DISARMAMENT AND SECURITY COMMITTEE (DISEC)

Assessing the Potential Risk of Weaponisation of Artificial Intelligence (AI) and Big Data

Study Guide

Contributors: Karakanas Petros, Zourka Stefania, Solinara Evridiki

Table of Contents

1. Welcoming Letter

Dear delegates of the DISEC Committee,

It is our great pleasure to welcome you all in this year's ARCMUN and we would like to express our deep enthusiasm about serving as members of the Board of your Committee. Furthermore, we are more than pleased to welcome you all in the 1st Committee of the General Assembly (DISEC)

Firstly we would like to congratulate you all for participating in the 17th edition of ARCMUN. We guarantee to do our best so as to facilitate you during our sessions and be part of an unforgettable experience with fruitful debates, as well as productive cooperation. This year we will be discussing a topic of global significance, which is the Potential Risk of Weaponisation of Artificial Intelligence (AI) and Big Data. It is generally known that the growth of new technologies involve significant dangerous activities if they are not used in an appropriate way.

This study guide points at helping you get a better insight into the Topic Area under discussion of our Committee and offers you a starting point for your research. Nevertheless, we highly recommend you to conduct a thorough examination of your country's position concerning the matter discussed and also elaborate on your key national policies within the context of the position paper you will be requested to deliver before the opening of the conference.

Should you need any clarifications or help, we remain at your disposal!

We look forward to meeting you all in person!

Petros Karakanas, Main Chair

Stefania Zourka, Co- Chair

Evridiki Solinara, Co- Chair

2. Introduction to the Committee

The Disarmament and International Security Committee (DISEC) was established in 1945 and comprises one of the main committees of the General Assembly[1]. The role of DISEC is described in Article 11, Chapter IV of the United Nations Charter: "The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments and may make recommendations with regard to such principles to the Members or to the Security Council or to both"[2]. As for article 11, the mandate of DISEC as a committee of General Assembly can be presented as, to promote the establishment and maintenance of international peace and security with the least diversion for armaments of the world's human and economic resources, after its reform in 1993[3,4]. The committee's responsibilities are spinning

[1] Un.org. (2019). *UN General Assembly - Functions and Powers of the General Assembly*. [online] Available at: http://www.un.org/ga/about/background.shtml [Accessed 5 Jan. 2019].
[2] Hrlibrary.umn.edu. (2019). *Charter of the United Nations: Chapter IV the General Assembly*. [online] Available at: http://hrlibrary.umn.edu/peace/docs/chapter4.html [Accessed 5 Jan. 2019].
[3] Un.org. (2019). *Chapter IV*. [online] Available at: http://www.un.org/en/sections/un-charter/chapter-iv/index.htm l [Accessed 5 Jan. 2019].

around issues of disarmament, global challenges and threats to peace, all of which imminently affect the international community. DISEC further searches for solutions to the challenges the stability of international security faces. Any disarmament and international security matter that appears in international stage, falls within the mandate of the Charter relating to the powers of the DISEC Committee[5].

3. Introduction to the Topic

The way the warfare is being conducted has been changing over the years, the decades, the centuries. Today knife and gun seem to be the last tool used and man to man battle has given its place to modern technology and its achievements. Drones or Unmanned Aerial Vehicles (UAV) and Big Data as modern technological achievements are often weaponized.[6] Drones comprising a new, at least with their current form, means of military weapon, thus there have been only a few recent attempts at regulating their operation, leaving space for countries with developed drone capacity to utilize them in multiple ways while their actions remain unpunished[7]. Big Data is something even newer and much more unknown in common life. This situation allows those having the know-how and the appropriate technology to use them against opponents for political or military purposes. Big Data seems to be the most up to date and most effective way of espionage among the states, while at the same time they can be the best way to prevent spying, based on who and how use them[8,9]. Potentially Big Data can underpin even cyber-attacks and consequently used as autonomous weapons.

Bearing in mind the aforementioned general information, in the next pages will follow a better explanation of the nature of Artificial Intelligence, how they are or can be used as weapons or means of spying and the dangers lurking, whenever types of Artificial Intelligence and Big Data are weaponised, fall into the hands of terrorist and spread without control or limitation.

