THE DUMB AND THE DANGEROUS ROAD AHEAD

by Hedi Nasheri[1]

> **“Ambitious corporations in the industrialized advanced nations driven by profit and greed are commercializing, developing and deploying AI on large scale**

The current state of world affairs is extremely alarming. The geopolitical tensions, global power struggles, conflicts in cyberspace, the global impact of the Covid-19 pandemic, cyber-attacks, the rise of far-right nationalist and extremist groups, the climate challenges, food and water security and the migration crisis are among many pressing factors impacting the world order, democracies and the global security.

As emerging technologies such as artificial intelligence, biotechnology, and quantum technology, as well as new weapons technologies such hypersonic weapons and directed energy weapons, continue to mature, they could hold significant implications for societies around the world.

While emerging technologies such as artificial intelligence (AI), often combined with related technologies such as robotics, have led to positive impact, among the others, in the field of medicine, transportation, telecommunications, housing, and have significantly contributed to scientific discoveries, at the same time these technologies, if not properly governed and used, could pose a threat to civilization and humanity as we know it. Highlighting the real risks associated with the misuse of AI can help understanding the current status of this technology and its potential negative consequences. At the time of writing this piece, the following major events occurred which highlights the good, the bad and the ugly side of emerging technologies such as AI. These technologies, which characterize the Fourth

1 Hedi Nasheri, is a Professor of Criminology and Justice Studies at Kent State University in the United States.

Industrial Revolution and are driving profound changes in society and the economy need safeguard mechanisms.

The first 3D housing community was completed and operational in Mexico. This is a housing development that can withstand climate challenges such as earthquakes and harsh weather. At the same time, we learned that Facebook is unintentionally spreading misinformation through the company's algorithms. Given the current geopolitical environment it is not surprising that AI poses profound changes to society. This emerging technology requires constant safeguard at every level and ongoing accountability to prevent its misuse. Although there is an enormous and growing number of policy initiatives to try to keep the potential for harm in check, such measures may be insufficient. Some researchers point out that the tech sector have been naïve about the technology they champion, how it will actually be used and what consequences their technological innovations will have.

Some of the problems this article highlights exist with or without AI, but new technological advances such as AI have the potential to magnify them at a level we cannot predict. This is why is so crucial to develop normative frameworks in order to make sure

that developments in this field respond to the principles of lawfulness, social acceptance, trustworthiness, responsibility and ethics.

The race to develop, commercialize and distribute

Ambitious corporations in the industrialized advanced nations driven by profit and greed are commercializing, developing and deploying AI on large scale. The distribution and production of robots for a wide range of use, such as autonomous weapon systems, pizza delivery drones, driverless delivery trucks, sex robots, recreational pets, cleaning robots, security application, competitive racing, photography, facial recognition software and surveillance technology are advertised and sold. AI has received considerable attention globally as a tool that can process vast quantities of data, discover patterns and correlations in the data unseen to the human eye. It is capable of enhancing effectiveness and efficiency in the analysis of complex information.

Humanitarian, recreational, military, and commercial applications of robots are truly global in nature. In light of this accelerated distribution and production, there is a growing interest amongst law enforcement and counter-terrorism agencies around the world in exploring AI technology. It is likely that the growth of these technologies will produce a new world.

Our changing world

In 2018 the London Times printed an editorial from Stephen Hawking, warning us that AI will likely outsmart humans. According to Hawking's legacy, AI will either be the best thing that is ever happened to us, or it will be the worst thing. If we are not careful, it very well may be the latter. Another important figure in the business circles, Elon Musk believes that AI is more dangerous than nuclear warheads and must be regulated. Musk believes that the race for AI could be the cause for World War III. He bases his belief on the past century of human behavior in regard to warfare. With developments such as Google's AlphaGo, Musk has seen how fast AI can improve without anyone predicting the rate of speed as well as its capabilities.[2]

Ambitious corporations in the industrialized advanced nations driven by profit and greed are commercializing, developing and deploying AI on large scale

According to Hawking's legacy, AI will either be the best thing that is ever happened to us, or it will be the worst thing

The development of AI is largely unchecked and many feel insufficient attention is given to its potential to create problems.[3] AI researchers warn that AI can develop negative behaviors based on their interactions with humans, they give examples of human induced negative behaviors. AI, as creations of humans can intrinsically absorb problems that their creators have not solved yet. This involves the replication of human problems in the solutions created by AI.

