Technology and terrorism

Technology has had a profound impact on our society, mostly due to its accelerating growth over the past two decades. The integration of technology has boosted productivity and efficiency in many different sectors of our society, such as consumer electronics and business logistics. However, its growth has created many uncertainties about its role in the future, as not all people use it for morally righteous reasons. Terrorism refers to the use of violence to instill fear in a particular group of people, often for some sort of political or societal gain. Technological advancements will offer terrorists new attack vectors, while potentially making it easier to afflict more damage. This essay examines how technology has changed the attack methods of terrorists, and how the rise of social media has aided terrorists efforts.

One of the main technological advances that terrorists have begun to utilize is unmanned aerial drones. These drones have various uses for terrorists, as they allow their users to provide surveillance and targeting support before and during attacks (Vision of Humanity 2023). Increased accuracy and the fear of always being watched would both contribute to more fear in potential targets. Another benefit that drones offer is their affordability and ease of use, which reduces the amount of training that terrorists need to operate them (Vision of Humanity 2023). This could eventually allow terrorists to control several drones at once, which further increases the risks. The drone market continues to grow and their capabilities are starting to expand as some models can even harness explosives (Vision of Humanity 2023). Fortunately, most military grade drones are too expensive for terrorists to currently acquire (Vision of Humanity 2023). However, they do have access to drones that can carry grenades and launch terrifying and precise attacks (Vision of Humanity 2023). When considering attributes such as the speed of drones and the relative cheapness, it also feels like defending against these technologies will be tougher as

use becomes more widespread. Obviously, drones can be used by both terrorists and counter-terrorists so there are some positive benefits from the bustling drone market. Therefore, drones are just another technology that needs to be regulated so that we don't lose track and put more lives in danger. Artificial Intelligence is another technology that can be weaponized by terrorists as it can create propaganda and malware to damage society (Vision of Humanity 2023). It can learn information much faster than humans and use data to solve complex problems. This technology is arguably even scarier due to its ability to assist terrorists in hacking critical infrastructure and stealing sensitive data stored on devices. Drones could even be improved with the use of AI, and terrorists could use it to upgrade existing ones. The possibilities are endless due to this frightening technology which is why world leaders must find ways to regulate its use. Some counter-terrorism groups have already begun to use this technology to fight back (GENEVA 2023). However, even if we are using this technology for good, we still have to ensure we are not violating any basic human rights. According to Geneva, counter terrorism efforts conducted by states and private actors are utilizing high risk surveillance technologies, potentially jeopardizing human rights (2023). Drones, biometrics, and artificial intelligence are some examples of technologies that fall under this category (GENEVA 2023). These technologies are not being regulated properly and should not be used until adequate safeguards are enforced (GENEVA 2023). It is also possible that the use of these technologies could antagonize terrorists even more.

Due to the advancement of technology, it is now becoming possible that small groups or individuals can launch catastrophic terrorist attacks (Kaur, pg. 81). Terrorists now have a plethora of technologies at their disposal such as precision guided ammunition and biochemical agents (Kaur, pg. 82). Biochemical agents are especially alarming since COVID-19 showed us

how disastrous a virus outbreak could be. Currently, many terrorists are still behind the curve when it comes to utilizing these technologies due to their environment or just the general lack of availability (Kaur, pg. 83). However, some of them have shown that they are capable of making bombs that can be programmed to explode months after they have been placed, causing confusion and making it harder to detect these attacks (Kaur, pg. 84). This could be dangerous in enclosed places such as sports stadiums and government buildings. There have also been advancements in the ability to forge documents and currencies, which terrorist groups are likely to engage in as well (Kaur, pg. 84). Having more money would allow them even greater access to these new devastating technologies. Terrorists organizations are also trending towards the ability to create nuclear weapons, which alarmingly coincides with the fact that countries such as the United States have misplaced thousands of pounds of nuclear material (Kaur, pg. 85, 86). The threat of terrorists making nuclear weapons is probably much more unlikely for the next few decades, but it is still something that should be addressed immediately, especially if a terrorist group is able to take over a major power or hack into their systems. Another fear is that different terrorist groups could start to cooperate and exchange nuclear arms information along with nuclear weapons, therefore speeding up the process of creating military grade nuclear weapons (Kaur, pg. 87). Nuclear technologies are becoming more widespread as more countries learn its technology, opening up the possibility of unstable countries having nuclear weapons (Kaur, pg. 88). As of now, only the major powers of the world have a large arsenal of nuclear weapons, which is most likely why we haven't seen many nuclear bomb incidents. Nuclear bombs have the capability of killing tens to hundreds of thousands of people, so even if terrorists can’t recreate a technology as devastating as that, a bomb with the ability to kill a few thousand would still be a serious threat to countries (Kaur, pg. 89). This is something people didn't have to worry about

much in the past unless a major war was going on, since only the major powers had access to these weapons. We have already seen the damage that could be caused by these weapons after the attacks in Japan coinciding with the end of World War II, as the bombs left lasting effects on Hiroshima and Nagasaki. In order to keep up with these dangerous technologies, we need smarter defensive and detective systems deployed everywhere, ensuring that everyone is protected.