4. Definition of key terms

Artificial Intelligence (AI): There is no universally agreed definition of AI. According to OECD and UNCTAD, AI is defined as "the ability of machines and systems to acquire and to apply knowledge and to carry out intelligent behaviour. This includes a variety of cognitive tasks such as but not limited to sensing, processing oral

---

[4] Un.org. (2019). *UN General Assembly - First Committee - Disarmament and International Security*. [online] Available at: http://www.un.org/en/ga/first/ [Accessed 5 Jan. 2019].
[5] Ibid
[6] Digital Trends. (2019). *Killer Drones: How We Can Detect Them And Defend Ourselves | Digital Trends*. [online] Available at: https://www.digitaltrends.com/cool-tech/weaponized-drone-defense-tech/ [Accessed 5 Jan. 2019].
[7] Stratfor. (2016). *The Unstoppable Spread of Armed Drones*. [online] Available at: https://worldview.stratfor.com/article/unstoppable-spread-armed-drones [Accessed 5 Jan. 2019].
[8] Allerin.com. (2019). *Big data and cyber espionage – you've got to know this!*. [online] Available at: https://www.allerin.com/blog/big-data-and-cyber-espionage-youve-got-to-know-this [Accessed 5 Jan. 2019].
[9] Završnik, A. (2018). Big data, crime and social control. New York: Routledge.

language, reasoning, learning, making decisions. They can also demonstrate an ability to move and manipulate objects accordingly. Intelligent systems use a combination of big data analytics, cloud computing, machine communication and the Internet of Things (IoT) to operate and learn"[10].

Big Data: UNECE (United Nations Economic Commission for Europe) has decided that Big Data are data sources that can be described as: high volume, veracity, velocity and variety of data that demand cost-effective, innovative forms of processing for enhanced insight and decision making[11,12]. However, the matter is not the amount of Data but how an organization or a corporation uses it and the range of its use.[13]

Weaponisation: Weaponisation, in general, is the process during which something gets equipped with arms or it is turned to a weapon[14].With the Weaponisation of AI, we refer to the construction or modification of a machine in order to perform as an autonomous lethal weapon without manual controlling[15]. The machine can behave intelligently and use melee or ranged weapons in absence of an operator[16]. Concerning Data they are weaponised, when applications, programs and algorithms are used in order to mine data of hundreds or million people in order to be exploited against them[17]. Most of the time the users have agreed previously with the storage of their Data, although they might not know how they are used[18].

Militarisation: Normally it refers to the process during which a society, state, party, group is organizing itself for military purposes or armed conflicts[19]. It can also refer to the process by which something or somebody is trained or modified in order to perform as a part of the military or for military activities and aims[20].

---

[10] Unescap.org. (n.d.). [online] Available at: https://www.unescap.org/sites/default/files/ESCAP_Artificial_Intelligence.pdf [Accessed 5 Jan. 2019].
[11] Unece.org. (2015). [online] Available at: https://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.44/2015/mtg1/WP18-Wirthmann_AD.pdf [Accessed 5 Jan. 2019].
[12] Unstats.un.org. (2015). [online] Available at: https://unstats.un.org/unsd/trade/events/2015/abudhabi/presentations/day3/01/2%20Classification%20of%20Big%20Data.pdf [Accessed 5 Jan. 2019].
[13] Sas.com. (n.d.). *What is Big Data and why it matters*. [online] Available at: https://www.sas.com/en_gb/insights/big-data/what-is-big-data.html?fbclid=IwAR1NJOvHwxL6IMCC0tqWKz1xB-TQysQqLUVC1MbxUrcVBR12l1yqMactZ-c#dmhistory [Accessed 5 Jan. 2019].
[14] Unidir.ch. (2018). [online] Available at: http://www.unidir.ch/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-artificial-intelligence-en-700.pdf [Accessed 5 Jan. 2019].
[15] Ibid
[16] Ibid
[17] Medium. (2018). *Data Weaponization and the Future of Privacy – RE: Write – Medium*. [online] Available at: https://medium.com/re-write/data-weaponization-and-the-future-of-privacy-d45a402048c6?fbclid=IwAR347sdJFs4uG5pqVNGfJLIEweXKLjEc2Y7W7B90ccC5dFdI6r789th9k54 [Accessed 5 Jan. 2019].
[18] Ibid
[19] Vocabulary.com. (n.d.). *Militarization - Dictionary Definition*. [online] Available at: https://www.vocabulary.com/dictionary/militarization [Accessed 5 Jan. 2019].
[20] Definitions.net. (n.d.). *What does militarization mean?* [online] Available at: https://www.definitions.net/definition/militarization [Accessed 5 Jan. 2019].

Unmanned Aerial Vehicle: An unmanned aerial vehicle (UAV), commonly known as remotely piloted aircraft or Drone is an aircraft without a human pilot aboard[21]. UAVs are a component of an unmanned aircraft system (UAS), namely an aircraft and its associated elements which are operated by no pilot on board. The flight of UAVs may be operated with various degrees of autonomy: either under remote control by a human operator or by onboard computers[22].