2 Barbaschow, A. (2018). AI 'more dangerous than nukes': Elon Musk still firm on regulatory oversight. Retrieved 2020, from https://www.zdnet.com/article/more-dangerous-than-nukes-elon-musk-still-firm-on-regulatory-oversight-of-ai/?ftag=TRE6a12a91&bhid=28036118512285295119801408296132

3 Leprince-Ringuet, D. (2021). US, China or Europe? Here's Who is Really Winning the Global Race for AI.

Without the right governance measures in place there is a risk that AI can result in anti-social or harmful actions.[4] At the same time, AI is being deployed as a weapon in modern militaries. AI is being integrated into weapons and used in automated vehicles, like unmanned aerial vehicles (UAVs), or small land vehicles. The dynamics between AI and social media also raise questions in terms of possible misuse to manipulate social media users.

There are only a handful of countries that have made striking advancement in the designing and production of AI technologies and the current debate is on who is leading the way. Recent reports suggest that some countries are exponentially progressing while others are still in an embryonic phase. This will contribute to widen the existing gap among countries in terms of development and progress.

There are also different approaches to AI: some countries have surpassed others in the area of defense - posing a major concern for the future of warfare – some others want to acquire the leadership in the development of AI, believing that AI is the focus of international competition and economic development. A prominent politician stated that whoever leads AI will rule the world.

A typical case of concern is the following: a country collects data from electric cars by claiming that the data is used for policy planning but there are obvious privacy implications. Auto makers worry the data could be used for industrial espionage but yet they comply with the laws so they can sell their cars in the country.5 Using surveillance to suppress dissent and facial recognition technology for mass surveillance purposes is also a case of concern.[6] Government officials use terrorist attacks as a justification for mass surveillance programs, despite the evidence that they do not meet the original expectations. Most of these programs are kept secret so little is known about the success rate. However, informa-

4 Waddell, K. (2018). AI might need a therapist, too. Retrieved 2020, from https://www.axios.com/ai-might-need-a-psychologist-1529700757-a21b0d80-727a-402f-91d8-3196150d59ed.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosm&stream=top

5 Kinetz, E. (2018). In China, your car could be talking to the government. Retrieved 2020, from https://apnews.com/4a749a4211904784826b45e812cff4ca?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

6 LeVine, S. (2019). A paradise for the age of the techno-autocrat. Retrieved 2020, from https://www.axios.com/us-china-artificial-intelligence-surveillance-addd458b-2e0e-4309-91d8-187aabc83814.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

tion that has been disclosed does not justify mass surveillance.[7]

National security risks

As academic institutions, major corporations, and government science and technology programs continue to develop and deploy AI capabilities, AI-enhanced systems will be trusted with increasing levels of autonomy and decision making, presenting the world with a host of economic, military, ethical, and privacy challenges. Furthermore, interactions between multiple advanced AI systems could lead to unexpected outcomes that increase the risk of economic miscalculation or battlefield surprise.

Artificial intelligence, digital security, physical security, and political security are inherently intertwined and connected. As AI systems extend further into domains commonly believed to be uniquely human (like social interactions), more sophisticated social engineering attacks will happen based on these capabilities. AI, if not properly designed and used, will significantly change the political power balance. It is

AI, if not properly designed and used, will significantly change the political power balance

not clear what the long-term implications of malicious uses of AI will be. Production and detection of misleading information, interference with elections, an epidemic of computer viruses only scratch the surface of the types of political and stability security risks.

