Alan Lis

Aleksander Ksawery Olech

TECHNOLOGY AND TERRORISM

ARTIFICIAL INTELLIGENCE IN THE TIME OF CONTEMPORARY TERRORIST THREATS

INSTITUTE
OF NEW
EUROPE

TEAM

AUTHORS:

Alan Lis

Aleksander Ksawery Olech

ANALYSTS:

Sylwia Gliwa

Natalia Matiaszczyk

Aymen Gatri

Jakub Klepek

Cosmin Timofte

ANALYTICAL SUPPORT:

Małgorzata Cichy

Stanisław Apriłaszwili

MAPS AND GRAPHICS:

Natalia Matiaszczyk

Aleksander Ksawery Olech

LINGUISTIC SUPPORT:

Małgorzata Cichy

Cosmin Timofte

TABLE OF CONTENTS

ABSTRACT

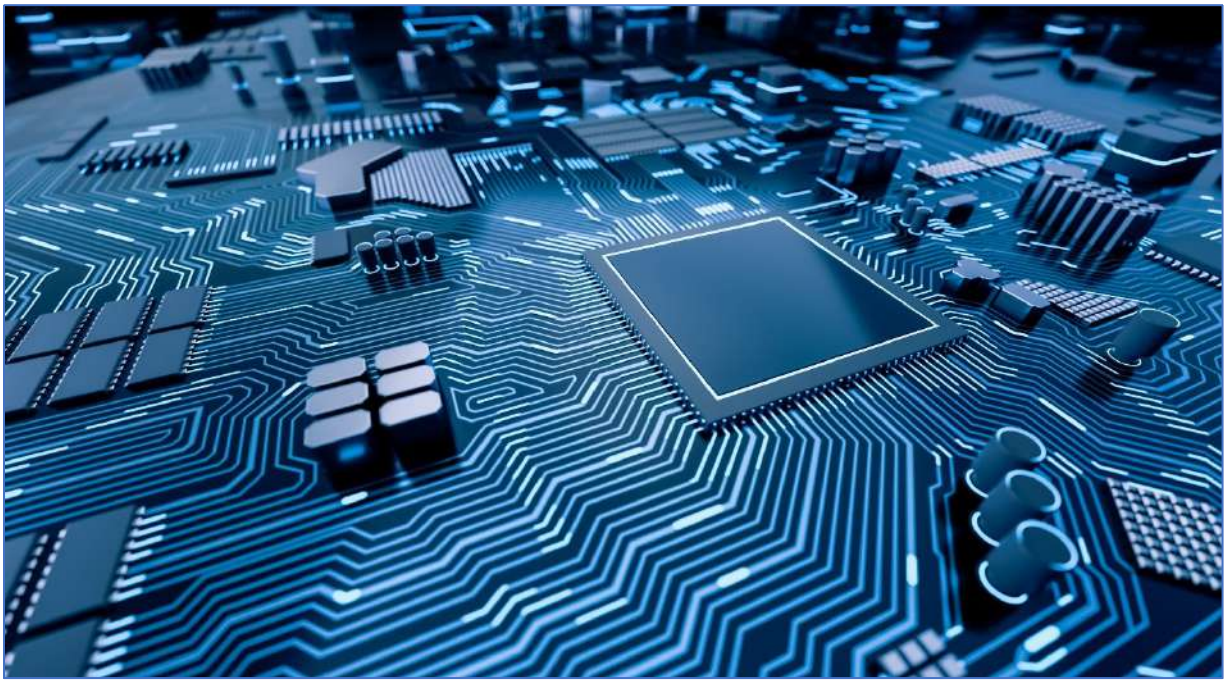
Technological breakthroughs are responsible for much of mankind's progress across history, revolutionising both peaceful lifestyles and armed conflicts across the centuries. Advanced technologies have also led to complete reconstructions of how states interact from one another, with the advent of nuclear weapons being one of many supporting examples. Presently, a novel set of security challenges focused on information, hybrid warfare and the embedding of technology within society, especially with artificial intelligence (AI), being used not only for the sake of mankind's progress but also for the forwarding of one's own strategic agenda over another's.

The report will begin by exploring the definitions and impacts of artificial intelligence. Among its countless benefits, a special focus will be placed on the retail, healthcare and military sectors, while the challenges posed by establishing an ethical conduct of research and its drawback on employment will be focused on in equal measure. Afterwards, the distinctive efforts made by the three competing world powers (USA, China, and Russia) to overtake one another in the new, apparent arms race for AI dominance will be analysed, with the three leading figures seeking to harness its potential for increasing both economic and military power.

The ubiquitous integration of technology in communities, and its exploitation by malign actors, places the concept of 'hybrid threats' in the spotlight, and the report will explore their elusive nature and strategies as part of a revolutionary type of warfare that involves both conventional, unconventional, and contemporary tactics. Among these threats, terrorist organisations will receive an equal amount of attention. After establishing an analytical framework, the following section will delve into the motivations and strategic advantages terrorists would have in using AI-supported technologies, supplied or requisitioned, with examples ranging from their tactical potential to nullify established defences at critical locations, towards using them for recruitment

purposes. As a follow-up, the risks of 3D printing used for terrorist purposes, such as the risk of creating untraceable, home-made weaponry, will be examined.

Finally, the aspect of artificial intelligence being a dual-use technology will be explored. The case studies of autonomous vehicles and deep fakes will be central to understanding both beneficial and nefarious uses of AI. After establishing a background on each, the report will proceed to highlight the environmental and social benefits of autonomous vehicles, while also highlighting the risk of them being hacked and becoming a physical danger to drivers and communities through turning a tool for organised crime or terrorist organisations. Equally, deep fakes will also benefit from an analysis into their impact on education and disinformation alike. The report will conclude with a number of recommendations on how to counteract these threats.



Key words: AI, terrorism, technology, hybrid threats, security, drones

INTRODUCTION

Terrorism is presently seen as a major threat to global order. The negative nature of this phenomenon, even if it were to be demonstrated in the form of a single attack, can entirely disrupt states and international organisations from functioning normally. The destructive effects of terrorist activities impact the victim's economic, political and social situation and hinder the process of strengthening their security potential. Moreover, an unexpected terrorist attack calls into question the effectiveness of the counterterrorism efforts and methods of combating dangers related to this threat.

The phenomenon has been used as a form of combat since the dawn of time. Indeed, the manifestation of beliefs and views of, among others, political, religious, or ideological nature through aggression and violence against a state, has been used numerous times in the past. Over the years, only the tools used by terrorists have evolved. While attacks with cold weapons are still common, nowadays terrorists also use explosives, machine guns, or even guided missiles. The present growth of the arms market has led to terrorist groups being heavily militarised, as they can successfully acquire new weapons and subsequently use them in their attacks. This state of affairs has directly affected the security of individual states and societies, and subsequently became a principal subject of discussion in international security forums.

Technology has also contributed to the aggravation of this threat. Technological progress has had a huge impact on peoples' lifestyles. First and foremost, it makes life much easier and convenient, offering rapid transportation options, easy shopping experiences, online contacts and more. With it ensues the development efforts of sectors such as military and IT. Technology is becoming ubiquitous, and the potential of what it can deliver with regard to the development of the future is practically limitless, as assessed by human perceptions. Thus, the emerging projects utilising artificial intelligence and their improvement of systems simulating human behaviour are considered by many as being a natural part of humanity's progression.

Artificial intelligence is deemed as a product of the future, which can become a breakthrough in humanity's technological progress. Its purpose is to lead to a significant acceleration of all processes where machine functions (within computers, specifically) are involved to acquire knowledge about the world, through machine learning and problem-solving. The main objective is to develop a system that is able to be controlled without human involvement. Moreover, on the basis of countless amounts of data, while performing certain tasks, artificial intelligence could make the best and most effective decisions based on its advanced and quick calculations. It seems to be an ideal example of how developed technologies significantly strengthen humanity's potential. The use of such IT solutions would certainly be applicable in every area of life, as well as in the area of conducting wars or terrorist actions.

It should be stressed that advanced IT systems are not just used to gain international prestige for being the world's most advanced state. It is also a part of an armed competition, where drones, controlled missiles, and command systems are able to be employed to gain a military advantage. On the other hand, wide popularity and regular use of new types of weapons will lead others (both state and non-state actors) to acquire them. Therefore, it becomes probable that terrorists, too, will eventually have access and employ advanced systems to conduct attacks. After all, they have previously employed drones and malign computer software (as part of cyberterrorism tactics) to that end.

These advanced technologies at the hands of terrorist organisations are a serious threat to the security of many countries and their citizens. Furthermore, the novel nature of these advanced technologies, employed by both states and terrorist organisations, can increase the threat and severity of conflicts and attacks simply due to their ground-breaking nature. In addition to the physical threats, there are also going to be new challenges of a cyber nature, with terrorists using state-of-art technologies and perhaps also AI to forward their goals.

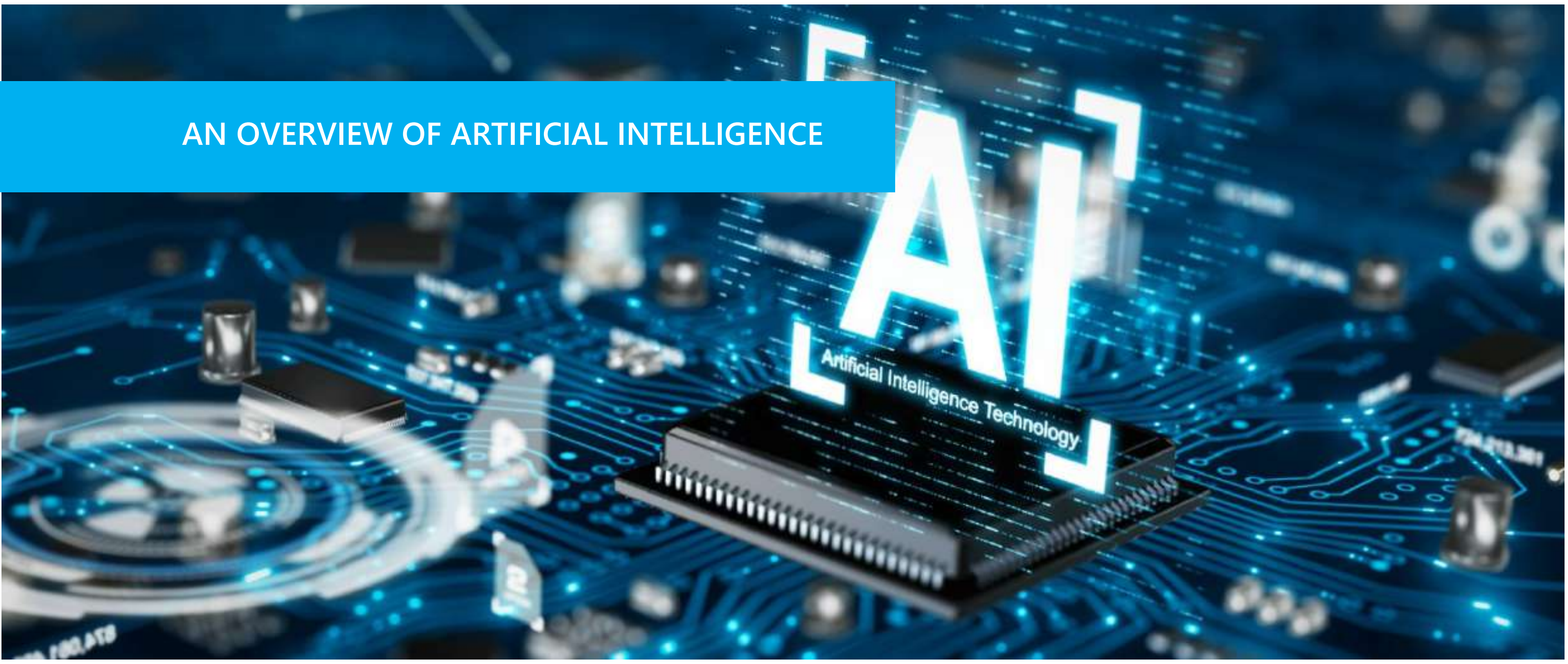
This report provides a comprehensive overview of the research into the impact artificial intelligence has with regards to terrorism, hybrid threats, and the disinformation phenomenon. At the same time, it constitutes a guide that aims to highlight multiple threats caused by modern tools that are also used by terrorist groups. In addition, due to the ongoing technological competition primarily between the USA, China and Russia, it is necessary to constantly analyse the emerging challenges to global security to prepare for future challenges rising as a result of this race. Without doubt, one of the greatest problems facing humanity is the purpose and methods through which advanced systems are employed. The time of action could not be more opportune than now, considering the risks of lethal weapons or otherwise revolutionary systems being continuously developed for the competing purposes of the world's superpowers, or requisitioned by terrorists in order to violate international order and coerce others into meeting their demands. The key focus for effective implementation of the security strategy is prevention, and identification and analysis of threats is the first stage in the process of combating terrorism.

The threat of terrorist organisations possessing and using AI does not seem to be decidedly distant. However, the difference between predictions and reality is noticeable; such dangers become more real when their visibility or proximity increases. Terrorism as a concept has many definitions since many countries define threats of terrorist nature differently. It is true that some actions may be characterised by one superpower as terrorism and by another as military acts executed for security reasons. Equally real is the use of a terrorist organisation by a state actor to achieve their own objectives.

This study also aims to be one of the stages in the scientific process centred at defining contemporary relations in the security environment.

This defining is of utmost importance, for as long as artificial intelligence has not fallen in the hands of terrorists, the world powers still have the chance to come up with security measures and regulations to prevent such a risk from manifesting into reality.

AN OVERVIEW OF ARTIFICIAL INTELLIGENCE



This section shall outline the general idea behind AI. In particular, it will be focused on providing its definition and explaining what AI is, as well as exploring some of the benefits that it brings (here, the focus will be put on positive changes the AI brings to the retail, healthcare, and military sectors). It shall also address some disadvantages associated with it and challenges it may pose, namely the issue of ethics and unemployment that AI may cause.

Definition of AI

Currently, there is no commonly agreed-upon definition of AI.[1,2] The AI field is going through constant and prompt changes and developments, which results in quite a proliferation of possible definitions and understanding of AI. For the past decade or so, there has been a significant revival of interest in the AI, and this technology is swiftly growing and attracting attention across many fields.[3] Indeed, since 2010, the amount of academic publications on artificial intelligence has risen 8 times.[4]

Knowing this, the term AI can be characterised as an umbrella term: it covers a broad range of applications and technologies and refers to the field within computer science which aims at 'building smart machines capable of performing tasks that typically require human intelligence'[5], which would be either fully or partially autonomous. AIs are able to mimic or exhibit functions associated with human behaviour, such as the ability to learn (a subject discussed below), reason, self-correct, or understand languages.[6] AI-based systems may be software-based and act in the virtual world (for instance, face and speech recognition systems, software designed for image analysis), as well as embedded in hardware devices (autonomous vehicles, drones, etc.).[7]

[1] McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online] p.4. Available at: <https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx> [Accessed 22 October 2020].

[2] Sayler, K., 2020. *Artificial Intelligence And National Security*. [online] Available at: <https://fas.org/sgp/crs/natsec/R45178.pdf> [Accessed 11 November 2020].

[3] Sayler, K., 2020. *Artificial Intelligence And National Security*. [online] Available at: <https://fas.org/sgp/crs/natsec/R45178.pdf> [Accessed 11 November 2020].

[4] Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] Available at: <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf> [Accessed 16 October 2020].

[5] Builtin.com. n.d. *What Is Artificial Intelligence? How Does AI Work?*. [online] Available at: <https://builtin.com/artificial-intelligence> [Accessed 1 November 2020].

[6] Techjury.Net, 2019. *Infographic: How AI Is Being Deployed Across Industries*. [online] Robotics Business Review. Available at: <https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/> [Accessed 28 October 2020].

[7] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.

There are different types of AI technology. A particularly prominent one is machine learning. It is the ability of AIs to learn or adapt to their environments (the latter in the case of robots) so that they are able to perform tasks without being specifically programmed to do so. AIs with such capabilities are based on algorithms that allow them to learn and improve through experience. Though there is a variety of methods based on machine learning, the three main ones are supervised learning, unsupervised learning, and reinforcement learning.[8] AIs with machine learning capabilities can forecast patterns, future behaviours or project outcomes, all without a need for human interference. Though machine learning is very popular, it is important to stress that a lot of 'highly capable AIs and robots do not make use of machine learning.'[9]

Advanced concepts of machine learning are referred to as 'deep learning' and they are another example of AI technology. Other kinds of AI are, for instance, natural language processing, machine vision, robotics, and robotic process automation.[10]

Benefits that AI offers

The benefits of artificial intelligence are vast, enhancing the quality of peoples' lives through its many diverse applications. Indeed, AI has had, and will certainly continue to have, a tremendous impact on peoples' lives, altering substantially their everyday reality. AI constitutes a positive change on many different levels in a number of industries, fields, and disciplines, such as education, media, agriculture, or banking. Unfortunately, as the range of benefits in these sectors and beyond are too vast to be explored individually here, the focus on the advantages of AI will be briefly presented on the example of retail, healthcare, and military sectors.

[8] Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] Available at: <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf> [Accessed 16 October 2020].

[9] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.

[10] Techjury.Net, 2019. *Infographic: How AI Is Being Deployed Across Industries*. [online] Robotics Business Review. Available at: <https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/> [Accessed 28 October 2020].

Retail sector

The retail industry has been substantially changed by AI in recent years. Artificial intelligence allowed businesses that have introduced its applications into their operations to gain a financial lead over the companies that decided to adhere to more traditional, or conservative, ways of running their interests. AI has proven its worth in the retail sector and will remain here, thus companies that do not use it at the moment will probably have to incorporate AI to remain in the competition.

Retail is one of the industries exceptionally rich in data, with virtually infinite factors that influence current and upcoming trends, and customer decisions. It is exceptionally hard to understand – and predict – these dynamics, but artificial intelligence offers retailers the help they need in doing just that. AI algorithms are able to analyse much more data than the human brain can process, much faster, and with a smaller probability of error than it is in the case of humans. Furthermore, artificial intelligence may be used for the purpose of spotting behavioural changes of customers, looking for unapparent data patterns, therefore allowing retailers to ‘serve the right promotion, at the right time, to the right person, on the right device’[11], or even identify and predict upcoming trends – all while doing it more efficiently, effectively, and in less time than people. Ultimately, AI can accelerate the decision-making process and help make better-informed decisions, thus allowing businesses to prosper.

Aside from the above, AI can be used in logistics and optimisation of the supply chains, saving both time and money.

[11] Saker, R., 2020. *The Impact Of Artificial Intelligence In Retail*. [online] My Total Retail. Available at: <https://www.mytotalretail.com/article/the-impact-of-artificial-intelligence-in-retail/> [Accessed 25 October 2020].

Healthcare

There are numerous examples illustrating how artificial intelligence, in addition to other technological advancements, can be used in medicine and healthcare. While only a handful will be provided here, its benefits beyond those mentioned below must be recognised with some notable examples being, for instance, improving patients' hospital experience through performing some of the administrative tasks, managing patient data and medical history, or even assisting in surgeries (the number of robot-assisted surgeries has been increasing extraordinarily in recent years). Moreover, AI also reduces healthcare system costs,[12, 13] but with the new applications of AI for healthcare and medicine being designed, an even larger amount of money will be saved.

A key benefit of the functions AI has in healthcare is improving the diagnostic process – indeed, AI-run algorithms are able to diagnose illnesses in a more accurate and faster manner than its human counterpart. An example of that is the case of clinical microbiologists working at the teaching hospital of Harvard University's Beth Israel Deaconess Medical Centre, who used AI-enhanced microscopes to diagnose blood diseases.[14] Due to using AI-enhanced equipment, they are were able to do so faster than it would take on average, and thus they increased patients' chances for recovery. Microbiologists taught the AI equipment they were using to recognise specific bacteria (one of which was E. coli) which, after being trained, achieved over 90% accuracy. 'With further development and training [...] the AI-enhanced platforms could be used as a

[12] University of California, 2016. *Big Data, Analytics & Artificial Intelligence. The Future Of Health Care Is Here*. [online] San Francisco. Available at: <https://www.gehealthcare.com/static/pulse/uploads/2016/12/GE-Healthcare-White-Paper_FINAL.pdf> [Accessed 9 November 2020].

[13] Daley, S., 2020. *32 Examples Of AI In Healthcare That Will Make You Feel Better About The Future*. [online] Built In. Available at: <https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare> [Accessed 22 October 2020].

[14] Mitchell, J., 2017. *BIDMC Researchers Use Artificial Intelligence To Identify Bacteria Quickly And Accurately*. [online] Bidmc.org. Available at: <https://www.bidmc.org/about-bidmc/news/bidmc-researchers-use-artificial-intelligence-to-identify-bacteria-quickly-and-accurately> [Accessed 4 November 2020].

fully automated classification system in the future.'[15] Furthermore, AI could solve the problem of the shortage of human technologists (the sector is expected to be even further understaffed in the coming years than it is now, for instance in the US).

Another function of AI in healthcare is aiding the development of new medicines. AI can offer biotechnological and biopharmaceutical companies more accurate and efficient ways of doing necessary research. For instance, a Toronto-based company named Deep Genomics uses an AI platform that aids its researchers to accelerate finding the right candidates for developmental drugs, which in turn significantly decreases time, potentially saving more lives, as well as cost.[16]

Aside from the above, AI has also been used to aid in combatting the outbreak and spread of the COVID-19 pandemic. An example of that will be provided in the section that explores China's approach to AI development.

Military sector

AI's growing potential could have significant implications for national security. As such, a number of countries have been engaged in developing AI applications for a range of military purposes. Indeed, AI is being used in the fields of information operations, intelligence collection and analysis, logistics, as well as in fully or partially autonomous vehicles. What is more, AI has already been integrated into military operations, for instance in those occurring in Syria and Iraq.

[15] Mitchell, J., 2017. *BIDMC Researchers Use Artificial Intelligence To Identify Bacteria Quickly And Accurately*. [online] Bidmc.org. Available at: <https://www.bidmc.org/about-bidmc/news/bidmc-researchers-use-artificial-intelligence-to-identify-bacteria-quickly-and-accurately> [Accessed 4 November 2020].

[16] Daley, S., 2020. *32 Examples Of AI In Healthcare That Will Make You Feel Better About The Future*. [online] Built In. Available at: <https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare> [Accessed 22 October 2020].

Of the many possible examples that could be brought up here, one of the advancements in image recognition and analysis,[17] through which information from a given image or video is extracted, as well as including its implications for military forces, will be explained. Among other areas, this advancement will find an especially suitable place in surveillance and threat monitoring operations. Surveillance usually involves long hours dedicated for searching through repetitive backgrounds, looking for alterations in rather unchanging environments. As machines can be taught to analyse images similar to how the human brain does – an even more thoroughly than people are able to do – such monotonous tasks might be better performed by unmanned vehicles equipped with AI, which can be employed, for instance, to patrol given areas, identify potential threats and enemies (be it insurgents, terrorists, or enemy soldiers), and share the obtained intelligence with their human coordinator, all while performing the task with a reduced chance of error than when using human soldiers. Indeed, AI may aid human operators in detecting unusual patterns in videos and images, enabling them to obtain mission results faster and safer, additionally lessening risk for soldiers on the ground. An example of that is the Maven Project, run by the U.S. military to identify potential enemy targets (this will also be mentioned in the section that covers the US development of AI).

Challenges the AI poses

Despite all the benefits associated with the AI, there is another side to its development, which ought to be addressed as well. This point will be explained on two examples: the issue of ethics and AI's potential to cause unemployment.

[17] Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] Available at: <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf> [Accessed 16 October 2020].

Ethics

Along with the development of AI, questions concerning the ethics and morality of this technology – linked to many different aspects that have been or will be altered by it – are arising. The issue of ethics is indeed one of the most, if not the most, often brought up subjects when discussing the disadvantages of AI. AI technology offers those in its possession powerful capabilities, which can be used not only for noble purposes, but also to inflict harm upon others, break the rule of law, or serve as means for undertaking any immoral and unlawful action its operators want to perform with it. Just to name a few, AI can be used for the purpose of violating peoples' right to privacy, subjecting them to biased and disproportionate surveillance (artificial intelligence is being misused in this particular way by the Chinese authorities, an aspect that will be brought up while describing China's approach to AI below), or violating freedom of speech (in India, AI tools have been used as automated content removal, which increases the risk of censorship).

The use of AI in warfare has been a topic of many debates and discussions. Though partially autonomous systems have been used by armed forces since World War II, significant advancements in AI development have pushed the usage of military automation to a critical point.[18] Although, as indicated above, AI has the potential to bring many advancements to the military sector that can be of much help for members of the armed forces, it needs to be remembered that artificial intelligence is also considered to alter warfare as much as 'nuclear weapons, aircraft, computers, and biotech'[19] have done. Indeed, using AI in warfare results in, at least, a few moral and ethical questions. One of them is the concern that AI systems used in combat, which lack human judgement, may violate the rules of International Humanitarian Law, for instance,

[18] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.

[19] Allen, G. and Chan, T., 2017. *Artificial Intelligence And National Security*. [online] Belfer Center for Science and International Affairs, p.1. Available at: <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> [Accessed 8 October 2020].

by violating the rule of proportionality, or by unlawfully targeting civilians, mistakenly taking them for enemy combatants. This, in turn, leads to another issue associated with AI being employed in warfare – accountability. Namely, who ought to be responsible for war crimes committed by an autonomous system – the person that programmed it in the first place, the one operating it, or the supervisor overseeing the operation. Despite the fact that some arguments on this topic have already been made, this issue constitutes an open debate, with various answers to the issues above.

Therefore, it is imperative for the development of AI technology, both for civilian and military usage, that it is carried out in accordance with certain rules and norms. One of the countries that have stressed in the recent past its commitment to the ethical development and use of AI technology for military purposes is the US. According to the statement released on 31 October 2019 by advisers from the Pentagon, who belong to the Defence Innovation Board, there is a need to take into account AI ethical principles.[20] Those ethics are an inseparable element in research on the use of artificial intelligence. The group of sixteen notable experts offered five main principles to follow in order to handle AI, and those are responsibility, equitability, traceability, reliability, and governability. In addition, the report indicates recommendations for the U.S. military, which could apply ethical principles in the future. The most apparent information is that humans are responsible for the development, deployment, usage, and future outcome of machines controlled by AI.[21] The Pentagon continuously cooperates with experts to avoid possible damages made either by American technology or AI which was improved by other states. It can be argued that the US wants to conduct transparent research on the development of imitation of human intelligence when it comes to ethics, and that it advocates developing the AI with the respect to the rule of law.

[20] U.S. Dept of Defense, 2020. *DOD Adopts Ethical Principles for Artificial Intelligence*, [online] Available at: <https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/> [Accessed 12.10.2020].

[21] U.S. Dept of Defense, 2020. *DOD Adopts Ethical Principles for Artificial Intelligence*, [online] Available at: <https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/> [Accessed 12.10.2020].

However, there are other initiatives carried out by various organisations and institutions in a number of countries aiming to ensure the ethical and moral development of AI in all sectors. This is the main purpose of, for instance, the German-based Institute for Ethics in Artificial Intelligence, the British Institute for Ethical Artificial Intelligence in Education, and the Institute for Ethical AI & Machine Learning.

What is more, only last year, the EU published its set of requirements that AI technology must meet in order to be trustworthy. The – quite comprehensive in scope – list of EU's proposed prerequisites include: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental wellbeing, and accountability.[22]

With all the arguments and perspectives presented, it is worth concluding this section by saying that AI development must be ensured to take place 'in ways that build trust and understanding, and respect human and civil rights'[23] in the name of guaranteeing safe and uncompromising harnessing of its potential.

Unemployment

It is true that the growing AI sector means that there is a constant need for more and more scientists, AI programmers, etc.; though people employed in other sectors do not necessarily share the enthusiasm for AI. The truth is that AI advancements in many sectors decrease the need for human operators, eventually leading to increased redundancies and unemployment.

As AI may perform a number of tasks better, cheaper, and faster than human beings – and indeed, it does so – many jobs are being automated, to the extent that

[22] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.

[23] Dignum, V., 2018. *Ethics in artificial intelligence: introduction to the special issue*. Ethics and Information Technology, 20, pp. 1-3.

the demand for people in employment decreases. AI may not cause mass unemployment as a result of its implementation, however, it may – on a large scale – replace humans performing low-skilled jobs who may end up with their chances to find employment in another place somewhat limited, due to lacking more sophisticated qualifications and skills. As it stems from the report published by McKinsey Global Institute in 2017, already developed technologies could automate as much as half of the work activities performed in countries like Thailand (55%), Indonesia (52%), or Malaysia (51%).[24] Though introducing AI to take over humans' tasks will certainly not happen instantaneously, it may still leave a large number of workers unemployed as it progresses through time.

In order to illustrate that AI may also cause unemployment in wealthier countries than the ones mentioned above, a closer focus should be put on the US. Since 2000, over 5 million factory jobs were lost in that country, devastating many families and communities. Los Angeles Times predicted that with the advancement of the era of driverless cars, as much as another 5 million jobs nationwide could be lost, and most of the drivers that will be made redundant will 'belong to the same demographic cohort'[25] as factory workers who had been fired before because their job was automated. To highlight this development further, a number of cities across the world have declared switching to autonomous buses in the future, amongst them being New York, Singapore, or Edinburgh.[26] However, drivers will not be the only ones in need of searching for new jobs, but also gas attendants or the people working in the parking lots.

[24] McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online] p.4. Available at:<https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx> [Accessed 22 October 2020].

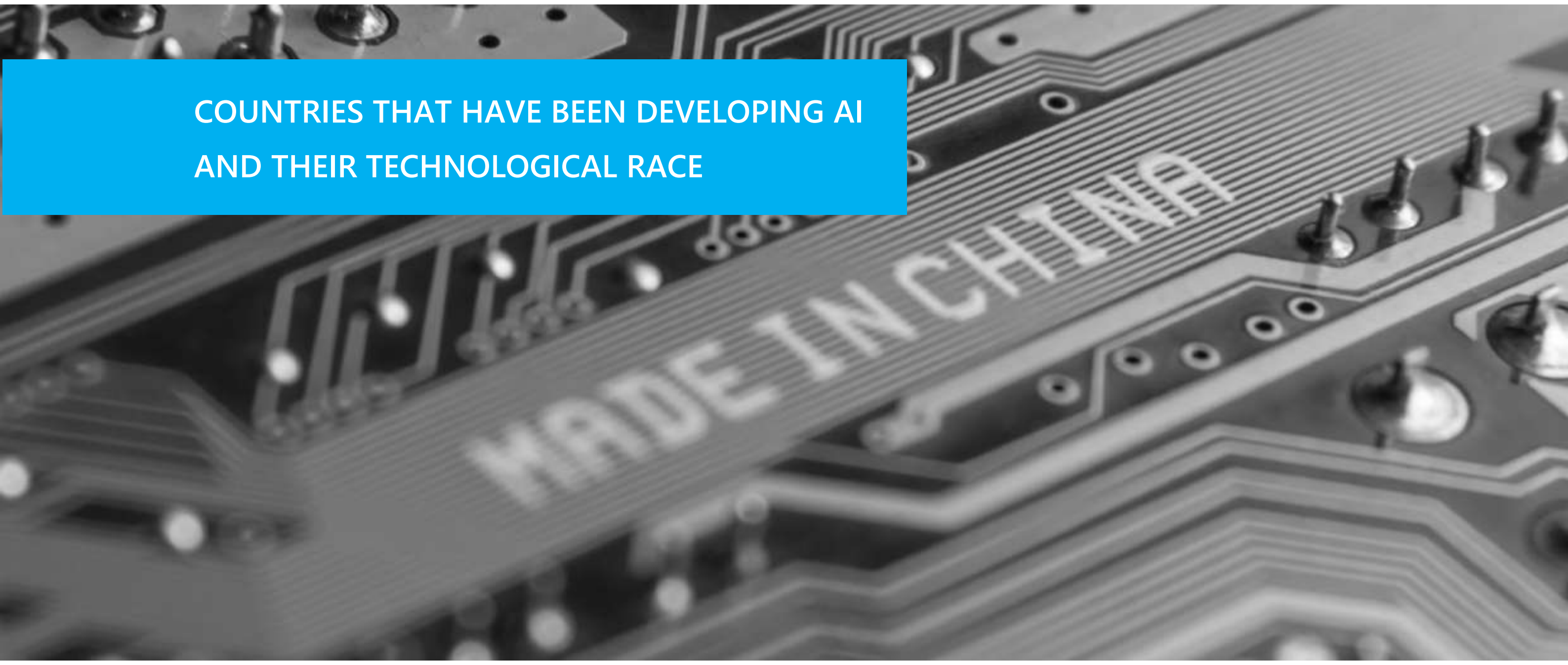
[25] Greenhouse, S., 2016. *Op-Ed: Autonomous Vehicles Could Cost America 5 Million Jobs. What Should We Do About It?*. [online] Los Angeles Times. Available at: <https://www.latimes.com/opinion/op-ed/la-oe-greenhouse-driverless-job-loss-20160922-snap-story.html> [Accessed 12 October 2020].