Espionage: the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government (political entity), a competing company or any other type of corporation[23]. Most of the countries characterize Espionage as the crime of spying, thus it is criminalized by their legislation.

Hybrid Warfare: "Hybrid Warfare consists a combination of two or multiple forms of warfare. It is clear that hybrid warfare refers to the simultaneous adoption of multiple modes of warfare"[24]. According to European Union hybrid threat "is a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat."[25]. On the other hand, hybrid conflict is a conflict during which the opponents refrain avoid the clash between their armed forces and focus instead on combination of military intimidation ("falling short of an attack"), on exploitation of economic and political vulnerabilities, and diplomatic or technologically advanced methods to achieve their aim. Lastly, hybrid war is conducted whenever a country combines the use of military force against another state or non-state actor with a composition of other means of pressure, such as but not limited to economic, political, and diplomatic compulsion[26].

5. History of the Topic

5.1 From Antiquity to Modern AI and BD

Big Data

Even though the notion of *Big Data* is relatively new and warm, their introduction dates back many years before the current surge in the volume of information. Their

---

[21] Unocha.org. (2014). [online] Available at: https://www.unocha.org/sites/unocha/files/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf [Accessed 5 Jan. 2019].

[22] Ibid

[23] Merriam-webster.com. (n.d.). *Definition of ESPIONAGE*. [online] Available at: https://www.merriam-webster.com/dictionary/espionage [Accessed 5 Jan. 2019].

[24] Tienhoven, M. (2016). IDENTIFYING 'HYBRID WARFARE'. [ebook] Leiden: Leiden University. Available at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/53645/2016_Tienhoven_van_CSM.pdf?sequence=1 [Accessed 5 Jan. 2019].

[25] Ibid

[26] Europarl.europa.eu. (2015). Understanding hybrid threats. [online] Available at: http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf [Accessed 5 Jan. 2019].

infancy took place during the 1940s and particularly in 1941 when for the first time the term 'information explosion' appeared.[27]

Long before the emergence of computers, there was a need to store, reproduce and analyze information. The last century, the volume of data that we get to manage increased rapidly and for that reason, on the grounds that technology evolved significantly, so did storing techniques, means and analysis so as to facilitate their management optimizing different tools, such as Internet and digital storage.[28]

Some of the fundamental milestones[29] of the developing idea of Big Data (BD) are:

- 1949: Survey about the capacity of data storage by 'the father of information theory' Claude Shannon
- 1965: The idea of 'First Data Centre' where all information would safely reside in
- 1997-2001: The Definition of Big Data – 2001 by Doug Laney described BD as a '3-dimensional data challenge of increasing data volume, velocity and variety'

Artificial Intelligence

The cradle of Artificial Intelligence lies around in antiquity, with myths, stories and rumours of artificial beings endowed with intelligence or consciousness. Its roots and the concept of intelligent machines may be found in Greek mythology.[30] Intelligent artefacts appear in literature since then, with real mechanical devices demonstrated to behave with some degree of intelligence. After World War II and the integration of modern computers in our life, complicated intellectual programs became a reality. From these programs, new tools were created which facilitated human lifestyle in many various fields such as technological (gadgets, smartphones, computers, vision systems), agricultural (food productions and industries) and last but not least medical (innovation of meds).[31]

The development of AI until today, based on chronological order:[32]

- 1965: First machines were constructed able to solve logic problems
- 1979: Stanford Cart and the first computer-controlled autonomous vehicle

---

[27] Forbes.com. (2013). A Very Short History Of Big Data. [online] Available at: https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#612725f065a1 [Accessed 10 Jan. 2019].

[28] Unstats.un.org. (2015). [online] Available at: https://unstats.un.org/unsd/trade/events/2015/abudhabi/presentations/day3/01/2%20Classification%20of%20Big%20Data.pdf [Accessed 5 Jan. 2019].

[29] DATAVERSITY. (n.d.). A Brief History of Big Data - DATAVERSITY. [online] Available at: https://www.dataversity.net/brief-history-big-data/# [Accessed 10 Jan. 2019].

[30] Aitopics.org. (n.d.). A Brief History of AI. [online] Available at: https://aitopics.org/misc/brief-history [Accessed 5 Jan. 2019].

[31] Richardson, J. (n.d.). Three Ways Artificial Intelligence is Good for Society - iQ by Intel. [online] iQ by Intel. Available at: https://iq.intel.com/artificial-intelligence-is-good-for-society/ [Accessed 10 Jan. 2019].