In his message8 the Secretary-General of the United Nations, António Guterres said: "machines with the power and discretion to take lives without human involvement are politically unacceptable, morally repugnant and should be prohibited by international law". Despite the many initiatives, including the United Nations Convention on Certain Conventional Weapons Group of Governmental Experts, so far, limited progress has been made in the adoption of new legally binding rules to regulate lethal autonomous weapons (LAWs). It appears that too many nations are not likely to enter into a treaty that would ban the use of AI decision making in weapons.

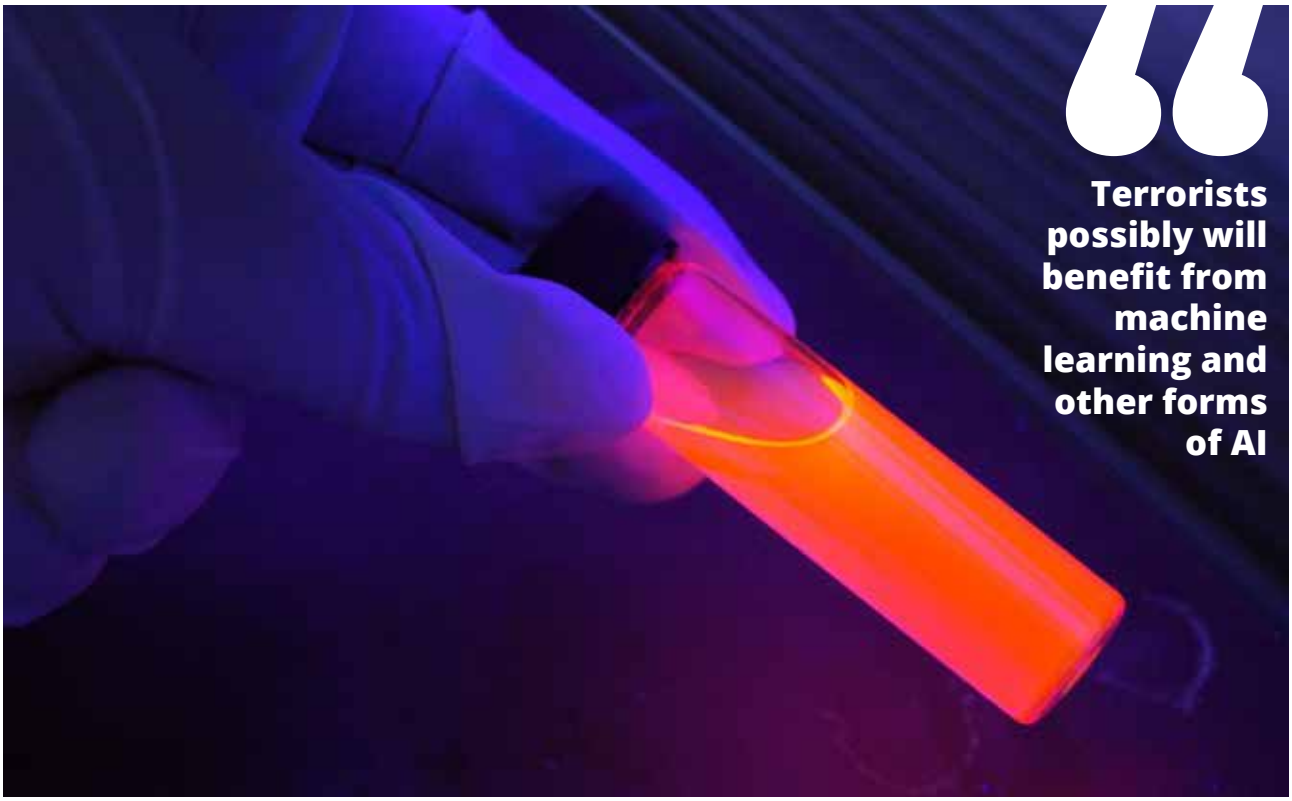
In the past several years we have seen that AI has been used to attack elections in different parts of the world. AI could become a growing threat to national security. The use of AI driven cyberattacks that can evade detection and use of AI driven phishing attacks are some examples of the types of threats. More advanced nations' intelligence agencies are working with the private sector to aide them in the development of defense AI systems.[9] Researchers expect that AI will be used to create more sophisticated malware. They expect that AI will be used in phishing, vulnerability recognition and autonomous attacks.[10] There are other threats such as AI being able to reproduce the biases of humans. AI is capable of creating, attacking or being misused such as, deepfakes, disrupting other AI controlled systems, large scale blackmail, fake news, misuse of military robots, learning

