IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

The Convergence of Technology and Terrorism in International Relations: Analyzing the Contemporary Technological Trends in Terrorism

LATIKA BANGARI, RESEARCH SCHOLAR
AMITY INSTITUTE OF INTERNATIONAL STUDIES
AMITY UNIVERSITY , NOIDA, INDIA

Abstract - This abstract examines the complex interactions between technology and terrorism in the context of international relation with an emphasis on identifying the evolving technological trends in terrorism and the extent to which they are relevant, regardless of whether they are a myth or a developing reality. Through the investigation of the complementary relationship between technology progress and terrorist groups' strategies, this research attempts to offer a thorough understanding of the complex aspects of this convergence and how they overlap and influence each other. The study looks at how terrorism and technology have interacted historically and currently in order to shed light on how this merging has influenced and contributed to the developing security consequences. In addition to examining the interplay between technology and terrorism as well as the current technological trends, the study also looks at the realistic or fictitious prospect of non-state actors such as terrorists utilizing these new technologies. Through an analysis of diverse technical trends exploited by terrorists, the research aims to provide a comprehensive understanding of the complicated interactions between terrorism and technology in various geopolitical contexts within the larger security dynamics.

INTRODUCTION

Today, with the world ever so firmly connected has made it feasible for both technology and terrorism to come together to form a very complex and dynamic nexus in the world events that has resulted in a significant effect on both political stability and international security. The way society functions is being shaped by technology breakthroughs, and terrorist groups as others are not too far behind in skilfully using these tools to achieve their goals. In order to fully understand the complex relationship between technology and terrorism, this research paper will analyse the evolving technological trends in terrorism and the extent to which they are relevant.

In recent years, the rise of digital communication platforms, encrypted messaging apps, and social media has facilitated the rapid dissemination of extremist ideologies and recruitment efforts on a global scale. Terrorist organizations leverage the borderless nature of the internet to radicalize individuals and coordinate activities, transcending traditional geopolitical boundaries. This phenomenon necessitates a nuanced understanding of the evolving dynamics in international relations, as the virtual realm becomes an integral battleground for ideological struggles and geopolitical influence.

In his 2018 Strategy on New Technologies, UN Secretary-General António Guterres noted that, “While these technologies hold great promise, they are not risk-free, and some inspire anxiety and even fear. They can be used to malicious ends or have unintended negative consequences”. Although there is no denying that technology has the ability to serve society, study on its malevolent usage is still in its infancy.

Throughout the centuries, we have noticed that terrorists are often early users of new technologies, which are often deadlier due to their lack of regulation and governance in nature. A regional and worldwide strategy is essential to preventing terrorists from taking advantage of regulatory gaps that could reveal weaknesses in emerging technologies, given the cross-border consequences of many technical systems and their international links. Building robust regulating frameworks that can react swiftly and efficiently to terrorists' destructive use of technology is imperative if we are to lessen its effects.

We've all seen or heard about the negative and harmful aspects or the dark side of technology, which are still mostly unexplored and have not gotten much attention. The truth is that when technology is utilized maliciously, it can be very hazardous. It is a potent tool with a track record in the field of cybercrime that could theoretically be used to support or enable terrorism and violent extremism that is conducive to terrorism. For example, it could be used to enhance cyberattacks on vital infrastructure, provide new avenues for physical attacks using drones or self-driving cars, or speed up and increase the dissemination of hate speech and incitement to violence. The question that arises here is, are the new technologies that are employed for terrorism is a reality or illusion? Through the lens of this research paper we shall also look forward to answering this question.

Nevertheless, we must always remember that terrorism is a dynamic threat that should never be taken lightly. We have witnessed numerous instances of terrorists using new and developing technologies, like drones, virtual currencies, and social media, more than 20 years into the twenty-first century. Technology is become easier to obtain, so it's important to remain on top of it and be ready for any situation where it can be misused.

Artificial intelligence (AI) and other new technologies have the potential to be very potent instruments that enable significant advancements in a wide range of study sectors. Although when ending up in the wrong hands, they can also be used very maliciously. Therefore, this research paper aims to provide insight into the possibility of terrorists employing new technologies by utilizing modern technology tools for terrorist activities.

1.1. Evolution of Terrorism: From Yesterday to Today

Technology has contributed significantly to the significant evolution of terrorism, despite the fact it was not the only factor. There is no lack of scenarios from recent history showing how terrorist and violent extremist groups are using a wide range of technologies in ever more sophisticated ways. This should not be shocking in many ways. Terrorists are ultimately "children of their time," just like everyone else in the world. Like any other ordinary person, they depend on and utilise the tools and equipment that are accessible to them as a whole. Indeed, all forms of technology—digital and analog—develop to the point that malevolent people might use them to commit crimes.

Although we frequently talk about terrorism as a contemporary issue, its roots can be traced back to historical periods. Historians have documented some of the first instances of terror, such as when the Tatars, besieging Kaffa in southwest Ukraine in the fourteenth century, threw plague-ridden bodies over the city walls to infect the defenders. The enemy's forces were weakened by the economical and successful approach of causing chaos.