[26] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.

It also needs to be emphasised that not only blue-collar workers are faced with the possibility of losing their source of income, as AI has already demonstrated its potential to reduce white-collar jobs too, ‘such as many in the post office and in customer service’.[27]

[27] Rotman, D., 2013. *How Technology Is Destroying Jobs*. [online] MIT Technology Review. Available at: <https://www.technologyreview.com/2013/06/12/178008/how-technology-is-destroying-jobs/> [Accessed 24 October 2020].

COUNTRIES THAT HAVE BEEN DEVELOPING AI AND THEIR TECHNOLOGICAL RACE



International competition for AI development

As already demonstrated above, artificial intelligence is a field of technology with substantial implications in a number of spheres, including security, at both an international and national level. Many countries, having recognised its significance, have entered in a competition to develop the most sophisticated and advanced AI systems for military and civilian purposes.

Amongst the countries that have been pursuing AI development are the US, China, Russia, Canada, Germany, United Kingdom, India, and Japan. Each of them has its own path for developing AI and focus on advancing different aspects of it. The leaders in the AI competition, according to a number of studies, are the US and China, and indeed, the vast majority of the countries that participate in the AI race find it hard to compete with either of them. For that reason, some of the countries are attempting to move to the forefront of specific areas of AI development, for instance, the UK, whose authorities announced in 2018 that they plan for the country to become the global leader on 'ethical AI'. Matthew Gould, the U.K. Director General for Digital and Media

Policy, stated that British researchers are to 'consider ethics every step of the way, rather than relegate it to an afterthought'.[28] Germany, on the other hand, recognising that the potential of its non-European rivals is far greater, laid in 2018 out its plan to become Europe's leading centre in AI.[29]

However, it is not only the economically powerful nation-states with large populations have been developing AI. Smaller ones, such as Vietnam and Malaysia, have shown their interest in pursuing AI development too.[30]

Countries around the globe are aware that AI will substantially transform the world's military power balance, and through such shift will come a change in the global political landscape itself. AI may offer considerable technological and military power to otherwise smaller states (in terms of their economic capabilities, population, or military capabilities[31]). It is certainly one of 21st century's most powerful force multipliers.

Out of all the countries that have been focusing to develop AI in recent years, this paper shall take into consideration the US, China, and Russia: the three countries that are most often perceived as the leading players in AI development. Those three main competitors have spent an enormous amount of money (though Russia is said to have spent somewhat less than the US and China) on AI development. Despite each of the aforementioned countries' efforts to develop AI warranting an exploration in

[28] Renstrom, J., 2018. *The UK Wants To Be The World Leader In Ethical AI*. [online] Slate. Available at: <https://slate.com/technology/2018/08/the-u-k-wants-to-be-the-world-leader-in-ethical-a-i.html> [Accessed 6 November 2020].

[29] European Commission, n.d. 2020. *Germany AI Strategy Report*. [online] European Commission. Available at: <https://knowledge4policy.ec.europa.eu/ai-watch/germany-ai-strategy-report_en> [Accessed 13 November 2020].

[30] McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online]. Available at:<https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx> [Accessed 22 October 2020].

[31] Kudzko, A., 2018. *Future Now: How AI Is Already Changing The Global And Military Landscape - GLOBSEC*. [online] GLOBSEC. Available at: <https://www.globsec.org/2018/02/06/future-now-ai-already-changing-global-military-landscape/> [Accessed 8 November 2020].

greater details, including a view on their heavy investments in their own research operations, the authors of this paper have understood that the threat of non-state actors misusing and abusing AI technology to fulfil their own agenda demands special attention within this paper. Regardless, the three mentioned state actors will benefit from a sweeping overview of their AI efforts below.

The United States

It may be argued that the United States was the greatest beneficiary of the last wave of technological development, and it should not be of any surprise that it is the home to some of the world's biggest and most important tech companies, including Apple, Facebook, or Google, to name only a few. With the AI advancement being the current wave of digital development, Donald Trump reportedly said that the 'continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States [...]'.[32] Indeed, a number of reports, analyses, articles, etc., confirms that it is the US that leads the global AI development competition, both in specific aspects of it, as well as in general terms.[33,34,35,36]

Over the past years, the U.S. authorities have demonstrated the seriousness they treat AI development with. Among many examples, *The U.S. National Defense Strategy*

[32] Srivastava, S., 2020. *State Of Artificial Intelligence In US: Becoming Technology Superpower*. [online] Analytics Insight. Available at: <https://www.analyticsinsight.net/state-of-artificial-intelligence-in-us-becoming-technology-superpower/> [Accessed 25 October 2020].

[33] Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?.* [online] Who Is Winning the AI Race: China, the EU or the United States?. Available at: https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf [Accessed 2 October 2020].

[34] Lopez, C., 2020. *Where It Counts, U.S. Leads In Artificial Intelligence.* [online] defense.gov. Available at: <https://www.defense.gov/Explore/News/Article/article/2269200/where-it-counts-us-leads-in-artificial-intelligence/> [Accessed 25 October 2020].

[35] Banerjee, I. and Sheenan, M., 2020. *America'S Got AI Talent: US' Big Lead In AI Research Is Built On Importing Researchers*. [online] macropolo.org. Available at: <https://macropolo.org/americas-got-ai-talent-us-big-lead-in-ai-research-is-built-on-importing-researchers/?rp=e> [Accessed 25 October 2020].

[36] McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online]. Available at:<https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx> [Accessed 22 October 2020].

of 2018 indicated artificial intelligence to be one of the technologies that will allow the US to 'fight and win the wars of the future'.[37] In order to not allow China or Russia to get ahead of the US in the AI arms race, the Joint Artificial Intelligence Centre was established within the Department of Defence in 2018. Amongst its main tasks are 'accelerating the delivery and adoption of AI; scaling the impact of AI across the Department [and] defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident'.[38] In February 2019, President Trump launched the American Artificial Intelligence Initiative, which is supposed to 'support AI innovation that [in turn shall] increase prosperity, enhance national security, and improve quality of life for the American people'.[39]

Interestingly, the authorities in the US decided to team up with the UK and recently signed a declaration on cooperation in AI research and development, through which they want to promote 'mutual wellbeing, prosperity, and security of present and future generations'.[40]

The US, along with its competitors in the AI race, pursues advancements in AI both for military and civilian purposes, the latter including projects that are meant to aid the fight with the COVID-19 pandemic.[41] The former, however, can be characterised with multiple examples. For instance, different branches of the U.S. military have been working on introducing semiautonomous and fully autonomous vehicles,[42] and some tests have been performed by the U.S. Air Force (Loyal Wingman programme), the

[37] 2018. *Summary Of The 2018 National Defense Strategy Of The United States Of America*. p.3.
[38] Taken from the Department of Défense's Chief Information Officer website. Available at: <https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/> [Accessed 22 October 2020].
[39] The White House Office of Science and Technology Policy, 2020. *American Artificial Intelligence Initiative: Year One Annual Reports*. p. iii.
[40] The Declaration is available at: <https://www.state.gov/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-artificial-intelligence-research-and-development-a-shared-vision-for-driving/> [Accessed 20 October 2020].
[41] Lopez, C., 2020. *Where It Counts, U.S. Leads In Artificial Intelligence*. [online] defense.gov. Available at: <https://www.defense.gov/Explore/News/Article/article/2269200/where-it-counts-us-leads-in-artificial-intelligence/> [Accessed 25 October 2020].
[42] Congressional Research Service, 2020. *Artificial Intelligence And National Security*. p.13.

Army (Robotic Combat Vehicles, with autonomous functions of surveillance, navigation, and IED removal[43]), or the Navy (Anti-Submarine Warfare Continuous Trail Unmanned Vessel, called 'Sea Hunter', which, if successfully entered into service, would 'provide the Navy with the ability to autonomously navigate the open seas, swap out modular payloads, and coordinate missions with other unmanned vessels',[44] while being able to remain continuously deployed for a period of several months[45]). Furthermore, a few years ago the U.S. military introduced an AI program called Project Maven, which uses techniques of machine learning to help American soldiers identify targets in videos made by drones. Project Maven has been deployed to various locations, for instance, in the Middle East and Africa.[46]

Another example is the new system intended for the US Air Force that launched this year, called Advanced Battle Management System (ABMS). At the beginning of September 2020, further tests took place, which significantly increased the possibility to use artificial intelligence and virtual reality headsets during a battle. ABMS includes the use of armed forces on the ground, air, and sea through the connection in cyberspace (with the considerable speed of 4G and 5G) which is supported by AI and supervised by human operators. Jointly the system combines 35 military platforms in 30 locations and is based on four military compounds. The Advanced Battle Management System is one of the main priorities for the Department of the Air Force, receiving financial support of about $3.3 billion in five years. Many of the U.S. commanders and chiefs were positively surprised about the ease of eliminating various threats. Although at the beginning of the test some of them were sceptical and concerned about the use

[43] Congressional Research Service, 2020. *Artificial Intelligence And National Security*. p.13.

[44] Congressional Research Service, 2020. *Artificial Intelligence And National Security*. p.14.

[45] Defense Advanced Research Projects Agency, 2018. *ACTUV "Sea Hunter" Prototype Transitions to Office of Naval Research for Further Development.* [online] Available at: <https://www.darpa.mil/news-events/2018-01-30a> [Accessed 18 October 2020].

[46] McLeary, P., 2018. *Pentagon'S Big AI Program, Maven, Already Hunts Data In Middle East, Africa*. [online] Available at: <https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa/> [Accessed 11 November 2020].

of artificial intelligence, yet after the possibilities of ABMS[47] were demonstrated, they indicated the need for the development of this kind of system. They added that this system is essential to compete in the international security environment and deter adversaries who are using such advanced technology too. Additionally, it was the biggest American military exercise involving the usage of AI.[48]

China

China is considered as one of the countries that are most intensively involved in the global competition for AI development. Seen by some as the world leader, while others more often place China behind the US in the AI race,[49] Beijing is said to have been making more rapid progress when it comes to AI development than any other states. Chinese authorities have announced their ambition for China to become the world leader in AI by 2030,[50] as they realised – along with other countries taken into consideration in this paper and beyond – that artificial intelligence is key to the future and whoever masters its development, in the words of the Russian President Vladimir Putin, 'will be the ruler of the world'.[51] Chinese senior leadership is very well aware that AI technology is inevitable for military development, as well as for the future global

[47] Daily Military Defense, *Hypervelocity weapons systems are tested in support of the Advanced Battle Management System*. [online] Available at: <https://www.youtube.com/watch?v=XgwZmkT8VX0&feature=emb_logo> [Accessed 16.09.2020].

[48] Pope, C., 2020. *Advanced Battle Management System field test brings Joint Force together across all domains during second onramp.* [online] Available at: <https://www.af.mil/News/Article-Display/Article/2336618/advanced-battle-management-system-field-test-brings-joint-force-together-across> [Accessed 16.09.2020].

[49] Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?*. [online] Who Is Winning the AI Race: China, the EU or the United States?. Available at: <https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf> [Accessed 2 October 2020].

[50] Webster, G., Creemers, R., Triolo, P. and Kania, E., 2017. All Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017). [online] Available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/> [Accessed 1 October 2020].

[51] The Verge, 2017. Putin Says The Nation That Leads In AI 'Will Be The Ruler Of The World'. [online] Available at: <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world> [Accessed 5 October 2020].

economic competition between major powers. Because of that, Beijing has been anything but parsimonious when it comes to developing artificial intelligence.

Indeed, China has already made enormous investments in the AI field, for instance, spending large sums of money on AI education. In 2018, Chinese Ministry of Education launched a number of initiatives that are aimed at, amongst others, developing 50 world-class AI research centres and training over 500 instructors and 5000 students over the next few years.[52]

China pursues AI both in ways that are beneficial for its citizens (and mankind in broader terms) as well as worrisome for one of many reasons. Beijing has been making rapid progress in healthcare, among other sectors, through developing AI-run 'unstaffed medical clinics', able to 'provide online consultations for more than 2,000 common diseases, and [capable to] immediately answer tens of thousands of medical and health queries for users, with an international standard accuracy level',[53] or developing deep learning for the purpose of accelerating medical image processing, which in turn shall aid detecting cancer and other serious diseases much faster. Furthermore, it needs to be emphasised that for the past few months, a number of Chinese AI researchers have been involved in combatting the Covid-19 pandemic.

Nonetheless, not every aspect of the Chinese AI development is beneficial for average citizens and noble in its nature. The government of China has been using artificial intelligence in ways that clearly violate civil liberties and people's privacy. According to the reports published in 2019, AI has enabled Chinese authorities to subject

[52] Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?*. [online] Who Is Winning the AI Race: China, the EU or the United States?, p.19. Available at: <https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf> [Accessed 2 October 2020].

[53] Koh, D., 2019. *Ping An Good Doctor Launches Commercial Operation Of One-Minute Clinics In China.* [online] Available at: <https://www.mobihealthnews.com/news/asia-pacific/ping-good-doctor-launches-commercial-operation-one-minute-clinics-china> [Accessed 8 October 2020].

Muslim minorities living in China, notably Uyghurs, to mass surveillance of an unprecedented scale.[54] Reportedly, it has been common for the Chinese authorities and police to use AI algorithms for the purpose of collating personal data, including that obtained through the facial recognition system, and thus identifying citizens for detention. Indeed, 'the Chinese government has already used surveillance systems to place over a million of its citizens in re-education camps for the crime of expressing their Muslim identity'.[55]

Russia

In 2019, Russia adopted its National Strategy for Development of Artificial Intelligence for the period until 2030.[56] This document aims at, amongst other things, increasing spending on research and development of AI technology, software research, as well as creating a regulatory system of social relations that will arise in connection with the use of AI technology. In addition, in 2020, a federal AI development project was launched under the Russian Federation's Digital Economy Programme.[57]

Along with intensive work on developing military-related AI, which will be explored below, Moscow has been advancing such technology for civilian purposes. One of the companies that run and oversee Russian railways has been testing autonomous

[54] Shu, C., 2019. *Leaked Chinese Government Documents Detail How Tech Is Used To Escalate The Persecution Of Uighurs*. [online] Available at: < https://techcrunch.com/2019/11/24/leaked-chinese-government-documents-detail-how-tech-is-used-to-escalate-the-persecution-of-uighurs/> [Accessed 7 October 2020].

[55] Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020. p. 14.

[56] Sukhankin, S., 2019. *Russia Adopts National Strategy for Development of Artificial Intelligence*. Eurasia Daily Monitor 16(163). [online] Available at: <https://jamestown.org/program/russia-adopts-national-strategy-for-development-of-artificial-intelligence/> [Accessed 18 October 2020].

[57] Министерство цифрового развития связи и массовых коммуникаций Российской Федерации, 2020. *Цифровая экономика РФ*. [online] Available at: <https://digital.gov.ru/ru/activity/directions/858> [Accessed 25 November 2020].

trains.[58] Furthermore, it has been attempting to use AI to predict the demand for transport and tickets, though this system still needs to be further developed, as it has demonstrated many irregularities so far. Moreover, AI technology has also found its purpose in the education sector. It shall be used in the future to analyse students' grades and their learning progress, as well as controlling students' activity during classes, their digital footprint, and participation in university life.

Similarly, to other states, Russia has been pursuing the development of AI for military purposes for some time. As Vladimir Putin stated, AI will have greater value for security than nuclear warheads.[59] In turn, the Russian Ministry of Defence made it clear on multiple occasions that the Russian military is already in possession of a wide range of weaponry based on the AI technology, for instance, drones (which reportedly were used during the aggression on Ukraine) or underwater robots.[60] In 2018, Putin revealed that Russia has developed an unmanned submarine, able to carry nuclear weapons.[61] It is estimated that such submarines will be produced by 2027.

Interestingly, however, despite all the AI projects carried out by Moscow, Kremlin's spending on AI does not match the investments made by other countries competing with Russia in the AI race, potentially leaving them behind the competition for AI superiority.

[58] Коновалова, Н. 2019. *Беспилотная «Ласточка». На железнодорожном салоне в Щербинке показали уникальную технологию.* [online] Available at: <https://spbvedomosti.ru/news/financy/bespilotnaya-lastochka-na-zheleznodorozhnom-salone-v-shcherbinke-pokazali-unikalnuyu-tekhnologiyu/> [Accessed 20.10.2020].
[59] IZ., 2019, *Путин сравнил преимущества искусственного интеллекта и ядерного оружия.* [online] Available at: <https://iz.ru/928464/2019-10-03/putin-sravnil-preimushchestva-iskusstvennogo-intellekta-i-iadernogo-oruzhiia> [Accessed 12.11.2020].
[60] Савчук, Т., 2020. *Пентагон занепокоєний використанням Росією штучного інтелекту у військовій сфері. Ось чому* [online] Available at: <https://www.radiosvoboda.org/a/pentagon-zanepokoyenyy-vykorystannyam-rosiyeyu-shtuxhnogo-intelektu-u-viyskoviy-sferi/30841807.html> [Accessed 12.11.2020].
[61] RBC. *Путин назвал срок спуска на воду подлодки с ядерным «Посейдоном»*. [online] Available at: <https://www.rbc.ru/politics/20/02/2019/5c6d2c779a7947c9343f1028> [Accessed 13.11.2020].

HYBRID THREATS & HYBRID WARFARE

Hybrid threats are considered as one of the most dangerous challenges in the 21st century, and in terms of impact they are often compared to regular military conflicts and natural disasters. They constitute a serious danger to global stability due to their potential destructive force, unclear methods of operation, and a high capacity of coordination (with the possibility of missions being undertaken in several countries simultaneously). Hybrid threats are known to carry out ‘hybrid attacks’, which are understood as a combination of regular and irregular warfare employed at varying degrees of intensity and length, undertaken by military forces as well as criminal organisations, terrorists, and even political movements.

While a clear definition of hybrid threats was not underpinned yet, one of the most common understandings surrounding its nature is that these types of actors apply the aforementioned combination of both aspects of conventional military tactics as well as unconventional (or so-called ‘soft’) methods, including information warfare, propaganda, or harnessing mass media to manipulate public awareness for perpetrators’ goals. Non-standard threats, that is unconventional, hybrid, or asymmetrical, are all elements that partake in armed conflicts to ranging extents using different battle tactics to their own advantage. Therefore, they demand special attention from analysts, experts, and researchers in the field of international security. Since these threats are elusive, they push for a redefinition of the concept of war and adaptation of security policies to effectively prevent them.

Threats of a terrorist nature are also part of the definition covering hybrid threats, whereas before they were originally only perceived military threats as part of its terminology. The phenomenon of hybrid threats is often characterised by the use of unconventional methods or making use of technological breakthroughs that revolutionise their existing combat capabilities.[62] Hybrid threats often involve the concept of hybrid warfare, understood as the coexistence between the classic and new methods of war.[63] This means, among other things, the use of tactics such as information warfare, cyberattacks, and terrorist activities with the purpose of impacting societies in various ways.[64]

European Union defined hybrid threats as a mixture of coercive and subversive activity, as well as conventional and unconventional methods (i.e., diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.[65]

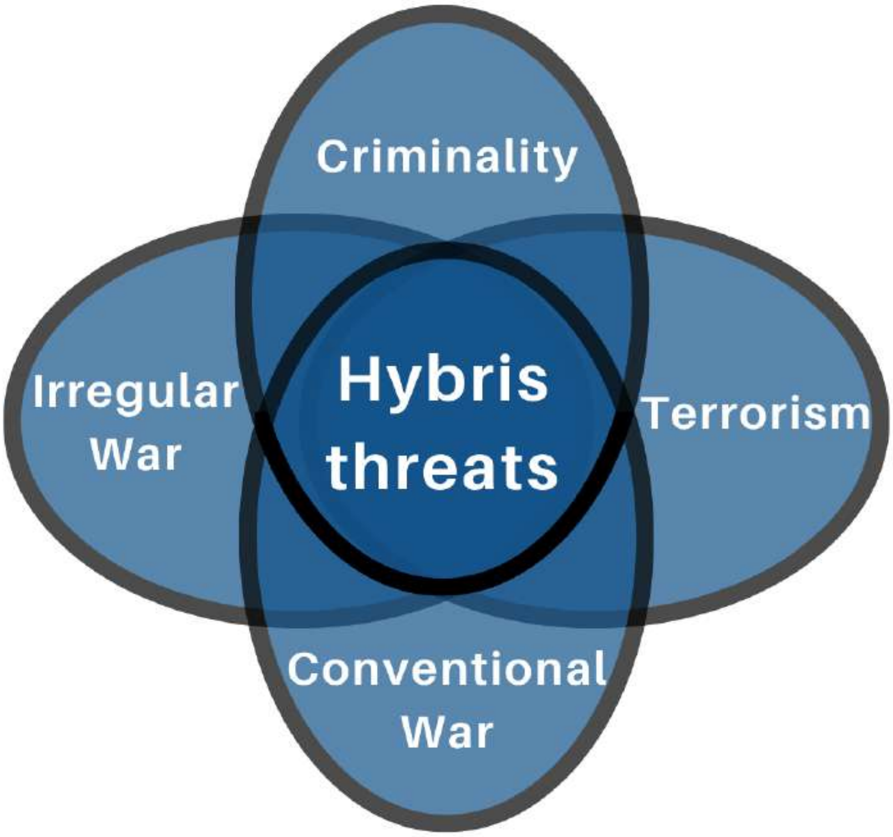
[62] Dziubek T., *Obronność państwa a zagrożenia asymetryczne*¸ [in:] *Nowe zagrożenia bezpieczeństwa. Wyzwania XXI wieku*, (red.) K. Hennig, Wyższa Szkoła Humanistyczno-Ekonomiczna, Kraków 2015, p. 17.

[63] Gruszczak A., *Hybrydowść współczesnych wojen – analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, (red.) W. Sokała, B. Zapała, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, p. 11.

[64] Kubaczyk T., *Wojna hybrydowa – (czy) nowy typ konfliktu zbrojnego we współczesnym świecie*, [w:] *Konflikt hybrydowy na Ukrainie. Aspekty teoretyczne i praktyczne*, (red.) B. Pacek, J. A. Grochocka, Piotrków Trybunalski 2017, p. 24.

[65] Maas J., *Hybrid Threat and CSDP*, pp. 125-130, [in:] J. Rehrl (Ed.), Handbook on CSDP - The Common Security and Defence Policy of the European Union, Vienna 2019.

Fig. Hybrid Threats



Source: Own study based on: S. Purton, *"What's in a name?... That which we call a rose by any other name would smell as sweet." Or, why half of winning an Irregular War is agreeing what it is...,* The International symposium on Military Operational Research, 26th Symposium, 2009, p. 9.

A key approach towards pinpointing the definitions of hybrid threats is to understand the strategy of actors who try to use those tactics to achieve their goals. A hybrid threat is first identified when a state or a non-state actor has the capacity and evident willingness to employ a hybrid strategy, which is understood as a comprehensive scheme to achieve one's own geopolitical and strategic objectives. A hybrid threat is manifested in activities that fall short of direct, conventional military action and which can be conducted for extended periods of time and with varying intensity.[66] Hybrid methods can be also observed in cases of power projection by terrorist organisations. Overall, as a result of its innovative strategy and methods, modern extremists are also not dependent on state support.[67]

An alternative description is offered by researchers specialising in digital interconnectedness, as well as systems of disseminating and storing information. In their view, hybrid threats are defined as a component of irregular warfare and cyberwarfare, characterised by the deliberate attempt to obfuscate the flows of accurate information to the public or to set stakeholder groups within a public or private sector entity. Hybrid attacks can be launched by both state and non-state actors, and they aim to exploit vulnerabilities to engender social, economic, or organisational discord within a targeted group.[68] Hybrid threats occupy the realm between international (or external) and intrastate (or internal) conflicts.[69]

NATO's perception of hybrid warfare is that of a violent conflict that features the simultaneous application of conventional and irregular warfare tactics, that can involve both state or non-state actors, which are used fluidly while disregarding the limitations of a physical battlefield or territory. Each attack contains its own combinations of the two and targets aspects of state and society as a means of achieving one's own objectives. The nature and tools required to wage hybrid warfare do not discriminate between state or non-state actors, with non-state actors (such as extremist groups) being

[66] NATO Energy Security Centre of Excellence, *Hybrid Threats: Overcoming Ambiguity, Building Resilience,* No 11 2017, p. 6.
[67] Dengg, A., Schurian, M. N., *On the Concept of Hybrid Threats*, p. 26, [in:] Networked Insecurity – Hybrid Threats in the 21st Century, Vienna 2016.
[68] Kaâniche, M., (ed.), *Applying Resilience to Hybrid Threats,* IEEE Security and Privacy Magazine 17(5), September 2019, p. 78.
[69] Raugh, D., *Is the Hybrid Threat a True Threat?,* Journal of Strategic Security 9(2), June 2016, pp. 1-13.

equally able to wage this kind of warfare in equal measure as a state actor and its military forces can.[70]

Recently, the term 'hybrid warfare'[71] has been used more frequently in political and scientific discussion forums concerning security policies, with the perception that this is a new form of threat. The media and the public also have adopted this term. Thus, 'hybrid warfare' appears to have become the latest term to symbolise this change in the waging of war by hybrid threats.[72]

Cyberwarfare serves as a leading example for the use of new technologies as part of the tactics employed by hybrid threats. At its core, cyberwar refers to a sustained effort of using computer network systems that launch cyberattacks on behalf of a state or non-state actor against the infrastructure of a target.[73]

The term 'hybrid warfare' was initially attributed to non-state actors from whom a combination of conventional and unconventional tactics was previously unexpected, requiring a new terminology to be formed. Because of the early nature of these contributions, what may be considered as part of the non-violent aspect of these tactics remains partially undefined, however, one of the numerous examples contributing to

[70] Bachmann, S., *Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats: mapping the new frontier of global risk and security management*, Amicus Curiae 2011 (88), pp. 24-25.

[71] Freier, N. P., *Known Unknowns: Unconventional "Strategic Shocks",* Defense Strategy Development, Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2008.
Freier points all of the efforts of hybrid campaigns toward containing U.S. influence without directly confronting the U.S. in a conventional military manner. The Russians are very likely interested in rolling back US/ Western influence in Eurasia, and these effects may be indicative of a Russian Grand Strategy, but the effects on the U.S. are not the sole reason for Russia to undertake a limited, hybrid action against its weaker neighbours. There are very real short-term strategic objectives that can be realised more safely and efficiently through hybrid means than with a full-scale military invasion.

[72] Armed Forces Journal, 2009. *The War of New Words: Why Military History Trumps Buzzwords*, Armed Forces Journal, [online] Available at: <http://www.armedforcesjournal.com/essay-the-war-of-new-words> [Accessed 24.10.2020].

[73] Bachmann, S., *Hybrid wars: the 21st-century's new threats to global peace and security*, Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, p. 82.

the formation of this new term is that of using the Internet for the purposes of spreading disinformation. The mobilisation of such tactics as in the cases of Islamic State and al-Qaeda could be seen as a clear example backing the inclusion of non-violent vectors to wage or support hybrid warfare tactics.[74]

Because it uses the aforementioned tactics frequently enough, the Islamic State can be considered a 'hybrid actor'; one that is able to achieve real operational successes through hybrid warfare, which was reflected in its major territorial expansion in Syria and Iraq.[75] In addition, the use of social media by ISIS for propaganda purposes also constitutes an important element of their hybrid activity.[76] Moreover, their success is also in part due to the decreased costs of running hybrid attacks, as they are much lower than those of a traditional war.

As terrorist organisations fulfil the conditions to be identified as hybrid threats, such features can become a staple for future fighting groups that conduct irregular activities, but also those who possess significant capabilities considered as equally advanced as those that were once previously exclusive only to state-level strategies and resources.[77] Furthermore, whilst most non-state actors do not have tools to conduct regular warfare at the same scale as a state actor, they may be sponsored by a state actor and be used as its strategic component, either as an independent factor or as part of a greater strategy.[78]

[74] Piazza, J. A., Guler, A., *The Online Caliphate: Internet Usage and ISIS Support in the Arab World*, Terrorism and Political Violence, May 2019.
Cohen-Almagor, R., *Jihad Online: How Do Terrorists Use the Internet?,* Advances in Intelligent Systems and Computing, Hull 2017.
Salama, B., *The Resilience of the Islamic State,* Institut für Friedenssicherung und Konflikt management, Vienna 2016.
[75] Tenenbaum, E. *La manœuvre hybride dans l'art opératif, Stratégique*, No 111, Paris 2016, p. 56.
[76] Taillat, S., *Un mode de guerre hybride dissymétrique ? Le cyberespace*, Stratégique, No 111, Paris 2016, pp. 89, 95.
[77] Hoorickx, E., *Countering "Hybrid Threats": Belgium and the Euro-Atlantic Strategy,* Security & Strategy No 131 October 2017, pp. 6-7.
[78] Lasconjarias, G., Larsen J. A., *(ed.), NATO's Response to Hybrid Threats,* Rome 2015, p. 101.

Some of the key characteristics used by terrorist organisations in hybrid warfare include:[79]

- Blending tactics: Organisations identified as hybrid threats synchronously combine their capabilities through launching conventional military forces together with smaller guerrilla units while maintaining a doctrine centred on high manoeuvrability.

- Flexible structures: Such threats persistently display both conventional formations of chains of command, as well as independent and distributed cells around the world. An overarching governing body, with various components and degrees of development, assert control and coordinate operations depending on their scale.

- Terrorism: The usage of terror tactics to proliferate both fear and hate is one of the options such groups have at their disposal. Apart from individuals and societies, they may target socio-cultural icons or elements that contribute to a form of identity or belief that oppose the assailant's ideology.

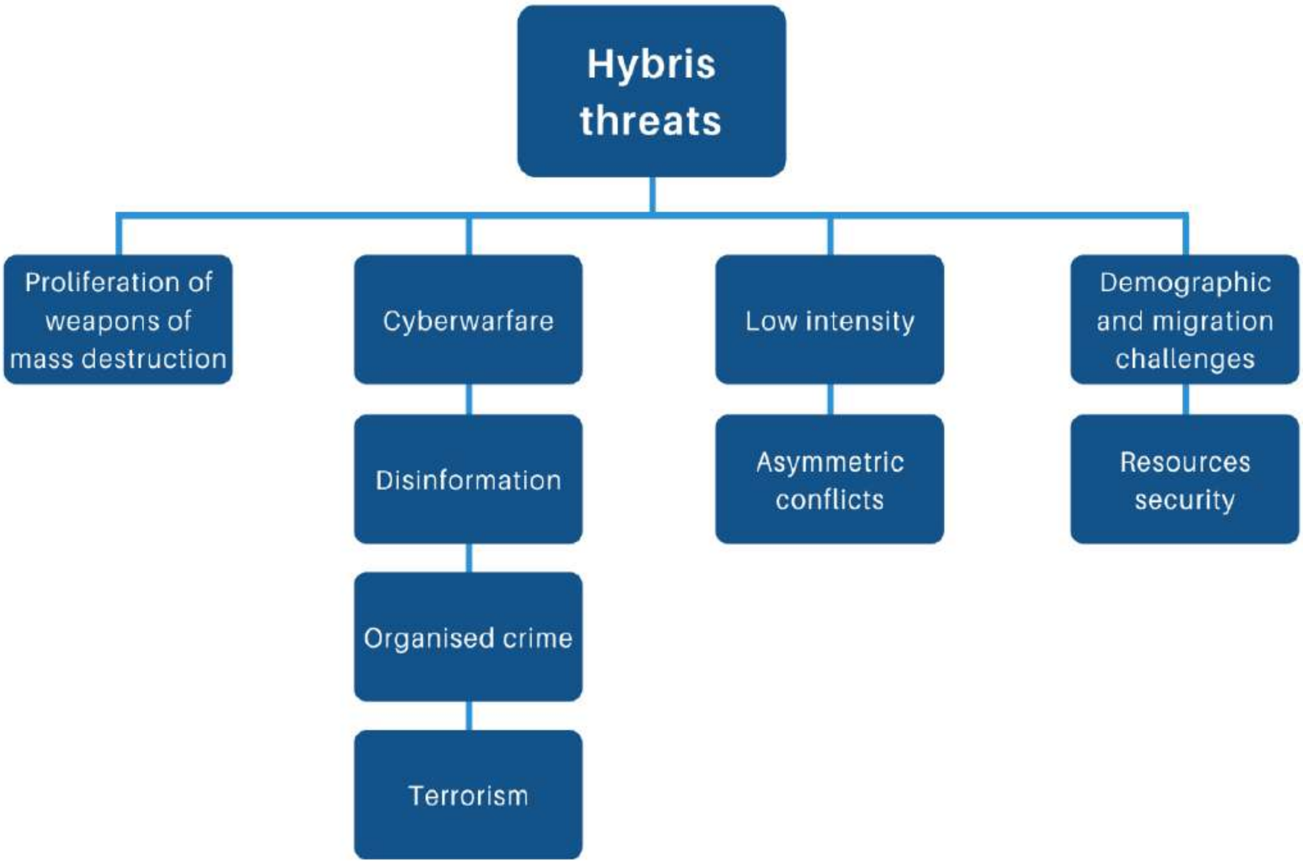
- Disregard for international law: Hybrid threats perceive international laws with cynicism, and therefore exhibit a disregard for their terms and values. Equally, these groups perceive these laws as a form of constraint against their own adversaries, seeing their limitations as an opportunity that shall be exploited.

