. As most social, functional, economic and defence activities are carried out or, at least, connected to cyber space, cyber-attacks are of great importance. They are characterized as a "grey zone" between war and peace

[1] US Deputy Secretary of Defense Bob Work confirmed this in his speech on the 28th of April 2016 in Brussels. He stated "*[…] But today, almost all of the technology that is of importance in the future is coming from the commercial sector, and all of the technology base is global. So that means any competitor and any adversary is going to have access to these types of technologies, and they can quickly mimic even the most powerful state*."

(Fitton, 2016) and are in the epicentre of hybrid campaigns. Cyber operations have become the new normal for attackers since they are a way for a state or non-state actor to cause a hit to their adversary, while avoiding military or other types of "hard" repercussions. They are easy to carry out, low risk, low cost and high impact (Missiroli, 2019). Most of them are not lethal, but in some cases they have been and they certainly have the ability to be in the future. Their low lethality does not lower their significance, since they can "paralyze" an entire organization, institution or state. The emergence of cyber warfare adds new elements to the concept of war in a way that could be compared to the use of airpower in warfare in World War I. Air was added to the domains that humans could conduct war after Land and Sea. Cyberspace is man-made, but also a new environment for new types of war operations.

According to Tabansky (2011), basic concepts of cyber warfare are: the weaponry, referring to the physical infrastructures necessary for cyber activities to which physical damage can be done as well as cyber weapons consisting of different types of software and hardware (e.g. malware, denial of service, encryption, camouflage of content and communications etc.), vulnerabilities, which are different for each actor and are the main targets of a cyber-attack, defence aiming to identify and tackle an unauthorized intrusion, locate the source, prevent damage and reconstruct and attack, which has a clear advantage against cyber defence.

Important victories can be made with cyber-attacks in the information domain, that would otherwise require large and ambiguous espionage operations. Big Powers have realised that cyberspace is the domain, into which critical hits against adversaries are being and will be carried out. Thus, substantial efforts are being made to gain the offensive advantage in the cyber field but also to ensure cybersecurity. Synergies between state and non-state actors are common in cyber warfare and cause the problem of attribution of an attack to a certain actor as seen happening with Russia, Turkey and other countries that deploy cyber-attacks against their adversaries.

Big Data and Surveillance

Big Data are defined as information, which has been "datafied" and is in digital form. Most information has been collected through a variety of sensors and virtual spaces. It comes from all users' internet activity, which is being processed, so that inferences can be deduced. Big Data can provide specificity that statistics cannot and it can isolate social groups of interest with specific characteristics such as location, time and preferences.

Except for their apparent commercial and marketing use, Big Data are providing insight into a society, institution and government, which is particularly important to an adversary, who would have to use espionage methods in order to gain a fraction of this information. Knowing one's enemy and knowing one's self are the most important elements to win a war, according to Sun Tzu. Big Data make this possible with a cyber-attack aiming to steal them, with open-data sources that exist in some states and surveillance aiming to prevent and punish criminal acts.

States have realised that through social media collective political and social power is expressed (NATO S&T Organization, 2020). Hence, Big Data can be used for population surveillance and control. Scholars argue that this is promoting the creation of a surveillance state while stepping on privacy rights of their citizens (Liaropoulos, 2016). Surveillance programmes are being conducted in China and Russia, but also in the US such as PRISM and "Bulk Collection of Telephone Metadata" by the NSA, which, according to Etzioni (2014), are collecting a large number of users' private communications. Others support that "traffic" data is collected, not content. The collection of private data could be justified with the third-party doctrine based on which the user voluntarily gives a third-party permission to their data, which are kept for short periods of time (Etzioni, 2014). Others support that Big Data operations should be carried out with common sense as a denominator so that free will and the right to privacy are protected (Cukier et al., 2014).

Big Data strategies provide knowledge that can be used in decision-making, command and control and even military strikes. Big Data has materialized the information society considering that digital data collected through a variety of means are shaping decision-making leading to actions in the physical realm.