[32] Cress, M. (2018). HISTORY OF THE AI WORLD – Artificial Intelligence Mania. [online] Artificial Intelligence Mania. Available at: http://artificialintelligencemania.com/2018/06/11/a-history-of-the-ai-world/ [Accessed 10 Jan. 2019].

- 1985: Harold Cohen and his drawing program, Aaron
- 1990: Achievement of advanced applications[33] such as data mining, games, language translation, vision systems
- 1997: Garry Kasparov and the 'The Deep Blue Chess Program'
- 2000: Innovation of Robots
- Today: Some of the applications[34] that are used nowadays are: Siri (Apple's digital assistant), Amazon (AI in the form of transaction), Netflix (AI in the form of analyzing data for the suggestion of movies)

6. Legal Framework

The first side event on drones by the 1st Committee of the GA

Growth of artificial intelligence and the increased and excessive use of Big Data, as well as, the fact that these terms are relatively new to the world of Science and Knowledge, it is generally known that there is a lack of precise regulatory framework or multilateral treaties to surround the fields of Artificial Intelligence and Big Data.

However, in October 2015, an initiative by the Permanent Mission of Costa Rica to the United Nations, lead to a discussion on the proliferation of armed drones extending to its legal, ethical, and political perplexities arising from their use.[35] This initiative was the first that led to the introduction of the importance of understanding the uprising of that kind of technologies to the international community and draw its attention to construct a further binding legal framework for new technologies that might resolve issues that could occur.

It is necessary, though, to mention some conventions that have enlightened the fields of AI and Big Data.

6.1 Convention on Certain Conventional Weapons (CCW)

The purpose of the convention, also known as the Inhumane Weapons Convention, adopted in 1980, is to prohibit or decrease the use of weapons that are characterized the ones to cause avoidable or inexcusable torment to soldiers of enemy military forces or to involve civilians aimlessly. The Convention applied only to situations of international armed conflict. Realizing that most conflicts today occur within the borders of a State, it was more than urgent to conduct amendments to the Convention in order to make it applicable to non-international conflicts. After a long time of debates with no outcome, it is questioned if CCW is legally binding in the way that it is constructed or the states need to investigate other legal mechanisms to reach effectiveness in a legal level.[36]

---

[33] www.tutorialspoint.com. (n.d.). Artificial Intelligence Research Areas. [online] Available at: https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_research_areas.htm [Accessed 10 Jan. 2019].

[34] Adams, R. (2017). 10 Powerful Examples Of Artificial Intelligence In Use Today. [online] Forbes.com. Available at: https://www.forbes.com/sites/robertadams/2017/01/10/10-powerful-examples-of-artificial-intelligence-in-use-today/#78340bf6420d [Accessed 10 Jan. 2019].

[35] Un.org. (2015). *Discussing Drones at the UN Headquarters – UNODA*. [online] Available at: https://www.un.org/disarmament/update/discussing-drones-at-the-un-headquarters-2/ [Accessed10 Jan. 2019].

[36] Unog.ch. (n.d.). *Where global solutions are shaped for you | Disarmament | The Convention on Certain Conventional Weapons*. [online] Available at:

6.2 Treaty in Open Skies

Entered into force in 2002, established a regime of unarmed aerial observation flights over state territories and enhances mutual understanding of and increase transparency in military forces and activities[37]. Enhancing openness and transparency in military activities, the Treaty on Open Skies is one of the most wide-ranging international arms control efforts, promoted by the Organization for Security and Co-operation in Europe (OSCE).

6.3 Riga Declaration on remotely piloted aircraft (drones)

This declaration came up with a 'decisive step towards the future of aviation'. European regulators spotted the need to find innovative and sustainable ways to benefit from the use of drones, as well as to accomplish a developed safe provision of drone services in addition to establishing proportionate rules for that kind of new type of aircraft. From 2016 onwards, the European aviation community is committed to fulfil and act in a way that is compatible with the principles of the Riga declaration.[38]

6.4 Notice of Proposed Amendment (NPA)/ Technical Opinion (2015) by the European Aviation Safety Agency

In a world that it was more than clear that the challenging growth of the unmanned aircraft changed traditional aviation, the Notice of Proposed Amendment, which is legally binding for European member states, affected national aviation authorities, aviation industry, and manufacturers and operators of drones. The purpose of this NPA is to strengthen EU regulations on drone operations, in addition, to provide efficient pieces of information to all the involved stakeholders on the operations of drones[39].