- Information warfare: Exploitation of the global flow of information to proliferate their own agenda is a common tactic. Terrorist organisations often use such channels to spread jihadist schemes, raise funds, recruit and train new people as well as operate more effectively.

[79] Jasper S., Moreland, S., *ISIS: An Adaptive Hybrid Threat in Transition,* Small Wars Journal, October 2016, p. 2.

- Organised criminal activity: Hybrid threats will also use crime, such as arms or drug trafficking and kidnapping people for ransom, as a way to generate revenue.

Multi-vector nature of hybrid threats



Source: own study based on: A. A. Otaiku, *A Framework for Hybrid Warfare: Threats, Challenges and Solutions*, Journal of Defense Management, Volume 8, Issue 3, 2018, p. 4.

Contemporary, hybrid threats can be considered more deadly and dangerous than in the past, especially due to their capacity to harness a wide array of evolving technologies. One key example is that of using artificial intelligence and autonomous systems as a new vector of attack. Unmanned Aerial Vehicles (UAVs) are being increasingly used due to their cheap, yet sophisticated, systems for the purpose of reconnaissance, disruption of critical infrastructure, and carrying out bomb attacks. Another example is the potential for state and non-state actors to unleash aggressions through online networks. This can take many forms, including that of hacking critical infrastructures or systems involved in the democratic process (such as voting registries), as well as launching persuasive disinformation or propaganda campaigns and damage national security by disseminating sensitive data online. In the worst cases, the cybercriminals may even take control of military assets or command structures.[80]

[80] Fiott, D., Parkes, R., *Protecting Europe. The EU's response to hybrid threats*, European Union Institute for Security Studies, Paris 2019, p. 5.

DEFINITION OF TERRORISM

The inherently destructive nature of terrorism has impacted state and non-state actors directly across history. The basis of these attacks, which are carried out by various groups or individuals, have constituted a part of the internationally perceived characteristics concerning terrorism. These perceived characteristics, originally emerging in the 20th century and which will be discussed below, have culminated in the understanding that such attacks generally feature a non-state actor carrying out a violent attack against a state actor. The definition now stands updated to include such forms of combat that are used to achieve a specific set of objectives. Thus, terrorist attacks are often characterised by violence and aggression with the intent to destabilise and spread fear, confusion, and unrest in society.

The aforementioned definitions and terms are connected to the analysis of the terrorism phenomenon and its related activities; with its interpretations being necessary for entities tasked to combat it, particularly due to various modifications and extensions to the definitions. However, another key fundamental issue relating to such interpretation is the difference between terror and terrorism.[81] Terror is commonly understood as excessive fear. However, within the paradigm of national and international politics, terror can be understood as the usage of fear by a powerful actor to assert domination over other entities. This tactic is most commonly observed in states under a totalitarian regime. Terrorism, on the other hand, is described as the usage of violence or aggression, commonly conducted by radical groups or organisations, with the intent of usurping influence from a regional or territorial power while also aiming to instate fear among the population. It is also used to provoke various actions or reactions, as well as drawing attention to their cause or simply to demonstrate their strength. These tactics are often associated with religiously motivated attacks, in recent times mainly carried out by followers of Islam.[82,83] It should be pointed out, however, that terrorist activities are also being taken against innocent Muslim followers, not leaving a single side immune to terrorism.[84]

To accurately understand what a terrorist threat is, one must first establish the framework for what can be defined as a threat. One definition of a threat can be non-militaristic in nature but to one’s own lifestyle: such as a sudden and drastic reduction in the quality of life of citizens from an economic standpoint, or a significant reduction in the political activities of a government or non-governmental entities within the state. Another equally acceptable definition can be perceived with military lenses, such as a clear indication of the possibility of harming someone, or signalling willingness to cause damage. Despite the various perceptions as to what can be considered a threat, the term itself offers connotations of concerns or risks applied to a target.

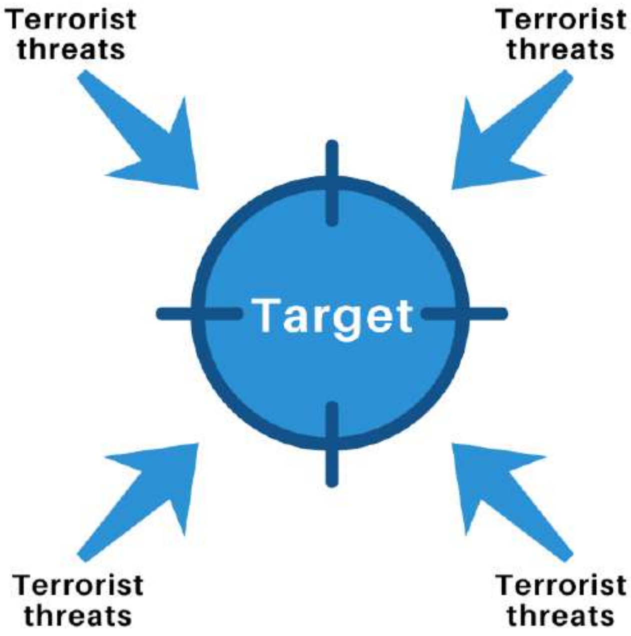
[81] Iulian R. I., *International terrorism in the 21st century – 16 years after 9/11 2001*, CBU International conference on innovations in science and education March 22-24, Prague 2017, Czech Republic.

[82] Abdulla, R. A., *Islam, Jihad, and Terrorism in Post-9/11 Arabic Discussion Boards,* „Journal of Computer-Mediated Communication”, 12(3), article 15, p. 1-16.

[83] Sikorski, C., Schmuck, D., Matthes, Binder, J. A., *“Muslims are not Terrorists”: Islamic State Coverage, Journalistic Differentiation Between Terrorism and Islam, Fear Reactions, and Attitudes Toward Muslims,* „Mass Communication and Society”, 2017, vol. 20, Issue 6: „Media, Terrorism and Society”, pp. 825–848.

[84] Kerdemelidis, M., Reid, M., *Wellbeing recovery after mass shootings: information for the response to the Christchurch mosque attacks 2019*, „Canterbury District Health Board”, 28.05.2019, pp. 2–5.

Fig. Multidimensional terrorist threats



Nonetheless, efforts were made to underpin what can be defined as a terrorist threat. The original international definition for security and defence was included in the League of Nations Convention of 16th November 1937. The Convention was signed by 25 states but ratified only by India and therefore never came into effect.[85] Then, in 1999, the UN Security Council adopted Resolution 1269, which stated that all practices, wherever and then, applied against security and which are threatening international order and peace, were terrorist activities.[86] Finally, in 2018, the United Nations Office on

[85] Law., R. D., *Terrorism: A History*, Cambridge 2009, pp. 155–157.
[86] Security Council, *Resolution 1269 (1999),* Adopted by the Security Council at its 4053rd meeting, on 19 October 1999.

Drugs and Crime (UNODC) has defined terrorism as using coercive methods or threatening to use violence to spread fear and achieve political or ideological goals.[87]

In the European Union, terrorist attacks are defined as offences under each of the members' national law. Due to the varied nature and context through these laws are enacted, this framework may seriously leave a state, or organisation established in said state, exposed to an attack that aims to intimidate a population, unduly compel a public or private entity to perform or abstain from performing any act, as well as seriously destabilise or destroy the fundamental political and socio-economic structures of said target. The EU directive defines terrorist offences as:[88]

1. Attacks upon a person’s life which may cause death;
2. Attacks upon the physical integrity of a person;
3. Kidnapping or hostage-taking;
4. Causing extensive destruction to government buildings or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public space or private property likely to endanger human life or result in major economic loss;
5. Seizure of aircrafts, ships, or other means of public goods;
6. Manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons;

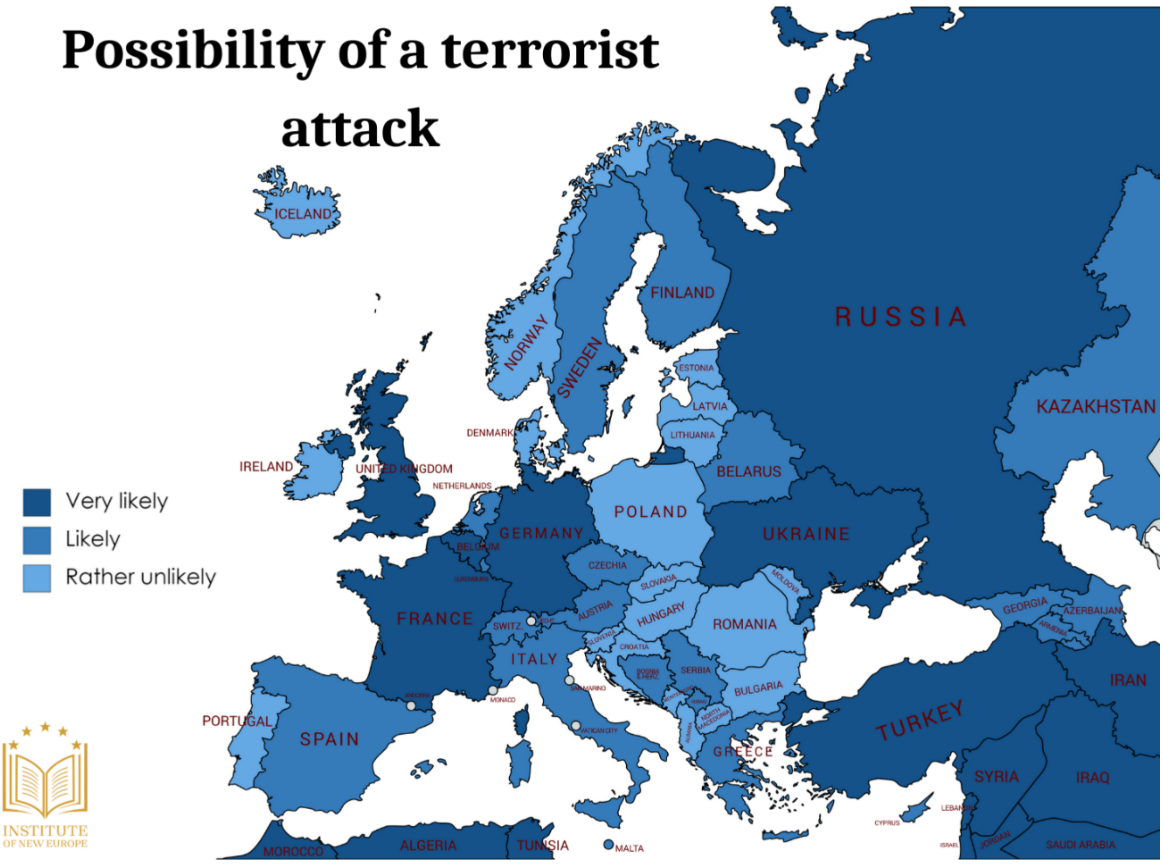
[87] United Nations Office on Drugs and Crime, *Education for justice university module series counter-terrorism – Module 1 introduction to international terrorism*, UN, Vienna 2018, p. 1.

[88] Directive (Eu) 2017/541 of the European Parliament and of the Council of 15 March 2017 *on combating terrorism* and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, 31.3.2017.

7. Spread of dangerous substances; causing fires, floods, or explosions with a purpose to endanger human life;

8. Interfering with or disrupting the supply of water, electricity, or any other fundamental natural resource, effecting in endangering human life.

Map. Level of terrorist threats in Europe



Terrorist attacks are carried out by individuals, groups, or organizations whose motives and beliefs are self-justified by religious, political, socio-economic, national and even environmental objectives.[89] Terrorism, as a whole, is a phenomenon that impacted virtually all nations across history, leaving a varying degree of impact on security that ranges in severity. Thanks to its ranging sizes and shapes, as well as aggression and varying usage of violence and intimidation, it was used as means to fight for particular political goals by various actors.[90]

However, there is no commonly accepted definition of terrorism, because there is a considerable number of varying understandings of it. They vary from a cultural perspective, affected by a place of origin, or from a legal standpoint where the national legislation that characterises them is concerned. In general, terrorism is a disturbing method that involves repeated acts of violence, which is used by individuals, groups, or state actors advocating for idiosyncratic, criminal, or political agendas where the ultimate aim does not lie with the direct victims of terrorism, but rather with wider ideas that are potentially unrelated to them. Direct victims of these acts may be selected at random as targets, or they may be chosen selectively, depending on their identity and symbolism, for the sake of these targets serving as platforms for delivering a striking message. The interaction process between the two parties, that of terrorists and their victims or targets, is that the terrorists would subject their selected targets to violent acts and threats in order to deliver a message towards their intended recipients, which could be people personally unaffected by the attack and within positions of influence.[91] This phenomenon is defined in different ways not only in different countries, but often diverging definitions can appear within a country's own understanding of terrorism.

[89] Zabłocki, E., *Kategorie, zagrożenia: system bezpieczeństwa narodowego*, Warszawa 2013, pp. 51–52.

[90] Bukowski, S., *Terroryzm europejski*, Słupsk 2010, p. 21.

[91] Jongman, A. J., Schmid, A. P., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Transaction Publishers, New Brunswick 1988.

There are further difficulties in reaching a consensus over the definition of terrorism due to a lack of consistency in its characterisation by researchers, politicians, and journalists. This is primarily due to a generalisation trend where most, if not all, major and abhorrent acts of violence against a society that are politically motivated, are referred to as 'terrorism.' Activities that may have little in common beforehand, such as poisoning of food, a stabbing at a train station, or kidnapping an individual, may now be included under the umbrella term of a 'terrorist' attack.[92] Because of this, the aggregated amount of terms and examples within this umbrella terminology increases the difficulty of pinpointing an accurate definition of terrorism. Furthermore, many scholars may also confuse all types of acts without distinguishing between their inherent nature as part of insurgent movements, wars, or even protests. This is related to the assumption that one's definition or perspective of terrorism is different for the other, with many terrorist organisations see themselves as being in a struggle against a greater evil that, for others who do not advocate terrorism, perceive these organisations as being a greater evil themselves.[93] To further back this, J. Arafat should be recalled here at the 1974 UN General Assembly, in which he compared a terrorist to a revolutionary. According to him, a clearly noticeable difference comes down to how an event is perceived. Whoever defends the right (of their) cause, fighting for their own rights and ideals, while struggling with the invader, cannot, according to J. Arafat, be called a terrorist.[94] However, this depends on the individual case studies, as generalisation will be a fundamental mistake in defining terrorism. Further difficulties in this problem are due to the lack of statistics that clearly state which of the crimes committed were of a terrorist nature. This is related to the confusion of terrorism with hybrid threats (and hybrid warfare), war and crime, where terrorism is a component of hybrid threats. There is also a lack of a single international definition that allows this kind of

[92] Borkowski, R., *Terroryzm ponowoczesny*, Wydawnictwo Adam Marszałek, Toruń 2006, p. 40.

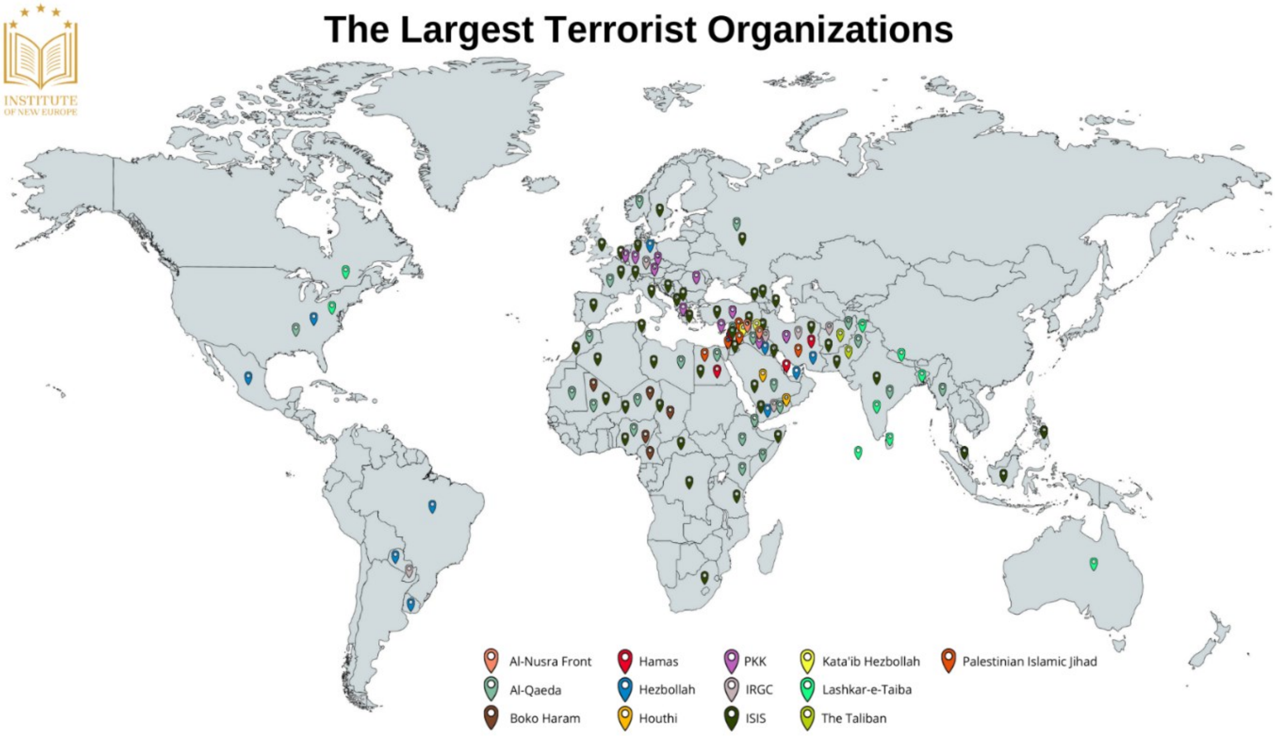
[93] Cesarz, Z. Stadmulller, E., *Problemy polityczne współczesnego świata*, Wrocław 2002, p. 351.

[94] United Nations, General Assembly, *Agenda Item 108 – Question of Palestine (Resumed from the 2268th meeting),* Wednesday, 13 November 1974, at 10.30 a.m. New York, A/PV.2282 and Corr.1.

classification in the first place. Often enough, the motives of a terrorist remain unknown, and therefore his actions may end up being described as a religious attack by default.

TERRORIST GROUPS

This particular section contains an overview of arguably the world's largest terrorist organisations. Their place of origin, potential places where they may be able to conduct their activities, as well as main sources of funding will be provided, following by a brief history and overview of activities of each of them.



AL-NUSRA FRONT/HAY'AT TAHRIR AL-SHAM (TAHRIR AL-SHAM)

Place of origin: Syria & Iraq (formed 2011, declared 2012).

Potential places of operation: Syria and Lebanon.

Sources of funding: Tariffs, taxes, fines collected within the territory of its operation, financial contributions by religious groups, weaponry tariffs on other rebel groups, foreign donations, oil sales, smuggling, kidnapping for ransom.

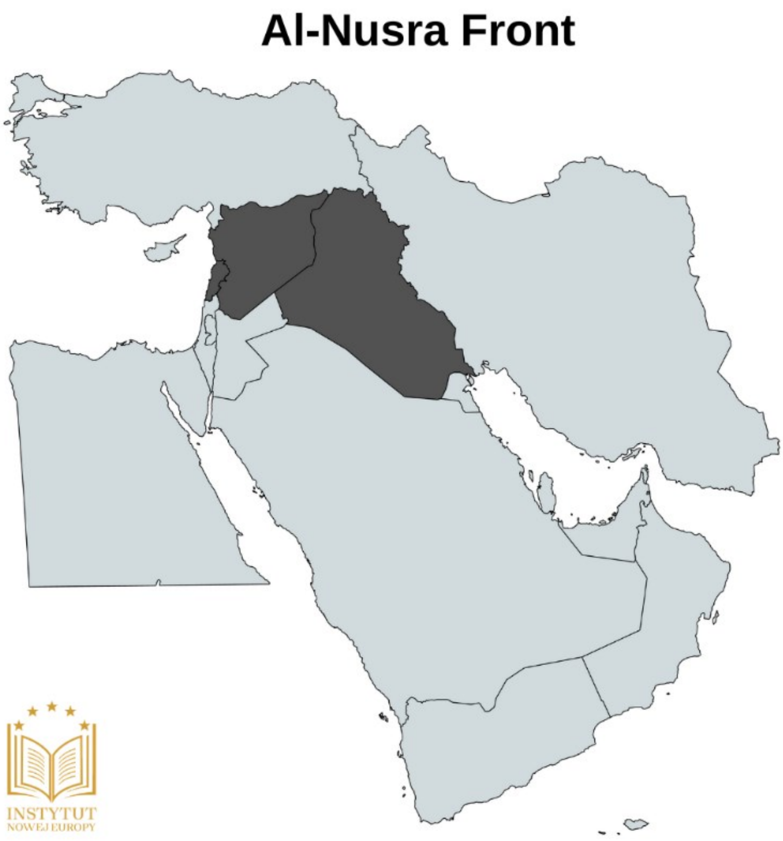
Executive Summary:

In 2011, Abu Bakr al-Baghdadi, the leader of the Islamic State in Iraq (ISI, formerly al-Qaeda in Iraq), sent operatives into Syria to establish a foothold in this country.[95] In January 2012, under the leadership of Abu Mohammad al-Julani, this group announced its existence as Jabhat al-Nusra ('Front of the Supporters') to launch offensives against Bashar al-Assad's regime. In 2013, al-Baghdadi, fearing al-Nusra's growing independence and differences in tactics, proclaimed the creation of the Islamic State of Iraq and the Levant (ISIL) and requested that Julani submits to his leadership. Al-Nusra rejected this and identified itself for the first time as an Al-Qaeda (AQ) branch. AQ's leadership supported al-Nusra by sending operatives to guide the group's formation. In July 2016, al-Nusra announced it was changing its name to Jabhat Fateh al-Sham (JFS, 'Front for Conquering Syria'), and claimed to be independent of any external entities. This rebranding was most likely done to obfuscate the group's ties to al-Qaeda and obtain more funding from Gulf states, to better form alliances with other rebel groups, and to complicate U.S. and Russian military campaigns against the group. In early 2017, JFS merged with four other organisations to form Hay'at Tahrir al-Sham (HTS). The State Department has consistently rejected the idea that these name changes have changed

[95] Center on Sanctions & Illicit Finance, *'Al-Qaeda's Branch in Syria: Financial Assessment*, Foundation For Defense of Democracies, Washington 2017.

the group’s close ties to AQ. The Syrian war has provided JN with a nearly ideal environment within which this strategy can be implemented on behalf of al-Qaeda, and JN has enjoyed worrying successes to date.[96]

Map. Main places of operation



[96] Cafarella, J., *Jabat al-Nusra in Syria: An Islamic Emirate for Al-Qaeda,* Middle East Security Report 25, 2014.

AL-QAEDA

Place of origin: Afghanistan & Pakistan (1988).

Potential places of operation: Globally.

Sources of funding: Private donors, Islamic charities and foundations, state sponsorship, drug trafficking, bank robberies, hostage-taking.

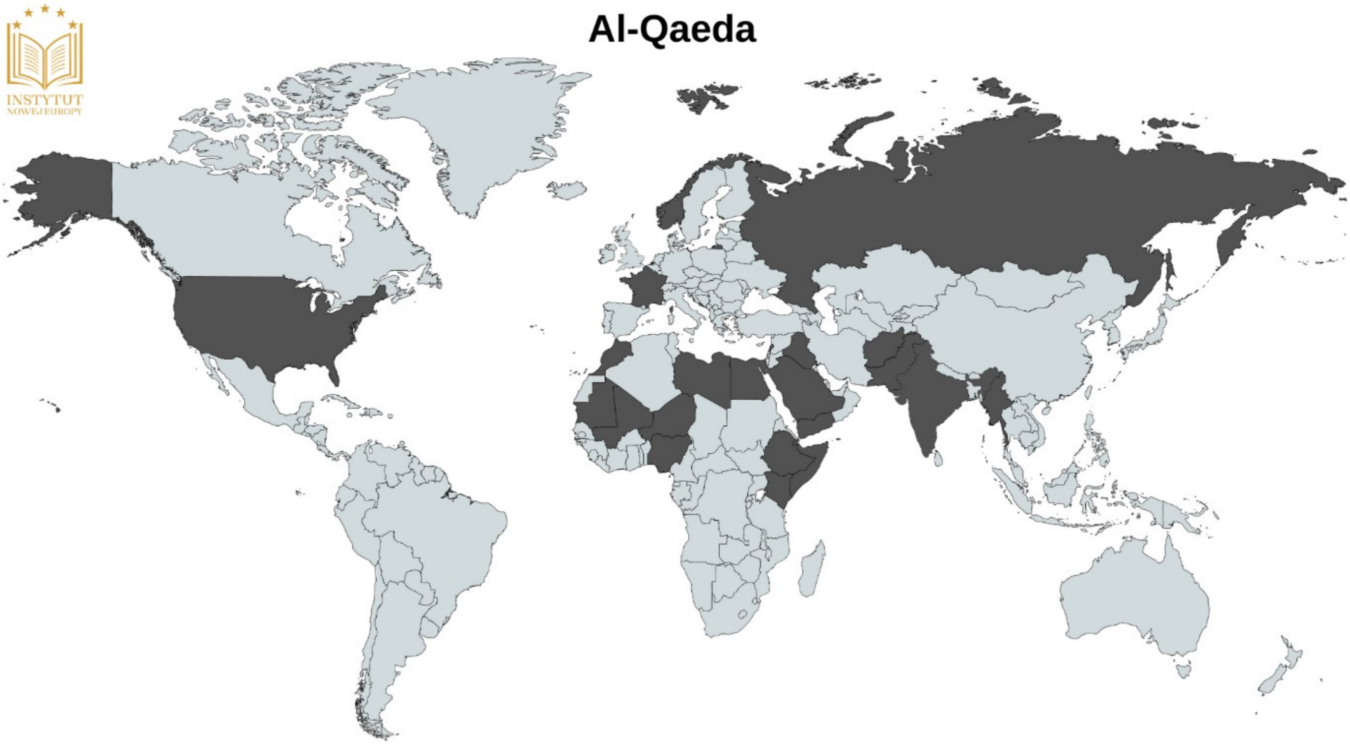
Executive Summary:

Al-Qaeda helped finance, recruit, transport, and train fighters for the Afghan resistance against the former Soviet Union. The group strives to eliminate Western influence from the Muslim world, topple 'apostate' governments of Muslim countries, and establish a pan-Islamic caliphate governed by its own interpretation of Sharia law that would ultimately be at the centre of a new international order. The three cornerstones of Al-Qaeda's doctrine stated by its longtime leader Osama bin Laden are: to unite the world's Muslim population under Sharia; to liberate the 'holy lands' from the 'Zionist-Crusader' alliance, and to alleviate perceived economic and social injustices.[97] Al-Qaeda's central command has traditionally been headquartered in Afghanistan and Pakistan. AQ has long pledged allegiance to the Afghan-based Taliban, which provided sanctuary to AQ after the United States turned its military focus on the group following the 9/11 attacks. The group also possesses regional commands in North Africa and Sahel (al-Qaeda in the Islamic Maghreb (AQIM)), East Africa (al-Shabab), Yemen (al-Qaeda in the Arabian Peninsula (AQAP)), territories of India, Myanmar, Bangladesh, Afghanistan, and Pakistan (al-Qaeda on the Indian Subcontinent (AQIS)), and Syria (Al-

[97] Foreign Policy Research Institute, 2013. *The Three Versions of Al Qaeda: A Primer*. [online] Available at: <https://www.fpri.org/article/2013/12/the-three-versions-of-al-qaeda-a-primer/> [Accessed 19.11.2020].

Nusra Front). Reportedly, al Qaeda's leader, Ayman al-Zawahiri, died of natural causes a few weeks ago, however, his death has yet to be confirmed.[98]

Map. Main places of operation



[98] Tim. S., 2020. *"Is al-Qaeda's leader dead? Report claims terror chief Ayman al-Zawahiri has died in Afghanistan from 'asthma-related breathing issues"*, [online] Available at: <https://www.dailymail.co.uk/news/article-8970231/Al-Qaedas-leader-Ayman-al-Zawahiri-died-reports-claim.html> [Accessed 20.11.2020].

ISLAMIC STATE IN IRAQ AND THE LEVANT (ISIL/ISIS)

Place of origin: Iraq (Al-Qaeda in Iraq: 2004; ISIS: 2013).

Potential places of operation: Globally.

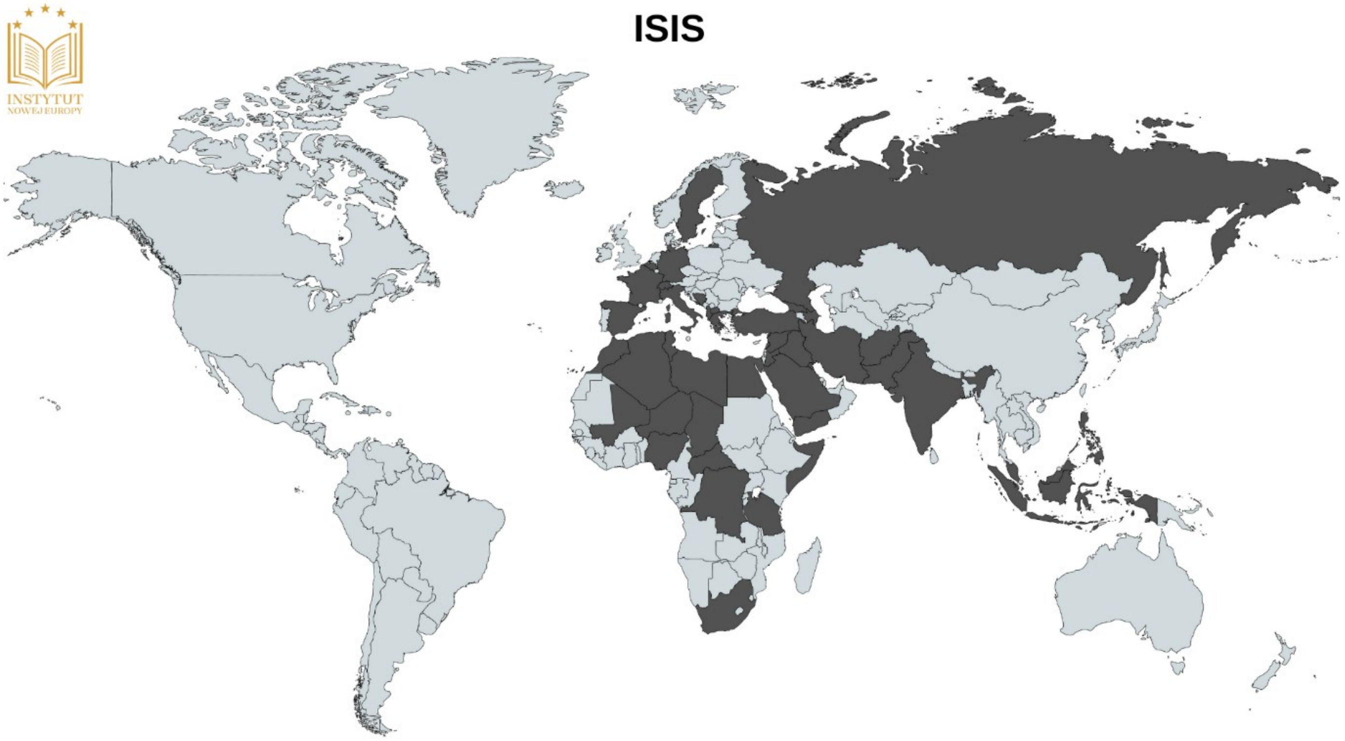
Sources of funding: Bank looting, extortion and human trafficking, control of oil and gas reservoirs, extorting agriculture, selling cultural artefacts, kidnapping for ransom, private donors, donations from non-profit organisations, fundraising through modern communication networks[99].