5th Generation Networks

Wireless communication networks became operational after World War II. These cell phone predecessors were called 0G systems. 0.5G wireless telephone systems followed and in 1980 the first cell phones were introduced with the 1G network technology, which had limited analog abilities. The second generation (2G) technology could provide text, picture and MMS messaging. It was safer than its predecessors due to digital encryption. 3G introduced a worldwide communication standard, wireless data, video calling and GPS, differentiating the mobile communications environment significantly from its ones before it. In the late 2000's 4G technology was introduced, which provided interoperability between different kinds of networks, higher speed, larger amount of data transmission and world-wide roaming (Meraj Ud In Mir & Kumar, 2015).

5th Generation networks were first introduced in 2019 and they operate differently than network technologies before them. Each geographic area is divided into smaller cells, in which internet connection and telephone services are provided through radio waves from a local antenna. Increased bandwidth provides 5G networks with very high speeds in each geographical cell. Large data transmission density is supported, which minimizes delays between devices and promotes networks' interconnectivity (Odell et al., 2019). 5G increases accuracy in relative location determination even in the absence of GPS and it is more resilient than the networks before it in jamming attempts. Moreover, it provides reliability in remote automation, which is significant for medical, technical and defence purposes (Odell et al., 2019).

The importance of 5G in the development and use of defence technologies can be found in its characteristics mentioned above. These new abilities 5G provides, promote the creation of a safe, fast and resilient network. 5G is key for the use of other technologies such as AI, which requires processing of great amounts of data, in high speed and interconnectivity among devices. The competition in the field of 5G networks development stresses its importance for national security. Implications arise as a huge amount of critical data is in the hands of few companies. Some have been accused of espionage and have been denied access to specific countries. The rising use of 5G networks in critical infrastructure and national security operations could lead to catastrophic consequences in case of an attack.

Artificial Intelligence

Artificial Intelligence (AI) is defined as the capability of a computer system to perform tasks that normally require human intelligence such as visual perception, speech recognition and decision-making (Cummings, 2017). AI's goal is to mimic human cognitive behaviour, so that the machine incorporates judgement in completing tasks without human assistance. For example, recognising patterns, learning from experience, drawing conclusions, making predictions, or taking action (NATO S&T Organization, 2020). AI-based technologies are being used in a plethora of systems from spelling and grammar checkers, self-driving cars and healthcare systems to unmanned military vehicles. What makes AI different from automated systems is that the latter are working in a rather deterministic way and with specific rules, while AI is considering the best course of action based on a specific data input. The technology, though in primitive stages, has been in place for decades. The boost to wide-range use was given by the development of 5G and the huge amount of Big Data collected through increased internet use for the past years.

AI's functionality is constantly improving and its role in military operations is increasing (Verbruggen, 2020). Military applications for AI include semi-autonomous and autonomous vehicles, command and control, intelligence, data analysis, surveillance, reconnaissance, logistics, cyberspace and information operations (Lin, 2020). AI can be used in nuclear-capable aircrafts, underwater detection and discovery of concealed nuclear weapons, which is a main element for deterrence. AI improves precision and speed, increasing the value of conventional weapons as well. The AI system's actions are carefully calculated statistical decisions on the grounds of the hypothesis of what the other part is expected to do.

The main problem with AI systems is the lack of explainability. Correlation is not causation, so, if a problem is caused, the AI system cannot explain its choice of action, which is considered as optimal with this specific data input (Lin, 2020). AI cannot view relativity in military and other types of capabilities; therefore, AI systems could be prone to miscalculation (Horowitz & Scharre,2021). As far as lethal AI systems are concerned, the ethical and technical implications need to be carefully examined. Some scholars argue that the ability of a non-human system to take the life of humans could cause a legitimacy issue on the use of such systems (Hoffman, 2021). Others suggest that, while AI-driven systems currently carry out hits on static military targets successfully, the situation changes when the operation would entail the hit on a moving human target (Cummings, 2017). Moreover, it could reduce time for decision-making and lead to mistakes (Verbruggen, 2020).

