Nowa Polityka Wschodnia 2022, nr 1 (32) ISSN 2084-3291

DOI: 10.15804/npw20223203 s. 44–60

www.czasopisma.marszalek.com.pl/pl/10-15804/npw

Aleksander Olech

Baltic Defence College
ORCID ID: https://orcid.org/0000-0002-3793-5913

Unmanned Aerial Vehicle – a Lethal Weapon of Tomorrow for Terrorists

Unmanned Aerial Vehicle – a Lethal Weapon of Tomorrow for Terrorists

Abstract

Terrorism has been used as a form of combat for centuries. Over the years, the tools used by terrorists have evolved. While attacks with cold weapons still take place, nowadays terrorists also use explosives, machine guns, guided missiles and increasingly often drones. The present growth of the arms market has led to terrorist groups being heavily militarized, as they can successfully acquire modern weapons and subsequently use them in their attacks. This state of affairs has directly affected the security of states and societies, and subsequently became a principal subject of discussion on international security forums. Contemporary global terrorist threats also harness artificial intelligence that supports weaponized 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 would back them up. The chance for terrorist organisations to gain access to artificial intelligence technologies only increased due to the global competition surrounding it. 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. The threat of terrorist organisations possessing and using swarms of drones does not seem to be very distant.

Keywords: terrorism, drones, artificial intelligence, technology, security

Беспилотный летательный аппарат – смертоносное оружие завтрашнего дня террористов

Аннотация

Веками терроризм существовал как один из видов боевой атаки. С годами методы, используемые террористами изменились. И хотя вооруженные атаки с применением холодного оружия все еще имеют место, то в настоящее время террористы также используют взрывчатки, пулеметы, управляемые ракеты и все чаще беспилотные летательные аппараты (БЛП). Нынешний рост рынка оружия привел к серьезной милитаризации террористических групп, поскольку теперь они могут успешно приобретать современное оружие и впоследствии применять его в своих атаках. Такое положение дел напрямую повлияло на безопасность государств и обществ и впоследствии стало основным предметом обсуждения на международных форумах по безопасности. Современные глобальные террористические угрозы также используют искусственный интеллект, в виде боевых роботов, ракет, а также БЛП. Подобный нарратив появился несколько лет назад, указывая на то, что террористы могут обладать большими возможностями, поскольку могут сотрудничать с некоторыми государствами, которые их поддерживают. Таким образом, вероятность того, что террористические организации получат доступ к технологиям искусственного интеллекта увеличивается благодаря конкуренции в этой сфере на мировом уровне. Вследствие потенциального распространени, у террористов появится возможность использовать оружие, поддерживаемое ИИ. Все это может развиться в очень тревожный сценарий, с которым придется столкнуться. Угроза того, что террористические организации получат на вооружение и будут применять беспилотные летательные аппараты не кажется слишком призрачной.

Ключевые слова: терроризм, беспилотники, искусственный интеллект, технологии, безопасность

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 militarized, 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.

Contemporary global terrorist threats mainly harness artificial intelligence[1] that supports weaponized 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 the US, 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

[1] There is no commonly agreed-upon definition of AI. The AI field is going through constant and prompt changes and developments, which results in the fact that authors of any publication on AI may present their very own definition of the term, which would be as appropriate and adequate as those presented by others. For the past decade or so, there has been a significant revival of the interest of AI, and this technology is swiftly growing and attracting attention across many fields. Indeed, since 2010 the amount of academic publications on the topic of AI has risen 8-fold.

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.

The authors examine a range of articles, reports and analyses made available by various experts and research organisations. The research conducted was based on methods such as synthesis and deduction, and the authors made an attempt to develop forecasts and scenarios to identify potential threats to international security. Furthermore, a case study encompassing the actions taken so far by terrorists (and highlighting their potential capabilities, especially in the region of the Middle East) is of key importance to this article. The whole study is complemented by conclusions based on the interdisciplinary research of the phenomenon of using advanced technology in the form of unmanned aerial vehicles for terrorist activities.

The threat of terrorist organisations possessing and using swarm of drones 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.

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 (Ware, 2019). 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 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 (Gibbons-Neff, 2016).

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 possible to the troops' position (Guibert, 2016). 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 weaponizing 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 (Rogoway, 2017).

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 (Morton, 2018). 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 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 (Kumar, 2019). 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 (Rieas, 2020).

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 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 (BBC, 2017). 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.

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.