Executive Summary

The Islamic State organisation (IS, aka. the Islamic State of Iraq and the Levant, ISIL/ISIS, or the Arabic acronym Da'esh) emerged as a major international security threat amid more than a decade of conflict in Iraq after 2003 and the outbreak of unrest and conflict in Syria in 2011.[100] IS marks both a continuation with and a breakaway from al-Qaeda. A shift has occurred from terrorism carried out by organisations that are small, mobile, poorly financed and dispersed, to that perpetrated by groups that are centralised, armed and exert control over territories rich in resources – all factors which allow the implementation of an ambitious financial strategy. Similarly, to Hezbollah, ISIS is structurally complex. The organisation concurrently brings to bear significant administrative capabilities, combined with a financial framework, an internationalised military apparatus as well as sophisticated communications and propaganda body.[101] ISIS is the organisation that inspires the largest number of lone-wolf terrorist attacks around the globe.

[99] FATF, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, Paris 2015.
[100] Congressional Research Service, *The Islamic State and U.S. Policy,* CRS, Washington, 2018.
[101] European Parliament, *The Financing of the 'Islamic State' in Iraq and Syria (ISIS),* European Parliament's Committee on Foreign Affairs, Belgium 2017.

Map. Main places of operation



BOKO HARAM

Place of origin: Nigeria (2002).

Potential places of operation: Nigeria, Chad, Cameroon, Niger, Mali, Tunisia, Algeria, Mali, Burkina Faso, Congo, Mozambique, Somalia, Egypt, Libya.

Sources of funding: Kidnaping for ransom, taxation, extortion, looting and spoils cash from the banking system, smuggling and trafficking, donations, commercial enterprises and agriculture, foreign donations.

Executive Summary:

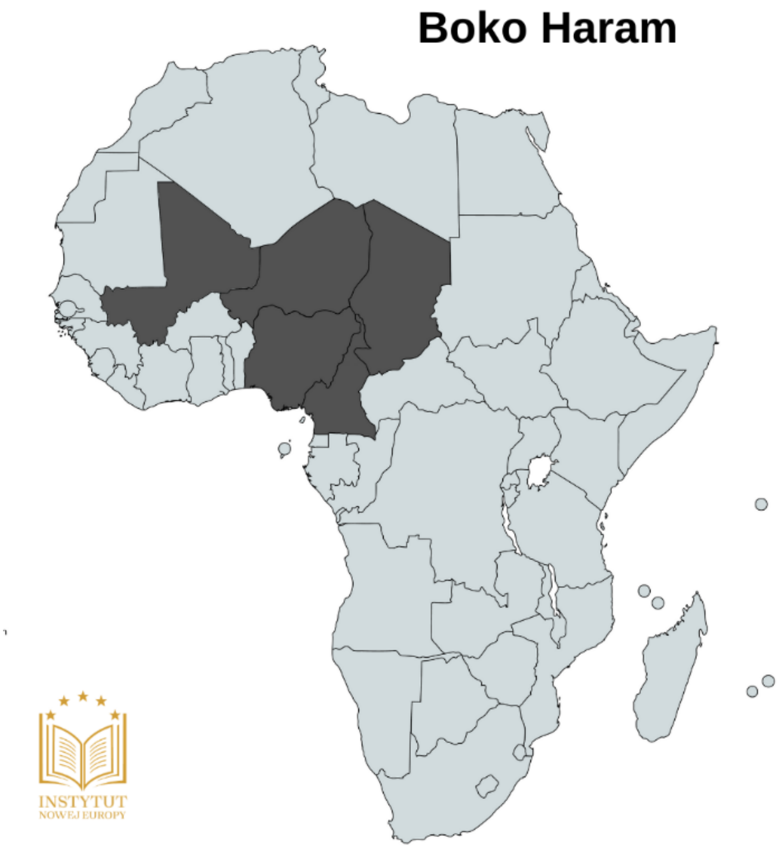
Boko Haram (which translates to 'Western education is a sin' or 'Western education is forbidden') is an ISIS-aligned jihadist group that promotes a Salafist-jihadist brand of Islam and seeks to establish a caliphate, or Islamic state, in Nigeria and its bordering countries. The movement is a fractious terrorist group with a decentralised organisational structure. The cells differ ranging from combat groups, welfare service providers, explosives experts, medical committee, and intelligence and surveillance experts. It has conducted many terrorist attacks on religious and political groups, local police, and military forces, as well as attacked civilians in busy areas. However, after a peak of violence in 2014 and 2015, the number of casualties attributed to the group fell dramatically.[102] However, at the end of November 2020, they killed approximately 120 people, including kids and women.[103] Boko Haram is a radical Islamist movement shaped by its Nigerian context, reflecting Nigeria's history of poor governance and extreme poverty in the North. Its stated goal is the establishment of a Sharia state, but it shows little interest in actually governing or implementing economic development. It is based on

[102] Global Conflict Tracker, 2020. *Boko Haram in Nigeria.* [online] Available at: <https://www.cfr.org/global-conflict-tracker/conflict/boko-haram-nigeria> [Accessed 1.12.2020].

[103] Agence France-Presse, 2020. *At least 110 dead in Nigeria after suspected Boko Haram attack.* [online] Available at: <https://www.theguardian.com/world/2020/nov/29/nigeria-attack-boko-haram-farm-workers-killed> [Accessed 1.12.2020].

the fundamentalist Wahhabi theological system and opposes the Islam of the traditional northern Nigerian establishment, which is broadly tolerant. Boko Haram and its more radical splinter, Ansaru (following the principles of Islamic fundamentalist Jihadism), are steadily expanding their area of operations. The Nigerian government's response has been to treat Boko Haram as a part of the international ISIS movement. Security service abuses are likely to be a driver of some popular support for or acquiescence to Boko Haram. The struggle between the government and Boko Haram has dire humanitarian consequences; many people have been internally displaced in northern Nigeria and many refugees have fled to neighbouring countries.

Map. Main places of operation



HOUTHIS

Place of origin: Yemen (1994).

Potential places of operation: Yemen, Saudi Arabia, Iran, Iraq, Libya, Lebanon, and Syria.

Sources of funding: State funding (Iran), outside donations (Hezbollah and other sources).

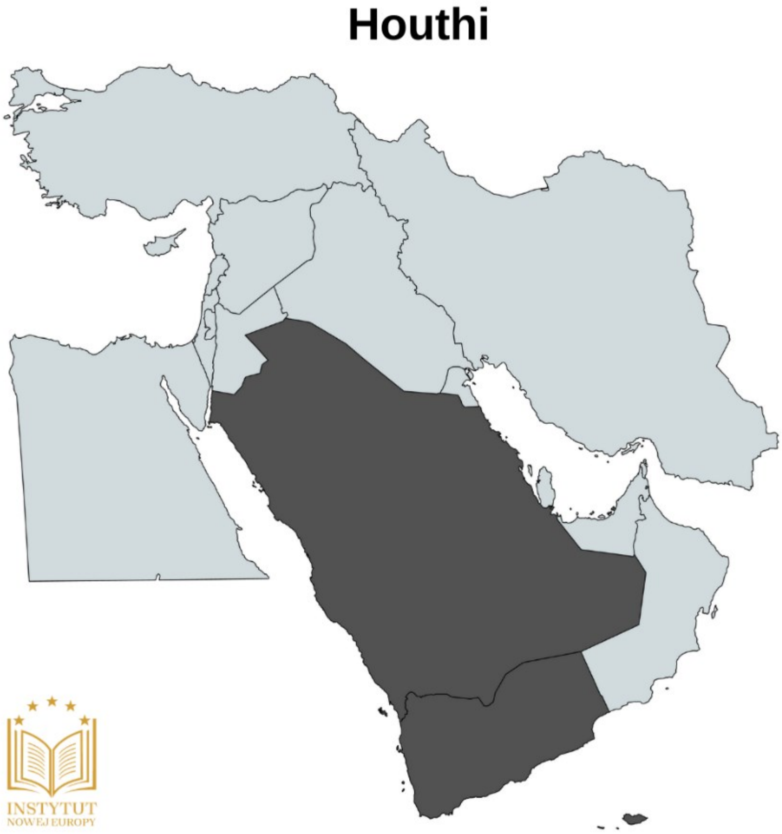
Executive summary:

The Houthis – officially known as Ansar Allah (Partisans of God) – are an Iranian-backed military and political movement. Its members, who subscribe to the minority Zaidi sect of Shiite Islam, advocate regional autonomy for Zaidis in northern Yemen. The Houthi movement began as an effort to maintain tribal autonomy in northern Yemen and to protest Western influence in the Middle East. Today, the Houthis seek a greater role in the Yemeni government and continue to advocate Zaidi minority interests.[104] The movement is known for its virulently anti-American and anti-Semitic rhetoric. Starved of many options for regional allies, Iran has routinely used sponsor-proxy relationships to expand its reach in the Middle East and to antagonise its adversaries while minimising the risk of inviting direct conflict. The Houthis have received training and military equipment from Iran's Islamic Revolutionary Guard Corps (IRGC).[105]

[104] The Wall Street Journal, 2015. *5 Things to Know About the Houthis of Yemen*. [online] Available at: <https://www.wsj.com/articles/BL-263B-3613> [Accessed 11.11.2020].

[105] Al Jazeera, 2018. *US hits Iran IRGC with sanctions over support of Yemen's Houthis,* [online] Available at: <https://www.aljazeera.com/news/2018/05/23/us-hits-iran-irgc-with-sanctions-over-support-of-yemens-houthis> [Accessed 12.11.2020].

Map. Main places of operation



HAMAS

Place of origin: Gaza Strip (1987).

Potential places of operation: Gaza Strip, West Bank, Israel, Qatar, Egypt, Lebanon, Iran, Turkey, Jordan, and Yemen.

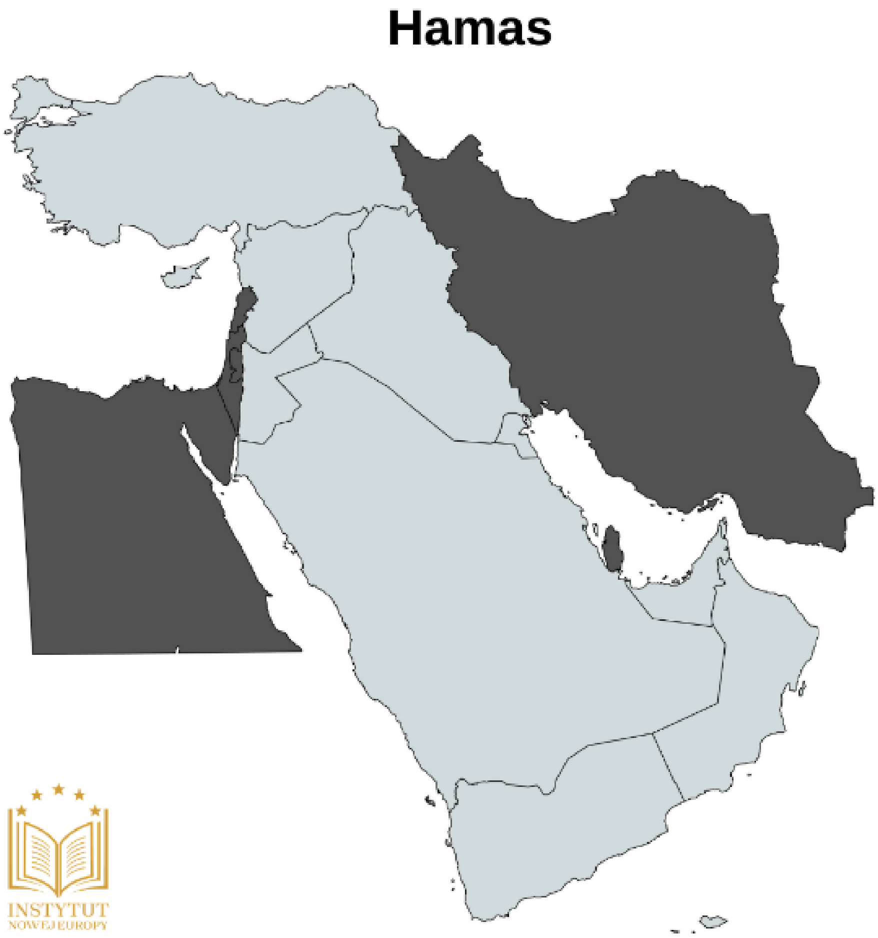
Sources of funding: charities, taxes and 'tunnel economy', cryptocurrencies, foreign investment, state funding (amongst others Iran, Qatar, Saudi Arabia).

Executive summary:

Hamas is an offshoot of the Muslim Brotherhood that emerged in the Gaza Strip in the late 1980s, during the first Palestinian 'intifada' (uprising) against Israel. The group's ideology blends Islamism with Palestinian nationalism and seeks the destruction of Israel and the creation of an Islamic state between the Mediterranean Sea and the Jordan River. Hamas strives to create an Islamist state based on the principles of Sharia (Islamic law). Hamas views the entirety of the land of Mandate Palestine – excluding the 80 percent of Palestine that became modern-day Jordan – as an Islamic birthright that has been usurped. Hamas's leadership has historically been split between its foreign-based political bureau and its Gaza-based government, which at times find themselves at odds. Various Hamas leaders have made contradictory claims on whether the group's military wing, the Izz ad-Din al-Qassam Brigades, operates independently or under the direction of the political wing. Hamas is often discussed alongside other groups in the region that engage in militant and terrorist activities to achieve their ends, yet Hamas has confined its militancy to Israel and the Palestinian territories – distinguishing it from the broader aspirations expressed by al-Qaeda and its affiliates.[106]

[106] Congressional Research Service, *Hamas: Background and Issues for Congress*, CRS, Washington 2010.

Map. Main places of operation



HEZBOLLAH

Place of origin: Lebanon (1985).

Potential places of operation: Lebanon, Syria, Germany, Mexico, Paraguay, Argentina, Brazil, Iran, United Arab Emirates, Iraq, United States, Yemen, Egypt, Turkey, Russia, and Sudan.

Sources of funding: State funding (Iran), transnational criminal activities, individual donations, charity organisations, financial benefits from international companies under its influence.

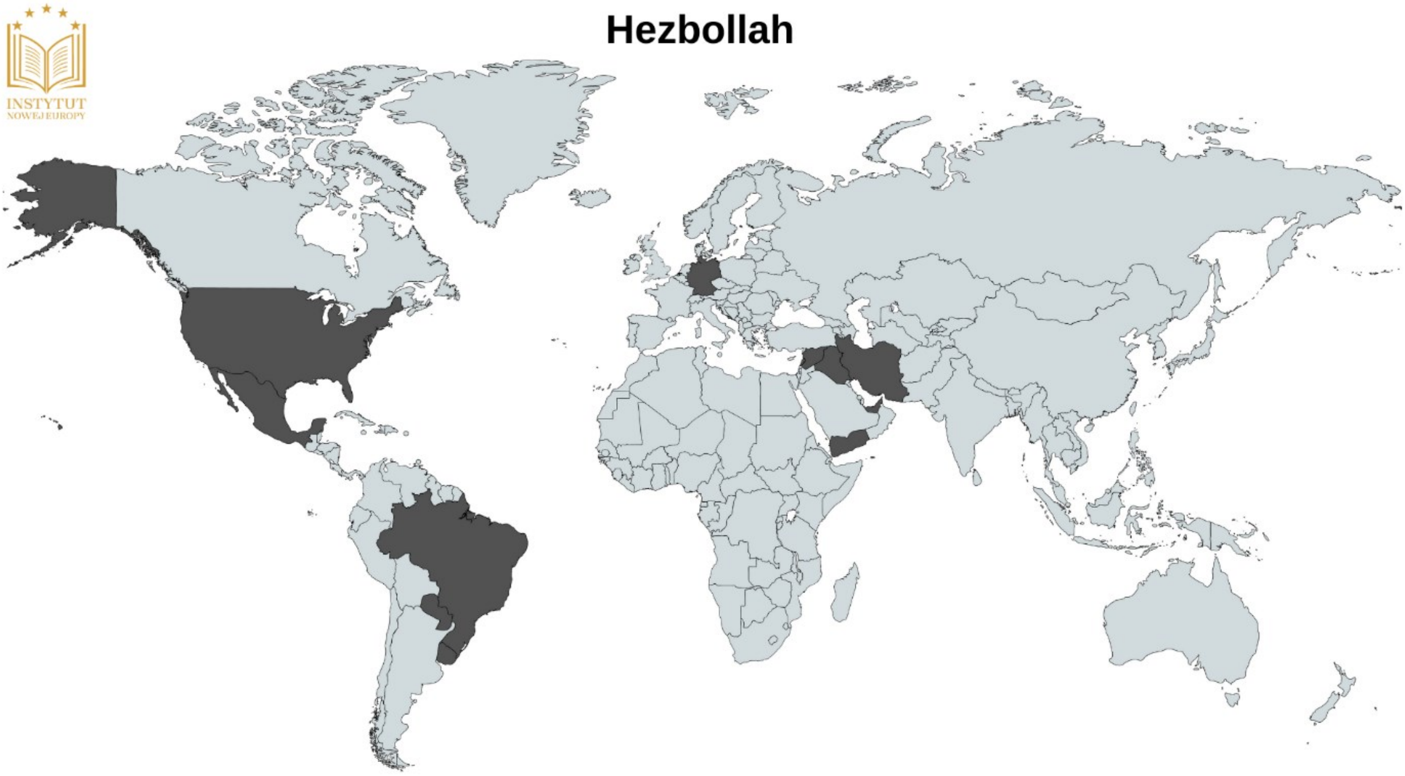
Executive summary:

The seeds of Hezbollah as a hybrid terrorist organisation were planted when it was established as an umbrella framework for pro-Iranian Islamic organisations in Lebanon that shared a belief in obedience to the supreme leader Khomeini [wilayat faqih], and a desire to ultimately establish an Islamic republic in Lebanon based on the Iranian model.[107] Iran provides financing and weapons to Hezbollah, as well as strategic guidance. Another country that influences Hezbollah is Syria, although the dynamics of that relationship have changed significantly in the past 17 years. Hezbollah's military intervention in Syria from 2012 to assist the Assad regime against the armed opposition has placed the Lebanese party on a partnership footing with Damascus.[108]

[107] Azani, E., *The Hybrid Terrorist Organization: Hezbollah as a Case Study*, in Studies in Conflict & Terrorism, 36:11, 2013, pp. 899-916.

[108] Middle East Institute, *Hezbollah's Evolution: From Lebanese Militia to Regional Player*, Washington 2017.

Map. Main places of operation



PKK - KURDISTAN WORKERS’ PARTY

Place of origin: Southeast Turkey (1978).

Potential places of operation: Turkey, Iraq, Syria, Iran, Czech Republic, Germany, Belgium, Romania, Austria, Greece, Egypt, Turkmenistan, Russia, Lebanon, and Cyprus.

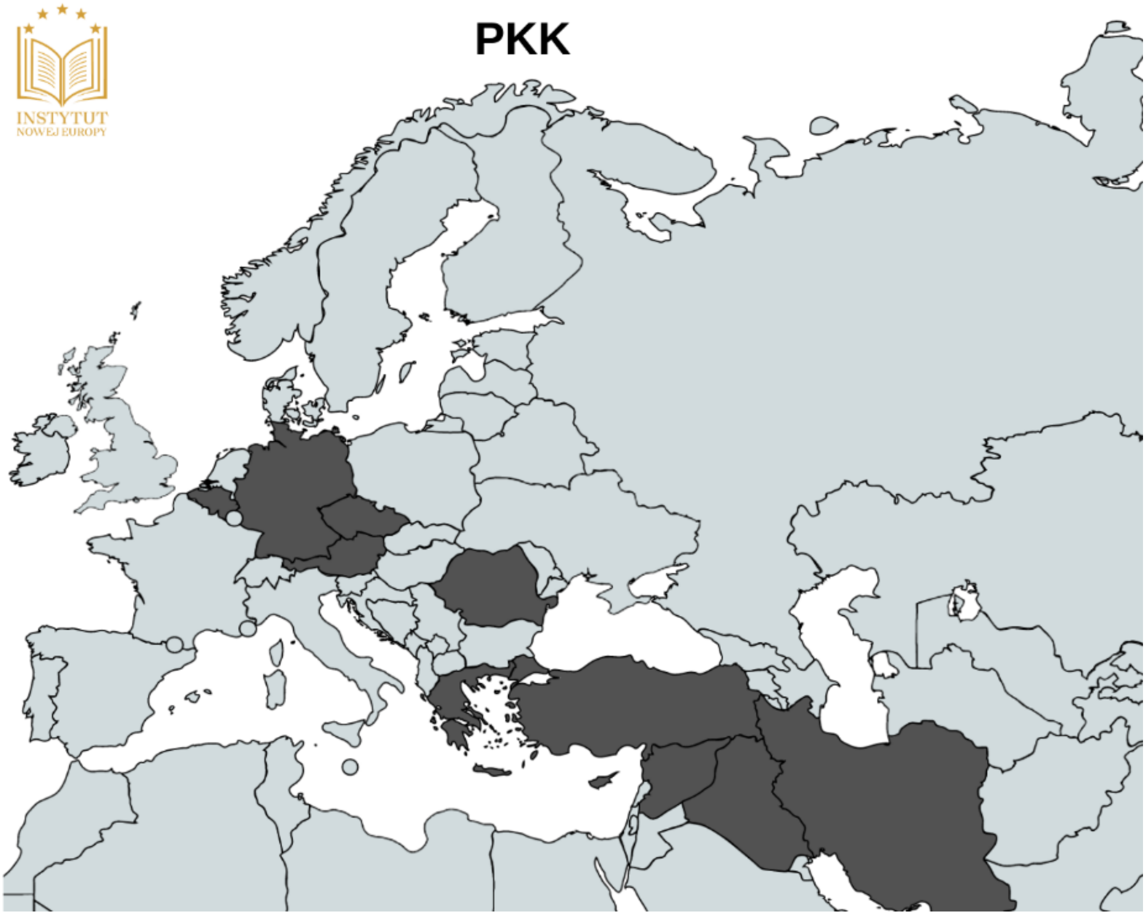
Sources of funding: Smuggling, drug trafficking, state funding (Syrian regime), Syrian groups in Lebanon, the Lebanon Communist Party, Palestinian organisations, Kurdish diaspora in Germany, money laundering.

Executive summary:

The PKK was founded during a meeting of Abdullah Ocalan and his associates in Diyarbakir, Turkey on 27th November 1978.[109] This meeting is more commonly known as the First Congress of the PKK. In its Statement of Foundation, the PKK made reference to the liberation of Kurds scattered in Turkey, Syria, Iran, and Iraq, and the formation of 'Greater Kurdistan’ in the region as its long-term objective.[110] To provide a new image for the Kurdish movement, as well as to coordinate the leadership of its political and military wings, the umbrella organisation KADEK (Kurdistan Freedom and Democracy Congress) was established in 2002. Consonant with Ocalan’s position, KADEK declared that the movement’s goal had shifted from an 'independent Kurdistan’ to a ‘democratic Turkey’. After the U.S. Department of State, on 1st May 2003, added KADEK to its list of Foreign Terrorist Organisations, KADEK was renamed Kongra-Gel (Kurdistan Society Congress), soon thereafter also declared a terrorist organisation by the State Department.

[109] Gergin, N., Duru, H., Çetin, H. C., *Profile and Life Span of the PKK Guerillas*, Studies in Conflict & Terrorism, 38:3, 2015, pp.219-232.
[110] Uslu, E., *Turkey’s Kurdish Problem: Steps Toward a Solution,* Studies in Conflict & Terrorism, 30:2, 2007, pp. 157-172.

Map. Main places of operation



KATA’IB HEZBOLLAH

Place of origin: Iraq (2006-2007).

Potential places of operation: Iraq, Syria, Iran, Jordan, Lebanon, Turkey.

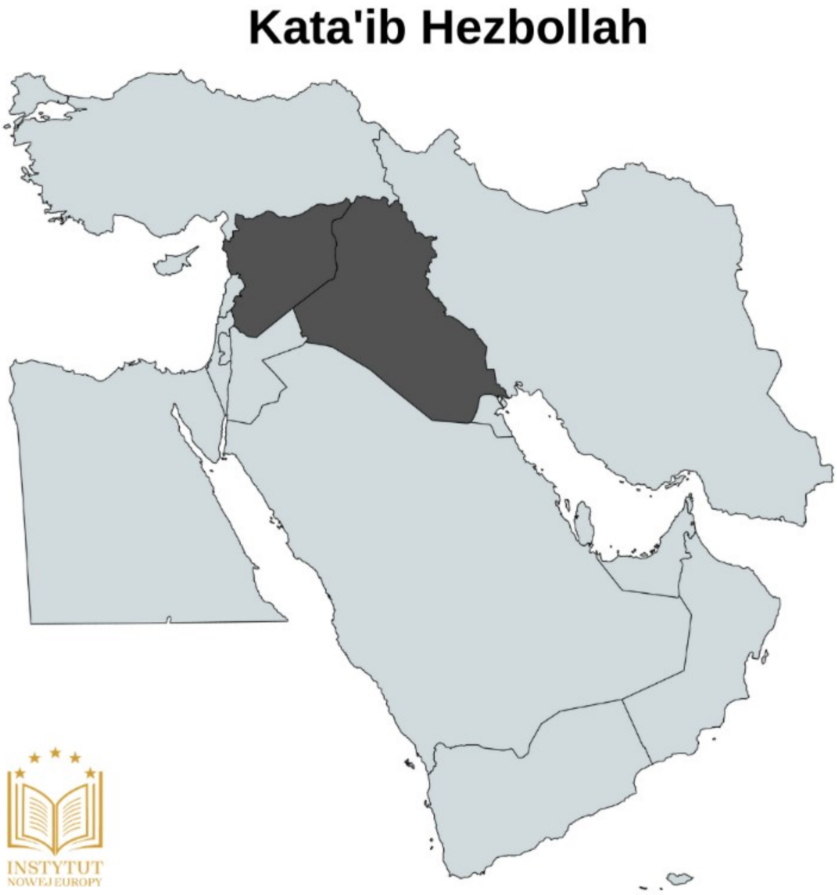
Sources of funding: State funding (mostly by Iran), abductions, ransom money.

Executive summary:

Kata’ib Hezbollah (KH) is an Iranian-sponsored, anti-American Shiite militia mainly operating in Iraq with ancillary operations throughout Syria. The group is virulently anti-American and ideologically loyal to the Iranian regime.[111] Kata’ib Hezbollah is a relatively small Iraqi Shiite militia, considered the most secretive Shiite militia operating in Iraq, which has sought to lure recruits by advertising its fight against the U.S. forces. It also serves as a means through which the Iranian Islamic Revolutionary Guards Corps-Quds Force (IRGC-QF) projects power in Iraq. Furthermore, following the start of the Syrian Civil War, the group also advertised its efforts to support Assad's forces in neighbouring Syria. KH has received a significant amount of training, logistical support, and weapons from the IRGC-QF.[112] The group is a leading member of the Popular Mobilisation Forces (PMF), an umbrella group of Shia militant movements that formed to fight IS in Iraq. From 2008-2011, KH directed the majority of its attacks against U.S. coalition forces in Iraq and was designated as a Foreign Terrorist Organisation by the United States on 2nd July 2009. Interestingly, KH also deployed its troops in Iraq to fight the Islamic State, often in conjunction with other PMF militias. After the defeat of the IS, Kata‘ib Hezbollah has begun to fill the power vacuum created by the fall of the caliphate.[113] In Iraq in 2017, KH intensified its targeting of U.S. forces.

[111] Counter Extremism Project, *Kata’ib Hezbollah*, [online] Available at: <https://www.counterextremism.com/threat/kata%E2%80%99ib-hezbollah> [Accessed 2 November 2020].
[112] United Against Nuclear Iran, *Kata’ib Hezbollah*, [online] Available at: <https://www.unitedagainstnucleariran.com/report/kataib-hezbollah> [Accessed 2 November 2020].
[113] Foundation for Defense of Democracies, *Kataib Hezbollah: Background and Analysis*, 2018.

Map. Main places of operation



IRGC (ISLAMIC REVOLUTIONARY GUARD CORPS)

Place of origin: Iran (1979).

Potential places of operation: Middle East.

Sources of funding: State funding (Iran).

Executive summary:

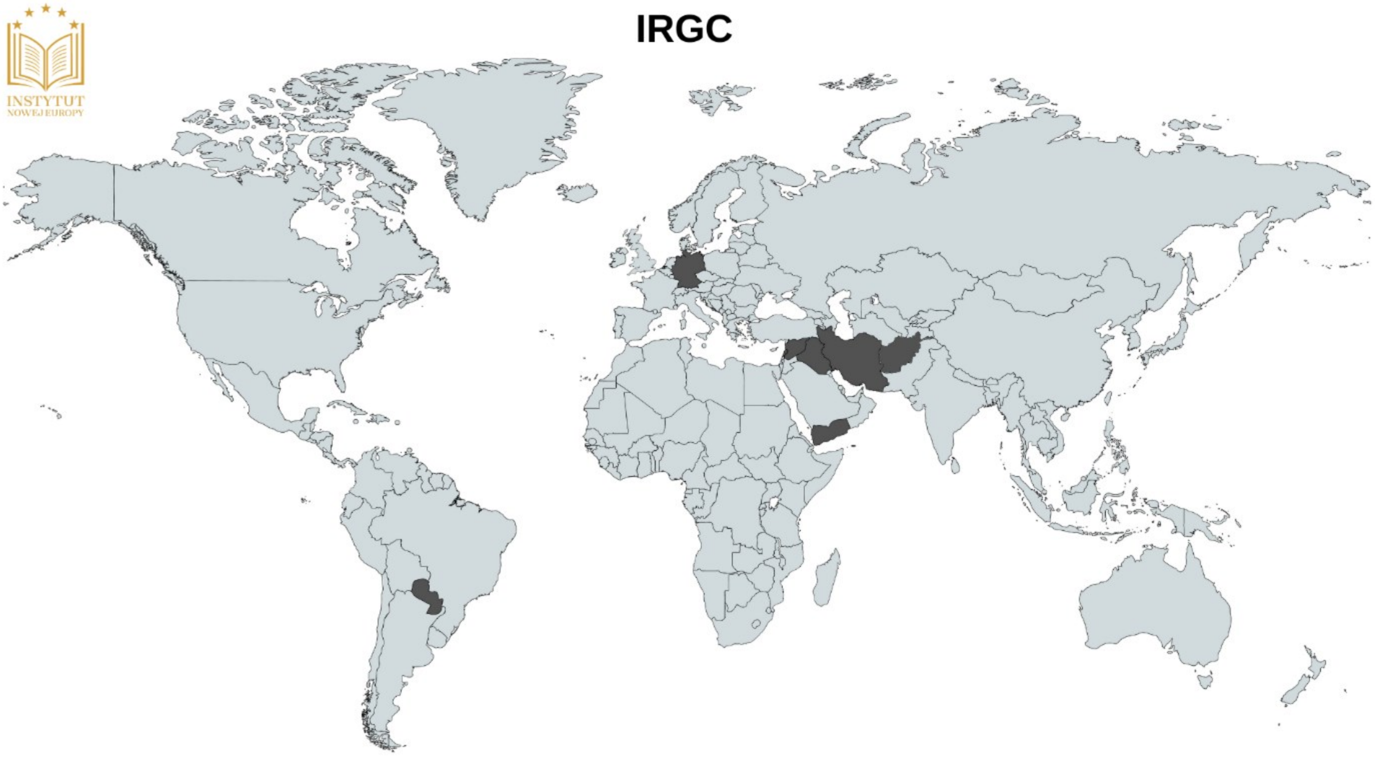
A key factor in the growth of the IRGC's power was the lack of trust the religious authorities had in the traditional Iranian military. This led the ruling clerics to form their own ideological military arm to defend the 1979 revolution and its achievements. This meant that the IRGC was given both a constitutionally legitimate existence and the legal right to become involved in the political scene to defend the revolutionary regime and its policies.[114] IRGC has been providing training for members of Hezbollah since the mid-1980s.[115] The IRGC-QF also has a foreign policy role in exerting influence throughout the region by supporting pro-Iranian policies; embodying approximately 10,000 to 15,000 personnel. The IRGC-QF operates in the conflict zones of Iraq and Syria, fighting ISIS, as well as the Syrian militants opposed to Bashar Al-Assad's regime. The coalition of Iranian forces, Hezbollah, and other supporting Iraqi and Syrian militias have had a profound impact in the defeat of ISIS.[116]

[114] Center for Strategic & International Studies, *The Iranian Islamic Revolutionary Guard Corps (IRGC) from an Iraqi View – a Lost Role or a Bright Future?.* [online] Available at: <https://www.csis.org/analysis/iranian-islamic-revolutionary-guard-corps-irgc-iraqi-view-%E2%80%93-lost-role-or-bright-future> [Accessed 2 November 2020].

[115] Wiegand, K. E., *Reformation of a Terrorist Group: Hezbollah as a Lebanese Political Party*, Studies in Conflict & Terrorism, 32 (2009), pp. 669-680.