AI should be considered a tool, just like other new technologies have been in the past, serving human-set purposes and objectives. It is important that knowledge and experience with AI should be gained in a low-stakes environment where the costs are relatively small (Lin, 2020), rather than in situations, where over-trusting AI could be proven fatal.

Case Studies

In this section, countries that use new technologies for defence purposes are being examined. Russia has been one of the first countries that used cyber-attacks on a large scale and complimentary to military means, showing the world what hybrid warfare, coming from a state, is capable of doing. China is second in line in the Big Power competition. R&D in new technologies is aiming to bridge the gap with the United States and bring it to the top, while expanding its influence worldwide. Israel, a state under constant threat, is actively involved in the development of new technologies and has shown recently how successful they can be at protecting the state and its interests.

Russia

The Russian Federation, after the collapse of the USSR, struggled to establish its position in the contemporary international system. In this context, Russia has transformed its former foreign policy into one that serves better the new raison d'état, which, beyond the state's survival, extends to the state acquiring its Big Power status once again.

From the creation of the USSR, the government has tried to establish its authority amongst its citizens and globally using ambiguous means. Propaganda, coercion, extortion and threats are some of the methods used by the state to influence public opinion and ensure survival for the regime. According to Ajir and Vailliant (2018), Soviet information warfare had been taking place as early as 1919, according to Bolshevik documents, using "active measures", referring to actions aimed at influencing events and behaviours of foreign countries. The active measures' budget of about 3-4 billion dollars and personnel of about 15,000 confirms the importance of information warfare for the Soviets. According to the Russian government's document "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space", information warfare is defined as "confronting a state in the information space by damaging information systems, processes, and resources. These are of critical importance to undermine any political, economic, or social system, through what Russia deems "massive brainwashing" of the population to destabilize the society and the state. It also forces the confronted state to make decisions in the interests of the confronting party" (Russian Federation, 2000).

Russia recognizes that it cannot compete conventionally with its adversaries. This leads to the increased use of hybrid, asymmetrical offensive methods and responses. These operations aim at destabilizing the West, mostly internally, and are, as president Putin has stated, "intellectually superior" compared to conventional ones. The West's strengths, such as freedom of speech and democracy are turned into vulnerabilities and are being exploited in order to serve propaganda objectives or even direct attacks to state institutions. Russia does not discriminate between the information space and cyberspace, with the latter enabling psychological and information warfare greatly (Ajir & Vailliant, 2018).

The 2007 cyber-attacks to Estonia took place at a time of political tension with Russia and lasted for 22 days, though Russia has not claimed responsibility. Most attacks originated from Russian computers. The targets included government websites, police, online media, civil services and banking systems. Estonia is a country that has incorporated the cyber domain in its state and civilian functions

to a high degree since the early 2000's, therefore cyber-attacks are direct threats to its national security. The cyber-attacks were combined with protests outside the Estonian embassy in Moscow as well as unofficial limiting of Russian-Estonian trade (Ottis, 2008). Georgia has been a victim of Russian cyber-attacks as well. Denial of service, propaganda, data theft and even an alleged terrorist cyber-attack to an oil pipeline took place in 2008 just before the Russian-Georgian war. The combination of cyber and military attacks against Georgia confirmed the "hybridity" of modern warfare. The difficulty to determine the offender in cyber-attacks as well as the inability to respond using military means are clear advantages for Russia.

President Putin has characterized the leader in the field of Artificial Intelligence as "master of the world". Nevertheless, Russia's prospects in the field of Artificial Intelligence began in 2019 with the "National Strategy for the Development of Artificial Intelligence Through 2030" after the boost was given by private Russian companies that wished to adopt AI for commercial purposes. Russia's AI strategy is aiming at eliminating the relative disadvantage of the country in the field by 2024. As of now, not enough progress has been made, although Russian Armed Forces possess and use AI-based unmanned vehicles in battle. Further research and development will take place with an aim to give the country a leading role in the field. Russian AI technologies are being increasingly developed, because of the larger attention the Russian government and major tech companies are paying to it (Markotkin & Chernenko,2020).