Several terms from antiquity's terrorism are still in use today, including "thug," "assassin," and "zealot." In the first century of the Roman Empire, zealots in the Roman provinces of the Holy Land exhibited tremendous religious and nationalistic enthusiasm. They occasionally set Jewish neighbours' homes on fire because they believed them to be fanatics or collaborators, and they also subjected Roman soldiers and officials to the sica, or dagger. These terrorists' brutality conveyed out a message of unwavering hostility to the Roman domination of their ancestral lands and posed a danger to anyone who dared to stray from the strict, traditionalist branches of Jewish thought. On the other hand, during the crusades of the eleventh and twelfth centuries, Assassins were followers of a Muslim sect called the Shi'ite Order of Assassins, who had vowed to drive out Christian invaders from Palestine. They hunted Christians who were unbelievers and killed Sunni Muslims whose customs and beliefs they deemed repulsive while travelling in small groups through what is now Syria, Iraq, and Israel. This motivated mission force is remarkably comparable to the Tamil Tigers of Sri Lanka and the Hezbollah bombers that are right now operating within Lebanon. For both ancient and contemporary assassins, success and suicide guarantee a spot in paradise and martyrdom. Such as seen in the case of contemporary suicide bombers who go forth with such a mentality.

During the French Revolution in the late 1790s, terrorism brought exceptional attention to political objectives. The Revolution's leaders were determined to put an end to dissent. They used fear itself in addition to the guillotine to eliminate opponents between 1793 and 1794. A reign of terror, known as the régime de la ter-reur, was purposefully imposed in order strengthen a weakened government and terrorise anyone who may challenge its hard-earned, recently acquired authority. The then-leader of the French Revolution, Robespierre, was a rather ruthless and passionate terrorist in his own way.

In the first ten years of the twentieth century, terrorism was characterised by political competition. The 1920s and 1930s saw a change in the face of terrorism. There was a tremendous deal of unrest and discontent throughout Europe as the hopes that had been aroused by the end of the First World War turned sour. A new significance was placed on terrorism when it became institutionalised in areas where groupings vying for power were willing to go to any lengths to alter political systems. The standard of conduct in Germany, Italy, Japan, Poland, Romania, Greece, and Hungary was the use of strongarm tactics that violated fundamental human rights. Enforcement of a single set of distinctive ideological beliefs was mandated. The streets were overflowing with hit squad armbands and jackboots, all intended to maintain order and discipline. With the use of radio and round-the-clock printing presses, the terror of those decades grew more and more into "techno-terrorism." Where in Debate or compromise had no place.

The world war that followed, having lasted from 1939 to 1945, had no limitations to human observation. Complete terror fostered total war. A lot of things happened, including the Nazi control of most of Europe, the Resistance's calculated, hidden hit-and-run strategy, and the savagery of massacre, all required terror. The peoples of Europe and Asia were overtaken by terrorism in all of its forms, which now forced civilians into some areas of conflict. The battling air forces were randomly bombed and fire-stormed, leading up to the nuclear destruction of Hiroshima and Nagasaki, which has been called the ultimate terrorist atrocity. Fighting a merciless enemy who disregarded the Geneva Conventions frequently resulted in the use of barbaric tactics for both attack and defence that were rationalised as necessary. 1945 saw the end of the war, and terrorism as violent political activism—became a new meaning. Despite the fact that the colonial authorities labelled them as "terrorists," the violence and horror that people had to endure during this time gave rise to growing voices and a desire for freedom.

Terrorists have employed primitive communication methods like telegraphy for coordination, as we have already explored. They have shown massive flexibility when they adopted radios and encrypted messaging throughout the shift to contemporary communication. While it is true that terrorist groups have historically utilised weapons, vehicles, and other items of "low-tech terrorism," the threat posed by terrorism is ever-present. The skills and technical knowledge required to use AI will decrease as it becomes more widely used, lowering entry barriers and acting as a threat perception for global security.

Terrorism has witnessed a completely new level of transformation in the twenty-first century, characterised by Sophisticated online recruitment efforts were made possible by early examples of using the media for propaganda, demonstrating the ongoing growth of communication techniques. Gradually, the use of computers for cyberterrorism emerged, with hackers emerging as powerful players in the virtual world. Transportation innovations, especially the use of aeroplanes, gave terrorists new ways to increase the effect of their attacks. A paradigm change in tactics was also observed at this time, with a shift away from centralised, well-publicized attacks and towards more decentralised and asymmetric strategies.

Terrorist organisations' flexibility in utilising technology reminds one of an endless game of cat and mouse with security forces. The potential for disastrous outcomes is highlighted by biological and chemical threats, underscoring the necessity of strong counterterrorism measures. As a result, the historical timeline offers a comprehensive knowledge of the complex relationship between technology and terrorism, establishing the foundation for understanding current security issues. This historical view provides a useful lens through which to evaluate the complex terrain of the convergence of technology and terrorism in international relations by looking at significant turning points and changes in strategies.

1.2. The Interplay Between Technology and Terrorism

Although terrorist strategies vary from group to group and individual to individual, it can be claimed that terrorist organisations, in particular, favour the tried-and-true effectiveness of weapons like guns and bombs and are somewhat reluctant to take risks when it comes to their weaponry. However, it is undeniable that terrorism is a dynamic threat. Over the years, terrorist organisations and individuals have demonstrated their ability to adapt and have changed significantly. They have shown the ability to innovate in a number of areas, such as their organisational structure, which has become global, franchised, and decentralised. Their methods have also changed dramatically; they went from scattered guerrilla warfare to indiscriminate strikes.

