**Technology**

Student’s Name

Institutional Affiliation

Course and Code

Instructor

Date

**Technology**

**How Technology is Used in Homeland Security**

First, technology can be used in identifying potential threats. Through technological advancement, it has become easier for security agencies to identify potential security threats and to take action before the threats affect members of society (Voeller, 2010). For example, technology can be used to screen members of the public and detect any weapons that they may have, hence reducing the likelihood of the threats causing both direct and indirect harm to the public. Furthermore, it has also become easier to identify potential threats through technological advancements such as identification of suspicious social media posts that are suspicious towards a specific person or a group of people (Voeller, 2010). Through advancements in technology, it has become easier for threatening messages are filtered to ensure that any potential threats are identified and the necessary action is taken in advance. Through the identification of threats, technology will reduce the possibility of the society being jeopardized, improving the quality of life in the process.

It has also become easier to share information internally and externally for the homeland security agencies, hence reducing the threat of insecurity within the society. Through technology, new methods of communication are emerging, leading to the improvement of how information is shared and distributed among security agencies and also to the public (Voeller, 2010). Advancement in technology has seen communication being more advanced through the use of measures such as encryption to keep messages secure and only available to the intended audiences. Also, it has become easier to distribute information to members of the public concerning potential security threats using technology, resulting in a situation whereby security threats do not have as much negative effects as it would have been initially expected (Voeller, 2010). Through the advancements in technology, it has been easier to communicate about security threats and avert any potential dangers that could harm the general public.

Technology has also led to the development of better equipment that will ensure better security in the society. The development of technology has resulted in a situation whereby the equipment used in securing the society has become more advanced in a way that will ensure that criminals of all types are subdued (Voeller, 2010). For example, the use of drones to survey an area will ensure that security agencies will stand a better chance of tracking criminals and stopping them from posing a threat to society. Furthermore, the use of technology to track down criminals will ensure that their movements are known and that the necessary action is taken to reduce the likelihood of security threats affecting the growth and development of society (Voeller, 2010). Through the advanced technological equipment developed, security agencies stand a better chance of preventing criminal activities and achieving the desired outcomes in terms of socioeconomic growth.

**How Technological Advancement can be Used in Emergency Management**

Advancement in technology has helped in the development of Geographic Information Systems. Geographic Information Systems is used in emergency management to map out hazards and reduce the likelihood of the damages and unwanted outcomes being too much (Chang, 2016). The GIS is also used in mapping out vulnerabilities in case of emergencies and to determine the resources available and those that are required to address the emergencies. It is also through such a technological advancement that it has become easier to track down the incidences taking place, hence informing the events and operations that are to be undertaken in response. Through the critical information provided by the GIS, it is easier for emergency management to be undertaken more effectively since it affects decision-making due to the situational awareness that the people concerned will have, resulting in a reduction of the unwanted outcomes and the people and property involved being secured (Chang, 2016). It is also easier for risk assessment to be undertaken through the GIS, given that it provides accurate information that can help in improving the outcomes that will be achieved.

Satellite imagery is also another important emergency management tool that has been developed as a result of technological advancement. Satellite imaging plays an important role in assessing the extent of the damage experienced as a result of the emergencies experienced, thereby informing the actions of first respondents when responding to the situations (Sakurai & Murayama, 2019). It is also through satellite imaging that the movement of people can be tracked so that the first respondents can determine how to reach them and provide them with the emergency services that they require immediately (Sakurai & Murayama, 2019). This being the case, rescue and relief operations are easier to undertake when satellite imagery is used, given that the first respondents will be operating with full knowledge and reduce the damage and unwanted outcomes that could have been otherwise experienced.

Technological advancement has also contributed to better preparation for emergency situations through the introduction of resources such as weather forecasting and early warning systems and procedures (Sakurai & Murayama, 2019). Through weather forecasting, it is easier for early warnings to be given to the people that are likeliest to be affected by the emergency, hence saving lives and property from being destroyed. It is also through the early warning systems that early precautions can be taken in case of expected natural disasters such as taking vaccines and strengthening their homes so that the disasters do not affect them.