Another attack vector that will likely be more lucrative to terrorists is large business in prominent countries. Businesses have seen many benefits following the inclusion of newer technologies in areas such as productivity, so naturally they rely on them heavily. However, Cyber attacks have been shown to negatively impact the market value of companies (Smith *et al*, pg. 386). Terrorism is about creating fear and uncertainty, and these attacks achieve that by attempting to ruin the trust consumers have in businesses, as successful attacks make consumers believe companies lack the capability to safely protect their data. Terrorists can either choose to go after personal data, or critical infrastructure that the company needs to operate. Therefore, these attacks can affect both the privacy and safety of consumers and businesses, making these terrorists even more formidable. Attacks can also obstruct a businesses online functionality and operations, causing them to lose money and potentially put consumers at risk if their services are critical (Smith *et al*, pg. 388). For example, attacking a power plant or water facility could be a direct safety concern. Merck suffered an attack like this, which prevented their HPV vaccine production and forced them to use the reserves for 18 months (Smith *et al*, pg. 394). Terrorism is often associated with physical violence, but attacks on global economies can be just as dangerous. Cyber attacks are likely underreported due to companies' fear of ruining trust with their customers (Smith *et al*, pg. 390). Even if counties have adequate security, third party

companies they work with can be attacked as well which leaves them vulnerable too (Smith *et al*, pg. 392). The author's analysis found that stock prices dropped around 3% three days after news breaks of a cyberattack on a company, and this trend continued for weeks after the attacks that they studied (Smith *et al*, pg. 397). If more attacks happen, it will help validate the implications these attacks have on the economy. Using resources to help prevent attacks is often less costly then rebuilding after an attack (Smith *et al*, pg. 385). One effective preventative method is defense in depth, which places multiple layers of firewalls and authentication in front of sensitive data, making it harder for attackers to access it (Smith *et al*, pg. 399). Having economic integrity is important, so securing companies from hackers is key to not letting terrorists get the upper hand due to technology.

Financing terrorism through cryptocurrencies is becoming a viable method for terrorist groups looking for additional financial support. Currently, there is not an abundance of research linking cryptocurrencies to their potential to fund terrorist organizations (Teichmann, pg. 514). However, this is likely due to the anonymity of cryptocurrency as it is challenging to identify the actual senders (Teichmann, pg. 514) Cryptocurrencies are not regulated by any government entity and can be hidden relatively easily in e-wallets (Teichmann, pg. 515, 516). This is because this newer currency is completely digital and is not distributed by banks or the government. One of the main uses of cryptocurrencies are for the purchase of illegal goods, including weapons that are used by terrorists (Teichmann, pg. 516). Most purchases for illegal weapons occur on the Dark Web, and cryptocurrency is almost always the desired currency for both consumers and sellers. It is also a good currency to use for demanding ransoms, due to the difficulty of tracking it and because it is relatively easy to buy it. Terrorists also realize that combining its anonymity with other methods such as using public wifi networks make it truly difficult to track its source

(Teichmann, pg. 516). Cryptocurrency is also very convenient since its holders can switch it back to regulated currencies very easily (Teichmann, pg. 515). In the terrorist world, these benefits are invaluable as countries under attack by these terrorists undoubtedly want to cut off their financial supplies. The more funds these terrorists can acquire, the longer they can keep fighting and thenturn around and attain more technology in order to carry out their attacks. However, the one drawback is that selling large amounts of bitcoin for a native currency will definitely garner attention, making it risky for terrorists. This is especially important because warfare usually costs a lot of money, so this directly puts terrorist groups at a disadvantage (Teichmann, pg. 515). It is also not common for people to be able to use cryptocurrency to buy everyday items from shops, but terrorists most likely don't need cryptocurrency for smaller purchases (Teichmann, pg. 516). The biggest issue is that law enforcement is not very familiar with detecting cryptocurrency and tracing its origin, since it is a relatively new technology. Therefore, this is something that should be addressed immediately since tracking funds would give them an upper hand on locating and stopping terrorist efforts.