Russia is using modern means in the application of its already existing military and information doctrines. It has a zero-sum mentality in the Big Powers competition (Ajir & Vailliant, 2018), that's why its attacks' objective is the destabilization of its adversaries. Russia is one of the few countries that have fully comprehended the endless offensive and defensive possibilities cyberspace and new technologies provide and has been materializing them against its actual and potential enemies.

China

Millenia of Chinese war wisdom have been codified in the timeless Sun Tzu's "The Art of War". It provides a useful insight into how warfare is perceived by the Chinese since ancient times. Information, deception and surprise are the main elements an actor should invest in and use to secure victory. The Chinese approach to foreign policy has been consistent for many years, with an emphasis on information operations and avoiding open conflicts (Riikonen, 2019).

The Chinese have been far-seeing in the field of new technologies. They are a valuable tool in information operations and interconnectivity, therefore important to China's objectives (Riikonen,

2019). The realisation that new technologies especially in military affairs is a domain of Big Powers' competition has pushed China to significant research and development in the field. President Xi Jinping confirms this in his statements on the importance of military innovation and the need for China to "keep pace with the times and adapt to the global Revolution in Military Affairs" that is taking place due to the emergence and use of such technologies.

Since the 1990's, Chinese military has focused on informatization, meaning that new technologies incorporated in warfare would assist the need for gathering and processing information faster and better than humans. The new "intelligentized" form of warfare calls for the incorporation of smart, autonomous technologies that limit the human factor or even exceed it. Chinese scientists and strategists support that these new technologies surpass the cognitive abilities of the human brain. Such Revolution in Military Affairs would require human transformation to keep up with the increasingly complex operations. Brain-machine fusion is a future paradigm for command and control, but also future combat. This could entail means for performance enhancement, psychological, cognitive and manipulative interference which could even end up in the subversion of combat styles and in a winning without fighting scenario (Kania, 2019a).

China has institutionalised this need for R&D with scientific teams in universities, research departments in the military (such as the PLA's Academy for Military Science), the National Innovation Institute for Defense Technology, the China Brain Project, the CMC Science and Technology Commission (S&TC) etc. Their research is about Artificial Intelligence, bio-technology, neuro-science for military applications, advanced biometric systems and many other fields of military innovation.

China has a national strategy of military-civil fusion (Kania, 2019a) through independent state research and cooperation with technology companies, to which most times the state is an important shareholder. The military-civil fusion is also confirmed by China's use of technologies like Big Data,5G and AI facial recognition for surveillance purposes. These technologies are aimed at preventing strategic surprise which is in the centre of Chinese war doctrine. Companies like Huawei are pioneers at 5G network infrastructure and have expanded significantly with more than 3 billion people using its devices globally. The company has been accused of sharing users' data with the Chinese state and even has been subjected to sanctions by the US. It has been involved in many infrastructure and network projects worldwide, which are not necessarily being built for surveillance purposes, but due to China's vague position on the subject there is a possibility that they could serve a global surveillance network (Kania, 2019b). Article 7 of the PRC's National Intelligence Law states "Any organisation and citizen

shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work." (Riikonen, 2019:125).

Clearly, China comprehends how new technologies serve its long-term approach towards warfare and foreign policy. Gaining the relative, if not total, advantage in the field is a long and short-term goal for the Chinese state, which is steadily being reached. Its main competitor, USA, though technologically advanced, has not been able to provide equal alternatives in R&D and global tech infrastructure projects. The EU as a "middle power" is lagging behind significantly in the field (Fricke, 2020) and is closer to a more "ethical approach" to new and emerging technologies, which could be translated into a disadvantage and lower military effectiveness in a warfare scenario (Lin, 2020).