7 Kirchner, L. (2015). What's the Evidence Mass Surveillance Works? Not Much. Retrieved 2020, from https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosdeepdives&stream=top

8 https://news.un.org/en/story/2019/03/1035381

9 Macaulay, T. (2020). UK spies must ramp up use of AI to fight new threats, says report. Retrieved 2020, from https://thenextweb.com/neural/2020/04/27/uk-spies-must-ramp-up-use-of-ai-to-fight-new-threats-says-report/

10 Osborne, C. (2018). This is how artificial intelligence will become weaponized in future cyberattacks. Retrieved 2020, from https://www.zdnet.com/article/this-is-how-artificial-intelligence-will-become-weaponized-in-future-cyberattacks/?ftag=TRE-03-10aaa6b&bhid=28036118512285295119801408296132



Terrorists possibly will benefit from machine learning and other forms of AI

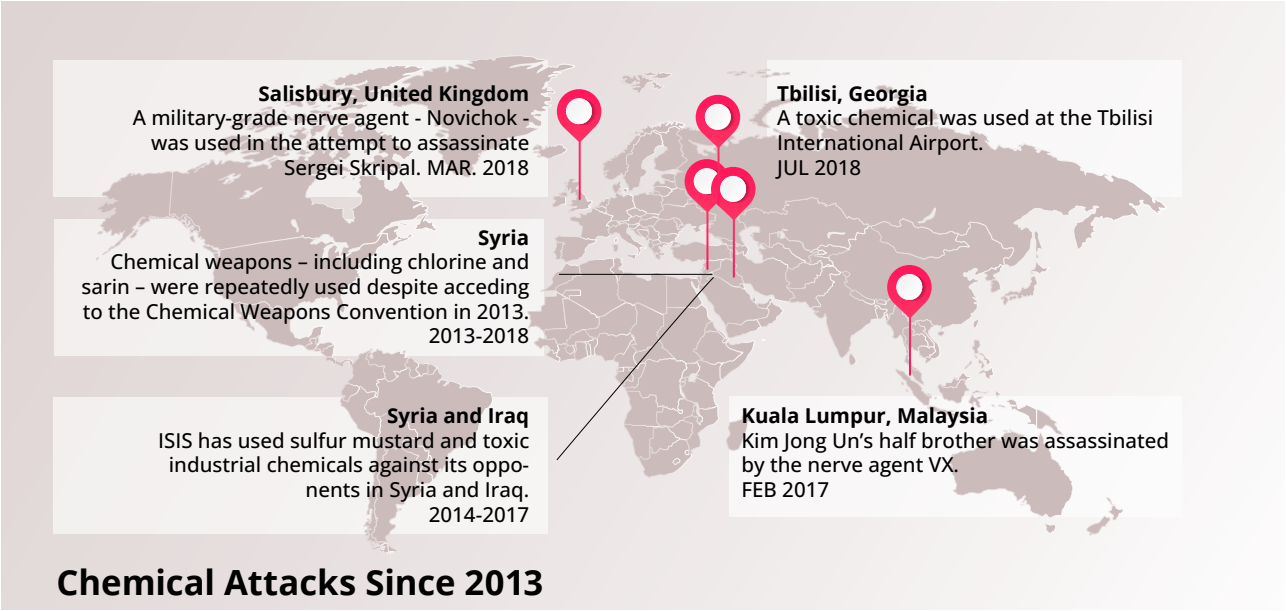
based cyber-attacks, autonomous drones attack, distributed denial-of-service (DDoS) attack, defeating facial recognition and the stock market manipulation.[11]

Terrorism and emerging technology

New technologies such as AI around the world can put sophisticated capabilities in the hands of individuals, state actors and nations. It is critical to understand the security implications for the advances in emerging technologies such as biotechnology and AI. A disturbing trend is the reported attempts of state- and non-state actors to acquire and use chemical and biological weapons in blatant violations of international norms.