6.5 UN Global Working Group on Big Data (GWG)

The UN Statistical Commission created in 2014, the UN Global Working Group on Big Data[40]. Considering the beneficial status of new data sources and technologies, the GWG addresses issues which are relevant with methodology, quality, technology, data access, legislation, privacy, management and finance, and provide efficient cost-benefit analyses[41]. Compatible with GWG's actions is the Big Data Conference, which is held annually for the purposes of discussing the progress of the Task Teams which are occupied to Mobile Phone Data Reports, Social Media Reports, Global Data Platforms and many other issues that concern GWG. The most important thing about

---

https://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B4C1257180004B1B30?OpenDocument [Accessed 7 Jan. 2019].

[37] Osce.org. (n.d.). [online] Available at: https://www.osce.org/library/14127?download=true [Accessed 7 Jan. 2019].

[38] Ec.europa.eu. (n.d.). [online] Available at: https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf [Accessed 7 Jan. 2019].

[39] Easa.europa.eu. (2015). [online] Available at: https://www.easa.europa.eu/sites/default/files/dfu/A-NPA%202015-10.pdf [Accessed 8 Jan. 2019].

[40] Division, U. (n.d.). — *UN GWG for Big Data*. [online] Unstats.un.org. Available at: https://unstats.un.org/bigdata/ [Accessed 8 Jan. 2019].

[41] Ggim.un.org. (2016). [online] Available at: http://ggim.un.org/meetings/2016-3rd_Mtg_EG_ISGI_Paris/documents/UN%20GWG%20Big%20Data%20presentation.pdf [Accessed 8 Jan. 2019].

GWG is illuminating the concept of Big Data and in addition to this, all these actions will actually boost the quality of official statistics[42].

7. Discussion of the Topic

7.1 Types of Artificial Intelligence and Big Data that are weaponised

Artificial intelligence and the use of Big Data, undoubtedly, can be (and in the future is likely to be) a definitive factor of success in boosting new aspects on research as well as on safety and security issues. Thus, it is crucial to examine which types of AI and Big Data are available to be weaponised.

The *lethal autonomous weapon system* is often defined as a system that can target and fire without substantial human control. As machines with embodied hardware and software, function separately from any other human control[43]. They, also, function on the basis of artificial intelligence, specifically in a way that algorithms assess a situational context and determine the corresponding response[44].

The majority of weapons systems, from UAS guided systems to defence batteries, are nowadays able to be autonomous albeit with varying stages of human control. Human controlled robots actually consist the main body of many countries' detecting system for spotting mines, traps or any other similar methods. It is more than urgent to understand that, even if lethal autonomous weapon system does not exist today, in the way that was previously explained, what currently human mind can practically manage and apply is very close to it.

As a category of computer science in general, it should not be forgotten that AI's main purpose is the creation of intelligent types of machines. In the view of its weaponisation, it is obvious that the only type of AI that is possible to cause various ethical, legal, and humanitarian problems and debates is *Artificial General Intelligence (AGI).* This type of AI, also known as Strong AI, or Human Level Artificial Intelligence, refers to a computer that is as smart as a human across the board—a machine that can perform any intellectual task that a human being can[45].

Baring in mind the possible sources of Big Data, on the other hand, it easily arrears to consist of streaming data, social media data, and publicly available sources.[46] The most likely to be weaponised, and threatened, are open data. Open data are produced by authorities, news media, universities, international organizations and other similar

---

[42] Division, U. (n.d.). *Meetings on Big Data for Official Statistics — UN GWG for Big Data*. [online] Unstats.un.org. Available at: https://unstats.un.org/bigdata/meetings.cshtml [Accessed 8 Jan. 2019].
[43] CNRS News. (n.d.). *A Guide to Lethal Autonomous Weapons Systems*. [online] Available at: https://news.cnrs.fr/opinions/a-guide-to-lethal-autonomous-weapons-systems [Accessed 8 Jan. 2019].
[44] Greene, T. (2018). *A beginner's guide to AI: Algorithms*. [online] The Next Web. Available at: https://thenextweb.com/artificial-intelligence/2018/08/02/a-beginners-guide-to-ai-algorithms/ [Accessed 8 Jan. 2019].
[45] Future of Life Institute. (n.d.). *Benefits & Risks of Artificial Intelligence - Future of Life Institute*. [online] Available at: https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/ [Accessed 8 Jan. 2019].
[46] Sas.com. (n.d.). *What is Big Data and why it matters*. [online] Available at: https://www.sas.com/en_gb/insights/big-data/what-is-big-data.html?fbclid=IwAR1NJOvHwxL6IMCC0tqWKz1xB-TQysQqLUVC1MbxUrcVBR12l1yqMactZ-c#dmhistory [Accessed 5 Jan. 2019].