Israel

Since its founding, in 1948, Israel has been facing multiple threats to its national security. Military capacity, technical capability and know-how, espionage and external support ensured its survival in the region since the first Arab-Israeli Wars (Göktuğ & Gökhan, 2021). Israel's security doctrine is based on its small population compared to its adversaries, its lack of strategic depth, regional volatility, the long- Israel's standing Arab-Israeli conflict and self-reliance in defence. Its security strategy is in accordance with 4 principles: early warning, decisive battlefield victory, cumulative deterrence and defence of the rear "home front" (Tabansky, 2020). Israel is a country that fully comprehends the security environment and has tried -successfully- to be an innovator in the field. Its lack of natural and limited human resources led to investment in technology.

A new field for warfare, deterrence and defence opened with the establishment of cyberspace. Saudi hacker "Ox Omar" carried out a series of cyber-attacks against Israeli targets in 2012, which sparked the interest for Hamas and other organizations to begin an "electronic Jihad" against Israel (Abu Saada & Turan, 2021). Prime minister Netanyahu's statements in 2012 about building a "digital iron dome" for cybersecurity confirm the important role cyberspace plays for Israel's national security.

Israel's innovative role in new technologies has given the country an important advantage to use its high-tech capabilities as means to elevate its position in the international and regional system. Israel is characterized as a "start-up" nation, is a leading country in the production and use for unmanned and autonomous systems, and is embedding Artificial Intelligence in security and civilian systems. According to Antebi (2021), AI has affected Israeli foreign and domestic security with AI military and

intelligence applications, Israel's foreign relations and international reputation by preserving the status of a technological leader and exporter, the economy and national resources by R&D and investments in AI, governability by overseeing decision-making and implementation through simulations and the strength of civil society by citizens' quality of life improvement.

The latest big Israeli-Palestinian conflict in May 2021 has been characterized as a "glimpse of future conflicts" and as "the first Artificial Intelligence war" (Kumon, 2021). Hamas fired multiple thousands of rockets towards Israel and the Iron Dome defence system successfully intercepted 90% of them. AI was used throughout the whole operation to determine which rockets would hit populated areas in order to intercept them. AI was also used for the determination of targets during the planning of the Gaza attacks. Combining sensors, intelligence and geographical data, 3D plans of the locations of rocket launchers were created, means and safer routes for the attacks were proposed (Kumon, 2021).

In the past 20 years Israeli authorities have created multiple cybersecurity institutions. The Critical Infrastructure Protection Arrangement has been in place since 2002 about the need to protect computerized systems concerning civilian and state entities. The National Cyber Initiative was launched in 2010 and addressed issues such as cyber technology development so that Israel becomes a leader in the field. In 2011 Israel's National Cyber Bureau was established in the Prime Minister's Office and it advises and recommends national policies in the cyber field. The National Cyber Security Authority was established in 2015 to protect Israeli civilian cyberspace against NSA-like practises and to build trust reducing tensions on the security-liberty dilemma. The entire effort is cooperative between the state, the private sector, NGOs and Academia. They share a "partnership of faith" to work together for the country's security (Antebi, 2021).

Israel due to the constant national security threats it is facing had to be inventive in order to ensure its survival. Its technological progress, as a result of research and synergies has made the country one of the leading forces in defence technology. The use of new technologies for military purposes is having a "spillover effect" to other fields such as medicine and commerce. Israel is a country able to contribute significantly to new technologies and is showing the world the results of their use. As Isaac Ben-Israel, head of Security Studies programme in Tel Aviv University and chief cybernetics adviser to prime minister Benjamin Netanyahu from 2010-2012, comments in a Science Business interview: "What makes Israel better in science and in business than other countries, that are pioneers in the new technologies field such as China, is the lack of fear for failure and the will to show others how to do things better and differently" (Kelly, 2019).