It is likely that terrorist organizations will use AI. Terrorists possibly will benefit from machine learning and other forms of AI, for instance in the preparations for their military operations and for the gathering of information. Particularly when carrying out cyber-attacks, automated tasks executed by using AI can make the scale and impact of these attacks potentially larger. AI technologies are sold to and used by instable states, not to mention the role that organized crime groups can play in this scenario. It is unlikely that at this time terrorist organizations will have the capabilities to develop and maliciously use AI technology, however,

11 Leprince-Ringuet, D. (2020). AI vs your career? What artificial intelligence will really do to the future of work. Retrieved 2020, from https://www.zdnet.com/article/ai-vs-your-career-what-artificial-intelligence-will-really-do-to-the-future-of-work/?ftag=TRE6a12a91&bhid=28036118512285295119801408296132&mid=12774060



Chemical Attacks Since 2013

they can possess this technology. An example: when an unstable state collapses due to internal conflicts, the chances that these technologies will end up in the hands of terrorist and criminal organizations is very likely.

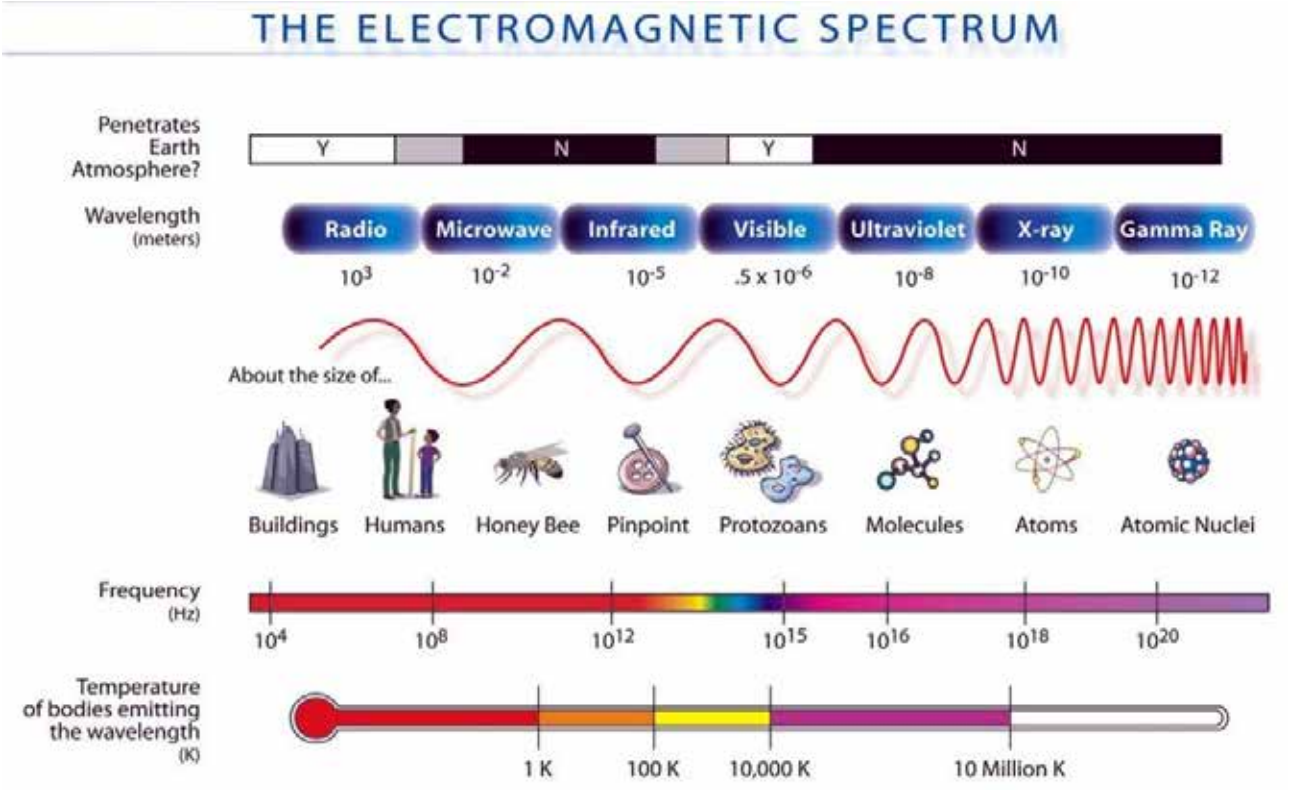
Chemical and biological weapons

In the recent years, some countries, and terrorist groups such as ISIS have used chemical weapons on the battlefield or in sponsored assassination operations (the responsibility of state actors is under investigation). These attacks have included traditional chemical weapon agents, toxic industrial chemicals, and the first known use of a Novichok nerve agent. The threat from biological weapons has also become more diverse as biological weapon agents can be employed in a variety of ways. The development of biological weapons is made easier by dual-use technologies. The following image demonstrates some of these attacks since 2013.[12]

Rapid advances in biotechnology, including gene editing, synthetic biology and neuroscience, will create new economic, military, ethical, and regulatory challenges worldwide as governments struggle to keep pace with these exponentially changing scenarios. These technologies hold great promise for advances in precision medicine, agriculture, and manufacturing. However, they also introduce risks, such as the potential for adversaries to develop novel biological warfare agents, threaten food security, and enhance or degrade human performance.