organisations and institutions. They are freely accessible- sometimes by means of a user-friendly interface, at other times only as an excel-file and can also be merged. The importance of this kind of data is spotted precisely because of their free access. Nonetheless, there is plenty of previous cases and incidents, which happened to cause serious problems to governments, due to a leak of fake news, as well as, the spread of inaccurate news, in order to promote individual interests. One of the most known incidents took place in India, in August of 2012, where the spread of fake news, reached the peak of causing panic and a massive exodus of an estimated 30.000 people. Fear was, also, reinforced throughout social media, especially Twitter and Facebook.[47]

7.2 Ways of Militarisation of both Artificial Intelligence and Big Data

Nowadays, social media consist one of the most used big data resources, where it takes place the collection and restoring of responsive data, information[48]. Additionally, no one could deny that social media influence the majority of people who use them, on a regular basis. Therefore, those who actually tend to have the interest of spreading fear, or broaden terrorist attempts, tend to exploit accessibility of social media to notify those attempts[49].

For instance, every time that the Islamic State tends to attack, not in an actual way, by means of actual attacks, it finds the way to spread throughout social media, rumours, fake news, which are related to threats of safety and security, possible ongoing conflicts etc. That way, and on a global basis, it could cause fear, panic, and practically raise awareness in the wrong way[50].

In addition to the aforementioned ways, an important example of the weaponisation of Artificial Intelligence is that during Obama's presidency, from 2009 to 2017, the number of American troops in war zones dropped by around 90%, but there were 10 times more strikes from drones[51]. The United States of America plan to enable its Abrams tanks, to control robotic wingman vehicles to attack the enemy while protecting the manned tank.

7.3 Cybersecurity

There are two directions that could initially set the prospect of worrisome AI-aided cyber-attacks. The first is the increasing prevalence of cyber-attacks; even this year Russia attacked Ukraine, North Korea attacked Sony, and China attacked the U.S.

---

[47] Yardley, J. (2012). *Panic Radiates From Indian State of Assam*. [online] Nytimes.com. Available at: https://www.nytimes.com/2012/08/18/world/asia/panic-radiates-from-indian-state-of-assam.html [Accessed 8 Jan. 2019].

[48] Pew Research Center: Internet, Science & Tech. (2018). *Social Media Use 2018: Demographics and Statistics*. [online] Available at: http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/ [Accessed 8 Jan. 2019].

[49] Usip.org. (n.d.). [online] Available at: https://www.usip.org/sites/default/files/sr119.pdf [Accessed 8 Jan. 2019].

[50] Berger, J. (2015). *The Evolution of Terrorist Propaganda: The Paris Attack and Social Media*. [online] Brookings. Available at: https://www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/ [Accessed 8 Jan. 2019].

[51] Rohde, Walt, Traub and Cook (2012). *The Obama Doctrine*. [online] Foreign Policy. Available at: https://foreignpolicy.com/2012/02/27/the-obama-doctrine/ [Accessed 8 Jan. 2019].

Office of Personnel Management[52]. Secondly, the "Internet of Things" implies that an escalating number of mechanical devices will be attached to the internet. Considering that software exists to autonomously control them, many internet-enabled devices, such as cars, it is possible to be hacked and then weaponised. This may motivate a decisive military advantage in a short span of time. Such an attack could be activated by a small group of humans aided by AI technologies, which would make it hard to detect in advance. Unlike other weaponisable technology, it could be very difficult to control the spread of AI, since it does not rely on any specific raw materials[53].

Generally examining cybersecurity, it is known that it consists of technologies, processes and controls that are designed to protect systems, networks and data from cyber-attacks[54]. Effective cybersecurity reduces the risk of cyber-attacks and protects organisations and individuals from the unauthorised exploitation of systems, networks and technologies. Cybersecurity involves implementing controls that are based around three pillars: people, processes and technology.

Since the Russian Federation brought the issue of cybersecurity to the United Nations' agenda in 1998 there are spotted numerous legal actions that have been developing the international and regional legal framework concerning the cyber sphere[55]. Undoubtedly, future wars could be accompanied by cyber operations, which will be complementary to conventional means of warfare[56]. Militaries now possess cyber tools and in the case of conflict, it remains unknown if they will be used either offensively or in a defensive manner, along with the classical tools[57]. Cyberspace is nowadays assumed to be the fifth battleground, added to the sea, the earth, the air and space[58].