[116] Malakoutikhah, Z., *Iran: Sponsoring or Combating Terrorism?,* Studies in Conflict & Terrorism, 43, (2020), pp. 913-939.

Map. Main places of operation



PALESTINIAN ISLAMIC JIHAD

Place of origin: Egypt (1979).

Potential places of operation: Israel, West Bank and Gaza, Lebanon, Syria, Iran, Jordan, Yemen, Iraq, and Turkey.

Sources of funding: State funding (Palestine and Iran).

Executive summary:

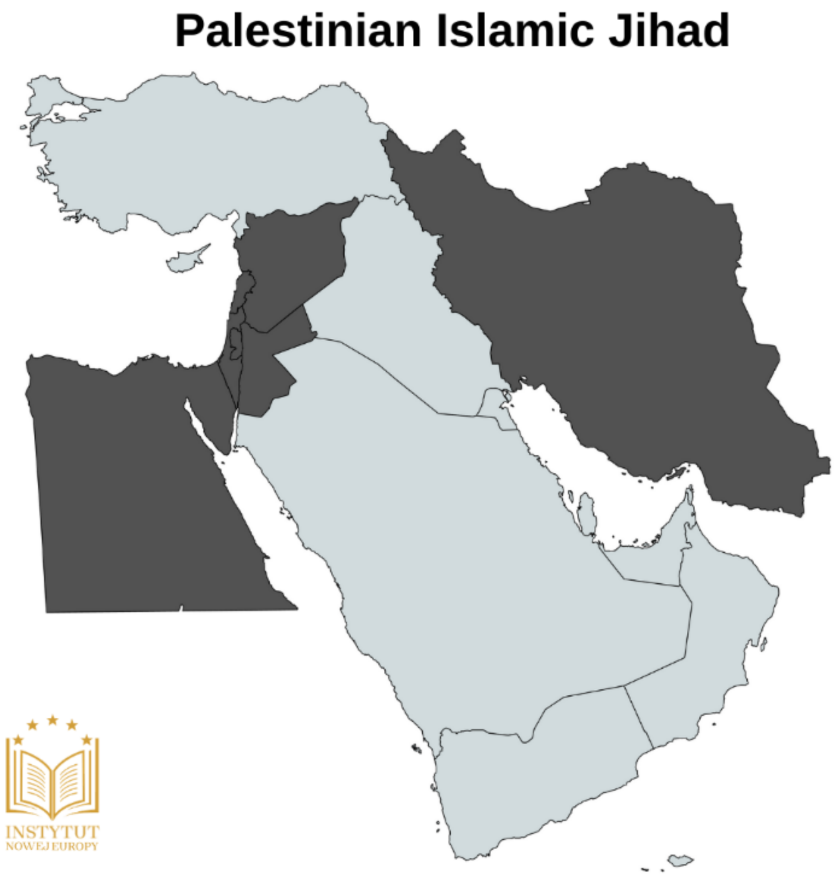
Palestinian Islamic Jihad (PIJ) advocates for an extremist Islamic ideology, which sees the destruction of Israel as part of the process of bringing about an Islamic revolution in the Arab world.[117] PIJ claimed responsibility for a number of terrorist attacks against Israel during the1990s and increased its terrorist activities since the outbreak of the Al-Aqsa Intifada. Unlike Fatah and Hamas, PIJ has no political ambitions and has never sought representation in the Palestinian Authority (PA). It is sustained mainly through external support from Iran. The Palestinian Islamic Jihad wants to re-establish a sovereign, Islamic Palestinian State with the geographic borders of the pre-1948 mandate Palestine. PIJ members see violence as the only way to remove Israel from the Middle East map and reject any two-state arrangement in which Israel and Palestine coexist.[118] In the Palestinian Territories, Hamas and PIJ are considered rivals despite their shared credentials as Sunni jihadist groups committed to violence against Israel. While there have been instances of cooperation between Hamas and PIJ operatives, in general, the two groups work independently and compete for support among both the Palestinian population and external supporters. Furthermore, Hamas and PIJ often articulate their differences publicly.[119]

[117] Palestinian public opinion and terrorism: A two-way street?, *Journal of Policing, Intelligence and Counter Terrorism,* 10, (2015), pp. 71-87.

[118] Council on Foreign Relations, *Palestinian Islamic Jihad.* [online] Available at: <https://www.cfr.org/backgrounder/palestinian-islamic-jihad> [Accessed 2 November 2020]

[119] Stanford University, *Mapping Militant Organizations.* [online] Available at: <https://web.stanford.edu/group/mappingmilitants/cgi-bin/pages/definitions> [Accessed 2 November 2020].

Map. Main places of operation



THE TALIBAN

Place of origin: Afghanistan (1994).

Potential places of operation: Afghanistan, Pakistan, Iraq, Russia, Turkmenistan.

Sources of funding: Illegal narcotics trade, state funding (including Pakistan and Saudi Arabia), opium production, foreign donations, illegal gem mining, kidnapping, extortion, taxes imposed on people living under its control.

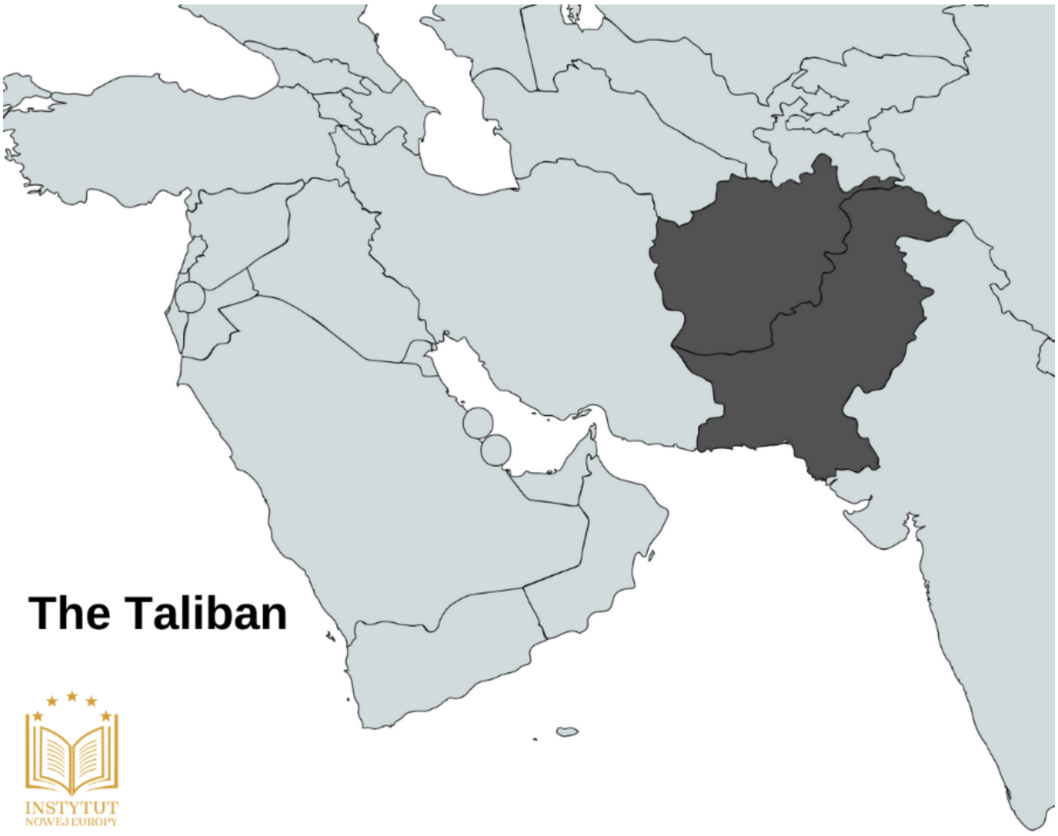
Executive summary:

The Taliban (which translates to 'students') is the predominant umbrella group for the Afghan insurgency, including the semi-autonomous Haqqani network.[120] The Taliban is an Islamist movement that seeks to establish a caliphate under Sharia (Islamic law). Its members embrace Salafism, an austere and radical interpretation of Islam, holding that Muslims should emulate the actions of the first generation of Muslim leaders, who are known as 'The Righteous'. Since 2001, the Taliban has actively fought to push U.S. and NATO military forces out of Afghanistan and delegitimise the current government of Afghanistan. The Taliban utilises both conventional and unconventional tactics to pursue its goals throughout participating in national politics and conducting terrorist attacks. The group's power is concentrated and maintained in the hands of mullahs from the Kandahari Pashtun tribes, known as the Quetta Shura.[121]

[120] Counter Extremist Project, *Taliban.* [online] Available at: <https://www.counterextremism.com/threat/taliban> [Accessed 2 November 2020].

[121] Semple, M., Rhetoric, *Ideology and Organizational Structure of the Taliban Movement,* United States Institute of Peace, Washington 2014.

Map. Main places of operation



LASHKAR-E-TAIBA (LET)

Place of origin: Pakistan (1987).

Potential places of operation: Pakistan, India, Kashmir, Sri Lanka, Bangladesh, Nepal, Maldives, US, Canada, Australia, Syria, Lebanon, and Egypt.

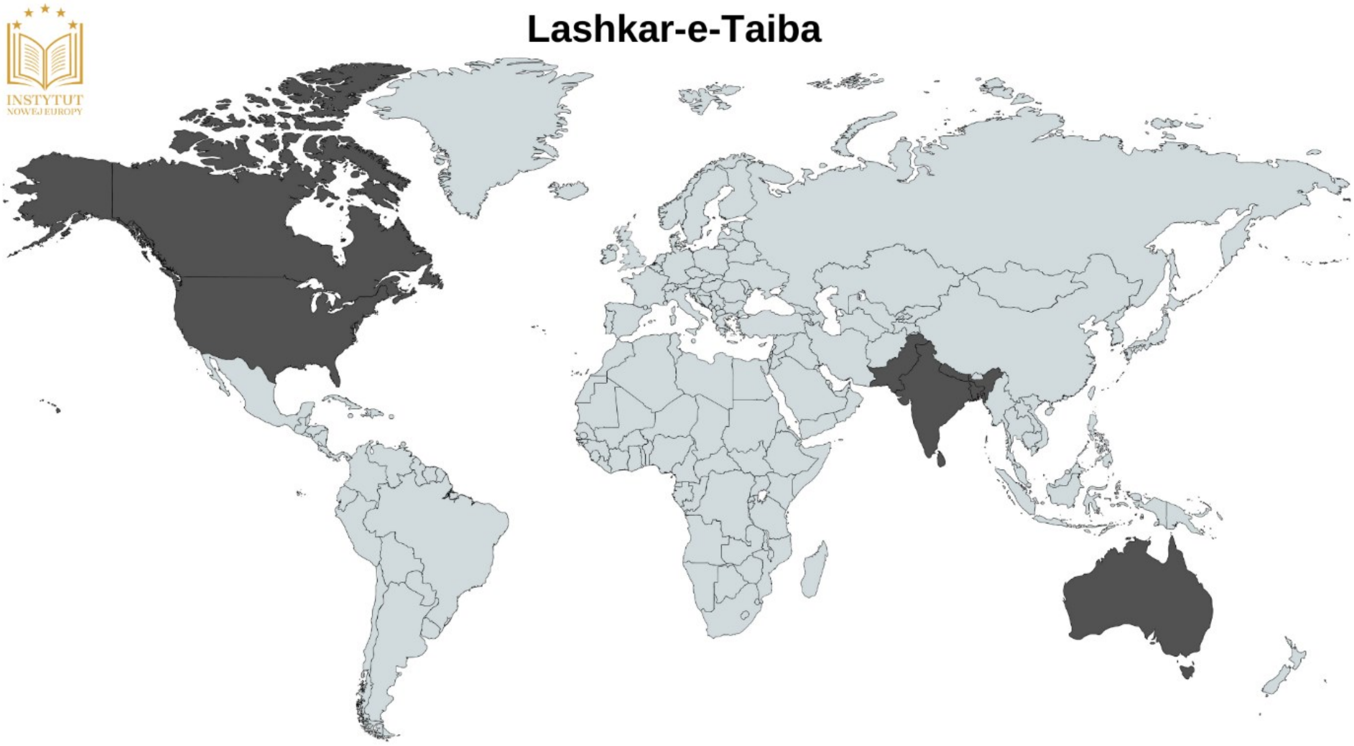
Sources of funding: Support from Pakistani companies, contributions from charities, private businesses, false trade invoicing, extortion, drug trafficking.

Executive summary:

Lashkar-e-Taiba (LeT), meaning 'Army of the Pure' is a violent Islamist group based in Pakistan. LeT sees the fight against Indian control over Jammu and Kashmir as part of a global struggle against the oppression of Muslims, and ultimately seeks to establish an Islamic caliphate in the Indian subcontinent.[122] Since its formation in the 1990s, LeT has carried out numerous attacks against military and civilian targets in India, particularly within the northern state of Jammu and Kashmir. LeT adheres to the Ahl-e-Hadith faith, a South Asian version of Salafism. Like al-Qaeda and other Salafist groups, LeT seeks to reclaim what it considers to be 'Muslim lands.' LeT has developed a robust infrastructure within Pakistan and has attracted new recruits through fostering an anti-corruption image. Because of this, the Pakistani state rewarded LeT with preferential treatment, which the group leveraged during the first several years following the 9/11 attacks to provide primarily covert assistance to al-Qaeda and other actors drawn to a global jihadi agenda.[123]

[122] Bajoria, J., *Lashkar-e-Taiba (Army of the Pure) (aka Lashkar e-Tayyiba, Lashkar e-Toiba; Lashkar-i-Taiba)*, Council on Foreign Relations, New York 2010.
[123] Tankel, S., *Laskar-e-Taiba: From 9/11 to Mumbai,* ICSR, London 2009 p. 5.

Map. Main places of operation



USAGE OF AI BY TERRORISTS

The risk of terrorists obtaining artificial intelligence

Due to the international threat of terrorism,[124] there is a widespread belief that extremist organisations are likely to use artificial intelligence to launch terrorist attacks. Among the organisations that have sufficient financial resources to obtain access to such advanced technologies, there are 10 that should be especially noted: al-Qaeda, ISIS, Hamas, Hezbollah, the Taliban, the Kurdistan Workers' Party (PKK), the Islamic Jihad Movement in Palestine, Kata'ib Hezbollah, Lashkar-e-Taiba and the Boko Haram. Apart from their own finances, state sponsorship is also a major factor in their ability to obtain these technologies, due to such support translating into major logistic and economic benefits for those organisations (such as Hezbollah).[125] Such cooperation usually occurs when countries want to advance their agendas using terrorists, instead of engaging with their own resources, such as their military.

[124] Institute for Economics &Peace, *Global Terrorism Index 2015 – Measuring and understanding the impact of terrorism,* Sydney 2015. Institute for Economics &Peace, *Global Terrorism Index 2017 - Measuring the impact of terrorism,* Sydney 2017. Institute for Economics &Peace, *Global Terrorism Index 2020 - Measuring the impact of terrorism,* Sydney 2020.

[125] M. Hoenig, *Hezbollah and the Use of Drones as a Weapon of Terrorism.* [online] Available at: <https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism> [Accessed 14.10.2020].

The possibility of obtaining AI to conduct a lethal attack is real, but in most cases, it is rather unlikely. Nonetheless, using the world's most advanced weapons, such as robot killers[126] – and testing them against terrorists – could be the first step towards AI-controlled weaponry reaching the black market. A black market for weapons already exists, and terrorist organisations are also scavenging and requisitioning Western equipment that would then be used against them. Terrorists always sought to seize highly advanced weaponry to get a greater advantage, but achieving this goal poses a considerable challenge. In this section, the paper will measure the possibilities of extremists seizing and utilising artificial intelligence technologies.

Should terrorists gain access to AI-controlled weaponry, this will greatly amplify their threat against the international community. First of all, they will no longer be limited by geography and borders to stage attacks in other countries. For example, terrorist organisations may attack facilities near one's border or deploy a drone within the US or Europe to carry out an attack. Secondly, the recruitment process of new members will boost their numerical strength and decrease the need for suicide bombers due to substituting them with drones. Thirdly, it will be easier for organisations to obtain classified information about opposing armies through AI-supported hacking operations. Finally, it is considered likely that terrorists will focus their attention against the US and its coalition as a result; since AI was already verified to be one of the main threats to the US military.[127] In this scenario, terrorist organisations lucky enough to get their hands on such technology become one of the greatest and innovative threats in the 21st century, but such a turn of events seems to be somewhat less likely. In the case of states offering their support to terrorists, it is extremely unlikely that they would give away the latest technologies out of fear of their proxies becoming uncontrollable; one

[126] H. Liu, L. Van Rompaey, M. Maas, *Beyond Killer Robots: Networked Artificial Intelligence Systems Disrupting the Battlefield?*, Journal of international humanitarian legal studies 10 (2019), p. 77-88.
[127] Johnson, K., 2019. *Defense Innovation Board unveils AI ethics principles for the Pentagon*, [online] Available at: <https://venturebeat.com/2019/10/31/defense-innovation-board-unveils-ai-ethics-principles-for-the-pentagon> [Accessed 17 September 2020].

needs to consider the repercussions of Hezbollah going rogue if Iran provides it with support of this kind.

Equally, the prospect of using AI in war appears both tempting and alarming. Whereas AI can extremely quickly become as effective as soldiers who gained skills and experience throughout the years, it does not possess a moral compass unlike human soldiers. The usage of AI weaponry also means limited or outright no inhibitions affecting their combat behaviour and doctrine in the long term. Terrorist organisations are responsible for thousands of deaths, civilian and military, and have no quarrel with using advanced technologies to increase that number. For such groups, AI is just another means of competing against enemies – with the only change being the tool, not the ideology. Their characteristically fanatical belief in the importance of their agenda is what they advance as a group with. Therefore, they will not be restrained by concepts of decency, morality or proportionality, which makes them barely different from AI-controlled robots. As a result, AI itself is nothing more than a means to maximise damage and minimise losses. Moreover, drones can be used for propaganda purposes to flaunt one's own advancements in technology; all while considering that the fanatic nature of terrorists will push them to use either a gun or a drone to attack against regular armies or civilian targets on a regular basis, even if AI is not critical to their operations.[128]

[128] Van der Veer, R., 2020. *Terrorism in the age of technology*, [online] Available at: <https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology> [Accessed 18 September 2020].

UNMANNED AERIAL VEHICLE – A LETHAL WEAPON OF TOMORROW FOR TERRORISTS

Contemporary global terrorist threats mainly harness artificial intelligence that supports weaponised robots, missiles as well as clusters of killer drones. This narrative arose a few years ago, indicating that terrorists may have a vastly greater array of options at their disposal because they may cooperate with some states that will back them up. The chance for terrorist organisations to gain access to artificial intelligence technologies only increased due to the global competition surrounding it. The reality of numerous articles, shows and films used on military training grounds, prepared by their respective wealthy countries, highlights each of the superpower's efforts to flaunt their achievements and solidify their lead in the AI competition. For most superpowers, the systems with AI support are imperative on the modern battlefield. This importance is only highlighted by the obstacles put in place by USA, China, Russia or Iran to ensure that their competitors' intelligence agencies put the efforts to both secure and steal research data, to ensure that they are not left behind in their race. Yet, increased interest will provoke further development and widespread usage of the technology. Due to this potential spreading, terrorists will have a chance to operate weapons supported by AI. These events then merge into a deeply concerning scenario which conceivably may have to be confronted.

UAVs, such as drones, can be the first types of weapon platforms that could be controlled by AI and manipulated for terrorist activities. Their simplicity enables terrorists to conduct an attack without the involvement of a high number of people or logistics. Depending on the scale of the attack, some strikes may even be coordinated by a single person. Furthermore, there are previous examples of terrorist organisations conducting drone attacks supported by artificial intelligence, listed below.

The use of AI drones by terrorists

Non-state actors, including terrorist organisations, have been trying to use drones against state actors for years. According to information in the media, there have been a significant number of incidents and none of them was fatal until the end of 2016. Drones were usually used to fly over a specific section of territory to check for potential weapons and gathering intelligence on military bases. Despite having limited capabilities, terrorists were able to carry out successful missions and even kill other terrorists. At the beginning of the 21st century, the most common region that saw their use was Israel and Pakistan. Progressively, the facilities of terrorist organisations improved and more attacks in different countries have been noticed in the last 5 years.

By adapting to technological improvements, extremists managed to achieve their goal and ultimately carried out a deadly attack with a UAV against a state actor, on the 2nd October 2016. It was the very first successful attack using this kind of technology, most likely perpetrated by ISIS.[129] Until then, according to information from the Pentagon, terrorists had only been using simple and basic versions of drones which are easy to purchase and use to conduct surveillance, as well as transporting explosives. As

[129] Ware, J., 2019. *Terrorist groups, artificial intelligence, and killer drones*, [online] Available at: <https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones> [Accessed 21.09.2020].

part of their tactics, the U.S. forces operated special equipment to defeat UAVs using anti-drone rifles to disrupt the signal between the machine and its remote.[130]

Tab. Few examples of terrorists using UAVs until 2015

DATE	LOCATION	PERPETRATOR	OUTCOME
14 JULY 2014	Ashdod, Israel	Hamas	Shot Down by Israeli Patriot Missile
23 AUGUST 2014	Near Raqqa Province, Northern Syria	Islamic State (IS)	Successful Operation
30 AUGUST 2014	Falluja, Iraq	Islamic State (IS)	Successful Operation
12 SEPTEMBER 2014	Kobani, Northern Syria	Islamic State (IS)	Successful Operation
21 SEPTEMBER 2014	Near Arsal, Northeastern Lebanon	Hizbollah	Successful Operation
APPX. 16 MARCH 2015	Near Fallujah, Iraq	Islamic State (IS)	Drone Destroyed by U.S. Coalition Airstrike

Source: R. J. Bunker, *Terrorist and insurgent unmanned aerial vehicles: use, potentials, and military implications,* Strategic Studies Institute and U.S. Army War College Press, August 2015, p. 13-15.

In another example, ISIS sent an unmanned aerial vehicle loaded with explosives to attack French and Kurdish positions in the northern part of Iraq: Erbil. Two Kurdish soldiers were killed, and other two French special operations soldiers were severely injured. Explosives were hidden in a small plane filled with Styrofoam. This is one of the ISIS' most popular methods when drones are used as a ruse in order to get as close as

[130] Gibbons-Neff, T., 2016. *ISIS used an armed drone to kill two Kurdish fighters and wound French troops, report says,* [online] Available at: <https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says> [Accessed 21.09.2020].

possible to the troops' position.[131] It must be underlined that this attack was the very beginning of terrorist activities reinforced by highly developed technologies, and also an indication in which direction extremists will go.

In 2017, ISIS announced the formation of a division named ‘Unmanned Aircraft of the Mujahideen’, whose main goal was to develop and use UAVs as part of a long-term strategy for advancing and weaponising drone technology. The group has been using drone technology for surveillance and targeting, mainly in Iraq and Syria. In spite of increasing losses of territory, ISIS is continuously making advances in modernisation, manufacturing and deployment of drones. In addition, the organisation was able to drone strike a battle tank in Mosul in 2017.[132]

In early 2019, an unprecedented kind of attack occurred: a swarm of drones attacked two Russian military installations in Syria. The drones in question had barometric sensors, which allowed them to change altitude, and highly developed GPS guidance with specific targets programmed to be destroyed.[133] In other words, the drones that took part in the attack did not require further instructions or guidance from terrorists after they were launched. Ten of such drones were equipped with explosive devices and descended over the Hmeimim airbase, while three other ones targeted the Russian Naval Combat Support ship close to Tartus. Other weaponry included shells filled with Pentaerythritol Tetranitrate (PETN), which were attached to their wings. To make matters worse, the UAVs were flying at low altitudes and could not be detected

[131] N. Guibert, 2016. *Irak : Paris confirme qu’un drone piégé a blessé deux membres des forces spéciales françaises à Erbil*, [online] Available at: <https://www.lemonde.fr/proche-orient/article/2016/10/11/irak-deux-commandos-francais-gravement-blesses-a-erbil-par-un-drone-piege_5011751_3218.html> [Accessed 21.09.2020].

[132] Rogoway, T., 2017. *ISIS Drone Dropping Bomblet On Abrams Tank Is A Sign Of What’s To Come*, [online] Available at: <https://www.thedrive.com/the-war-zone/7155/isis-drone-dropping-bomblet-on-abrams-tank-is-a-sign-of-whats-to-come> [Accessed 21.09.2020].

[133] Morton, M., 2018. *Inside The Chilling World Of Artificially Intelligent Drones*, [online] Available at: <https://www.theamericanconservative.com/articles/inside-the-chilling-proliferation-of-artificially-intelligent-drones> [Accessed 20.09.2020].

by radar systems. It is unknown whether the drones were controlled by artificial intelligence and whether communicating with one another. Yet, their attacks were synchronised in such a fashion that their multi-angled attack confused air defence systems. Eventually, the attack, which had been probably prepared by a Syrian rebel group, failed. Russian systems reacted through the combined use of kinetic and electronic air protection models.

Later that year a craft remotely piloted by Houthi attacked Saudi Arabia's oil facilities in Abqaiq and Khurais. The rebels aimed at the world's largest oil processing facility, which is essential to global energy supplies.[134] The perpetrators sent between 10 and 25 drones which carried out the operation as a swarm. The UAVs attacked in at least two waves and caused enough damage that putting out the fires posed a considerable challenge. The verification of satellite images revealed that there was a minimum of 19 strikes that damaged 14 storage containers. Although Saudi Arabia has MIM-104 Patriot missile defence systems, it was not able to detect them due to flying too low and from multiple angles, thus once again rendering the air defence ineffective. Besides, there have been hundreds of attacks with drones and missile against Saudi Arabia's infrastructure in the past two years.[135]

Such types of attacks are the first step to symbolise that technological advancements can allow weapons to (in part or fully) independently destroy the infrastructure of an enemy. Most of the countries progressing through the AI race offer smaller, faster, and virtually autonomous drones, which in time will only increase the severity of future attacks. At the same time, governments and private companies have control over these types of advanced technologies and because of this, the data is at a considerable risk of being targeted for espionage (for example, their sheer numbers offer many options

[134] Kumar, N., 2019. *Saudi Arabia Drone Attack: Sign of Changing Character of Hybrid War*, [online] Available at: <https://www.vifindia.org/article/2019/october/01/saudi-arabia-drone-attack-sign-of-changing-character-of-hybrid-war> [Accessed 22.09.2020].

[135] Rieas, 2020. *The Saudi oil industry under Houthi attacks*, [online] Available at: <https://rieas.gr/researchareas/editorial/4556-the-saudi-oil-under-houthi-attacks-2> [Accessed 22.09.2020].

for actors to steal the information through cyberattacks). Non-state actors already use similar equipment to gain information about the location of armed forces, type of armament or potential movements of soldiers. In this regard, terrorists operate similarly to state forces and owning advanced technologies will allow them to fight at a more equal footing with them by finding new ways to combat them (similarly to how private military companies also operate similarly to state forces due to the possession of advanced technology). Due to this, it seems that each actor (state or non-state) must accept a world where the UAVs controlled by artificial intelligence become a primary tool on the battlefield, even though there are debates and questions about the ethics of deploying drones on the battlefield.[136] The usage of drones has created an atmosphere of fear where it is imperative to develop counter-measures to prevent their use. Hence, it is obligatory to improve defensive and offensive armament if a state wants to be a key player in the global race and the future.

Nevertheless, the truth is that UAVs are relatively inexpensive and easily manufactured meaning that their loss has little impact on terrorist activity. The most prominent organisations are currently developing means of electronically hardening their drones and adjusting their strategies to make them less susceptible to defensive measures. Non-state actors are also boosting their chances of using swarming drones controlled by AI. Only a few technologies are so effective in reducing the physical, financial or psychological costs of deployment for an operation, which is a commonly accepted benefit favouring drone usage.

There are at least a few factors which lead to the frequent usage of UAVs by criminal groups, terrorists, separatists or rebels. It strongly depends on the logistical, financial and territorial opportunities. In this vein, the following aspects should be indicated.

[136] BBC, 2017. *Anti-drone protest at RAF Waddington,* [online] Available at: <https://www.bbc.com/news/uk-england-lincolnshire-41536818> [Accessed 20.10.2020].

Long-distance usage

Most terrorist groups can conduct an attack from long distances. Having the technology which allows for tracking down a target, as well as coordinate a set of actions with an objective in mind is a perfect weapon for war. The biggest terrorist organisations have their headquarters set in the Middle East and Africa, or are trying to seize a part of the territory in their region. If it is a region where they are regularly clashing with the state's army or it is close to a border, it is far more cost-effective to send in drones with bombs. The distance from the headquarters of the terrorist group could be challenging to traverse, but if there is a possibility to send an UAV then this becomes an easier task. Moreover, aerial superiority is a key tactic that is used by many states while fighting terrorists. If organisations achieve air superiority through using UAVs, then this not only becomes an issue of distance or logistics, but also an issue of a force multiplier. In a long-distance attack with drones, the main goal of terrorists is to surprise the opponent and then do as much damage as possible, ideally without using their own forces. Artificial intelligence, through controlling drones, is able to track down, eliminate a target and immediately go back to the terrorists' shelter. In this scenario, the long-distance battle with terrorists has never been more believable.

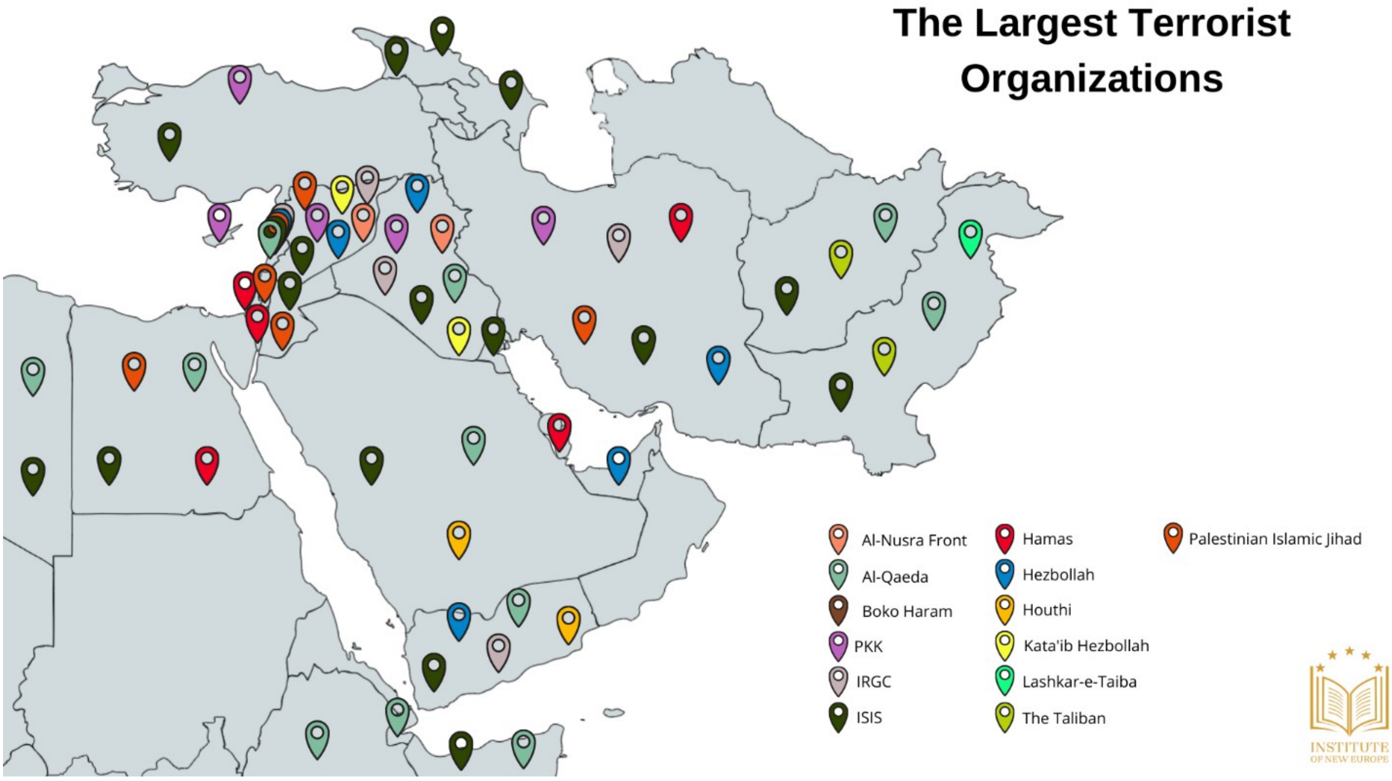
Additionally, where terrorists can carry out an attack with drones, it will demand a response from state authorities against said attack. At the same time, terrorists use that as a form of distraction to carry out a similar attack in a different location. When all state resources are focused on eliminating the threat in one location, the natural absence of forces will be exploited. For instance, Anders Breivk detonated a bomb outside the office of the Prime Minister of Norway to distract everyone, and then went to the Utoya island where he killed 69 people. A terrorist may work to acquire and prepare multiple drones to launch a synchronised attack in multiple parts of densely populated areas. Where one drone strikes, the authorities will respond, and this will be a repeating pattern with more drone strike occurring successively; thus straining the resources of local authorities and causing substantially more chaos and panic. The perpetrator may or may not even be required to physically participate in the attack, as artificial intelligence will be able to coordinate and carry out the attack with little or no input from the terrorist. This will also offer the terrorist increased anonymity due to not being required to reveal himself or offering a greater window of relocation away from the authorities, allowing him greater survivability and therefore chances to carry out more attacks into the future.