Regarding technology, this innovative tendency is particularly noticeable when it comes to social media and the Internet, which have shown to be quite beneficial to terrorists. The Internet and social media, along with their extensions to other ecosystems like online gaming platforms, have become crucial tools for terrorist organisations to recruit, raise and distribute funds, purchase and transfer weapons, radicalise, inspire, and incite violence, as well as to claim responsibility for attacks. For instance, the perpetrator of the 2019 Christchurch massacre in New Zealand streamed the event live on Facebook. The incident was widely publicised, increasing its impact and repercussions on the victims, even if the video was removed a few minutes later.

The extent of this growing epidemic is demonstrated by initiatives like the Referral Action Day organised by Europol. In a single day, as part of 2020 Referral Action Day, 1,906 URLs pointing to terrorist content across 180 platforms and websites were found and evaluated for removal by Europol and 17 participating countries. Over the last two years, Facebook has removed more than 26 million pieces of content from groups such as the Islamic State of Iraq and the Levant (ISIL) and Al-Qaida, and in the first three months of 2020, it removed approximately 4.7 million pieces of content related to "organised hate," an increase of more than 3 million pieces of content from the fourth quarter of 2019.

In general, there are numerous methods to see how technology and terrorism interact. **Firstly**, in order to carry out their assaults, terrorists rely on technology. In actuality, as technology has advanced, the character of terrorist strikes has evolved dramatically over time. From the use of knives and pistols to aircraft hijackings and other vehicle-based operations, terrorist groups' arsenals have grown dramatically over the ages. Some have even shown some degree of willingness to obtain and deploy chemical, biological, or radiological weaponry. Perhaps one of the biggest changes brought about by technological advancement is the automatic rifle. In many regions of the world, terrorist groups now prefer to use automatic rifles as their primary weapon due to its affordability and high lethality. **Secondly**, compared to their relatively local threat infliction prior to the 21st century, terrorist and criminal groups have become more powerful due to technological advancements in transportation and logistics. These advancements have allowed them to increase the speed, reach, and magnitude of their operations and have turned them into global operations. **Thirdly**, in the modern period, advancements in information and communication technologies have made it possible for terrorist organisations and individuals to interact more swiftly and secretively over greater distances, as well as to disseminate information and videos that go viral quickly, in order to promote terror more quickly and broadly. By doing this, they have been able to connect with possible recruits and improve the efficacy and efficiency of their attacks. The most notable examples of this in today's age are mobile phones, the Internet, and, more recently, social media.

Modern technology has been used by terrorists in a variety of sophisticated ways. For example, the 2008 Mumbai attacks culprits used mobile phones, the Internet, and global positioning system (GPS) devices to plan, coordinate, and execute their objective. This might not seem all that innovative in the modern era, but at the time it represented a creative application of the newest technology developments. More recently, terrorists have utilised crowdfunding, mobile banking, and blockchain-based virtual assets like "Bitcoin" to raise money or fundraise, while the dark web acts as a marketplace for goods including bogus documents, weapons, and supplies.

However, there is evidence to show that lone terrorist actors, in particular, tend to employ easily accessible and publicly available technologies for transportation, weaponry, and communication. Low-tech equipment that can be purchased from do-it-yourself stores seems to be the preferred option. Terrorists, particularly lone actors, look for methods to turn everyday items like kitchen knives, cars, and trucks into weapons in the context of "low-tech terrorism." Nevertheless, cutting edge technology—once exclusive to specialised communities—becomes more and more available to the broader population every day. One such example is that, although it might have been unimaginable a decade ago, a terrorist organisation manipulating an army of drones carrying explosive devices is an urgent concern today. Law enforcement, counterterrorism teams, and other security forces may find themselves "off-guard" by innovative terrorist organisations and individuals who have discovered new and unexpected ways to use affordable and commercial technologies for malevolent ends. This is due to the expansion of technological potential. Given this and taking into account current patterns, advancements, and technological potential, the question that follows is whether, or perhaps even when, artificial intelligence will be incorporated to the arsenal of terrorist tools.

1.3. Cyber Terrorism

The concept of cyberterrorism has its origins in the early 1990s, when the United States' highly networked and tech-dependent society began to face potential risks as a result of the discussion surrounding the "information society" and the rapid development in Internet use. The National Academy of Sciences in 1990 declared, “We are at risk. Increasingly, America depends on computers. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb.” Economic, political, and psychological factors have come together to fuel the fear of cyberterrorism. From a psychological standpoint, the phrase "cyberterrorism" combines two of the biggest phobias of the modern era: technology and terrorism. Individuals tend to consider an unknown threat as more dangerous than one that is well-known. Terrorist bombs can have an equally potent psychological effect on insecure society. Furthermore, the greatest obstacles to comprehending the true threat posed by cyberterrorism are ignorance or, worse, an abundance of false information, as well as a fear of the unknown.

The process of defining the term "cyberterrorism" in a way that is both consistent and clear has encountered various obstacles. Cyberterrorism, to put it simply, is the fusion of terrorism and cyberspace. It describes the use of the internet, information channels, and communication platforms for terrorist attacks and terrorist cause promotion. These cyberattacks are the purposeful application of cyber power, frequently by non-state actors, with the main goal of inciting terror, widespread fear, or disruption in a government, organisation, or community. Another way to describe it would be as an act of cyberattack or threat-making against computers, networks, and the information they store and share.