Biotechnologies, such as the low-cost gene-editing tool CRISPR-Cas9 have the potential to alter genes or create DNA to modify plants, animals, and humans. Such biotechnologies could be used to enhance (or degrade) the performance of military personnel. The proliferation of synthetic biology that is used to create genetic codes that do not exist in nature can be used to increase the number of actors able to create chemical and biological weapons. Adversaries may be less restrained in both researching and applying biotechnology, particularly as it relates to human performance modification and biological weapons.

12 United States Senate Intelligence Committee, 29 January 2019.



■ Table: The electromagnetic spectrum spans radio waves to gamma waves. Credit: NASA

Directed energy and hypersonic weapons

The recent growth and development of electromagnetic weapons is attributed to defense against terrorist attacks, chemical, biological, radiological, and nuclear materials for the purpose of national security and protection of civilian. A directed-energy weapon (DEW) is a ranged weapon that damages its target with highly focused energy, including lasers, microwaves, particle beams, and sound beams.

Potential applications of this technology include weapons that target personnel, missiles, vehicles, and optical devices.

Scientists believe that U.S. embassies, personnel and diplomats around the world have been targeted with high-power microwaves.[13] The technology behind these weapons are not new. The latest episodes of so-called "Havana Syndrome" took place in Berlin. The U.S. embassy has handed over evidence of this attack to authorities in Germany for investigation.[14] The first reported cases date back to 2016 in Havana, however these cases go back for many years. Physicians, scientists, and government officials have been trying to find out what causes the "Havana Syndrome". The electromagnetic weapon market is

13 The Conversation, 2020, Retrieved in 2021, https://theconversation.com/scientists-suggest-us-embassies-were-hit-with-high-power-microwaves-heres-how-the-weapons-work-151730

14 Germany investigates possible 'sonic weapon attack' against US embassy staff, the Guardian, https://www.theguardian.com/world/2021/oct/08/germany-havana-syndrome-sonic-weapon-us-embassy-staff

Is this the future we want for humanity? Do we want to let emerging technologies such as AI to make decisions for us?

anticipated to grow exponentially in the emerging technology market. This technology is cheap and easy to use with high precision for targets in any setting.