Affordable price for advanced technology

Due to the technological race and rivalry between powerful countries, it is much more likely that terrorist groups will finally obtain AI drones. The price for that unique technology has been increasing by the day, and its common deployment by the USA, China, Russia, India, the United Kingdom, or Germany on the field will result in an easier access to that weapon. Overall, the difficulty in acquiring AI drones will be smaller than one believes, and there are a few factors that lead to this affirmation. The global involvement of superpowers in wars within the Middle East and Africa, as well as the continuous improvement of defence systems and the determination of state interests being centred on economic and regional security (thus committing further resources in the region) allows terrorist organisations an opportunity to scavenge, requisition or even purchase such equipment where possible. It is not a case of 'if' but 'when and against who' will they use them, leading to AI drone usage by these extremists bringing new dynamics on the battlefield with a weapon that is already commonly fielded by state armies. Their resourcefulness can allow them to either acquire them on their own, or become recipients of these technologies through state sponsorships.

The novelty of these technologies will make them hard to acquire and purchase at first. However, it is a matter of time until the first group gains access to them and conducts terrorist attacks on their own means. It can be sold by a specific country, or it can be acquired through illegal investments in third countries. Nevertheless, the cost of purchase and future handling will diminish to manageable levels by at least a few terrorist organisations with a lot of finances supporting their operations already.

Map. Potential places of operation in the Middle East



Undemanding process of exploitation

It appears that terrorists will most likely not develop their own artificial intelligence and drones that would be supplied to the international market. There is no time for such a long-term and financially demanding process – extremist groups must be supplied with specific weapons which are ready for immediate use. The acquisition process is dependent on the supplier, especially when the organisation does not have its own industry or relevant engineers. Only a few technical issues are up to the operator: determining the target of the attack, arming the platform, and maintaining it. Obstacles to programming a drone and providing technical support should not be an issue if the weapon assembled and delivered to them and thus it is ready for use. However, even if the weapons provided are ready for use, terrorists will still have the opportunity to improve their AI capabilities and can become a massive threat to the international community, with states seeing its security jeopardised as a result. Terrorists would be able to receive weaponry from across the world, with this being subjected to the secrecy surrounding the supplier. Since UAVs will be equipped with AI in the future, engineers familiar with this kind of software will face no difficulty in modifying or adapting it, making terrorists able to use them with ease.

Labelling terrorist activity

The information about terrorists involved in an attack carried out with AI drones could be made public depending on the needs of the perpetrator, the international context and, above all, whether there is enough evidence to blame an organisation and not a state provider instead. Some terrorist organisations such as the Islamic State, Al-Qaeda, and Hamas might prefer to make an impact and loudly manifest their new success. It could be done to announce to the international community that they have this kind of weapon and can continuously compete with state armies. Moreover, they could use their first attacks as means of spreading panic by threatening their enemies with the following raids. On the other hand, there will be groups which would prefer not to be associated with murderous attacks of this kind, and those are probably smaller nationalist or separatist groups, but still want to coerce their opponents.

Given the tendency for terrorist organisations to show their presence and power, they may characteristically mark their drones with flags or post their usage on social media. This ensures accountability towards blaming extremist organisations, since it would be difficult in these circumstances to hide their allegiance. Most of the largest terrorist organisations have their territories under control, and from there, they will conduct an attack at long distance. Meanwhile, if a strike happens in a foreign country, where terrorists are required to activate a drone from a distance, there will be no need to deploy terrorists there and proceed with traditional ways of carrying out an attack. The machine can be sent, for example, from the suburbs of Paris to hit the Eiffel Tower, with the rest depending on the response of local authorities.

Anti-aircraft warfare improvement

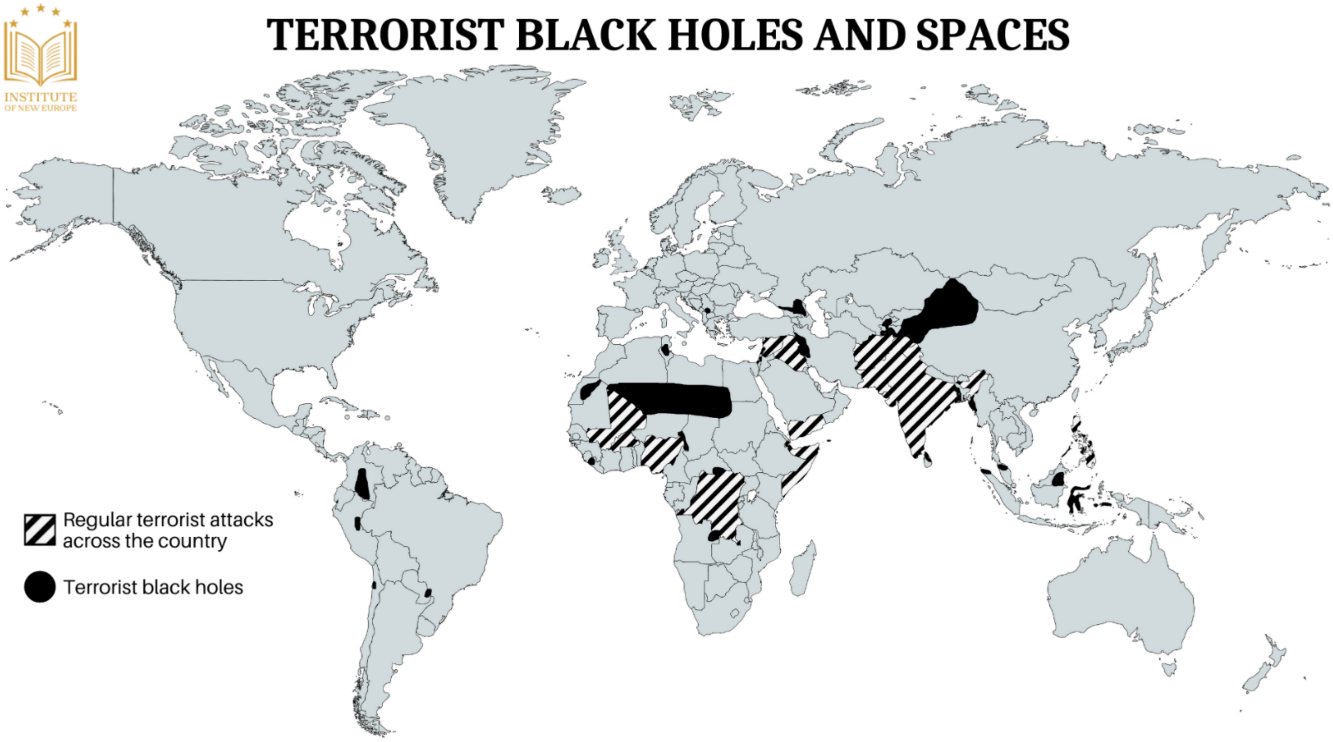
Recently, the deployment of drones has accelerated across many battlefields; becoming a natural extension to the tools already available for war. Additionally, new tests are permanently being conducted, which will increase the combat potential of Unmanned Aerial Combat Vehicles (UACV) in many situations, such as destroying or misleading anti-aircraft defences. Having the advantage of using untraceable UAVs controlled by artificial intelligence would become the most essential element of one's own armament.

It is quite evident that most countries which are involved in conflicts such as those in Syria and Libya are testing new weapons. Furthermore, some of these attempts offered outstanding results. During the conflict in Libya, Turkey supplied drones for the Government of National Accord that allegedly destroyed a Pantsir missile system (Pancyr-S1) given by the Russians to the oppositional Libyan National Army (LNA). The incapacity to eliminate the airborne threat indicates the need to bolster the effectiveness of their air defences. It is strongly related to the ongoing conflicts where new technologies are being used, which leads to global competition in defeating anti-aircraft systems.[137]

[137] Parachini, J. V., Wilson, P. A., 2020. *Drone-Era Warfare Shows the Operational Limits of Air Defense Systems*, [online] Available at: <https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html> [Accessed 21.09.2020].

Terrorist organisations will certainly try to obtain these kinds of advanced weapons. They are endeavouring to operate on the same level as state organisms, frequently marking their atrocious presence. In one of many examples, a number of Saudi Arabian oil facilities were the targets of missile and drone strikes in September 2019, carried out by Houthi rebels. Even fully equipped countries with powerful security capabilities can fall victims to terrorist attacks, resulting in loss of both human life and critical infrastructure integrity, since they could be exposed to a possible attack. Currently, targets, especially critical infrastructure, cannot be secured or moved if air defences fail to protect it, and attackers have a wide range of electronic and kinetic weapon options to utilise at their disposal.

Map. Terrorist black holes and spaces


INSTITUTE OF NEW EUROPE
TERRORIST BLACK HOLES AND SPACES
▨ Regular terrorist attacks across the country
● Terrorist black holes

Source: own study based on: Korteweg, R., Ehrhardt, D., *Terrorist Black Holes,* Center for Strategic Studies, Den Haag 2005, p. 34.

Quest for drones' attacks

As long as these highly developed technologies, which have the potential of outsmarting or overwhelming defences and shocking the international community, are not available to terrorist organisations, there is little need for concern. Unfortunately, bilateral agreements and self-serving interests are more important for the majority of countries, resulting in highly demanded products, which are often desirable and easy to sell on the black market, becoming available. For terrorists, every new technology is worth its weight in gold. Some state actors will collaborate and share advanced technologies to reach their objectives. Therefore, extremists will get drones controlled by AI sooner rather than later. Terrorists would be ecstatic at the opportunity of using these tools for perpetuating an attack in the name of their ideology. The very first step of having that capability is to share with them the new technologies and deliver a small number of drones to carry out attacks. Alternatively, terrorist combatants may be presented with the opportunity to scavenge or requisition equipment fielded by their opponents on the battlefield, as it happened on multiple occasions during areas of conflict. Extensive usage of AI-supported equipment may increase the chances of terrorists to seize such devices through sheer increase in the number of opportunities of seizing them. Subsequently, not only will terrorists continue to have an impact on the situation in the global security environment, but artificial intelligence will also play an amplifying role as it will be able to carry out attacks as well. Eventually, the threat will be doubled and spiral out of control.

The harnessing of AI systems by terrorists may not be immediate because they must adapt and understand the new technology. Nevertheless, they have knowledge about cybersecurity, which involves the hacking of security systems or sending malicious applications to take control of smartphones and computers and that also offers transferrable skills that will allow them to quickly grasp the notions of AI software.

Concluding thoughts on drones

Swarms of drones pose a massive threat for a states' defensive systems all over the world. A large number of aerial vehicles ready to eliminate the opponent, each carrying more than 200 kg of explosives, could be challenging to stop. Weapon fire could be unleashed by some drones and others may simultaneously drop bombs, perfectly executing a mission. However, it is relatively impossible to carry out this kind of attack by humans controlling the drones. No division of soldiers could control the flight path of each vehicle in a swarm as effectively as AI. In the event of a complex and specific type of mission, only one person should be responsible for one drone. In this scenario, human control would be comparatively more chaotic than AI control due to the lack of a quick and clear communication channel during the rapid attack. Moreover, anti-drone technology enables defenders to jam the signal from the controller. Thus, only artificial intelligence, which launches an attack by itself, is able to steer a vast number of machines avoiding air defence systems in a perfectly synchronised fashion while maintaining command of its assets.

In addition, it is feasible that drones will have a combat load of up to 10 tons sooner rather than later. Russia, one of the major developers of AI technology, has already started their work on advanced drones which will operate at low altitudes at a speed of 1,400 kilometres per hour and carry payloads of 2.8-8 tons.[138] Therefore, an attack made by a swarm of drones carrying at least a few tons of explosives would become the deadliest weapon in the world, excluding nuclear weapons.

Apart from using AI drones to boost their power, terrorists can also weigh on the possibility of using them for the purpose of anonymity, such as to allow the human factor to remain concealed when carrying out an attack ending in success or failure. However, a key limitation to this tactic prevents the organisation from exploiting this

[138] McDermott, R., *Moscow Unveils Further Advances in Drone Technology,* Eurasia Daily Monitor, Volume: 16, Issue: 139, 2019.

from sowing chaos by attempting to pose as a state actor: intelligence agencies are extremely resourceful entities able to collate information and identify the background of the device used based on the features of the object, the circumstance in which the object (or others similar to it) may have been received or used and the patterns that compose an attack. Intelligence agencies are already aware of the possibility of terrorists harnessing drones for attack, as they have caught some in the past. Furthermore, intelligence agencies, even those in rival states, would be inclined to share certain pieces of intelligence with one another in the interest of combating a common enemy, like a terrorist organisation, and states would not immediately resort to pointing blame and playing into the attackers' hands without knowing all the facts.

Scale wise, it is possible that drone warfare between state and non-state actors would also be akin to the fights between state's air forces for asserting the dominance of the skies. Terrorists would have the ability to fight a superpower's air dominance and even harness aerial equipment, but thus gaining the ability to subvert key advantage superpowers and state actors have enjoyed for many years in the fight against terrorism.

3D PRINTING AS A FUTURE TERRORIST

3D Printing can be described as a virtual design of a particular object, which will then be created (or 'printed'). It is a process by which 3D solid objects of any shape or geometry can be created from a digital file. There are a few programs which allow compiling a project by using a 3D modelling software. The object can be replicated based on copying an existing model, or it can be built up from scratch. Generally, a 3D scanner, which is inside the 3D Printer, precise copy of the scanned physical object and uploading its schematics as a digital file.[139] The vital element is to digitalise the real object. In order to obtain a complex digital file, it is necessary to use a professional industrial device which creates a 3D model thanks to the thousands of horizontal lines. A 3D printer consists of a set of components that operate simultaneously to produce the desired output from the inputted digital file.[140] When a whole multi-layered model is uploaded in the 3D printer, the software creates a detailed object that blends each layer, consequently delivering a three-dimensional project ready to print. There is a number of various 3D scanners that use different technologies to scan a target such as

[139] Syed, A., Elias, P., Amit, B., Susmita, B., Lisa, O., Charitidis, C., *Additive manufacturing: scientific and technological challenges, market uptake and opportunities,* Materials today 2017, Vol. 1, pp. 1-16.
[140] Mkhemer, S., *3D Printing Technology,* Birzeit University, December 2014, pp. 3-5.

time-of-light, modulated light and many more that are still being improved. Everything depends on the scale, the number of details of an object, the materials that were used to create it and, finally, its compatibility with other elements with which the object will be used.[141]

3D printing is widely developed all over the world. It creates new opportunities for companies looking to improve their manufacturing efficiency. Conventional thermoplastics, ceramics, graphene-based materials and metal are the materials that can be printed now by using 3D printing technology,[142] which is increasingly applied for the mass customisation or production of any types of open-source designs in the fields of agriculture, healthcare, as well as the automotive and aerospace industries.[143] However, the present development of this technology, as well as its capabilities of using AI, leads to the popularisation of many high-tech systems which could be dangerous in the hands of extremists.

Using 3D printing to produce small arms would probably only be relevant for terrorist organisations, because states have other options and capabilities at their disposal for carrying out similar operations.[144] It is likely that terrorists can obtain said technology to produce guns with the intent of carrying out attacks. It is becoming more and more popular among these groups to create weapons on their own, rather than investing in the black market to buy guns or explosive materials. Because of 3D printing, needed armaments are easily accessible. However, a 3D printed weapon cannot be loaded with a bullet which was not adjusted to the gun – it requires verifying the strength of materials. Besides, in most cases, the printed weapon can be used only once

[141] Almaliki A. J., *The Processes and Technologies of 3D Printing*, International Journal of Advances in Computer Science and Technology, Volume 4 No.10, October 2015, pp. 161-162.

[142] Ze-Xian, L., Yen, T., Ray, M., Mattia, M., Metcalfe, I. Patterson, D., *Perspective on 3D printing of separation membranes and comparison to related unconventional fabrication techniques*, Journal of Membrane Science 2016, Vol 523, No.1, pp. 596-613.

[143] Shahrubudina, N., Leea, T.C., Ramlana, R., *An Overview on 3D Printing Technology: Technological, Materials, and Applications*, Procedia Manufacturing 35 (2019), pp. 1286–1296.

[144] Brockmann, K., Kelley, R., *The Challenge of Emerging technologies to non-Proliferation Efforts controlling Additive Manufacturing and intangible Transfers of Technology,* Solna 2018, p. 36.

to fire a short burst of missiles or a single bullet. Nevertheless, the fact that terrorists can print guns for themselves in every place in the world poses an utmost significant security threat. The quality of 3D printing increases and access to the technology develops the risk and effectiveness of terrorists using printed guns.[145] It can result in a multiplication of terrorist attacks in many countries due to the accessibility to this technology. In the French Republic, almost 50% of attacks conducted by Islamic terrorist were perpetrated with the usage of the pistol.[146]

3D Printing and terrorist attacks

One of the most notable examples of using 3D printing for terrorist's purposes was an attack at the Halle synagogue. An extremist, identified as the 28-year-old German citizen named Stephan Balliet, decided to conduct a terrorist attack during the Jewish holiday of Yom Kippur on the 9th October 2019. He launched the attack trying to enter the synagogue firing shots and using homemade explosives. When he could not smash the doors, he started shooting bystanders next to the temple and killed one woman. Another man who was passing by, wanting to help the wounded woman, survived only because the extremist's gun jammed. Frustrated by his inability to get into the synagogue, the attacker decided to kill people who looked like migrants. He drove in a rented car to the kebab shop nearby, where he killed a 20-year-old man with a shotgun. Next, he fled to Landsberg, about 15 kilometres from Halle, where he started shooting at pedestrians, thus wounding two more people. The terrorist live-streamed the entire attack through the streaming service Twitch, as he hoped to present it to a broad public and to encourage other like-minded people to carry out similar acts. The police investigation proved that the attacker was a far-right and antisemitic extremist.

[145] Van der Veer, R., 2020. *Terrorism in the age of technology*, [online] Available at: <https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology> [Accessed 27 September 2020].

[146] Fondation Pour L'Innovation Politique, *Les attentats islamistes dans le monde 1979-2019*, Paris 2019, p. 32.

Ultimately, the terrorist could have killed approximately 52 people who were in the Halle synagogue and more pedestrians outside, if he was better trained. He also put more people at risk during his dangerous and fast ride to the neighbouring city. One year later, a prosecutor stated that the attacker had been bearing 8 firearms, several explosive devices, a helmet, vest, and he wanted to kill as many people as possible. The terrorist was charged with 13 crimes including murder, attempted murder, bodily harm, incitement and other charges.

The terrorist attack in Halle is very particular due to the usage of the 3D printer technology, which enables the construction of homemade weapons. Only by using free Internet guides, which are accessible for everyone, the terrorist was able to print a weapon. Besides, the terrorist himself admitted that he had fabricated his own gun in order to prove that it is easy to conduct the attack with an improvised weapon. The 3D printed parts of the weapon used in the Halle attack were not necessarily designed for that purpose. However, as the quality of 3D printing increases and the technique becomes more known and available, the risk and effectiveness of terrorists producing their weapons are likely to increase further. This can be the first step in an escalation towards creating sturdy, 3D printed weapons for terrorist attacks. If terrorists already support their firearm manufacturing with 3D components, then it will only be a matter of time until terrorists will be able to outright make their own sturdy guns.

Metal 3D printing is a new technology that will also become more common. In 2013, a Texas company printed a metal replica of an M1911 pistol which successfully fired 600 rounds.[147] Another case in the United States was a prohibition made by a federal judge against Defence Distributed which designs blueprints for printing guns. The company was selling online instructions on how to print parts for AR-15s and other weapons. For this reason, it is vital to put emphasis on the current threats to security

[147] Farivar, C., 2013. *"Download this gun": 3D-printed semi-automatic fires over 600 rounds*, [online] Available at: <https://arstechnica.com/tech-policy/2013/03/download-this-gun-3d-printed-semi-automatic-fires-over-600-rounds> [Accessed 1.12.2020].

which are on the rise due to technological developments. People are increasingly combining 3D printed parts with metal parts to build up weapons, which in turn increases the risk of attacks due to their accessibility.[148]

Nevertheless, considering the increase of right-wing terrorism, the attack in Halle will be remembered, in all likelihood, as historically significant for being the apparent first instance of a terrorist ever using homemade firearms inclusive of some 3D printed components. It is very similar to the activity of terrorists of Islamic State who operated in Western Europe and who fashioned their own weapons, such as knives or explosives. It is also becoming more difficult for security services to find perpetrators due to the lack of buyers of prohibited items that could be traced, as they can independently 'create' deadly items using blueprints the Internet.[149]

The widespread availability of 3D printing and the simplicity with which computer files can be transferred might ultimately affect nuclear proliferation, as they are affecting conventional weapons right now. For example, Raytheon company prints components of a guided weapon, which can serve as an element of the system for a nuclear warhead. It is a part of the future technology when states will use 3D printing to develop a nuclear weapon.[150]

The technology can be both advantage and disadvantage. The use of 3D printing has already made it possible to create different types of objects such as knives, bullets, guns, components of military machines or other dangerous items which can be used against humans. It is not possible that 3D printing will remain limited only to

[148] Daalder, M., 2019. *German attack raises questions about 3D printed guns,* [online] Available at: <https://www.newsroom.co.nz/germany-shooting-raises-questions-about-3d-printed-guns> [Accessed 26.10.2020].

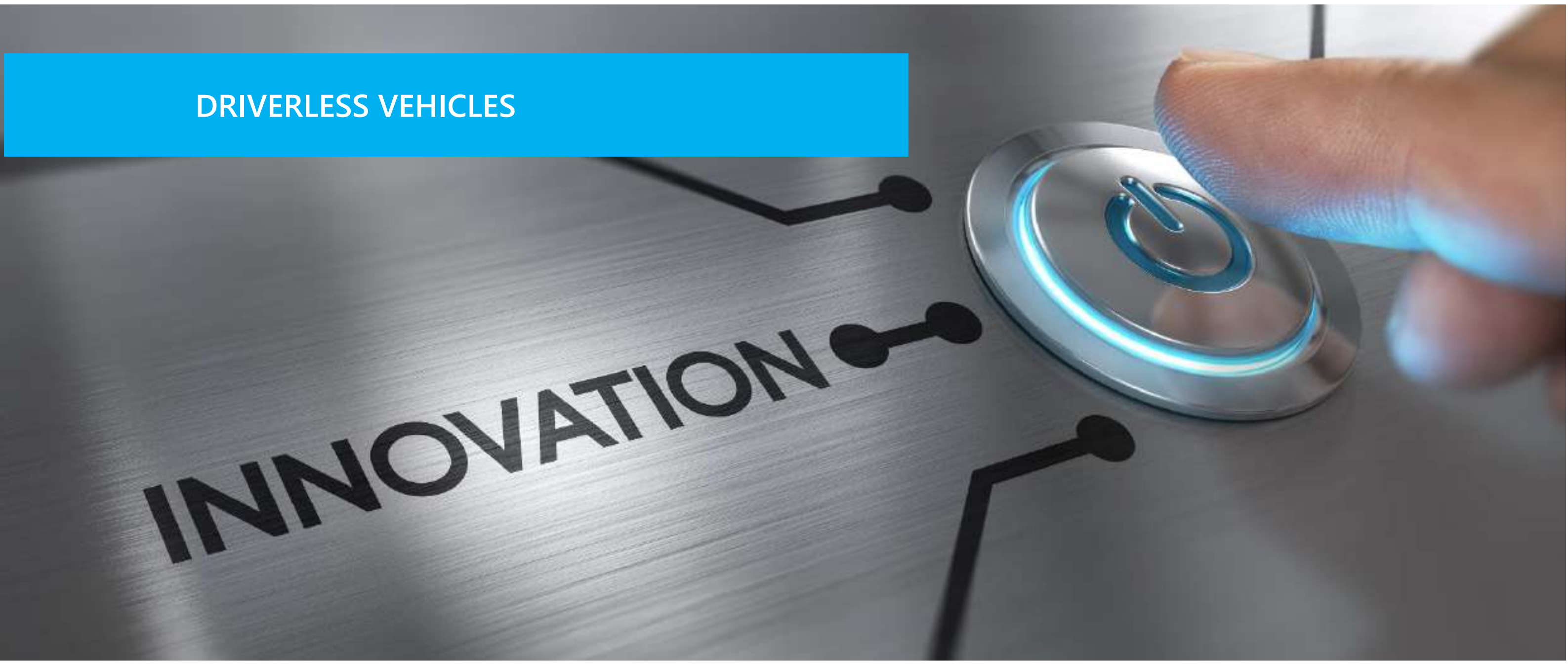
[149] Koehler, D., *The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat*, CTC Sentinerl, December 2019, Vol. 12, Issue 11, p. 18.

[150] Nelson, A., 2015. <*The truth about 3-d printing and nuclear proliferation*> [online] Available at: <https://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation> [Accessed 10.11.2020].

certain groups of people or organisations, as it happens with explosives or weapons.[151] The main idea should be to prevent terrorists and criminals from obtaining guns without being detected. For this reason, it is essential to verify which materials are bought and monitor the people who can buy and print their own weapons. Moreover, the technological race is a global process in which the governments, as well as security services, must adapt or they will be overwhelmed by the increased proliferation and availability of such printers.

[151] Shahrubudina, N., Leea, T.C. Ramlana, R., *An Overview on 3D Printing Technology: Technological, Materials, and Applications*, Procedia Manufacturing 35 (2019), p. 1287.

DRIVERLESS VEHICLES



An autonomous vehicle system can be explained as a 'combination of hardware and software (both remote and on-board) that performs a driving function, with or without a human actively monitoring the driving environment'.[152] Driverless cars are an example of AI that still has not been fully implemented into peoples' lives. Autonomous vehicle technology has been undergoing tests in recent years, but fully autonomous cars are still regarded as part of the future of transportation, though perhaps not so distant now. What the industry promises is that people will no longer be needed to drive, or their role will be more limited than now, as the vehicles will either partially or fully perform this function themselves.

Autonomous vehicles are said to bring a number of benefits. Indeed, they are considered to have a positive effect on the environment through reducing pollution and energy consumption, increasing mobility for those unable to drive (such as disabled, elderly, blind or otherwise too young) ultimately reducing social isolation, as well

[152] The U.S. Department of Transportation, 2016. *Federal Automated Vehicles Policy - Accelerating the Next Revolution in Roadway Safety*, [online] Available at: <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016> [Accessed 25.11.2020].

as also decreasing the frequency of car crashes.[153] Nonetheless, driverless cars, as any other example of AI technology, suffers from drawbacks as well. Driverless vehicles can, in addition to increasing unemployment amongst bus, truck, and taxi drivers, as well as gas attendants (an aspect previously signalled in this paper), relatively decrease many cities' profits from parking lots and public transport, ultimately reducing their budgets.[154]

Furthermore, a grave possible scenario is the one where autonomous vehicles may themselves become a weapon of choice for terrorists, or at least offering a new means enabling them to carry out their attacks. Indeed, in 2014, the Strategic Issues Group, a part of the FBI's Directorate of Intelligence, forecasted that 'autonomy [will open up ways for a car] to be more of a potential lethal weapon that it is today.'[155] As the case of weaponising drones is becoming a primary choice in asymmetrical warfare and has had an impact on changing terrorist strategies, the possibility of autonomous vehicles being part of such strategies has profound consequences that require a deeper analysis as well. Development of autonomous cars will change the tactics adopted by terrorists even further, for instance by using such a car as part of a bombing and thus removing the necessity for martyrdom when carrying out an attack, as 'the driver does not have to remain with the vehicle upon detonation.'[156] Changes adopted by terrorists in their tactics could have grave results, and even though the risk of terrorists using a technologically advanced car to perpetrate a terrorist attack seem to be somewhat low now, over the next years it may rise significantly. Therefore, the possibility of terrorists using fully autonomous or semi-autonomous cars needs to be thoroughly examined.

[153] Anderson J. M., et al., *Autonomous Vehicle Technology: A Guide for Policymakers,* Santa Monica, RAND, 2014.

[154] Anderson, J.M., et al., *Autonomous Vehicle Technology: A Guide for Policymakers* Santa Monica, RAND, 2014.

[155] BBC News, 2014. *FBI: Google's Driverless Cars Could Be Lethal Weapons*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-28344219> [Accessed 6 November 2020].

[156] Bunker, R., 2016. *Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs): Insurgent Use and Terrorism Potentials,* Claremont Colleges, [online] Available at: <https://core.ac.uk/download/pdf/148362649.pdf> [Accessed 7 November 2020].

Car Bombs: Vehicle Borne Improvised Explosive Device (VBIED)

Among other examples, car bombs being used by terrorists is an extremely wide topic, often analysed by terrorism and security researchers. Car bombs are referred to as Vehicle Borne Improvised Explosive Device (VBIED). Using cars as explosive devices is a common tactic employed by a number of terrorist organisations and linked individuals throughout the past decades and virtually across the world. Examples of such can be, for instance, the IRA usage of car bombs from the 1970s to the 1990s, or the 1993 bombing of the World Trade Centre. In the past two decades, however, car bombs were detonated most often in the Middle East, especially across Iraq and Syria. Hugo Kaaman's explanation of a terrorist's usage of VBIED encompasses their tactics best: 'the VBIED can either be parked and then remotely detonated, or it can be driven by a suicide bomber who ultimately controls the detonation mechanism.'[157] In the latter case, the vehicle used shall be referred to as Suicide Vehicle Borne Improvised Explosive Device (SVBIED), or a suicide car bomb.[158]

Given that terrorists have made a frequent, and deadly, use of non-autonomous cars, the argument that they would expand their tactics into fully or partially autonomous vehicles and use them as explosive delivery systems is certainly valid. Reportedly, terrorists have already begun making use of automation, as illustrates the example of ISIS developing remotely-controlled car bomb.[159] In this particular case, terrorists even put a fake driver filled with thermostats to avoid detection by security scanners.

Using autonomous and semi-autonomous cars would constitute a great advantage for terrorists – as indicated above, there would be no need for terrorists to

[157] Kaaman, H., 2017. *The Evolution Of Suicide Car Bombs Examined*. [online] AOAV. Available at: <http://aoav.org.uk/2017/evolution-suicide-car-bombs/> [Accessed 18 November 2020].
[158] Kaaman, H., 2017. *The Evolution Of Suicide Car Bombs Examined*. [online] AOAV. Available at: <http://aoav.org.uk/2017/evolution-suicide-car-bombs/> [Accessed 18 November 2020].
[159] Ramsay, S., 2016. *Exclusive: Inside IS Terror Weapons Lab*. [online] Sky News. Available at: <https://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883> [Accessed 11 November 2020].

drive the vehicle and subsequently die in the result of an explosion, as the car would drive itself to a selected location, or be driven there remotely, and be detonated from distance. Not only would the damage be as devastating, but the terrorist organisation's ranks would also not be reduced, therefore would-be suicide bombers could be employed with other tasks. Even if their capabilities in this regard may not be outstanding at the moment, the possibility of using a fully or partially autonomous vehicle as a car bomb sometime in the future cannot be neglected.

Driving vehicles into crowds

Terrorists around the globe have also been using vehicles for the simple purpose of driving them into crowds. In 2010, in the second edition of the al-Qaeda in the Arabian Peninsula's (AQAP) online magazine *Inspire* – its propaganda tool – there was an article which contained an encouragement to use trucks as weapons to 'mow down the enemies of Allah'[160] in countries that support the 'Israeli occupation of Palestine, the American invasion of Afghanistan and Iraq or countries that had prominent role in the defamation of Muhammad.'[161] Over the past years, there were many attacks with trucks used as weapons, tragic examples of which were those in Nice, France and Berlin, Germany – both of which took place in 2016. In the former, a Tunisian national named Mohamed Lahouaiej Bouhlel deliberately drove a 20-ton truck into a crowd on the Promenade des Anglais,[162] killing 86 people and injuring many others. The latter, too, was perpetrated by a Tunisian, who drove a lorry into the Christmas market in Berlin,

[160] CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. Available at: <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html> [Accessed 3 November 2020].

[161] CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. Available at: <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html> [Accessed 3 November 2020].