Cyberterrorism usually consists of assaults with political, ideological, or social motivations that target vital infrastructure, cause a great deal of damage, or seriously jeopardise national security. Strong cyberattacks have the potential to cause violence against people or property, or at the absolute least, do enough damage to make people frightened. Cyberterrorism frequently causes explosions, airline crashes, water pollution, serious political or economic losses, or even death or bodily injury. Cyberterrorism against critical infrastructure may be carried out if it has a significant impact. It is not necessary to report attacks that disrupt services that are essential or that are just bothersome.

1.3.1. The Appeal of Cyberterrorism for Terrorists

For an array of reasons, cyberterrorism is an appealing prospect for modern terrorists. First of all, it is less expensive than conventional terrorist tactics. The terrorist only needs an internet connection and a personal computer. Terrorists can produce and distribute computer viruses using a phone line, cable, or wireless link in place of purchasing weapons like guns and bombs. Second, compared to conventional terrorist tactics, cyberterrorism is more anonymous. Terrorists, like many Internet users, go by online labels, or "screen names," or visit websites as anonymous "guest users," which makes it extremely difficult for law enforcement and security organisations to figure out who the terrorists really are. Furthermore, there are no actual obstacles to overcome within online, such as borders to cross, checkpoints to avoid, or customs officers to deceive. Thirdly, there are a huge quantity and variety of targets. Cybercriminals may target public utilities, private airlines, governments, individuals, and so on using their computers and computer networks. There is an absolute certainty that terrorists will find cracks and vulnerabilities to exploit due to the enormous amount and complexity of potential targets. Numerous studies have demonstrated that critical infrastructures, like electrical power grids and emergency services, are susceptible to cyberterrorist attacks due to the complexity of the computer systems that power these infrastructures and the inability to completely eradicate all vulnerabilities. Fourth, the ability to carry out cyberterrorism from a distance appeals greatly to terrorists. Cyberterrorism is less demanding than traditional forms of terrorism in terms of physical training, psychological commitment, risk of death, and travel, which facilitates recruitment and retention of followers for terrorist groups. Finally, compared to conventional terrorist tactics, cyberterrorism may directly impact a higher number of individuals, leading to increased media attention—exactly what terrorists hope to achieve.

1.3.2. Impact on International Relations

Understanding how technology is becoming increasingly vital to security dynamics is necessary for investigating cyber-terrorism and its impact on international relations or world politics. Attacks on computer systems and networks with the intention of causing disruption or harm are included in the category of cyberterrorism. International relations may be significantly impacted by this as countries struggle to protect their digital infrastructure and counteract cyberattacks. Cyberterrorism's potential threat has caused a great deal of concern. The threat posed by cyberterrorists breaking into government and private computer networks and destroying the financial, military, and service sectors of developed nations has been made widely known by a number of security experts, lawmakers, and others. Influencing the entire world as a result.

Beyond the conventional physical sphere, cyberterrorism impacts diplomatic, economic, and political dynamics in international relations. To combat potential risks, nations are forming alliances and investing in cybersecurity capabilities. Tensions may escalate and diplomatic relations can be strained by incidents like ransomware attacks, cyber-espionage, and information warfare. Cyberterrorism also has a big impact on world politics. For example, it uses social media and the internet to propagate propaganda and sway public opinion, which can affect foreign policy and political events.

The ability of political leaders and organisations to communicate with the public and with one other can be disrupted mainly by cyberattacks on communication networks, such as email or phone systems. Privacy-compromising cyberattacks have the potential to erode public confidence in political figures and organisations. In order to handle the intricate and multidimensional nature of cyber-terrorism, international diplomatic strategies must constantly adapt as technology evolves and the nature of cyber threats transforms. broadly, cyberterrorism has the potential to significantly impact world politics and exacerbate social and political unrest on a worldwide scale.

1.4. Current Technological Trends in Terrorism

Technology is utilised to foster social advancement both as a tool and as a means of growth. Yet as emerging technologies are more affordable and simpler to obtain, terrorists and non-state actors are exploiting them more frequently. The world of terrorism is not an exception when it comes to the misuse of technology and trustworthy online resources. Terrorists are getting better at masking their footprints and actions through the use of tools and services that provide anonymization and encryption. Trends in technology use brought about by the digital revolution have an effect on how terrorists and organised crime operate. The coordination of destructive activity is further facilitated by enhanced, anonymous communications capabilities through the Internet and mobile devices.

In the twenty-first century, people and devices are connecting to the Internet at a speed that makes it feasible for vulnerabilities associated with technology to foster and grow, possibly enormously so. In this way, when new technologies proliferate, there will be a corresponding rise in security flaws which will enable malicious actors to target people, companies, and entire countries.

1.4.1 Social Media and Online Radicalization

The use of social media by terrorists currently constitutes the kind of activity that law enforcement reports on the most. Social media is an important instrument employed by terrorist organisations for recruiting Individuals, propaganda, inciting acts of terror, and taking credit for attacks. Social media platforms were originally created to be used for communication and information sharing, however now it is unintentionally evolved into a channel for terrorist organisations' recruiting and radicalization campaigns.

Some terrorist groups have made extensive use of social media to propagate their goals and accomplishments. Terrorist organisations now frequently rely on platforms that either take a long time to erase content or exhibit flexibility by switching platforms as needed when their content is routinely removed. Since information spreads quickly and easily online, it appears that radicalization is a process that is challenging to regulate, even when certain platforms—like Facebook and YouTube—remove the content quickly. The speed at which their acts get
spread online is evidence of their effective strategy.