Cyberspace

Conflicts between states are taking place in space through cyber operations and attacks. Cyberspace has become a critical security concern for all governments around the world. This concern has grown exponentially over the years and the COVID-19 pandemic has exacerbated relevant vulnerabilities. Denial of service or destructive malware, cyber espionage or intelligence activity and breach of confidentiality of data are some examples of cyberattacks. Global access to space services has expanded for civil, commercial, intelligence, and military purposes, in part because of technological innovations, private-sector investments, international partnerships, and the demand from emerging markets. Foreign governments will continue efforts to expand their use of space-based reconnaissance, communications, and navigation systems - including by increasing the number of satellites, quality of capabilities, and applications for use.

Cyber attacks can disrupt Chemical, Biological, Radiological and Nuclear (CBRN) facilities. Such facilities are automated and run by computers that are connected to larger networks that can be compromised. When these facilities are penetrated through cyber-attacks the facilities themselves can become the equivalent of weapons of mass destruction themselves. These potential threats are near impossible to predict. Terrorist organizations want to acquire CBRN material which poses a major threat for the international community. The cyber domain is considered as major international security risks. More attention needs to be paid to terrorist activities online. Two prominent areas that terrorist organizations and groups have had much success with are communication of their propaganda and their recruitment efforts.[15]

The rise of a GPS society and the decline of human intelligence

Conflicts between states are taking place in space through cyber operations and attacks. Cyberspace has become a critical security concern for all governments around the world. This concern has grown exponentially over the years and the COVID-19 pandemic has exacerbated rele-

15 Nasheri, H. Economic Espionage and Industrial Spying, Cambridge University Press, New York, London, 2005, 270 pp.

vant vulnerabilities. Denial of service or destructive malware, cyber espionage or intelligence activity and breach of confidentiality of data are some examples of cyberattacks. Global access to space services has expanded for civil, commercial, intelligence, and military purposes, in part because of technological innovations, private-sector investments, international partnerships, and the demand from emerging markets. Foreign governments will continue efforts to expand their use of space-based reconnaissance, communications, and navigation systems - including by increasing the number of satellites, quality of capabilities, and applications for use.

Cyber attacks can disrupt Chemical, Biological, Radiological and Nuclear (CBRN) facilities. Such facilities are automated and run by computers that are connected to larger networks that can be compromised. When these facilities are penetrated through cyber-attacks the facilities themselves can become the equivalent of weapons of mass destruction themselves. These potential threats are near impossible to predict. Terrorist organizations want to acquire CBRN material which poses a major threat for the international community. The cyber domain is considered as major international security risks. More attention needs to be paid to terrorist activities online. Two prominent areas that terrorist organizations and groups have had much success with are communication of their propaganda and their recruitment efforts.[16]

THE AUTHOR

Hedi Nasheri is a Professor of Criminology and Justice Studies and the Director of Graduate Program in Criminology in the Department of Sociology at Kent State University in the United States. She is a Visiting Professor in the Faculty of Law at the University of Turku in Finland. Professor Nasheri's academic research and teaching, as well as her practical experience, has focused for a number of years on issues related to cybersecurity and technology crimes, intelligence and national security and transnational crimes as it relates to global security. She has collaborated throughout the years with members of the Intellectual Property Section of the Department of Justice and members from the Federal Bureau of Investigation Counterterrorism Section on a number of educational and research presentations domestically and internationally for a broad range audience including, the private sector, law enforcement and academia. More recently, she was appointed as Senior Fellow to the Policy Division of the Business Executives for National Security (BENS). Her work at BENS addressed the relationship of theft of sensitive and propriety information and its risk to U.S. national security.

16 Nasheri, H. Economic Espionage and Industrial Spying, Cambridge University Press, New York, London, 2005, 270 pp.