[162] Smith-Spark, L., 2016. *France Pays Tribute To Nice Attack Victims*. [online] CNN. Available at: <https://edition.cnn.com/2016/10/15/europe/france-nice-attack-memorial/index.html> [Accessed 10 November 2020].

killing 12 people and injuring over 50.[163] The attacks mentioned above are only two of the far greater number of reported attacks of this kind.[164]

Referring to the Nice attack, John Carlin, Assistant US Attorney General for National Security said 'if they're trying to get people to drive truck into crowds, then it doesn't take too much imagination to think they are going to take an autonomous car and drive it into a crowd of people.'[165] Unfortunately, Mr. Calin's assertion seems to be correct. Should terrorists obtain or exploit autonomous vehicle technology, it is more than certain they would attempt to use it in a way that serves their fight. Despite voices that autonomous vehicles are much safer than non-autonomous cars and are programmed to follow the road rules and restrictions (speed limit, keeping certain distance from other vehicles) resulting in, among previously mentioned, a decreased number of car crashes, terrorists can be expected to meddle the vehicles' algorithms so that they would break their programmed safety instructions and leave the street to enter a sidewalk or go to other places full of people, with the purpose of inflicting harm upon as many of them as possible. It is an ominous scenario, however, one that needs to be taken into consideration given the terrorists' quick adaptability when it comes to newly available technologies and their never-ending attempts to outsmart law and security enforcement by using new methods of carrying out attacks.

Hacking vehicles

One of the methods allowing terrorists to take over control of an autonomous or semi-autonomous vehicle, apart from using their own programmed cars, is that they can hack into somebody's vehicles and make their cars do it instead. Indeed, in mid-

[163] BBC News, 2016. *Berlin Lorry Attack: What We Know*. [online] BBC News. Available at: <https://www.bbc.com/news/world-europe-38377428> [Accessed 15 November 2020].

[164] For a brief overview of more examples see https://edition.cnn.com/2017/05/03/world/terrorist-attacks-by-vehicle-fast-facts/index.html

[165] Industry Week, 2016. *Connected, Self-Driving Cars Pose Serious New Security Challenges*. [online] Industry Week. Available at: <https://www.industryweek.com/technology-and-iiot/emerging-technologies/article/22006985/connected-selfdriving-cars-pose-serious-new-security-challenges> [Accessed 9 November 2020].

2017, RAND Senior Information Scientist Nidhi Kalra said in the hearing conducted by the US Congress House Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection that vehicle hacking – itself a very real threat – creates an opportunity for terrorists.[166] To cite FBI's public announcement, 'vulnerabilities may exist within a vehicle's wireless communication functions, within a mobile device – such as a cellular phone or tablet connected to the vehicle via USB, Bluetooth, or Wi-Fi – or within a third-party device connected through a vehicle diagnostic port.'[167]

To date, there have been many 'hacking-tests' aimed at proving that current vehicles – not fully autonomous, but technologically advanced – are vulnerable to cyber-attacks. An experiment involving the hacking of a car in 2015 serves as an example, when a vehicle was hacked into and the hackers took control over its climate control system, radio, windshields, as well as brakes and steering.[168] While taking control over the first three pieces of equipment does not pose a great danger for the driver or others on the road, taking control over brakes and steering has the potential to cause serious injuries and can be life-threatening.

Though it would require specific knowledge and a set of competencies, a scenario where members of a terrorist organisation acquire the possibility of hacking vehicles cannot be ruled out. There are several possible scenarios that can be brought up here, but a successful cyberattack against a vehicle would enable terrorists, for example, to make the said vehicle accelerate and either steer it into crowds or crash with other cars on the road, both of which will have the ability of taking many lives. An even more worrying scenario is the one where terrorists gain control over multiple vehicles

[166] Jones, S., 2017. *'Autonomous Vehicles Provide An Avenue For Terrorism,' Congress Is Told*. [online] CNSNews.com. Available at: <https://www.cnsnews.com/news/article/susan-jones/autonomous-vehicles-provide-avenue-terrorism-congress-told> [Accessed 15 November 2020].
[167] FBI Public Service Announcement, 2016. *Motor Vehicles Increasingly Vulnerable To Remote Exploits*. [online] Ic3.gov. Available at: <https://ic3.gov/Media/Y2016/PSA160317> [Accessed 14 November 2020].
[168] Greenberg, A., 2015. *Hackers Remotely Kill A Jeep On The Highway—With Me In It*. [online] Wired. Available at: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> [Accessed 14 November 2020].

simultaneously, thus gaining the ability to cause multiple crashes, ultimately blocking the roads, whilst also simultaneously carrying out an attack with more traditional means (i.e., using explosive materials). Due to the blocked roads, ambulances would not be able to reach those injured, which in turn would aggravate the chaos and sow more panic.

Nonetheless, terrorists can hack vehicles for other purposes than using them as weapons as well. Among others, another possible scenario is for them to do so for ransom to obtain money needed to finance their other activities, for instance through breaking into vehicles computer, stealing personal data, and threatening to make it public.

DEEP FAKES

Term 'deep fake' is used to 'describe realistic photo, audio, video, and other forgeries generated with artificial intelligence (AI) technologies',[169] and was first used in 2017. Most often, deep fakes are created through the use of techniques in machine learning, particularly Generative Adversarial Networks (known as GANs). In the process of competition between two different machine learning systems, one of them (generator) creates a type of output data (be it photos, video footage, or audio recordings), and the other one (discriminator) which learns how to identify fake outcomes of the generator's work. The 'competition' goes as long as the former perfects its generation to the degree so that the latter is not able to make a distinction between the real and the fake.

[169] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. Available at: <https://crsreports.congress.gov/product/pdf/IF/IF11333> [Accessed 2 November 2020].

Deep fakes can be used for a variety of beneficial purposes. They can be used, for instance, in education by teachers to deliver ‘innovative lessons that are far more engaging than traditional visual and media formats’[170] by, for instance, ‘bringing back to life’ historical figures. In medicine, it is useful for the purpose of synthesising ‘fake medical images to train disease detection algorithms for rare diseases and to minimise patient privacy concerns’;[171] or in culture and entertainment: one of the museums in Florida created an exhibition dedicated to Salvador Dalí, which featured ‘a life-size re-creation of Dalí using the machine learning-powered video editing technique.’[172]

Despite the indication above, deep fakes can also pose a wide range of threats for national and international security. Indeed, the authors of a study undertaken at the University College London in 2020 argued that ‘fake audio or video content has been ranked by experts as the most worrying use of artificial intelligence in terms of its potential applications for crime or terrorism […].’[173]

Nefarious use of deep fakes

Using artificial intelligence to create deep fakes is rather cost-effective and can be done with widely available software, resulting in the fact that ‘even unskilled operators could download the requisite software tools and, using publicly available data, create increasingly convincing counterfeit content.’[174] Although certainly not everyone

[170] Jaiman, A., n.d. *Positive Use Cases Of Deepfakes*. [online] Toward Data Science. Available at: <https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387> [Accessed 3 November 2020].

[171] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. Available at: <https://crsreports.congress.gov/product/pdf/IF/IF11333> [Accessed 2 November 2020].

[172] Lee, D., 2019. *Deepfake Salvador Dalí Takes Selfies With Museum Visitors*. [online] The Verge. Available at: <https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum> [Accessed 4 November 2020].

[173] University College London, 2020. *‘Deepfakes’ Ranked As Most Serious AI Crime Threat*. [online] Available at: <https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat> [Accessed 4 November 2020].
Link to the study: <https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8>

[174] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. Available at: <https://crsreports.congress.gov/product/pdf/IF/IF11333> [Accessed 2 November 2020].

would be able to produce deep fakes of a quality sufficient enough to fool others, creating deep fakes does not require people to have as much knowledge and technical abilities as one would believe.

One example of using deep fakes for nefarious purposes is releasing fake videos of public figures, especially politicians, conducting inappropriate behaviour, which could undermine peoples' trust in such persons. An example can be a manipulated video that showed U.S. House Speaker Nancy Pelosi as if she was intoxicated with alcohol.[175] Such an operation may be undertaken to influence an election, which, in turn, would undermine the democratic process itself. Another is creating fake photos or videos to blackmail individuals with influence and power to make them share classified information,[176] which could have detrimental effects for their states.

Terrorists, too, can use deep fakes for the purpose of advancing their cause. Out of the possible scenarios, there is the option for members of a terrorist organisation using deep fakes to impersonate somebody's relatives or somebody's work supervisors, ultimately aiming at extracting funds which could be used for funding their activities. Terrorists could do so by attempting to replicate their voice; in such cases, they could use a program that clones voices (interestingly, such software is not only able to 'mimic an input voice, but it can also change it to reflect another gender or even a different accent[177]). Only last year, it was reported that cybercriminals acted in this very way: they used AI technology to impersonate a company's chief executive's boss and

[175] Zegart, A., 2019. *In The Deepfake Era, Counterterrorism Is Harder*. [online] The Atlantic. Available at: <https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/> [Accessed 17 November 2020].

[176] Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. Available at: <https://crsreports.congress.gov/product/pdf/IF/IF11333> [Accessed 2 November 2020].

[177] Future Work Institute, n.d. *Deepfake Video And Audio Recordings*. [online] Future Work Institute. Available at: <https://futureworkinstitute.com/deepfake-video-and-audio-recordings/> [Accessed 7 November 2020].

scammed him into making a transfer of 243.000 dollars.[178] Drawing on the fact that a simple bomb that was meant to be detonated during the 2006 World Cup in Germany and was created with 'a propane tank, alarm clock, batteries and a plastic bottle filled with gas'[179] cost as little as 500 dollars, the number of attacks terrorist would be able to finance, and thus the damage they would be able to inflict with this kind of money, is immeasurable.

Another dangerous option is terrorists generating realistic-looking content (photo or video) aimed at increasing radicalisation efforts and boosting their recruitment campaigns. Such fake content could show, for instance, American, British, or French soldiers committing war crimes (i.e., beating up captured jihadists, or torturing them in some other way), which would not only delegitimise counterterrorism efforts but also appeal to vulnerable recruits. This is best illustrated in the outcomes following certain policies during the War on Terror.

It is widely recognised that not all counterterrorism measures employed by the US in the War on Terror brought expected results. In fact, in some of them the contrary happened: they contributed to either creating new enemies or empowering existing ones. Amongst them were, for instance, mistreating prisoners by subjecting them to torture or extraordinary renditions. Even weak allegations of Muslims being tortured by Western soldiers do have a profound impact on Muslims' perceptions of the West and are therefore likely to motivate them to inflict harm against the Western countries. A case study from the War on Terror supporting this hypothesis is the Abu Gharib scandal, which was only one of the many facilities where terrorism suspects were sub-

[178] Stupp, C., 2019. *Fraudsters Used AI To Mimic CEO'S Voice In Unusual Cybercrime Case*. [online] WSJ. Available at: <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402> [Accessed 10 November 2020].

[179] Temple-Raston, D., 2014. *How Much Does A Terrorist Attack Cost? A Lot Less Than You'd Think*. [online] NPR. Available at: <https://www.npr.org/sections/parallels/2014/06/25/325240653/how-much-does-a-terrorist-attack-cost-a-lot-less-than-you-think?t=1605889247748> [Accessed 5 November 2020].

jected to enhanced interrogation techniques including 'physical violence [...] sexual humiliation, chaining, electrical shocks and sensory deprivation.' Photos of tortured suspects were made public in 2004, and subsequently 'the hooded man, the slavering dog oppressing inmates [became] the iconic symbols of the Western war effort'[180] which, in turn, eventually began fuelling jihadists' propaganda by presenting those tortured as unjustly harmed by the US personnel, and, ultimately boosting terrorists' recruitment efforts. AI technology available today would allow terrorists not only to create fake photos containing Muslims being mistreated by members of Western military forces but also videos of them doing so. Through creating such deep fakes and spreading disinformation of this kind, terrorists would act to facilitate and empower radicalisation process of a number of potential recruits, and thus boost their recruitment efforts, or motivate people to carry out lone-wolf attacks in places they live.

[180] Kennedy-Pipe, C. (2015). *IEDs, Martyrs, Civil Wars and Terrorists.* [in]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, p.158.

TERRORISTS USING NEW TECHNOLOGY FOR DISINFORMATION AND PROPAGANDA

Sylwia Gliwa

As stated before, terrorist organisations would seize the first opportunity of gaining advanced technologies – particularly ones which can guarantee the achievement of one of their primary objectives: international exposure. Attracting media attention not only gives them the possibility to achieve their main political goals but also to intimidate adversaries, find recruits, and exert influence on international relations. Generally, these aims are reinforced by the same actions: inflicting massive fear by threatening people with the potential use of violence and also with more and more sophisticated ways of attack.

Certainly, there is no possibility to achieve said aim without acquiring new technology. Terrorists must, out of necessity or choice, adapt themselves to communication changes and media patterns. They easily adapt any technological innovations that can help them participate in the infosphere more effectively. Some of the tools adopted by terrorists to help them increase their exposure are the internet and social media.

Before the era of social media, terrorist organisations tried to use 24-hour cycles, nationwide or international television news channels. Contrary to immediate impressions, the relation between terrorists and media has not been parasitic, but symbiotic in its nature. During a terrorist attack, the media received shocking footage which in turn guaranteed high audience records, whilst terrorists achieved their goals: that of reaching out to the wider public with planned communication techniques and gaining exposure as a result. However, this relation had some limitations, which have disappeared with the popular rise of social media, such as the censorship of bloody records by mainstream media that can shock people, whilst also attracting potential new recruits. Traditional media always have presented terrorists in a clearly negative way, but social media have also given a voice for their supporters instead. What is more, they also create an opportunity for transmitting in real time and for reaching a much bigger audience without age restrictions.

The Internet and social media have allowed two types of advantages. Firstly, they speed up and facilitate communication between members of terrorist organisations, which allow them to coordinate global attacks easily. Furthermore, they allow them to reach out to all internet and social media users with their tailored content. Secondly, social media have given terrorists a chance to broadcast their attacks in real time and also to carry out long-term operations in the cyberspace, such as propaganda campaigns. The activities in the infosphere of Islamic State or Hezbollah have shown that these organisations conduct not just single, independent actions but coordinate series of them, which can be described as an ‘infowar’ in cyberspace. Not only do they focus on the intimidation aspects, but also on increasing their number of supporters, attracting recruits who are eager to arrive in the controlled areas to support ISIS in building a social life whilst also conducting terrorist acts on their own as the lone wolves.

Propaganda materials produced and published by the Islamic State indicated some of the ways terrorists use technological innovations. The level of sophistication and advancement of these materials depends on the level of organisational development they achieved at that time. Propaganda was used to achieve a variety of aims: threatening opponents, encouraging young men to join ISIS fighters and young women to contribute in building an ISIS society, and last but not least motivate people to conduct terrorist attacks as lone wolves. Assembling supporters and people willing to provide military and social support to the organisation, done through the production of specially prepared video materials and releasing a large amount of fake news or conducting direct communication with potential recruits, returned positive outcomes. There are a lot of examples of women and men recruited to join the ranks of terrorists, which were discussed in media.[181] Not only were network and social media platforms used to publish and send videos encouraging people into active participation, but also to transmit instructional materials, which facilitate the planning of a terrorist attack. To produce these kinds of materials, they used graphics, including animations and even drones to prepare aerial videos. The high quality and preparation of this type of material certainly favoured a better reception from internet users, who get used to the appropriate level of video content that they encounter every day online. The most skilful organisations were the most effective in tailoring their own media activity to meet the conditions of the people.

Another negative example of terrorists using social media is the promotion of their activities in real time. A famous example of such negative use of social media was the attack carried out on March 2019 in Christchurch (New Zealand), when a right-wing extremist broadcasted live on Facebook for less than 17 minutes an attack in which 51 people were killed. From the first report about the harmful content being broadcasted,

[181] A recruitment to the Islamic State takes place through various factors. Potential recruits were tempted by a promise to have a stable place to live, build a family life based on religious values, gain fame or fight in the name of Allah.

social media platforms received it only after 29 minutes after its beginning. More than 4000 people had watched material before it was removed from Facebook. The video was so popular that during the first 24 hours there were more than 1.5 million attempts to upload this material again (1,2 million were blocked at the time of uploading).[182] Despite the fact that the video was removed from Facebook, it is still accessible through other internet services. It should be emphasised that not only the terrorist could broadcast the event, but the witnesses who had a connection to the Internet and a video camera on a smartphone could be narrators since they can broadcast and interpret the event from their personal devices. These people were dictated not only by fear and emotions but also by false information, significantly amplifying the level of fear and chaos in the community

Social media platforms are aware of their role in disseminating disinformation and propaganda and, in order to stop it, have taken numerous steps to detect and remove harmful content. At the end of November 2019, as part of the joint work between the European Union Internet Referral Unit of Europol, Eurojust, and online platforms, a significant number of websites and social media accounts were suspended.[183] A similar discovery was made by the Institute for Strategic Dialogue, which found a gigantic repository of IS data in October 2019. The authorities of Great Britain and the United States were informed about it, but despite that the repository grew steadily.[184]

[182] Facebook statement "Update on New Zealand", [online] Available at: <https://about.fb.com/news/2019/03/update-on-new-zealand/> [Accessed 11.10.2020].

[183] Kozłowski, A., *Europol uderza w serwery ISIS. Cios w propagandę Państwa Islamskiego*. [online] Available at: <https://cyberdefence24.pl/europol-uderza-w-serwery-isis-cios-w-propagande-panstwa-islamskiego> [Accessed11.10.2019].

[184] Silva S., *Islamic State: Giant library of group's online propaganda discovered.* [online] Available at: <https://www.bbc.com/news/technology-54011034> [Accessed 11.10.2019];
ISD, *Click reveals ISD discovery of huge pro-ISIS online cache.* [online] Available at: <https://www.isdglobal.org/isd-in-the-news/click-reveals-isd-discovery-of-huge-pro-isis-cache/> [Accessed 11.10.2019].

The Internet and social media have been created to bring people together. Despite the innumerable advantages, they have also become an area of activity for criminals and terrorists. Many examples prove that, by influencing the public opinion through disinformation, violates the security and public order of the 'online' world.[185] Despite numerous initiatives to combat malicious activity online, the implemented solutions are still insufficient to stop terrorists and criminals.

[185] Such an example were the 2020 riots in the United States triggered by the death of George Floyd and fuelled by harmful third-party activities on social media.

COUNTERTERRORISM RESPONSE IN SOCIAL MEDIA AND SOCIETY

Due to the international terrorist threats and an increasing number of terrorist organisations, there is a need to improve national strategies to sustain a high level of security. Each country uses different measures to protect its citizens but one of the most significant parts of every security system is technology. Highly advanced technologies have become integral to the efforts of ensuring security for one's own state and society. For instance, face recognition technologies integrated into cameras offer more swift identification of perpetrators, particularly if they are emplaced in areas riddled with high criminal activity or in the event of a terrorist attack. Their installation into densely populated areas such as airports or train stations already showcases the benefits of using technology in keeping people safe, and their enhancement with AI capability will only improve their effectiveness through, among other things, quicker identification, faster data sorting and greater coordination between multiple components of a security network.

The extent of which states are able to deploy highly advanced technologies to reinforce their security depends on the available funds and decision-making process. Available time, accessibility and financing for AI technology will affect its deployment in the security sector as well. Despite this, the coordination between local authorities and intelligence agencies will also constitute a pillar of security strategies. Another key pillar in these strategies is surveillance, and artificial intelligence can greatly benefit security forces in managing and collecting intelligence on key threats, as well as tracking suspected people and overseeing high-risk areas. However, the size and complexity of a state, and its society, prevent artificial intelligence from being a 'silver bullet' in dealing with security threats. Therefore, the responsibility to ensure people live in safety also lies with the citizens and society as a whole.

The number of people who have an account on popular Internet sites is growing every day. For this reason, it is vital to take advantage of this opportunity and use its global services for communication as well as a tool to inform people about security threats and, perhaps more important, to educate them how to recognise these threats and radicalised people.[186] Citizens can inform security services through special forms on the website offered by Police.[187] This kind of communication significantly increases the number of people fighting terrorism from a small group of trained counterterrorist officers to all citizens of the country who can share their opinions and views through the Internet, provided people don't misuse the hotline due to misinterpretations or other mistakes, risking to strain resources of authorities. The use of weaponry by anti-terrorist troops cannot be expected to successfully and entirely fight terrorism. A more comprehensive approach that includes encouraging citizens to act collectively in co-operation with authorities will help ensure society is more secured. The cooperation between the civilian and security sectors can go to a long way to preventing multiple terrorist attacks. When a citizen informs the police of an attack, the cooperation between the two can be seen. This also applies to using social media as a means to track

[186] The National News, *Convicted ISIS supporter carried out deadly terrorist attack in Vienna.* [online] Available at: <https://www.thenationalnews.com/world/europe/convicted-isis-supporter-carried-out-deadly-terrorist-attack-in-vienna-1.1104434> [Accessed 16.11.2020].

[187] Polizei Wien, [online] Available at: <https://twitter.com/LPDWien/status/1323364631734341633> [Accessed 16.11.2020].

down possible terrorists, whereas for example they would get reported online and the authorities will take action swiftly, greatly mitigating the time of response and allowing for pre-emptive action to be taken.

On the 9th December 2020, the EU Commission offered a press release that vows to improve the bloc's counter-terrorist capabilities. The focus of this commitment is centred on increasing intelligence sharing frequency and quality between member states and the bloc's Intelligence and Situation Centre (EU INTCEN) for identifying future threats while investing in new technologies (e.g. artificial intelligence), as well as tackling radicalisation online and in prisons through education programs and removal of terrorist content. They also stated that a new ‘EU Pledge on Urban Security and Resilience’ will focus on guaranteeing funding for securing densely populated and symbolic areas, whilst separately upping Europol's mandate and police information exchange programmes.[188]

[188] European Commission, *Security Union: A Counter-Terrorism Agenda and stronger Europol to boost the EU's resilience*, Press release, 9 December 2020, Brussels.

CONCLUSIONS

Terrorism does not constitute a constant and repetitive tactic, but rather a series of varying styles of action intended to destabilise and sow unrest. The recent attacks in Europe were carried out using with knives and machine guns, while explosives are more often used in the Middle East. Therefore, considering the difficulty of stopping terrorists despite knowing what tools they use nowadays, it should be recognised that it will become even more challenging when requisitioned high-tech software and hardware is going to be utilised by them on a regular basis. Over time, modern systems will be available to an increasing number of actors, including members of terrorist organisations. Obtaining drones, including those that can be remotely controlled by artificial intelligence or which are able to affect the systems of states' critical infrastructure, will only become the next stage in the evolution of how the attacks are conducted. Many terrorist groups are already using state-of-the-art technology that was previously acquired or delivered.

On the basis of the existing analyses, it should be pointed out that there is a growing number of threats and challenges in the fight against terrorism. These are exacerbated by the political and social engagement of terrorist groups, which results in these organisations becoming the recipients of further support from certain states or institutions. It also gives rise to multi-faceted threats, which often involves combating not a sole terrorist organisation, but entire states or even ideologies. The threat of terrorism - which is defined as a form of combat - cannot be understated; it is responsible for the deaths of countless civilians and soldiers and has left a permanent mark on international security discussions. Equally, the threat posed by a hybrid of threats in the form of multidimensional and unconventional tactics undertaken by terrorist organisations against the state offers a grave new dynamic to international security that will leave an impact as great (if not more) than terrorism itself.

With a new arms race between the major powers, USA, China and Russia intend to use artificial intelligence not only for not only for boasting their technological prowess or for the betterment of its citizens, but also for developing their own firepower. If one country strengthens its military potential, other international actors will automatically seek to improve their offensive and defensive structures as well, causing an international security dilemma. Thus, the global race would be intensifying. This time, however, artificial intelligence is being implemented, which undoubtedly is having a significant impact on the overall existing relations between the involved actors and the use of military capabilities.

Therefore, further development and usage of advanced information systems, to supervise attacks during military missions, must be closely monitored. However, the scenario where the regular use of modern weapons is involved has many more consequences. Multiple coordinated attacks carried out in different parts of the country may lead to total paralysis. As a result, a key element in the development of any advanced military system is to determine who will have access to it and against whom it will be used. In this respect, two likely scenarios are being considered in the current perspective. Firstly, terrorists might resort to conducting more attacks in response to advanced technologies against them, or secondly, they themselves may start using advanced weapons regularly against individual states and organisations should they get access to them.

The study submitted is to inform on the issue of contemporary technological and terrorist threats, as well as to demonstrate key issues in the process of developing artificial intelligence by global powers. At the same time, it should be stressed that the dynamics of the security environment and rapid technological progress make it impossible to take into account all the variables which are decidedly important for the verification of modern threats.

RECOMMENDATIONS

1. Due to international terrorist threats and the possible procurement by terrorists of advanced technologies, it is vital to start the global debate about the future challenges linked with them. Policymakers working with international organisations such as the European Union, the North Atlantic Treaty Organization, the United Nations, the Arab League, or the African Union should cooperate to prevent the harmful use of new technologies by non-state actors, as well as to control their development by the military or civilian sectors owned by states developing AI.

2. Researchers have to thoroughly collaborate to verify and indicate the most susceptible sectors where new technologies, especially artificial intelligence, could be maliciously used.

3. Engineers, IT specialists, physicists and military operators that specialise in artificial intelligence and are responsible for developing new technologies for their countries must be aware that they may develop machines that will be used by terrorists for nefarious purposes. It is a common, global responsibility to prevent that from happening.

4. Given that the competition for developing AI has already started, experts from different fields should intensify discussions about the usage of artificial intelligence. It is essential to quickly offer new, international policies surrounding AI development, particularly in states that develop it or wish to harness it.

5. The international debate should take into account the views from the private sector. The increasing involvement of private investors is visible. Their voice will be impactful in analysing current issues in the environment of security. It must

be emphasised that many of these companies also develop advanced technologies and artificial intelligence as well, so their expertise is recognisable. Therefore, the joint cooperation between the public and private sector could lead to valuable solutions and agreements.

6. The development and testing of technology must be conducted in a safe environment. Experiments with new AI weapons should not be undertaken during wars or against terrorist organizations as it was done during the war in Syria, where the major powers tried out their newest weapons on the field to test their efficacy.

7. Research and development data need to be as secure as possible with the use of cybersecurity techniques. Given that the importance of developing such technology cannot be overstated, many actors would resort to cyberattacks and beyond to steal them. Ranging from major state actors towards non-state actors, artificial intelligence data will be subjected to many hacking operations with the intent of being stolen and integrated into one's own efforts. In this regard, entities involved must bolster the IT training of staff, as well as improve their anti-hacking and identification software to prevent hackers from gaining easy access to information. Artificial Intelligence can also prove to be a formidable tool for both cybersecurity and cyberattacks, as it would be able to operate much more quickly than humans would in the event of such an attack being carried out by an actor, or an entity being subjected to it.

8. Gradual integration of artificial intelligence and machines using it into day-to-day life will ease society's embrace over them. Whilst doing so, education must play a key role in educating state's citizens of the benefits and drawbacks in utilising these machines. Through doing this, communities and individuals will be trained in understanding and identifying possible terrorist threats related to

these new technologies, as once was the case of drones being banned from flying in major cities due to the threat of an attack .

9. Understanding the power of artificial intelligence may lead to formal agreements between states on how it should be used. However, military usage of AI has led to fruitful results, which can lead to self-serving interests taking priority instead. The potential of artificial intelligence may bring about dozens of new conflicts, as well as be a part of a new Cold War between the major powers.

10. The militarisation of AI will lead to superpowers denying each other of its more liberal use. Furthermore, one of the many international challenges in regulating such technologies is that states may just simply not cooperate at all out of self-interest, leading to talks degenerating quickly. The leading powers in AI development will at best be heavily reluctant to cooperate on this matter, whereas if that happens it will lead to a lacklustre or interpretative compliance with its terms.

11. Current and future strategies must be created knowing that AI and other advanced technologies will become part of the new international security landscape. Due to the expected escalation between major powers centred on the race for superiority over artificial intelligence, it is now more important than ever to establish new international laws, reinforced by international organizations backed by the signatories of most, if not all of its members. There should be repercussions for those that break these laws, complete with sanctions or other punitive actions warranted against state or non-state actors which break its agreements. Additionally, the foundation of an international organization centred on overseeing military AI development is recommended to avoid it from spiralling out of control.

12. The persistent usage of unmanned aerial vehicles on the battlefield leads to the digitisation of regular wars. Moreover, UAVs can be used to transport explosives, weapons, drugs or dangerous chemicals. Special attention should be given to the dual use of various technologically advanced tools that can both benefit average peoples' everyday life, and terrorists. Artificial intelligence will only serve to at least automate this process further and proliferate the use of drones for dangerous purposes.

13. Every purchase, acquisition or usage of UAVs must be marked to provide information about the user of that particular machine. This is similar to air missile systems of particular states or the purchase of weapons by individuals where users and providers must share their information to use the weapons.

14. 3D printing is bound to become one of the key threats for state security. The possibility to create one's own weapon at home can lead to frequent clashes between criminals, terrorists and police. For this reason, new regulations about sharing blueprints of weapons on the Internet, as well as their open sale, must be reinforced. National security services must concentrate on surveilling people who search for blueprints for 3D printed guns or share their knowledge on how to build weapons on social media. One form of regulating the distribution of blueprints is the issuing of government-approved certificates that allows trusted companies to sell their blueprints to vetted individuals. This can further be reinforced by the creation of a state-wide database that keeps track of who is allowed to buy or purchase these items.

15. International cooperation to fight terrorism must be sustained. However, current efforts in the Middle East and Africa need international support not only to restore the peace. The peacekeeping and military operations within the Middle

East and Africa should be followed with thorough reconstruction efforts supported by the international community but led by the governments of the affected states. States which participated in conflicts should also consider the moral duty of assisting such reconstruction efforts given that their contribution resulting in damages within war-torn regions of a MENA state. Western countries, after their interventions end, must leave the damaged countries so as not to exacerbate the conflict. From then on, training of military forces and state authorities should be offered to the governments who struggle with terrorism.

16. Terrorism is very often sponsored or supported, including financially, by different states. Therefore, international sanctions should be imposed on countries which support terrorist activities overtly or covertly. This can include financial penalties to both the state, and to the application of the travel bans and asset freezing of particular persons of interest. Furthermore, it is also worth considering the establishment of observation committees that will supervise weapons exports in relevant conflict regions.

17. States that maintain a military presence for too long, resulting in the draining of the host countries' natural resources, should also be punished with international sanctions due to their activity; which brings about reactions from local communities that can be perceived as terrorist attacks. This will lead to aggravation of the conflict and further aggressive use of advanced technologies by either side.

18. It is only a matter of time that futuristic technologies, such as drone swarms, will be developed into usable assets by military forces. Policymakers, as well as civil society, have a considerable period of time to implement appropriate measures and tools to regulate or combat their inevitable exploitative usage. Many researchers concentrate too hard on future possibilities rather than on current threats. It is crucial to find a balance and define short-term and long-term strategies. The high adaptability of terrorist organizations has been proven and, for this reason, it is necessary to prevent and counteract their efforts quickly.

19. Regarding answering of current and future threats, the international community must endeavour to establish a new status quo, where global standards centred on AI development and deployment are set for the members of the international community to follow; thus, minimising unregulated and anarchic usage of the technology. By balancing them, it will be possible to integrate much more focused and effective policies aimed at securing the future use of advanced technologies. It will offer a chance to simultaneously improve the national and international systems, as well as appropriately prepare for future challenges due to the global technological race.

BIBLIOGRAPHY

1. Abdulla, R. A., *Islam, Jihad, and Terrorism in Post-9/11 Arabic Discussion Boards,* „Journal of Computer-Mediated Communication", 12(3), article 15, p. 1-16.
2. Agence France-Presse, 2020. *At least 110 dead in Nigeria after suspected Boko Haram attack.* [online] Available at: <https://www.theguardian.com/world/2020/nov/29/nigeria-attack-boko-haram-farm-workers-killed>
3. Al Jazeera, 2018. *US hits Iran IRGC with sanctions over support of Yemen's Houthis,* [online] Available at: <https://www.aljazeera.com/news/2018/05/23/us-hits-iran-irgc-with-sanctions-over-support-of-yemens-houthis> [Accessed 12.11.2020].
4. Allen, G. and Chan, T., 2017. *Artificial Intelligence And National Security.* [online] Belfer Center for Science and International Affairs, p.1. Available at: <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf> [Accessed 8 October 2020].
5. Almaliki A. J.*, The Processes and Technologies of 3D Printing*, International Journal of Advances in Computer Science and Technology, Volume 4 No.10, October 2015, pp. 161-162.
6. Anderson J. M., et al., *Autonomous Vehicle Technology: A Guide for Policymakers,* Santa Monica, RAND, 2014.
7. Armed Forces Journal, 2009. *The War of New Words: Why Military History Trumps Buzzwords*, Armed Forces Journal, [online] Available at: <http://www.armedforcesjournal.com/essay-the-war-of-new-words> [Accessed 24.10.2020].
8. Azani, E., *The Hybrid Terrorist Organization: Hezbollah as a Case Study*, in Studies in Conflict & Terrorism, 36:11, 2013, pp. 899-916.
9. Bachmann, S., *Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats: mapping the new frontier of global risk and security management*, Amicus Curiae 2011 (88), pp. 24-25.
10. Bachmann, S., *Hybrid wars: the 21st-century's new threats to global peace and security*, Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, p. 82.