A significant threat to countries' prosperity and security in each and every field, concerning but not limited to industrial activities, national security and army, could be the upcoming espionage throughout the cyber field. Next-generation technologies such as Artificial Intelligence, actually, make it easier for those international actors, for instance, foreign intelligence services, to spy on other counties sensitive information[59]. Espionage is possible to be used for many reasons and in different ways. Access to networks individually or in a governmental way has raised concerns about the gain of access to information which should remain confidential. Despite

---

[52] Csis.org. (n.d.). [online] Available at: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity [Accessed 9 Jan. 2019].
[53] Medium. (2018). *A Brief History of Hacking Internet-Connected Cars – New World Crime – Medium*. [online] Available at: https://medium.com/s/new-world-crime/a-brief-history-of-hacking-internet-connected-cars-and-where-we-go-from-here-5c00f3c8825a [Accessed 9 Jan. 2019].
[54] Itgovernance.co.uk. (n.d.). *What is Cyber Security? | IT Governance UK*. [online] Available at: https://www.itgovernance.co.uk/what-is-cybersecurity [Accessed 9 Jan. 2019].
[55] Unsystem.org. (n.d.). *Action on Cybercrime and Cyber Security | United Nations System Chief Executives Board for Coordination*. [online] Available at: https://www.unsystem.org/content/action-cybercrime-and-cyber-security [Accessed 9 Jan. 2019].
[56] Theses.ubn.ru.nl. (2014). [online] Available at: https://theses.ubn.ru.nl/bitstream/handle/123456789/1178/Westerburger%2C_Steffen_1.pdf?sequence=1 [Accessed 9 Jan. 2019].
[57] Inss.org.il. (n.d.). [online] Available at: http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/2_Iasiello.pdf [Accessed 9 Jan. 2019].
[58] Ifpa.org. (n.d.). [online] Available at: http://www.ifpa.org/pdf/USAFreportweb.pdf [Accessed 9 Jan. 2019].
[59] Dni.gov. (n.d.). [online] Available at: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf [Accessed 10 Jan. 2019].

improvements in cybersecurity, cyber espionage extends to offer threat actors a comparably low-cost, high-yield field of approach to a broad spectrum of intellectual property or even the organization of military forces.

7.4 Proliferation of Weaponised Drones

During the 71st Session of the United Nations General Assembly First Committee on "New Challenges for States on Armed Drones Use and Proliferation" the interest of the stakeholders focused on the legality of using armed drones, and the importance of transparency[60]. Importance of Transparency was highlighted due to the current high level of secrecy in the sector of armed drones use[61]. Lack of transparency implies the possibility of inability to determine the legality of the use of weaponised drones[62]. An increasing number of countries and non-state actors interested to use both commercial and military drones may cause havoc considering the fragile status of international peace and security and the tense transnational relations[63]. The current situation along with the elation of terrorist attacks prove the international community's commitment to establish norms and international legal obligations on the use and transparency of drones.

Acquisition of drone technology does not automatically imply the necessary know-how demanded their operation. However, bearing in mind its accessibility and lack of transparency concerning their proliferation, no one could debar the possibility that militant groups will manage to have adequate information and knowledge to adequately operate weaponised drones[64]. At least access to new technology is one of the easiest tasks in the modern world, not to say an inevitable fact[65].

7.5 AI & BD into the hands of terrorism

Even though artificial intelligence has enabled improvements and efficiencies in many sectors, AI and Big Data not only can be used for positive applications but also they can be exploited by rogue States, criminals or terrorists.

As far as terrorism[66] is concerned, AI and BD can be used to either provoke martial tensions between States or social and political confusion. These are fake videos and intelligent bots (i.e. robots) with the aim of manipulating news, public opinion and governments, seize control of drones and autonomous vehicles which can be used in attacks or for blackmail, holding crucial infrastructures to ransom and armed drones

---

[60] Un.org. (n.d.). *The Drone Dialogues: New challenges for States on Armed Drones Use and Proliferation – UNODA*. [online] Available at: https://www.un.org/disarmament/update/the-drone-dialogues-new-challenges-for-states-on-armed-drones-use-and-proliferation/ [Accessed 5 Jan. 2019].

[61] Ibid

[62] Ibid

[63] Files.ethz.ch. (n.d.). [online] Available at: https://www.files.ethz.ch/isn/191911/CNAS%20World%20of%20Drones_052115.pdf [Accessed 5 Jan. 2019].