These evildoers are taking advantage of every internet communication possibility. From popular platforms like Facebook and Telegram to online gaming hubs, chat rooms, betting sites, and pornographic websites. These online spaces serve as rich breeding grounds for both unintentional and intentional recruiters as well as for the spread of violent propaganda. The significance of "digital terror squads" was emphasised when ISIS awarded its "media mujahids" the same status as its ground combatants in 2016. This gave the radicals on the internet prominence that was previously only given to the warriors wreaking havoc on the ground. This is only one example of how crucial, intricate, and significant cyber operations are to terrorist groups in the modern day.

Law enforcement organisations have observed an increasing trend in the process of self-radicalization, which could be attributed to the ease and speed with which online propaganda can be accessed. This appears to streamline the process of radicalising "lone actors," who can be persuaded by radical ideologies while seated in front of a computer screen and encouraged to carry out acts of terror within their own nations, bypassing the need to visit combat zones to promote the terrorist cause. Certain occurrences imply that terrorist organisations specifically target or attract people who are violent, mentally unstable, or have a criminal record. It’s not necessary that these people always share the same religious beliefs that certain terrorist organisations propagate. For example, the 2015 San Bernardino shooting, which was carried out by married Californian couple Syed Rizwan Farook and Tashfeen Malik, demonstrated how the murderers' exposure to extremist content on social media radicalised them. Therefore, the degree of anonymity provided by social media platforms, as demonstrated in the scenario above, greatly aids in recruitment attempts. In addition, recruiters can operate covertly on several platforms, even managing to avoid law enforcement's prying eyes through the use of closed groups and private chat. The work of law enforcement organisations is made more difficult by the fact that many recent incidents appears as a result of individual responses to terrorist propaganda efforts rather than the direct involvement of terrorist groups' "leadership."

Likewise it could be argued that the internet serves certain purposes that allow someone to more effectively incorporate themselves into the radicalization process. First of all, it gives the user easy access to a lot of extremist and terrorist content. This may strengthen the user's arguments and support his ideological inclinations. Furthermore, the user has the ability to filter out material that contradicts his preconceived notions and only take in data that confirms them, essentially using the internet as a "echo chamber." Lastly, the user can discover that making connections with people of similar beliefs online is smoother than doing it in the outdoors. For example, if an individual finds challenging to discuss his extreme beliefs with others in his real surroundings, he might be able to locate others willing to talk to him online.

In general terms, the internet and social media can be seen as places where someone who is already on the route to radicalization can legitimise his opinions and receive support and affirmation from others. Through cooperation Between social media companies and law enforcement we can combat online radicalization. Nowadays, a lot of social media sites use machine learning and artificial intelligence algorithms to detect and filter extremist content. For example, YouTube revealed that in just one quarter of 2020, it eliminated over 9 million videos containing extremist content, illustrating the scope of challenge.

1.4.2. Encryption and Decryption

To put it simply, encryption is the process of transforming data—messages or other bits of information—so that illegal access is prevented. whereas, Reversing encrypted data back to its original state is called decryption. Encryption is now absolutely necessary for government organisations, corporations, and the general public to protect the confidentiality, integrity, and accessibility of their communications and stored information in a culture where basic daily functions have grown more and more digital. Since encryption allows users to interact and share information securely while maintaining their anonymity, individuals with more sinister motives, such as terrorists and criminals, also use it as a powerful and useful tool to prevent unauthorised access. For these kinds of people or groups, decryption is equally appealing since it can let them obtain access to information or data that would otherwise be private. Terrorist groups now find it easier than ever to handle outreach and organisation, identify recruits, and maintain end-to-end encryption and virtual private networks (VPNs).

In a prominent case from 2012, the court was shown numerous encrypted emails transmitted between terrorist organisation members, and the French national involved was given a five-year prison sentence. It was alleged that the terrorist group was enabling secretive online conversations among its members by using the encryption programme "Mujahedeen Secrets." Additionally, it was seen that certain terrorist groups profited from the use of stenography and encryption to conceal the distribution and sharing of information with programmes like WinZip and Camouflage. Encryption tools driven by AI are presently undergoing extensive exploration. AI developments could lead to even more powerful encryption and decoding methods. Members of terrorist organisations would be able to communicate more easily and without risking the integrity of the data if they relied on AI-powered sophisticated encryption techniques. Terrorist groups would therefore have easier access to critical encrypted intelligence that is shared by counterterrorism organisations thanks to AI-powered decryption tools.

Terrorists are increasingly using encryption techniques, such as encrypted communication software, in accordance to reports from law enforcement authorities. Numerous studies and counterterrorism initiatives have revealed that members of Al-Qaida and ISIL equally utilise encryption. Terrorist organisations are using masking software and encryption to conceal their identities while they plan attacks, communicate, buy illicit goods, and conduct financial activities. Additionally, there is indication that terrorist organisations collaborate to share knowledge about how to stay undetected online and evade detection by law enforcement. The OPSEC handbook, which was created by a terrorist organisation and shares best practices and guidelines for online security, is a fantastic illustration of this approach. Furthermore, certain terrorist organisations have even created specially designed terrorist instruments, such encryption software. However, there is no guarantee that these will be used methodically or appropriately in the absence of adequate training or direction.