**Current and Future Issues that Need to be Addressed**

The threat of cybersecurity is still a critical issue facing technology. Cybersecurity has become a critical issue for individuals and businesses due to the increase in unwanted activities such as malware that affect the activities of the individuals and businesses in question (Nižetić et al., 2020). The prevalence of data breaches is due to the advanced knowledge that attackers have and their desire to exploit the vulnerabilities that organizations and individuals have and to gain an advantage over them (Nižetić et al., 2020). If data breaches are successful, then the safety and continuity of the activities that individuals and businesses undertake will be threatened, resulting in underwhelming outcomes in both the short and long runs.

The widening of the skill gap in the technology industry is another issue that needs to be addressed. Technology is only as good and effective as the people managing and using it, and therefore this means that the skills of the users will determine the quality of outcomes achieved when technology is used (Nižetić et al., 2020). The widening gap between the existing skills and the desired ones means that there are unmet needs that only improvement of skills can help in solving and overcoming any unwanted outcomes as a result (Nižetić et al., 2020). Without bridging the gaps, it will be impossible for innovation and improvements to be achieved, thereby holding back the growth and development of society.

The successful implementation of artificial intelligence is another critical issue that needs to be addressed. Businesses and organizations need to implement artificial intelligence in their operations so that they can experience an improved likelihood of their operations running more smoothly and the desired outcomes being achieved in shorter periods and the outcomes lasting for longer (Nižetić et al., 2020). The implementation of artificial intelligence alongside human labor is also a challenge that needs to be addressed, given that the two are currently incompatible, especially since human labor considers artificial intelligence to be a disruptive force that threatens their job security and operations.

Finally, it is a difficult task to regain trust in technology from the general public due to the negative perception that technology has been getting in the recent past. The spread of misinformation on the dangers of technology has been the major issue, given that technology has been shown as a disruptive force that has more negative outcomes than the positive ones, hence making some people suspicious of the application of technology in different aspects of life (Nižetić et al., 2020). Furthermore, the rise in instances of cyberattacks has led to an increase in the levels of distrust for technology, thereby losing the support of the public in technology (Nižetić et al., 2020). The disruption of activities as a result of lags in technology also increases the skepticism that people have against technology, hence the need for improved knowledge on technology, its uses and how to properly interact with it.

**How to Address the Issues in Technology**

To solve the issue of unskilled manpower in technology, there is a need for an improvement in the education offered to the learners. Segregation and specialization in technological education is required so that the learners can specialize in specific aspects of technology instead of being bombarded with unnecessary information that they will not use in their future careers (Mitcham, 2022). Through improved approaches towards technological education, it will be easier for the learners to be more skilled and achieve higher levels of efficiency in addressing current and future technological needs of the society.

Secondly, data security can be improved only if stricter regulations are applied on a global level. The use and distribution of data needs to be regulated globally so that data will be more protected and in a better position to improve user experiences and outcomes in both the short and long runs (Mitcham, 2022). It is also necessary that the general public is taught on safety measures that they can use when handling data so that the data does not fall into the wrong hands and security is compromised in the process (Mitcham, 2022). Improved security measures also need to be taken to ensure that the security of data is assured and that better outcomes will be achieved when the necessary actions are undertaken.

To address the takeover of artificial intelligence in technology, it is necessary that the parties involved undertake more research on the subject matter. Research and development on artificial intelligence will ensure that the use of artificial intelligence is based on facts and not misinformation, thereby resulting in a situation whereby artificial intelligence is effectively included in daily life without disrupting the operations that were previously enjoyed (Mitcham, 2022). When this happens, it will be easier to achieve positive outcomes and improve daily operations of society due to the higher levels of efficiency that will have been achieved when artificial intelligence is included in socioeconomic activities of the society.

**References**

Chang, K. T. (2016). Geographic information system. *International encyclopedia of geography: people, the earth, environment and technology*, 1-10.

Mitcham, C. (2022). *Thinking through technology: The path between engineering and philosophy*. University of Chicago Press.

Nižetić, S., Šolić, P., Gonzalez-De, D. L. D. I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of cleaner production*, *274*, 122877.

Sakurai, M., & Murayama, Y. (2019). Information technologies and disaster management–Benefits and issues. *Progress in Disaster Science*, *2*, 100012.

Voeller, J. G. (Ed.). (2010). *Wiley Handbook of Science and Technology for Homeland Security, 4 Volume Set*. John Wiley & Sons.