Conclusions

In conclusion, the international system's nature demands that states who wish to elevate their position in a security dilemma environment have to strive for internal and external balancing of their capabilities. This requires investments in innovation concerning all fields, with an emphasis on the technological one due to the rapid technological development of the past decades. The emergence of new technologies has shown that beyond their commercial use, they can also be used for defence purposes and minimize the gap between two or more asymmetrical opponents. The cyber domain is being widely used in hybrid warfare operations and provides endless possibilities on its own or even used complimentary to other means. Big Data provides more insight than ever for a potential adversary and their use for surveillance is of equal -if not more- importance to espionage. 5G has enabled the use of new technologies, but presents safety implications concerning the infrastructure development and data safety. Artificial Intelligence presents a plethora of uses for commercial and defence purposes and is the most promising new technology. It presents implications on its ethical and practical aspect, as far as lethality and data input are concerned. Russia, China and Israel are states actively involved in R&D and operational use of new technologies in order to serve their national interests. Examining their course of action on the field, it is apparent that new technologies' incorporation in defence is very promising and contributes to successful military or solely cyber campaigns. States that deal with security dilemmas or asymmetrical opponents should invest heavily in new technologies as they could be the alternative to the expensive and bloody weapons' race that has been taking place for centuries.

References

Abu Saada, M., & Turan, Y. (2021). İsrail-Filistin Siber Çatışması. *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 16(1), 186–204. Available at: https://doi.org/10.17153/oguiibf.869178

Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70-89. Available at: https://www.jstor.org/stable/26481910

Allison, G. (2021). Thucydides's trap has been sprung in the Pacific. *Financial Times*. Available at: https://www.ft.com/content/5d695b5a-ead3-11e1-984b-00144feab49a (Accessed: 30/07/21).

Antebi, L. (2021, February). Artificial Intelligence and National Security in Israel. *Institute for National Security Studies*, Memorandum no.207. Available at: https://www.inss.org.il/wp-content/uploads/2021/02/Memo207_AntebyENG_9.pdf

Cummings, M. (2017, January). Artificial Intelligence and the Future of Warfare. *International Security Department and US and the Americas Programme*. Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings.pdf

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber Conflicts. *Connections*, 16(2), 5-24. Available at: http://www.jstor.org/stable/26326478

Etzioni, A. (2014). NSA: National Security vs. Individual Rights. *Intelligence and National Security*, 30(1), 100–136. Available at: https://doi.org/10.1080/02684527.2013.867221

Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *Connections*, 15(2), 109-119. Available at: http://www.jstor.org/stable/26326443

Franklin, A. (2018). An International Cyber Warfare Treaty: Historical Analogies and Future Prospects. *Journal of Law & Cyber Warfare*, 7(1), 149-164. Available at: https://www.jstor.org/stable/26777966

Fricke, B. (2020). Artificial Intelligence, 5G and the Future Balance of Power. *Konrad Adenauer Stiftung*, No 379/January 2020. Available at: http://www.jstor.org/stable/resrep25281

Göktuğ, S., & Gökhan, B. (2021). Iron Dome Air Defence System: Basic Characteristics, Limitations, Local and Regional Implications. *ORSAM Policy Brief*, 169. Available at: https://www.orsam.org.tr/d_hbanaliz/iron-dome-air-defense-system-basic-characteristics-limitations-local-and-regional-implications.pdf

Hoffman, F. G. (2019). Healthy Skepticism about the Future of Disruptive Technology and Modern War. *Foreign Policy Research Institute*. Available at: https://www.fpri.org/article/2019/01/healthy-skepticism-about-the-future-of-disruptive-technology-and-modern-war/ (Accessed: 30/07/2021).