Terrorist organisations misuse a number of legal services, including mitigation tools such as distributed denial-of-service attacks (DDoS), which are used to mask the true IP address of websites hosting propaganda. Additionally, terrorist organisations employ Middle Eastern bulletproof hosting providers to stay anonymous and evade detection while exchanging and hosting data. The misuse of social media and the Internet is another area where terrorist organisations' capacity at adapting, particularly to new situations, is clearly witnessed. Notably, in May 2020, militant groups in Syria and members of Hay'at Tahrir al-Sham (previously known as Al-Nusra Front for the People of the Levant) were urged to switch from using Telegram, Facebook Messenger, and Viber to other encrypted applications like Conversations, Riot, Signal, and Wire. In fact, policy leaders and counterterrorism experts are quite concerned about the possibility that terrorists could "go dark" and communicate securely, eluding detection, as a result of these platforms' deployment of end-to-end encryption (E2EE).

Moreover, terrorist organisations are increasingly using messaging apps that frequently provide end-to-end encryption not just for informational purposes but also as a means of advertising other illicit transactions. Terrorists are becoming more and more invested in their online security, rendering investigations more difficult. As a result, they are using more and more multi-layered encryption, VPNs, Tor, and similar services.

1.4.3 Drones and Unmanned Aerial Vehicles (UAVs)

With the start of the twenty-first century, interest in unmanned aircraft is growing in practically every developed nation. Unmanned aerial vehicles (UAVs) have shown to be an effective application for a wide spectrum of operations carried out by both state and non-state actors as a result of the revolutionary development of a set of technologies. Terrorist organisations have recently started using artificial intelligence (AI) and drones. Both have the ability to be used to efficiently address a variety of security issues, but they also have the capacity to bring about a dystopian future that is only found in sci-fi movies and literature.

The UN Security Council Counter-Terrorism Committee has named drones and unmanned aerial vehicles (UAVs) as one of the main terrorist threats. Unmanned Aerial aircraft (UAVs), also called as drones, are aerial aircraft that are remotely piloted, pre-programmed, or controlled. Used for the first time in World War I and refined further throughout the Cold War, their use was significantly boosted by the 9/11 terror attacks and the ensuing "Global War on Terror." Drones are utilised by the military for direct or indirect strikes, targeting assistance, surveillance, and reconnaissance. Strikes in Afghanistan and Yemen in 2001–2002 signalled the beginning of military operations that became more and more drone-focused. Currently, the "weapon of choice" for locating and eliminating terrorists and insurgents is a drone. It has been said that the ongoing conflict between Russia and Ukraine is the "first full-scale drone war". Nowadays, both state actors and non-state actors are equally capable of obtaining drones and of assembling and using commercially available drone technology (COTS). 65 non-state actors are reportedly able to use drones at this time, while there are 113 states with military drone programmes. By 2024, the civilian small and micro drone market—which weighs between 200g and 50 kg—could grow to around USD 43 billion.

Terrorists are drawn to UAVs for a variety of reasons, one of which is that this technology is inexpensive and requires little training. They are also appealing because they provide the ability to launch a wide-scale attack with the goal of killing as many people as possible, especially in urban areas through the use of chemical or biological weapons. They can also target objectives that are challenging to access by land. These extremist groups also favour drones and unmanned aerial vehicles (UAVs) because they may be used to prepare attacks in a covert manner, providing flexibility in selecting a launch location, and potentially achieve acceptable precision and a long range using relatively cheap and readily available technology. As a result, terrorists have begun using drones to target civilian centres, diplomatic missions, energy infrastructure, international trade, and state military assets. The growth in drone attacks has also been aided by state funding of terrorist organisations. The uncontrolled civilian market, the Dark Web's technology, the availability of unguarded explosives for use as payloads, and the internet and social media's access to technical knowledge all contribute to terrorists' use of UAVs.

The problem of saturation drone strikes is becoming more and more pressing. Weaponized drones can be deployed in coordination with other unarmed unmanned aerial vehicles (UAVs) to target and take down air defence systems, so creating an opening for an assault of missiles, rockets, and other armed drones. Drone users can start basic "swarms" by combining internet lessons and downloaded software. Five to ten drones can be "hooked-up" to a single device.

At present, Armed non-state actors are using drones to carry out deadly attacks, targeted killings, and reconnaissance both inside and outside of war zones. The impact on civilian populations is catastrophic from a humanitarian standpoint. Although non-state actors are yet unable to get more advanced military drones (such as the MQ-9 Reaper and RQ Global Hawk), terrorists may be able to use civilian drone technology to their advantage by turning it into a restricted air-based military tool. A further serious concern to national security that governments will have to deal with is hostile use of small unmanned aerial vehicles (UAVs). Swarm production technology is a multifaceted, uncontrollable new menace. The US Department of Defence’s current framework contains certain tactics for dealing with drones, but it lacks a plan for dealing with armed drone swarms in the future.

Additionally, drones are being utilised for **targeted assassinations** primarily by state actors, but terrorists and criminals are also using them increasingly. An unsuccessful attempt was made to assassinate President Nicolás Maduro of Venezuela in August 2018. Additionally, Iraqi Prime Minister Mustafa Al-Kadhimi narrowly avoided being assassinated in 2021. A Taliban drone team took credit for contributing to the victory in 2021 after carefully killing Piram Qul, an ethnic Uzbek warlord.