Communication has always been important in society, as the exchange of information can be advantageous in many scenarios. The main purpose of terrorist attacks, outside of creating fear through violence, is to communicate a message to an audience, usually one that persuades people either to fight for their cause or instill fear in their targets. A popular example is ISIS posting beheadings and executions on social media in order to spread fear (Mahmood, pg. 128). Before technology became so advanced, terrorists couldn’t easily reach potential supporters around the world in an instantaneous manner. The nature of social media also allows content to go “viral”, further helping them spread propaganda with less work on their end. This could be through videos with hashtags that conveniently leave out details in order to persuade people that

terrorists actions are justified. Another use for communication technology is to help finance and plan attacks, as it has accelerated the speed and availability of communications (Mahmood, pg. 128). People don't need to be face to face to coordinate plans and can instantaneously contact people anywhere where they have a connection. The ability to learn information is one of the biggest benefits of the internet, but unregulated forums can also teach people how to carry out crime and terrorism. Terrorists know this and are attempting to educate people on how to carry out terrorist attacks using social media and other internet platforms. On the positive side, communications technology has also improved counterterrorism capabilities such as highlighting the dangers of terrorism (Mahmood, pg. 131). Governments have used communications technology to spread propaganda, which can help thwart terrorist groups (Mahmood, pg. 131). This shows that communications technology can be considered as another weapon of war. Surveillance of online spaces and surveillance using cameras can also prevent attacks from happening, as both have led to arrests of potential perpetrators. Terrorist groups can also be the victim of hacking as agencies try to get information from terrorists' computers. There can also be scenarios where potential attacks are foreshadowed due to posts on social media, and some attackers can be traced through these posts as well. (Mahmood, pg. 132) Therefore, despite the improvement that terrorists grouped gained from communications technology, law agencies also gained access to these technologies and thus have been able to prevent attacks as well, thus evening the playing field.

The most interesting section to me was about high technology terrorism, as there is a lot of uncertainty around it. The belief that terrorists could access nuclear weapons is very scary, since those can be fired at targets on the other side of the world, meaning virtually everyone is a potential victim. Smart bombs could also be a problem as they could be placed weeks or months

in advance, and targets would have no idea where. This also led me to be more curious about bio-terrorism, which is now a potential topic for another research paper that I will write. The drone section is interesting too, because I could imagine much scarier drones in the future as well, since weapons could be hooked up to those. Since I have played lots of video games, I know how terrifying drones could be, and although the majority of these designs were science fiction, technology is evolving so rapidly that those devices may become real. I have always been someone who has worked with technology, so the social media section didn't surprise me. I have seen some terrorist actions on social media sites such as Twitter, and was astonished at how much engagement they got on their posts and propaganda. The online radicalization unit forced me to remember that as well. I'm glad that it touched on the memes because those are dangerous, but not many people talk about their influence especially on the younger generations. This paper definitely taught me how technology has changed all of our lives, and not just those of terrorists. It's always mind-blowing to see how much we rely on technology, and how much influence it has on our day to day actions. For example, drones are fairly new, and I have even purchased one. I never gave much thought to their use in combat, since I believed only the military could accomplish such feats. This was until I realized how cheap drones were, despite how innovative and amazing they were to me. In conclusion, it was interesting seeing what technologies and potential vulnerabilities the future terrorists could exploit, and I think this will be important to keep in mind as I continue my career in cybersecurity.

Works cited

GENEVA. (2023, March 14). Alarming misuse of high-risk technologies in global fight against ... Office of the High Commissioner for Human Rights. https://www.ohchr.org/en/press-releases/2023/03/alarming-misuse-high-risk-technologies-global-fight-against-terrorism-says

Unmanned Aerial Vehicles & AI: Policy Measures & Challenges. Vision of Humanity. (2023, September 11). https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/#:~:text=Threats%20Posed%20by%20UAS,energy%20infrastructure%2C%20and%20civilian%20centres.

Herre, B., Samborska, V., Ritchie, H., Hasell, J., Mathieu, E., & Roser, M. (2023, December 28). Terrorism. Our World in Data. https://ourworldindata.org/terrorism?insight=most-terrorist-attacks-target-private-citizens-the-military-and-the-police#introduction

Teichmann. (2018). Financing terrorism through cryptocurrencies – a danger for Europe? Journal of Money Laundering Control, 21(4), 513–519. https://doi.org/10.1108/JMLC-06-2017-0024

Mahmood, & Jetter, M. (2020). Communications Technology and Terrorism. The Journal of Conflict Resolution, 64(1), 127–166. https://doi.org/10.1177/0022002719843989

Smith, Smith, L. M., Burger, M., & Boyle, E. S. (2023). Cyber terrorism cases and stock market valuation effects. Information and Computer Security, 31(4), 385–403. https://doi.org/10.1108/ICS-09-2022-0147

Kaur. (2007). High Technology Terrorism: A Threat to Global Security. India Quarterly, 63(2), 81–95. https://doi.org/10.1177/097492840706300204