11. Bajoria, J., *Lashkar-e-Taiba (Army of the Pure) (aka Lashkar e-Tayyiba, Lashkar e-Toiba; Lashkar-i-Taiba)*, Council on Foreign Relations, New York 2010.
12. Banerjee, I. and Sheenan, M., 2020. *America'S Got AI Talent: US' Big Lead In AI Research Is Built On Importing Researchers*. [online] macropolo.org. Available at: <https://macropolo.org/americas-got-ai-talent-us-big-lead-in-ai-research-is-built-on-importing-researchers/?rp=e> [Accessed 25 October 2020].
13. BBC News, 2014. *FBI: Google's Driverless Cars Could Be Lethal Weapons*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-28344219> [Accessed 6 November 2020].
14. BBC News, 2016. *Berlin Lorry Attack: What We Know*. [online] BBC News. Available at: <https://www.bbc.com/news/world-europe-38377428> [Accessed 15 November 2020].
15. BBC, 2017. *Anti-drone protest at RAF Waddington,* [online] Available at: <https://www.bbc.com/news/uk-england-lincolnshire-41536818> [Accessed 20.10.2020].
16. Bird, E., Fox-Skelly, J., Jenner, N., Larbey, R., Weitkamp, E. and Winfield, A. *The Ethics Of Artificial Intelligence: Issues And Initiatives*. Brussels 2020.
17. Borkowski, R., *Terroryzm ponowoczesny*, Wydawnictwo Adam Marszałek, Toruń 2006, p. 40.
18. Brockmann, K., Kelley, R., *The Challenge of Emerging technologies to non-Proliferation Efforts controlling Additive Manufacturing and intangible Transfers of Technology,* Solna 2018, p. 36.
19. Builtin.com. n.d. *What Is Artificial Intelligence? How Does AI Work?*. [online] Available at: <https://builtin.com/artificial-intelligence> [Accessed 1 November 2020].
20. Bukowski, S., *Terroryzm europejski*, Słupsk 2010, p. 21.
21. Bunker, R., 2016. *Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs): Insurgent Use and Terrorism Potentials,* Claremont Colleges, [online] Available at: <https://core.ac.uk/download/pdf/148362649.pdf> [Accessed 7 November 2020].

22. Савчук, Т., 2020. *Пентагон занепокоєний використанням Росією штучного інтелекту у військовій сфері. Ось чому* [online] Available at: <https://www.radiosvoboda.org/a/pentagon-zanepokoyenyy-vykorystannyam-rosiyeyu-shtuxhnogo-intelektu-u-viyskoviy-sferi/30841807.html
23. Cafarella, J., *Jabat al-Nusra in Syria: An Islamic Emirate for Al-Qaeda,* Middle East Security Report 25, 2014.
24. Center for Data Innovation, 2019. *Who Is Winning The AI Race: China, The EU Or The United States?.* [online] Who Is Winning the AI Race: China, the EU or the United States?. Available at: https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf [Accessed 2 October 2020].
25. Center on Sanctions & Illicit Finance, *'Al-Qaeda's Branch in Syria: Financial Assessment*, Foundation For Defense of Democracies, Washington 2017.
26. Cesarz, Z. Stadmullller, E., *Problemy polityczne współczesnego świata*, Wrocław 2002, p. 351.
27. CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. Available at: <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html> [Accessed 3 November 2020].
28. CNN, 2010. *New Issue Of Magazine Offers Jihadists Terror Tips*. [online] Edition.cnn.com. Available at: <https://edition.cnn.com/2010/WORLD/meast/10/12/mideast.jihadi.magazine/index.html> [Accessed 3 November 2020].
29. Congressional Research Service, *Artificial Intelligence And National Security*, CRS, Washington 2020.
30. Congressional Research Service, *Hamas: Background and Issues for Congress*, CRS, Washington 2010.
31. Congressional Research Service, *The Islamic State and U.S. Policy,* CRS, Washington, 2018.
32. Council on Foreign Relations, *Palestinian Islamic Jihad.* [online] Available at: <https://www.cfr.org/backgrounder/palestinian-islamic-jihad> [Accessed 2 November 2020]

33. Counter Extremism Project, *Kata'ib Hezbollah,* [online] Available at: <https://www.counterextremism.com/threat/kata%E2%80%99ib-hezbollah> [Accessed 2 November 2020].

34. Counter Extremist Project, *Taliban.* [online] Available at: <https://www.counterextremism.com/threat/taliban> [Accessed 2 November 2020].

35. Daalder, M., 2019. *German attack raises questions about 3D printed guns,* [online] Available at: <https://www.newsroom.co.nz/germany-shooting-raises-questions-about-3d-printed-guns> [Accessed 26.10.2020].

36. Daily Military Defense, *Hypervelocity weapons systems are tested in support of the Advanced Battle Management System*. [online] Available at: <https://www.youtube.com/watch?v=XgwZmkT8VX0&feature=emb_logo> [Accessed 16.09.2020].

37. Daley, S., 2020. *32 Examples Of AI In Healthcare That Will Make You Feel Better About The Future*. [online] Built In. Available at: <https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare> [Accessed 22 October 2020].

38. Defense Advanced Research Projects Agency, 2018. *ACTUV "Sea Hunter" Prototype Transitions to Office of Naval Research for Further Development*. [online] Available at: <https://www.darpa.mil/news-events/2018-01-30a> [Accessed 18 October 2020].

39. Dengg, A., Schurian, M. N., *On the Concept of Hybrid Threats*, p. 26, [in:] Networked Insecurity – Hybrid Threats in the 21st Century, Vienna 2016.

40. Dignum, V., 2018. *Ethics in artificial intelligence: introduction to the special issue*. Ethics and Information Technology, 20, pp. 1-3.

41. Directive (Eu) 2017/541 of the European Parliament and of the Council of 15 March 2017 *on combating terrorism* and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, 31.3.2017.

42. Dziubek T., *Obronność państwa a zagrożenia asymetryczne*, [in:] *Nowe zagrożenia bezpieczeństwa. Wyzwania XXI wieku*, (red.) K. Hennig, Wyższa Szkoła Humanistyczno-Ekonomiczna, Kraków 2015, p. 17.

43. European Commission, n.d. 2020. *Germany AI Strategy Report*. [online] European Commission. Available at: <https://knowledge4policy.ec.europa.eu/ai-watch/germany-ai-strategy-report_en> [Accessed 13 November 2020].

44. European Parliament, *The Financing of the 'Islamic State' in Iraq and Syria (ISIS),* European Parliament's Committee on Foreign Affairs, Belgium 2017.
45. Facebook statement "Update on New Zealand", [online] Available at: <https://about.fb.com/news/2019/03/update-on-new-zealand/> [Accessed 11.10.2020].
46. Farivar, C., 2013. *"Download this gun": 3D-printed semi-automatic fires over 600 rounds,* [online] Available at: <https://arstechnica.com/tech-policy/2013/03/download-this-gun-3d-printed-semi-automatic-fires-over-600-rounds> [Accessed 1.12.2020].
47. FATF, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, Paris 2015.
48. FBI Public Service Announcement, 2016. *Motor Vehicles Increasingly Vulnerable To Remote Exploits*. [online] Ic3.gov. Available at: <https://ic3.gov/Media/Y2016/PSA160317> [Accessed 14 November 2020].
49. Fiott, D., Parkes, R., *Protecting Europe. The EU's response to hybrid threats*, European Union Institute for Security Studies, Paris 2019, p. 5.
50. Fondation Pour L'Innovation Politique, *Les attentats islamistes dans le monde 1979-2019*, Paris 2019, p. 32.
51. Foreign Policy Research Institute, 2013. *The Three Versions of Al Qaeda: A Primer*. [online] Available at: <https://www.fpri.org/article/2013/12/the-three-versions-of-al-qaeda-a-primer/> [Accessed 19.11.2020].
52. Foundation for Defense of Democracies, *Kataib Hezbollah: Background and Analysis*, 2018.
53. Freier, N. P., *Known Unknowns: Unconventional "Strategic Shocks",* Defense Strategy Development, Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 2008.
54. Future Work Institute, n.d. *Deepfake Video And Audio Recordings*. [online] Future Work Institute. Available at: <https://futureworkinstitute.com/deepfake-video-and-audio-recordings/> [Accessed 7 November 2020].
55. Gergin, N., Duru, H., Çetin, H. C., *Profile and Life Span of the PKK Guerillas*, Studies in Conflict & Terrorism, 38:3, 2015, pp.219-232.

56. Gibbons-Neff, T., 2016. *ISIS used an armed drone to kill two Kurdish fighters and wound French troops, report says,* [online] Available at: <https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says> [Accessed 21.09.2020].

57. Global Conflict Tracker, 2020. *Boko Haram in Nigeria.* [online] Available at: <https://www.cfr.org/global-conflict-tracker/conflict/boko-haram-nigeria> [Accessed 1.12.2020].

58. Greenberg, A., 2015. *Hackers Remotely Kill A Jeep On The Highway—With Me In It*. [online] Wired. Available at: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> [Accessed 14 November 2020].

59. Greenhouse, S., 2016. *Op-Ed: Autonomous Vehicles Could Cost America 5 Million Jobs. What Should We Do About It?*. [online] Los Angeles Times. Available at: <https://www.latimes.com/opinion/op-ed/la-oe-greenhouse-driverless-job-loss-20160922-snap-story.html> [Accessed 12 October 2020].

60. Gruszczak A., *Hybrydowść współczesnych wojen – analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów,* (red.) W. Sokała, B. Zapała, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, p. 11.

61. H. Liu, L. Van Rompaey, M. Maas, *Beyond Killer Robots: Networked Artificial Intelligence Systems Disrupting the Battlefield?,* Journal of international humanitarian legal studies 10 (2019), p. 77-88.

62. Harris, L., 2020. *Deep Fakes And National Security*. [online] Congressional Research Service. Available at: <https://crsreports.congress.gov/product/pdf/IF/IF11333> [Accessed 2 November 2020].

63. Hoorickx, E., *Countering "Hybrid Threats": Belgium and the Euro-Atlantic Strategy,* Security & Strategy No 131 October 2017, pp. 6-7.

64. Industry Week, 2016. *Connected, Self-Driving Cars Pose Serious New Security Challenges*. [online] Industry Week. Available at: <https://www.industryweek.com/technology-and-iiot/emerging-technologies/article/22006985/connected-selfdriving-cars-pose-serious-new-security-challenges> [Accessed 9 November 2020].

65. Institute for Economics &Peace, *Global Terrorism Index 2015 – Measuring and understanding the impact of terrorism,* Sydney 2015.
66. Institute for Economics &Peace, *Global Terrorism Index 2017 - Measuring the impact of terrorism,* Sydney 2017.
67. Institute for Economics &Peace, *Global Terrorism Index 2020 - Measuring the impact of terrorism,* Sydney 2020.
68. Iulian R. I., *International terrorism in the 21st century – 16 years after 9/11 2001*, CBU International conference on innovations in science and education March 22-24, Prague 2017, Czech Republic.
69. IZ., 2019, *Путин сравнил преимущества искусственного интеллекта и ядерного оружия.* [online] Available at: <https://iz.ru/928464/2019-10-03/putin-sravnil-preimushchestva-iskusstvennogo-intellekta-i-iadernogo-oruzhiia> [Accessed 12.11.2020].
70. Jaiman, A., n.d. *Positive Use Cases Of Deepfakes*. [online] Toward Data Science. Available at: <https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387> [Accessed 3 November 2020].
71. Jasper S., Moreland, S., *ISIS: An Adaptive Hybrid Threat in Transition,* Small Wars Journal, October 2016, p. 2.
72. Johnson, K., 2019. *Defense Innovation Board unveils AI ethics principles for the Pentagon,* [online] Available at: <https://venturebeat.com/2019/10/31/defense-innovation-board-unveils-ai-ethics-principles-for-the-pentagon> [Accessed 17 September 2020].
73. Jones, S., 2017. *'Autonomous Vehicles Provide An Avenue For Terrorism,' Congress Is Told*. [online] CNSNews.com. Available at: <https://www.cnsnews.com/news/article/susan-jones/autonomous-vehicles-provide-avenue-terrorism-congress-told> [Accessed 15 November 2020].
74. Jongman, A. J., Schmid, A. P., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, Transaction Publishers, New Brunswick 1988.
75. Kaaman, H., 2017. *The Evolution Of Suicide Car Bombs Examined*. [online] AOAV. Available at: <http://aoav.org.uk/2017/evolution-suicide-car-bombs/> [Accessed 18 November 2020].

76. Kaâniche, M., (ed.), *Applying Resilience to Hybrid Threats,* IEEE Security and Privacy Magazine 17(5), September 2019, p. 78.
77. Kennedy-Pipe, C. (2015). *IEDs, Martyrs, Civil Wars and Terrorists.* [in]: C. Kennedy-Pipe, G. Clubb and S. Mabon, ed., Terrorism and Political Violence. London: Sage, p.158.
78. Kerdemelidis, M., Reid, M., *Wellbeing recovery after mass shootings: information for the response to the Christchurch mosque attacks 2019*, „Canterbury District Health Board", 28.05.2019, pp. 2–5.
79. Koehler, D., *The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat*, CTC Sentinerl, December 2019, Vol. 12, Issue 11, p. 18.
80. Koh, D., 2019. *Ping An Good Doctor Launches Commercial Operation Of One-Minute Clinics In China.* [online] Available at: <https://www.mobihealthnews.com/news/asia-pacific/ping-good-doctor-launches-commercial-operation-one-minute-clinics-china> [Accessed 8 October 2020].
81. Коновалова, Н. 2019. *Беспилотная «Ласточка». На железнодорожном салоне в Щербинке показали уникальную технологию.* [online] Available at: <https://spbvedomosti.ru/news/financy/bespilotnaya-lastochka-na-zheleznodorozhnom-salone-v-shcherbinke-pokazali-unikalnuyu-tekhnologiyu/> [Accessed 20.10.2020].
82. Kozłowski, A., *Europol uderza w serwery ISIS. Cios w propagandę Państwa Islamskiego*. [online] Available at: <https://cyberdefence24.pl/europol-uderza-w-serwery-isis-cios-w-propagande-panstwa-islamskiego> [Accessed11.10.2019].
83. Kubaczyk T., *Wojna hybrydowa – (czy) nowy typ konfliktu zbrojnego we współczesnym świecie*, [w:] *Konflikt hybrydowy na Ukrainie. Aspekty teoretyczne i praktyczne*, (red.) B. Pacek, J. A. Grochocka, Piotrków Trybunalski 2017, p. 24.
84. Kudzko, A., 2018. *Future Now: How AI Is Already Changing The Global And Military Landscape - GLOBSEC*. [online] GLOBSEC. Available at: <https://www.globsec.org/2018/02/06/future-now-ai-already-changing-global-military-landscape/> [Accessed 8 November 2020].

85. Kumar, N., 2019. *Saudi Arabia Drone Attack: Sign of Changing Character of Hybrid War,* [online] Available at: <https://www.vifindia.org/article/2019/october/01/saudi-arabia-drone-attack-sign-of-changing-character-of-hybrid-war> [Accessed 22.09.2020].

86. Lasconjarias, G., Larsen J. A., *(ed.), NATO's Response to Hybrid Threats,* Rome 2015, p. 101.

87. Law., R. D., *Terrorism: A History*, Cambridge 2009, pp. 155–157.

88. Lee, D., 2019. *Deepfake Salvador Dalí Takes Selfies With Museum Visitors*. [online] The Verge. Available at: <https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum> [Accessed 4 November 2020].

89. Lopez, C., 2020. *Where It Counts, U.S. Leads In Artificial Intelligence.* [online] defense.gov. Available at: <https://www.defense.gov/Explore/News/Article/article/2269200/where-it-counts-us-leads-in-artificial-intelligence/> [Accessed 25 October 2020].

90. M. Hoenig, *Hezbollah and the Use of Drones as a Weapon of Terrorism.* [online] Available at: <https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism> [Accessed 14.10.2020].

91. Maas J., *Hybrid Threat and CSDP*, pp. 125-130, [in:] J. Rehrl (Ed.), Handbook on CSDP - The Common Security and Defence Policy of the European Union, Vienna 2019.

92. Malakoutikhah, Z., *Iran: Sponsoring or Combating Terrorism?,* Studies in Conflict & Terrorism, 43, (2020), pp. 913-939.

93. McDermott, R., *Moscow Unveils Further Advances in Drone Technology,* Eurasia Daily Monitor, Volume: 16, Issue: 139, 2019.

94. McKinsey & Company, 2017. *Artificial Intelligence And Southeast Asia's Future*. [online] p.4. Available at: <https://www.mckinsey.com/~/media/mckinsey/featured%20insights/artificial%20intelligence/ai%20and%20se%20asia%20future/artificial-intelligence-and-southeast-asias-future.ashx> [Accessed 22 October 2020].

95. McLeary, P., 2018. *Pentagon'S Big AI Program, Maven, Already Hunts Data In Middle East, Africa*. [online] Available at: <https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa/> [Accessed 11 November 2020].

96. Middle East Institute, *Hezbollah's Evolution: From Lebanese Militia to Regional Player*, Washington 2017.

97. Mitchell, J., 2017. *BIDMC Researchers Use Artificial Intelligence To Identify Bacteria Quickly And Accurately*. [online] Bidmc.org. Available at: <https://www.bidmc.org/about-bidmc/news/bidmc-researchers-use-artificial-intelligence-to-identify-bacteria-quickly-and-accurately> [Accessed 4 November 2020].

98. Mkhemer, S., *3D Printing Technology,* Birzeit University, December 2014, pp. 3-5.

99. Министерство цифрового развития связи и массовых коммуникаций Российской Федерации, 2020. *Цифровая экономика РФ*. [online] Available at: <https://digital.gov.ru/ru/activity/directions/858> [Accessed 25 November 2020].

100. Morton, M., 2018. *Inside The Chilling World Of Artificially Intelligent Drones,* [online] Available at: <https://www.theamericanconservative.com/articles/inside-the-chilling-proliferation-of-artificially-intelligent-drones> [Accessed 20.09.2020].

101. Moy, G., Shekh, S., Oxenham, M. and Ellis-Steinborner, S., 2020. *Recent Advances In Artificial Intelligence And Their Impact On Defence*. [online] Available at: <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf> [Accessed 16 October 2020].

102. N. Guibert, 2016. *Irak : Paris confirme qu'un drone piégé a blessé deux membres des forces spéciales françaises à Erbil,* [online] Available at: <https://www.lemonde.fr/proche-orient/article/2016/10/11/irak-deux-commandos-francais-gravement-blesses-a-erbil-par-un-drone-piege_5011751_3218.html> [Accessed 21.09.2020].

103. NATO Energy Security Centre of Excellence, *Hybrid Threats: Overcoming Ambiguity, Building Resilience,* No 11 2017, p. 6.

104. Nelson, A., 2015. <*The truth about 3-d printing and nuclear proliferation*> [online] Available at: <https://warontherocks.com/2015/12/the-truth-about-3-d-printing-and-nuclear-proliferation> [Accessed 10.11.2020].

105. Palestinian public opinion and terrorism: A two-way street?, *Journal of Policing, Intelligence and Counter Terrorism,* 10, (2015), pp. 71-87.

106. Parachini, J. V., Wilson, P. A., 2020. *Drone-Era Warfare Shows the Operational Limits of Air Defense Systems,* [online] Available at:

<https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html> [Accessed 21.09.2020].

107. Piazza, J. A., Guler, A., *The Online Caliphate: Internet Usage and ISIS Support in the Arab World*, Terrorism and Political Violence, May 2019.
Cohen-Almagor, R., *Jihad Online: How Do Terrorists Use the Internet?,* Advances in Intelligent Systems and Computing, Hull 2017.
Salama, B., *The Resilience of the Islamic State,* Institut für Friedenssicherung und Konflikt management, Vienna 2016.

108. Polizei Wien, [online] Available at: <https://twitter.com/LPDWien/status/1323364631734341633> [Accessed 16.11.2020].

109. Pope, C., 2020. *Advanced Battle Management System field test brings Joint Force together across all domains during second onramp.* [online] Available at: <https://www.af.mil/News/Article-Display/Article/2336618/advanced-battle-management-system-field-test-brings-joint-force-together-across> [Accessed 16.09.2020].

110. Ramsay, S., 2016. *Exclusive: Inside IS Terror Weapons Lab*. [online] Sky News. Available at: <https://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883> [Accessed 11 November 2020].

111. Raugh, D., *Is the Hybrid Threat a True Threat?,* Journal of Strategic Security 9(2), June 2016, pp. 1-13.

112. RBC. *Путин назвал срок спуска на воду подлодки с ядерным «Посейдоном»*. [online] Available at: <https://www.rbc.ru/politics/20/02/2019/5c6d2c779a7947c9343f1028> [Accessed 13.11.2020].

113. Renstrom, J., 2018. *The UK Wants To Be The World Leader In Ethical AI*. [online] Slate. Available at: <https://slate.com/technology/2018/08/the-u-k-wants-to-be-the-world-leader-in-ethical-a-i.html> [Accessed 6 November 2020].

114. Rogoway, T., 2017. *ISIS Drone Dropping Bomblet On Abrams Tank Is A Sign Of What's To Come,* [online] Available at: <https://www.thedrive.com/the-war-zone/7155/isis-drone-dropping-bomblet-on-abrams-tank-is-a-sign-of-whats-to-come> [Accessed 21.09.2020].

115. Rotman, D., 2013. *How Technology Is Destroying Jobs*. [online] MIT Technology Review. Available at: <https://www.technologyreview.com/2013/06/12/178008/how-technology-is-destroying-jobs/> [Accessed 24 October 2020].

116. Saker, R., 2020. *The Impact Of Artificial Intelligence In Retail*. [online] My Total Retail. Available at: <https://www.mytotalretail.com/article/the-impact-of-artificial-intelligence-in-retail/> [Accessed 25 October 2020].

117. Sayler, K., 2020. *Artificial Intelligence And National Security*. [online] Available at: <https://fas.org/sgp/crs/natsec/R45178.pdf> [Accessed 11 November 2020].

118. Semple, M., Rhetoric, *Ideology and Organizational Structure of the Taliban Movement,* United States Institute of Peace, Washington 2014.

119. Shahrubudina, N., Leea, T.C. Ramlana, R., *An Overview on 3D Printing Technology: Technological, Materials, and Applications*, Procedia Manufacturing 35 (2019), p. 1287.

120. Shu, C., 2019. *Leaked Chinese Government Documents Detail How Tech Is Used To Escalate The Persecution Of Uighurs.* [online] Available at: < https://techcrunch.com/2019/11/24/leaked-chinese-government-documents-detail-how-tech-is-used-to-escalate-the-persecution-of-uighurs/> [Accessed 7 October 2020].

121. Sikorski, C., Schmuck, D., Matthes, Binder, J. A., *"Muslims are not Terrorists": Islamic State Coverage, Journalistic Differentiation Between Terrorism and Islam, Fear Reactions, and Attitudes Toward Muslims,* „Mass Communication and Society", 2017, vol. 20, Issue 6: „Media, Terrorism and Society", pp. 825–848.

122. Silva S., *Islamic State: Giant library of group's online propaganda discovered.* [online] Available at: <https://www.bbc.com/news/technology-54011034> [Accessed 11.10.2019];

ISD, *Click reveals ISD discovery of huge pro-ISIS online cache.* [online] Available at: <https://www.isdglobal.org/isd-in-the-news/click-reveals-isd-discovery-of-huge-pro-isis-cache/> [Accessed 11.10.2019].

123. Smith-Spark, L., 2016. *France Pays Tribute To Nice Attack Victims*. [online] CNN. Available at: <https://edition.cnn.com/2016/10/15/europe/france-nice-attack-memorial/index.html> [Accessed 10 November 2020].

124. Srivastava, S., 2020. *State Of Artificial Intelligence In US: Becoming Technology Superpower*. [online] Analytics Insight. Available at: <https://www.analyticsinsight.net/state-of-artificial-intelligence-in-us-becoming-technology-superpower/> [Accessed 25 October 2020].

125. Stanford University, *Mapping Militant Organizations.* [online] Available at: <https://web.stanford.edu/group/mappingmilitants/cgi-bin/pages/definitions> [Accessed 2 November 2020].

126. Stupp, C., 2019. *Fraudsters Used AI To Mimic CEO'S Voice In Unusual Cybercrime Case*. [online] WSJ. Available at: <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402> [Accessed 10 November 2020].

127. Sukhankin, S., 2019. *Russia Adopts National Strategy for Development of Artificial Intelligence*. Eurasia Daily Monitor 16(163). [online] Available at: <https://jamestown.org/program/russia-adopts-national-strategy-for-development-of-artificial-intelligence/> [Accessed 18 October 2020].

128. *Summary Of The 2018 National Defense Strategy Of The United States Of America*. 2018. p.3.

129. Syed, A., Elias, P., Amit, B., Susmita, B., Lisa, O., Charitidis, C., *Additive manufacturing: scientific and technological challenges, market uptake and opportunities,* Materials today 2017, Vol. 1, pp. 1-16.

130. Taillat, S., *Un mode de guerre hybride dissymétrique ? Le cyberespace*, Stratégique, No 111, Paris 2016, pp. 89, 95.

131. Taken from the Department of Défense's Chief Information Officer website. Available at: <https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/> [Accessed 22 October 2020].

132. Tankel, S., *Laskar-e-Taiba: From 9/11 to Mumbai,* ICSR, London 2009 p. 5.

133. Techjury.Net, 2019. *Infographic: How AI Is Being Deployed Across Industries*. [online] Robotics Business Review. Available at: <https://www.roboticsbusinessreview.com/ai/infographic-how-ai-is-being-deployed-across-industries/> [Accessed 28 October 2020].

134. Temple-Raston, D., 2014. *How Much Does A Terrorist Attack Cost? A Lot Less Than You'd Think*. [online] NPR. Available at: <https://www.npr.org/sections/parallels/2014/06/25/325240653/how-much-does-a-terrorist-attack-cost-a-lot-less-than-you-think?t=1605889247748> [Accessed 5 November 2020].

135. Tenenbaum, E. *La manœuvre hybride dans l'art opératif, Stratégique*, No 111, Paris 2016, p. 56.

136. The Declaration is available at: <https://www.state.gov/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-artificial-intelligence-research-and-development-a-shared-vision-for-driving/> [Accessed 20 October 2020].

137. The National News, *Convicted ISIS supporter carried out deadly terrorist attack in Vienna.* [online] Available at: <https://www.thenationalnews.com/world/europe/convicted-isis-supporter-carried-out-deadly-terrorist-attack-in-vienna-1.1104434> [Accessed 16.11.2020].

138. *The Next Revolution in Roadway Safety,* [online] Available at: <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016> [Accessed 25.11.2020].

139. The U.S. Department of Transportation, 2016. Federal Automated Vehicles Policy – Accelerating the Next Revolution in Roadway Safety, [online] Available at: <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016> [Accessed 25.11.2020].

140. The Verge, 2017. Putin Says The Nation That Leads In AI 'Will Be The Ruler Of The World'. [online] Available at: <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world> [Accessed 5 October 2020].

141. The Wall Street Journal, 2015. *5 Things to Know About the Houthis of Yemen*. [online] Available at: <https://www.wsj.com/articles/BL-263B-3613> [Accessed 11.11.2020].

142. The White House Office of Science and Technology Policy, 2020. *American Artificial Intelligence Initiative: Year One Annual Reports*. p. iii.

143. Tim. S., 2020. *"Is al-Qaeda's leader dead? Report claims terror chief Ayman al-Zawahiri has died in Afghanistan from 'asthma-related breathing issues"*, [online] Available at: <https://www.dailymail.co.uk/news/article-8970231/Al-Qaedas-leader-Ayman-al-Zawahiri-died-reports-claim.html> [Accessed 20.11.2020].

144. U.S. Dept of Defense, 2020. *DOD Adopts Ethical Principles for Artificial Intelligence,* [online] Available at: <https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/> [Accessed 12.10.2020].

145. United Against Nuclear Iran, *Kata'ib Hezbollah*, [online] Available at: <https://www.unitedagainstnucleariran.com/report/kataib-hezbollah> [Accessed 2 November 2020].

146. United Nations Office on Drugs and Crime, *Education for justice university module series counter-terrorism – Module 1 introduction to international terrorism*, UN, Vienna 2018, p. 1.

147. United Nations, General Assembly, *Agenda Item 108 – Question of Palestine (Resumed from the 2268th meeting),* Wednesday, 13 November 1974, at 10.30 a.m. New York, A/PV.2282 and Corr.1.

148. University College London, 2020. *'Deepfakes' Ranked As Most Serious AI Crime Threat*. [online] Available at: <https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat> [Accessed 4 November 2020].

149. University of California, 2016. *Big Data, Analytics & Artificial Intelligence. The Future Of Health Care Is Here*. [online] San Francisco. Available at: <https://www.gehealthcare.com/static/pulse/uploads/2016/12/GE-Healthcare-White-Paper_FINAL.pdf> [Accessed 9 November 2020].

150. Uslu, E., *Turkey's Kurdish Problem: Steps Toward a Solution,* Studies in Conflict & Terrorism, 30:2, 2007, pp. 157-172.

151. Van der Veer, R., 2020. *Terrorism in the age of technology*, [online] Available at: <https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology> [Accessed 18 September 2020].

152. Ware, J., 2019. *Terrorist groups, artificial intelligence, and killer drones,* [online] Available at: <https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones> [Accessed 21.09.2020].

153. Webster, G., Creemers, R., Triolo, P. and Kania, E., 2017. All Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017). [online] Available at: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/> [Accessed 1 October 2020].

154. Wiegand, K. E., *Reformation of a Terrorist Group: Hezbollah as a Lebanese Political Party*, Studies in Conflict & Terrorism, 32 (2009), pp. 669-680.

155. Zabłocki, E., *Kategorie, zagrożenia: system bezpieczeństwa narodowego,* Warszawa 2013, pp. 51–52.

156. Zegart, A., 2019. *In The Deepfake Era, Counterterrorism Is Harder*. [online] The Atlantic. Available at: <https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/> [Accessed 17 November 2020].

157. Ze-Xian, L., Yen, T., Ray, M., Mattia, M., Metcalfe, I. Patterson, D., *Perspective on 3D printing of separation membranes and comparison to related unconventional fabrication techniques*, Journal of Membrane Science 2016, Vol 523, No.1, pp. 596-613.

ABOUT THE AUTHORS

Alan Lis

Director of Analysis and Project Coordination at the Institute of New Europe. Graduate of two British universities: University of York (BA in Politics with International Rela tions) and University of Warwick (MA in International Security). Erasmus student at the University of Bergen, Norway. His previous professional experience includes, amongst others, working for the the Department of Strategic Studies of the Chancellery o f the Prime Minister of Poland and Euractiv.pl. Participant of the 'School of Leadership 'course run by the Warsaw-based Instytut Wolności. His main research interests are international security, terrorism, and hybrid threats.

Aleksander Ksawery Olech

Director of the European Security Programme at the Institute of New Europe. Specialist in the field of security and international relations. PhD candidate in security sciences at the War Studies University in Warsaw. He gained research experience at the Université Jean Moulin III in Lyon, the Institute of International Relations in Prague, and the Institute of Peace Support and Conflict Management in Vienna. Scholarship holder of the OSCE & UNODA Peace and Security Program and of the Casimir Pulaski Foundation. His main research interests are terrorism, international cooperation for security in Eastern Europe and the role of NATO and the EU in the environment of hybrid threats.

Civil Society Organisations Development Programme for 2018–2030 CSODev

NIW

Sfinansowano przez Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Rozwoju Organizacji Obywatelskich na lata 2018-2030.

INSTITUTE OF NEW EUROPE

THE INSTITUTE OF NEW EUROPE FOUNDATION (INE)

Non-governmental organization conducting analytical and research activities in the field of economy, politics and the legal system in the national and international context. Our activity is aimed at a substantive support for the processes of making strategic decisions for the state by preparing proposals for solutions in the form of postulates as well as specific legislative solutions, and participating in the process of their implementation.

IF YOU APPRECIATE OUR WORK, JOIN OUR GROUP OF DONORS!

We will finance further publications from the received funds. Direct payment to the account of the Institute of New Europe:
95 2530 0008 2090 1053 7214 0001

Title: **"donation for statutory purposes"**

www.ine.org.pl/en kontakt@ine.org.pl