Drones have been employed in battle by a number of non-state entities, including ISIL, Boko Haram, Hamas, Hezbollah, and the Houthi rebels. Smaller drones help in target acquisition to improve accuracy and lethality from ground-based weaponry. They are utilised for intelligence, surveillance, and electronic warfare operations. Decoys from drones are employed to divert attention while strikes are made elsewhere. By instilling terror, drones can contribute to the psychological aspect of terrorism. ISIL uses UAVs to drop little bombs, similar to those found in grenades, in areas of battle. Drone attacks were even carried out by ISIL in northern Iraq to eliminate enemy combatants. They established a unit called "Unmanned Aircraft of the Mujahedeen." In 2017, ISIL carried out 70 drone strikes in Syria to disable Iraqi security forces for a full day. Also the Houthi rebels gained international attention in 2019 when their drones, also known as "Qasef" drones, were responsible for approximately 6% of the world's oil supply being cut off through deliberate strikes on Saudi oil facilities. According to reports from the Monitoring Team (MT), in 2021, there was evidence of an increasing UAV capability in some regions of West and East Africa belonging to affiliates of ISIL and al Qaida. Drones are also employed by Al-Shabaab in East Africa for surveillance and reconnaissance purposes. It could be feasible for them to attack civil aviation.

1.4.4. 3D Printing and Weaponization

A variety of technology known as 3D printing are capable of creating three-dimensional objects by depositing, joining, or soldering a material (generally but not entirely thermoplastic) layer by layer. This cutting-edge technology is being used for civilian applications in a variety of fields, such as the manufacture of rockets, medical equipment, and supplies for humanitarian relief. However, analysts have warned against the dual-use nature of 3D printing and its potential use by terrorists ever since the online open-source hardware organisation Defence Distributed published the digital designs for the Liberator, the world's first pistol made almost entirely of 3D printed materials, in 2013. The fact that the files were downloaded over 100,000 times in the 48 hours following their publication indicates the extent of usage. Since then, the price of 3D printers has dropped as the technology has become more accessible to amateurs due to advancements in production quality, user-friendliness, and the availability of tutorials and technical knowledge. In today's marketplace, you can get several excellent 3D printers for less than $1,000 US on the market, with entry-level models starting at $200 US.

What were previously thought to be purely hypothetical threats turned real in 2019 when a far-right terrorist carried out a lethal attack in Halle, Germany, using a rifle that had been partially 3D printed. Since then, Sweden, Finland, Spain, Ireland, and the United Kingdom have all reported multiple incidents of terrorists using 3D printing to manufacture weapons. However, data indicates that the primary focus of terrorists appears to be the 3D printing of weapons. The internet plays a crucial role in the sharing and distribution of 3D printed weapon designs, which feeds extremist and violent communities. Online knowledge exchanges have the power to radicalise and boost organisations that might have otherwise restricted their activities to video games. Similar to the 3D printing of firearms, 3D bioprinting procedures are also widely known in internet groups that promote do-it-yourself projects. DIY communities not only share theoretical information, but they also offer advice on how to use 3D printing in real-world situations.

3D-printed weapon blueprints have been extensively shared on peer-to-peer filesharing services, the dark web, and encrypted internet forums. Although these platforms aren't always intended for terrorist or extremist purposes, the actors in question frequently utilise them to spread recruiting, training, and propaganda materials. Some, like the ones who share such schemes on hidden websites related to the Islamic State or communities disseminating hate speech targeted at certain racial or religious communities, are obviously part of extremist or terrorist organisations. Social media platforms need to take into account the ways that online technologies and physical violence interact. Although anybody may access the technology, producing or assembling these expertly manufactured weapons effectively requires a certain amount of skill. Now even that knowledge is acquired online.

One of Myanmar's principal rebel groups, the People's Defence Forces (PDF), has reportedly been seeing using 3D-printed weapons. This was one of the earliest documented instances of rebel factions using 3D-printed weaponry in combat. Additionally, there is evidence that the FGC-9 weapon type is being manufactured and distributed widely in the nation; eleven 3D-printed guns were discovered being moved through a combat zone following a recent arrest by security authorities in Myanmar. Despite the unfavourable circumstances under which they were probably manufactured, an inspection of the weapons based on the images supplied by the government suggests that they are well-made.

With the state of technology today, 3D printing is still a difficult skill that takes months of trial and error and a foundational grasp of mechanical engineering to perfect. However, video-streaming platforms are becoming a hub for online resources like lessons, films, and recommendations on 3D printing guns. While acquiring the necessary knowledge and abilities to 3D print dependable weapons entails overcoming considerable challenges, it is not entirely unattainable. Since commercial or hobbyist 3D printers also use the same materials as to make firearms, the growing popularity of home-based 3D printing additionally suggests that terrorists and extremists can hide their operations from law authorities.

Gun culture and a robust do-it-yourself program converge at the link of 3D-printed guns. Prioritising tracking and monitoring of the 3D-printed weaponry sector should continue until platforms are able to create regulations that specifically address the concerns. It is acceptable to use DIY content for 3D printing weapons of all kinds, but it is important to limit the content's reach when it starts to represent extreme and terrorist viewpoints. Platforms should additionally decrease the likelihood that consumers would come across this kind of content by accident rather than deliberately seeking it out. Since 3D printing technology is dynamic, it will continue to develop and open up new and terrifying possibilities. Therefore, in order to reduce the risks associated with these technological advancements, both present and future ones must be carefully considered and regulated by policies.

1.5. Terrorists Employing New Technologies: Illusion Or Reality?

After examining the current trends regarding the use of technology by terrorists and the various threats that arise from this malicious use, a crucial question that remains to be answered is whether these threats are based on real threats, or is the use of technology for terrorist purposes merely science fiction?