Horowitz, M., & Scharre, P. (2021). AI and International Stability: Risks and Confidence-Building Measures. *Center for a New American Security*. Available at: http://www.jstor.org/stable/resrep28649.5

Kania, E. (2019a). Minds at War: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology. *PRISM*, 8(3), 82-101. Available at: https://www.jstor.org/stable/26864278

Kania, E. (2019b). Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy (pp. 11-13). *Center for a New American Security*. Available at: https://www.jstor.org/stable/resrep20451

Kelly, É. (2019). Israel sets out to become the next major artificial intelligence player. *Science|Business*. Available at: https://sciencebusiness.net/news/israel-sets-out-become-next-major-artificial-intelligence-player (Accessed: 12/08/21).

Kozieł, M. (2018). NATO's Defense Institution Building in the Age of Hybrid Warfare. *Connections*, 17(3), 39-51. Available at: https://www.jstor.org/stable/26934689

Liaropoulos, A. N. (2016). Reconceptualising Cyber Security. *International Journal of Cyber Warfare* and Terrorism, 6(2), 32–40. Available at: https://doi.org/10.4018/ijcwt.2016040103

Lin, H. (2020). A somewhat contrarian view of AI in warfare [Presentation]. In GLOBSEC (2020, November 25). *The Future of Warfare and the Role of New and Emerging Technologies* [Video], Bratislava, Slovakia. Available at: https://www.youtube.com/watch?v=eK99qZwBTBI&t=5886s

Meraj Ud In Mir, M., & Dr. Kumar, S. (2015). Evolution of Mobile Wireless Technology from 0G to 5G. International Journal of Computer Science and Information Technologies (IJCSIT), 6(3), 2545–2551. Available at: https://ijcsit.com/docs/Volume%206/vol6issue03/ijcsit20150603123.pdf

Missiroli, A. (2019). From hybrid warfare to “cybrid” campaigns: the new normal?. *NATO Defense College*. Available at: http://www.jstor.org/stable/resrep19847

NATO S&T Organization. (2020, March). NATO Science & Technology Trends 2020–2040. *NATO Science & Technology Organization.* Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Odell, L., Wagner, R., Adams, T., Fauntleroy, J., Thompson, G., Rabren, T., & DiLorenzo, C. (2019). Implications and Considerations of 5th Generation Mobile Networks (5G) for the US Department of Defense. *Institute for Defense Analyses*. Available at: http://www.jstor.org/stable/resrep22697

Riikonen, A. (2019). Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China. *Strategic Studies Quarterly*, 13(4), 122-145. Available at: https://www.jstor.org/stable/26815049

Russian Federation. (2000, September). Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. *Russian Federation.* Available at: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

Sweijs,T., Zilincik, S., Bekkers, F., & Meessen, R. (2021, January). Framework for Cross-Domain Strategies against hybrid threats. *The Hague Centre for Strategic Studies*, Available at: https://mk0hcssnlsb22xc4fhr7.kinstacdn.com/wp-content/uploads/2021/01/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf

Tabansky, L. (2011). Basic Concepts in Cyber Warfare. *Military and Strategic Affairs*, 3, no. 1(May). Available at: https://www.inss.org.il/wp-content/uploads/2017/02/FILE1308129610-1.pdf

Tabansky, L. (2018). Sticking to their Guns: The Missing RMA for Cybersecurity. *Military Cyber Affairs*, 3(1). Available at: https://doi.org/10.5038/2378-0789.3.1.1039

Tabansky, L. (2020). Israel Defense Forces and National Cyber Defense. *Connections*, 19(1), 45-62. Available at: https://www.jstor.org/stable/26934535

U.S. Congress, Office of Technology Assessment (1998). The Defense Technology Base: Introduction and Overview–A Special Report. Available at: https://ota.fas.org/reports/8810.pdf

Verbruggen, M. (2020). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume III South Asian Perspectives (pp. 11-16) (TOPYCHKANOV P., Ed.). *Stockholm International Peace Research Institute.* Available at: http://www.jstor.org/stable/resrep24515.8

Work, B. (2016). Remarks by Deputy Secretary Work on Third Offset Strategy. *US Department of Defense*. Available at: https://www.defense.gov/Newsroom/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy/ (Accessed: 11/08/2021).