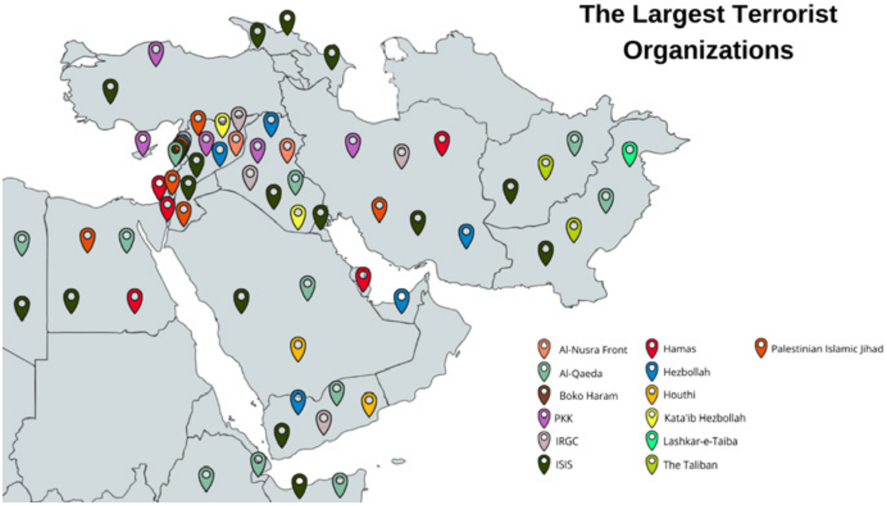
Additionally, where terrorists can carry out an attack with drones, it will demand a response from state authorities against said attack. At the same time, terrorists use that as a form of distraction to carry out a similar attack in a different location. When all state resources are focused on eliminating 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.

Due to the international threat of terrorism, there is a widespread belief that extremist organisations are likely to use unmanned aerial vehicles controlled by artificial intelligence and 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) (Hoenig, 2014). Such cooperation usually occurs when countries want to advance their agendas using terrorists, instead of engaging with their own resources, such as their military.



Map. 1. Potential places of operation of the largest terrorist organizations in the Middle East
Source: own study

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 (Parachini, Wilson, 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.

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.

Conclusion

Swarms of drones pose a massive threat for 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 fired 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 its 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 (McDermott, 2019). 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 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.

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. 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 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.

ALEKSANDER OLECH, PHD

Baltic Defence College
Riia 12, 51010 Tartu, Estonia
aleksander.olech@baltdefcol.org

Bibliography

BBC. (2017). *Anti-drone protest at RAF Waddington.* Retrieved from: https://www.bbc.com/news/uk-england-lincolnshire-41536818.

Gibbons-Neff, T. (2016). ISIS used an armed drone to kill two Kurdish fighters and wound French troops, report says. *The Washington Post*. Retrieved from: 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/.

Guibert, N. (2016). *Irak: Paris confirme qu'un drone piégé a blessé deux membres des forces spéciales françaises à Erbil.* Retrieved from: 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.

Hoenig, M. (2014). *Hezbollah and the Use of Drones as a Weapon of Terrorism.* Retrieved from: https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism.

Kumar, N. (2019). *Saudi Arabia Drone Attack: Sign of Changing Character of Hybrid War.* Retrieved from: https://www.vifindia.org/article/2019/october/01/saudi-arabia-drone-attack-sign-of-changing-character-of-hybrid-war.

McDermott, R. (2019). Moscow Unveils Further Advances in Drone Technology. *Eurasia Daily Monitor, 16*(139).

Morton, M. (2018). *Inside The Chilling World Of Artificially Intelligent Drones.* Retrieved from: https://www.theamericanconservative.com/articles/inside-the-chilling-proliferation-of-artificially-intelligent-drones.

Parachini, J.V., Wilson, P.A. (2020). *Drone-Era Warfare Shows the Operational Limits of Air Defense Systems.* Retrieved from: https://www.rand.org/blog/2020/07/drone-era-warfare-shows-the-operational-limits-of-air.html.

Rieas. (2020). *The Saudi oil industry under Houthi attacks.* Retrieved from: https://rieas.gr/researchareas/editorial/4556-the-saudi-oil-under-houthi-attacks-2.

Rogoway, T. (2017). *ISIS Drone Dropping Bomblet On Abrams Tank Is A Sign Of What's To Come.* Retrieved from: https://www.thedrive.com/the-war-zone/7155/isis-drone-dropping-bomblet-on-abrams-tank-is-a-sign-of-whats-to-come.

Ware, J. (2019). *Terrorist Groups, Artificial Intelligence, and Killer Drones*. War on the Rocks. Retrieved from: https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/.