Emerging Technologies and AI in the Security and Defence Sectors – 2022 and beyond

A number of governments have invested considerable resource and research into emerging technologies including China, US, UK, Canada, Russia and Germany. The AI global market was valued at $59 billion in 2021 and is estimated to reach $422 billion by 2028[1]. Over the next decade further advances in AI applications will be a game changer for the security sector. Military grade surveillance is now available to anyone who knows where to look. The Internet has helped enable access to technologies and systems that were previously limited to states and intelligence services.

We are in the midst of an information technology revolution, which is accelerating at an unprecedented rate. A survey of over 1,600 board level executives and data-science leaders from the world's largest organisations found that nearly 75% of companies have already integrated AI into their business strategies[2]. Furthermore the ambition amongst nations to maintain a comparative advantage is ever more apparent in embracing these technologies to augment their capabilities and provide the upper hand in a conflict environment. Nations need to consider whether warfare utilising AI and machine learning could lead to unintended destabilising consequences.

Regulation and ethics are being addressed with investment in technologies using AI and developing AGI[3], which is seen as the next phase in AI transcending to a heightened human level of understanding. Ethical issues are coming into question with surveillance bringing huge advantages to law enforcement agencies and security services. The negative implications are the risk of embracing the technology and sleep walking into an Orwellian[4] police state. Democratic governments and institutions are having to navigate within an increasingly complex security and regulatory environment.

Autonomous drones and machines present real concerns if nefarious groups or hostile states use this technology to pursue their political goals. Dystopian visions of the future depicted in social media, notably slaughter bots[5], and augmented humans[6] are now conceivable as governments and private industry continue to commit to investing resource into advanced military and defence technologies and setting the path towards a new arms race. Self-learning algorithms using AI to operate

[1] https://www.bloomberg.com/press-releases/2022-06-27/-422-37-billion-global-artificial-intelligence-ai-market-size-likely-to-grow-at-39-4-

[2] https://www.accenture.com/gb-en/insights/artificial-intelligence/ai-maturity-and-transformation?c=acn_glb_aimaturityfrompgoogle_13140680&n=psgs_0622&gclid=CjwKCAjwi8iXBhBeEiwAKbUofUtPGmo-1HytMv1JUaHwSql1dYkHFHsJb03JAonoayuebQm_PwMXyRoCHrsQAvD_BwE

[3] AGI Artificial General Intelligence is the ability to understand or learn any intellectual task that a human being can.

[4] Orwellian is a societal condition that George Orwell identified as being destructive to the welfare of a free and open society and denotes a brutal policy of draconian control by propaganda, surveillance and disinformation.

[5] https://www.youtube.com/watch?v=O-2tpwW0kmU

[6] AI/human augmentation is a view that sees the story of humans and machines as one of cooperation. It puts the human in the driver seat and focuses on how AI becomes assistive to enhancing human capabilities.

autonomously will lead to situations where human control is lost or no longer required.

Recent advances in quantum[7] technologies could also lead to challenges to existing encryption, "secure" networks and critical systems. The technology is an emerging field of physics and engineering and will herald breakthroughs in speed, decision making, and scientific discovery but at what cost? If quantum technology provides the means for encryption to be obsolete what kind of society will we face? Will privacy be confined to off line systems in the future?

Leading nations are also investing heavily in cyber, space, and satellite warfare systems with the advent of AI. The UK recently published a paper on integrating AI into its Defence Strategy[8]. We are facing new and novel asymmetric threats and hybrid warfare has now advanced to the point that numerous countries and actors now have the potential to inflict significant damage to adversaries and vice-versa. With a rapidly changing security landscape the risk around rules of engagement are more likely to result in a greater chance of escalation, miscalculation and conflict.

Cyber attacks that can inflict damage at scale are now ever more frequent; critical infrastructure has been disrupted in countries across the world, and supposedly secure government institutions and bodies have been hacked on numerous occasions. In February 2022, Nvidia, the world's largest semiconductor chip company was compromised by a ransomware attack. In May 2022, The Costa Rica Government for the first time declared a national emergency in response to a similar attack, which severely affected computer networks and multiple government agencies. Any system on the grid is vulnerable despite the huge investment by companies and institutions to safeguard systems. Companies such as Crowdstrike, Darktrace and SAPNS2 have integrated AI into their security products[9] to help organisations deal with ever more sophisticated cyber threats.

It is evident that the global security apparatus has leveraged technology to strengthen their capabilities in this space. AI and the Internet of Things[10] are purposely developing systems and applications to augment their military effectiveness. Conventional warfare is increasingly being replaced by approaches that combine cyber warfare, and emerging technologies with increased connectivity and autonomous systems with AI to support minimum human intervention. As AI is utilized more in the defence sector to automate predictive outcomes, AI automated judgements will become a critically important and controversial issue when considering tactical and strategic decision making. What will be the agreed

[7] Quantum technology is an emerging field of physics and engineering using technologies that rely on the properties of quantum mechanics. Quantum computing, sensors, cryptography, simulation and imaging are examples of emerging quantum technologies.

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082416/Defence_Artificial_Intelligence_Strategy.pdf

[9] https://www.analyticsinsight.net/top-10-cybersecurity-companies-using-ai-to-the-fullest-in-2022/

[10] Internet of Things (**IoT**) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

parameters for removing human interaction in a myriad of military or security scenarios?

In summary the security landscape is changing rapidly with new disruptive technologies. Lethal autonomous weapons, intelligent systems, and AI are major drivers for both defensive and offensive capabilities. Identifying innovative technologies to implement into any security related operation or business model will continue at pace for both government and private industry to dominate this sector over the coming decades.

17th August 2022