These days, technology is a necessary component of everyone's everyday life and is utilised by many people, frequently without their knowledge. Unquestionably, the world is witnessing a rapid expansion of new technological capabilities. Most of the materials needed to build and implement such technologies are available for purchase, and some are even open-source. For instance, the open-source site GitHub may make it easier for terrorists and other bad actors to exploit AI by lowering the bar for use and access. However, if the capacity to utilise technology is inadequate, then its accessibility alone is insufficient.

It is challenging to determine the motivations of any terrorist organisations or individuals due to the nature of terrorism. However, it is essential to examine how well-suited new and developing technologies are for terrorism in order to assess terrorists' intent to employ them. It is evident that non-state actors are constantly looking for cutting-edge weaponry that is affordable, easy to use, portable, discreet, and efficient—qualities that developing technology may not always have. In actuality, technology is not impeccable in itself. It can and frequently does fail, in contrast to how it is frequently portrayed in the media and in popular culture.

It requires a lot of time, money, and effort to develop and deploy new technology weapons in a reliable and efficient manner. Since, rifles and explosives are dependable and efficient they been the main weapons used by terrorist organisations for over a century. The primary factors that need consideration in these discussions are the incentives and motivations behind a terrorist or terrorist organization's decision to employ sophisticated technological methods. It is not always necessary for them to do so—for example, they already have willing human suicide bombers, therefore they do not need AI suicide bombers—and it is not always cost-effective—small weaponized drones are far more expensive than guns, vans, or knives.

In spite of the aforementioned considerations, technology does appear to be appealing to terrorists in many ways, which gives rise to the likelihood that they may be interested in it and something we cannot ignore. As previously said, there have been displays of interest in new technologies from terrorist organisations. For example, organisations such as ISIL are increasingly incorporating drones into their operations. It is also wise to at least take into account the possibility that terrorist organisations may have some degree of intention to investigate or seek to understand how emerging technologies can be used for malicious purposes, given the lengthy history of how these groups have innovated and embraced new technology.

A couple of years ago, in March 2020, an ISIL fan posted a video demonstrating the potential applications of facial recognition software on Rocket.chat, a decentralised social media site that ISIL has utilised to disseminate terrorist content and promote online cooperation and coordination. According to the aforementioned video, people may be recognised by their facial features alone, even if they had attempted to hide their identities by wearing a facial covering or digitally blurring their face. The video went on to say that this feature will undoubtedly help law enforcement stop terrorist schemes and catch those behind them. Even though the video may have overstated the current capabilities of this technology, the fact that it was acknowledged and that it was quickly shared on multiple other channels proves that terrorist organisations are aware of the potential of emerging technologies and are, at the very least, loosely following their trends and developments.

In the end, even if it might seem that organisations like ISIL are incapable of designing, creating, and utilising cutting-edge technology like artificial intelligence (AI), it is not impossible for these organisations or individuals to become capable of using these technologies in near future. It is necessary to recognise that historically, significant advancements in capacity have happened rather quickly. It is noteworthy that, despite indicating an early interest in incorporating drone technology into their arsenal, it took ISIL less than a year to employ drones
in combat. Even though low entry barriers are now the most alarming technology, with time, hostile actors are expected to develop the capabilities necessary for more sophisticated attacks.

Technology has a significant influence on how terrorists operate, as this research paper focuses on and has been observed on multiple occasions. It can no longer be considered a remote possibility that terrorist organisations and individuals will not use new technologies like AI in the not too distant future, whether it be through one or more of the nefarious tools as detailed in this research paper or in some other as yet unimaginable way, given the rapid integration of technology into daily life. In this context, it is important to acknowledge the advancement and development of new technologies in addition to the growing curiosity of terrorist organisations and individuals in these fields.

REFERENCES

[1] Taneja, K., & Saran, S. (2019). Technology and Terror: A new era of threat in a borderless online world. Delhi: ORF

[2] Voronkov, V., & Meo, Antonia. (2021). Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes. United Nations Office of Counter-Terrorism (UNOCT) & United Nations Interregional Crime and Justice Research Institute (UNICRI). https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

[3] Whittaker, David J. (2004). Terrorists and Terrorism in the Contemporary World. Taylor & Francis e-Library.

[4] Ganeles, C. (2002). Technological advancements and the evolution of terrorism. ILSA Journal of International & Comparative Law: Washington D.C., USA, Vol. 8:617

[5] Riedel, B. (2011). The Grave New World: Terrorism in the 21st Century. Brookings: Washington D.C., USA.

[6] Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ, PMID: 38259881

[7] Dr. Liang, C. Preventing Terrorists from Using Emerging Technologies. Vision of humanity.
https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies
[Accessed on: 3rd February, 2024]

[8] Miasnikov, E. (2005). Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspect. Center for Arms Control, Energy and Environmental Studies at MIPT, pp. 3- 26

[9] Dass, R, & Mok, B. (2023). Assessing the Impact of 3D-Printed Weapons on the Violent Extremist Milieu. The Global Network on Extremism and Technology (CNET).

[10] Inglis, S. (2017). Technology and the Crime-Terror Nexus: Threat Convergence in a Digital Age. The International Affairs Review, pp. 4-13

[11] Onat I, Bastug MF, Guler A, Kula S. (2022). Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison. Taylor & Francis online, Behavioral Sciences of Terrorism and Political Aggression, pp.1-17