[64] Bulletin of the Atomic Scientists. (2017). *Militant groups have drones. Now what? - Bulletin of the Atomic Scientists*. [online] Available at: https://thebulletin.org/2017/09/militant-groups-have-drones-now-what/ [Accessed 5 Jan. 2019].

[65] Alyssa Sims, T. (2016). *The Consequences of Global Armed Drone Proliferation*. [online] The Diplomat. Available at: https://thediplomat.com/2016/07/the-consequences-of-global-armed-drone-proliferation/ [Accessed 5 Jan. 2019].

[66] Forbes.com. (2018). Weaponizing Artificial Intelligence: The Scary Prospect Of AI-Enabled Terrorism. [online] Available at: https://www.forbes.com/sites/bernardmarr/2018/04/23/weaponizing-artificial-intelligence-the-scary-prospect-of-ai-enabled-terrorism/#3d9243477b6d [Accessed 10 Jan. 2019].

with grenades (e.g.2017 Battle for Mosul– ISIS) for the harassment of opponents. [67] Also, instituted autonomous weaponised machines such 'killer robots' that will lead human to lack of control, especially in war situations and systems themselves to malfunction, "Virtual planner" models of terrorism via social media, in which operatives can offer recruitment, coordination of the target, timing of attacks and providence of technical assistance on topics like bomb-making. Last but not least, social-network mapping, artificial intelligence technology such as computer-synthesized voice created to deceive someone and forgery and manipulation of already existing data or information by technological bots.[68]

However, what needs to be underlined is that AI can also be utilized as an instrument of preventing and combating terrorism as well. As Facebook officially announced, artificial intelligence is applied to monitor and remove terrorist content from its platform.[69] The use of images-matching expedient to identify and prevent photos and videos from known terrorists, the machine-learning algorithms to search for patterns and trends in terrorist propaganda so as to be removed from the newsfeed of others and the establishment of an industry database that documents the digital fingerprints of terrorist groups and organisations can constitute remarkable applications by which terrorism can be countered.[70]

7.6 The exploitation of AI and BD in hybrid warfare

Hybrid warfare (HW) isn't something new. Its roots date since the Cold War and what has changed today is its scale, velocity and volume. It is used as an alternative solution for conventional military conflicts.[71] In HW the value of Artificial Intelligence and Big Data is undeniably significant and the relation between the two of them is very strong as they go hand in hand.

Using Big Data means analyzing opponents in every feature and orientation and that includes characteristics of society, geographic and demographic structure. Since HW can be carried out by military or non-military means such as diplomacy and political force, one way of Big Data exploitation is misinformation, that means gathering a large range of information, manipulate them to provoke political and later martial disorder.[72] Also, forms of propaganda (disruption of elections) and the produce of algorithms based on encrypted data consist a common and useful tool too.[73]

---

[67] Defense One. (2018). AI Experts List the Real Dangers of Artificial Intelligence. [online] Available at: https://www.defenseone.com/technology/2018/02/ai-experts-list-real-dangers-artificial-intelligence/146291/ [Accessed 10 Jan. 2019].
[68] Arxiv.org. (n.d.). [online] Available at: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf [Accessed 10 Jan. 2019].
[69] BBC News. (n.d.). Facebook's AI wipes terrorism-related posts. [online] Available at: https://www.bbc.com/news/technology-42158045 [Accessed 10 Jan. 2019].
[70] Forbes.com. (2009). [online] Available at: https://www.forbes.com/2009/06/18/ai-terrorism-interfor-opinions-contributors-artificial-intelligence-09-juval-aviv.html#3d3504e855a0 [Accessed 10 Jan. 2019].
[71] CNN.gr. (n.d.). Υβριδικός πόλεμος. [online] Available at: https://www.cnn.gr/news/politiki/story/26822/yvridikos-polemos [Accessed 10 Jan. 2019].
[72] Tat, E. (2017). The Strategic Race for "Algorithmic Warfare" and AI Development. [online] NAOC. Available at: http://natoassociation.ca/strategic-race-algorithmic-warfare-ai-development/ [Accessed 11 Jan. 2019].
[73] Greene, T. (2018). *A beginner's guide to AI: Algorithms*. [online] The Next Web. Available at: https://thenextweb.com/artificial-intelligence/2018/08/02/a-beginners-guide-to-ai-algorithms/ [Accessed 8 Jan. 2019].

Concerning Artificial Intelligence, emerging technologies have been always playing a crucial role. It draws more the attention, but not limited, to practical military actions, in addition to BD. Surveillance techniques, robots that execute missions on their own, the rise of unmanned aerial vehicles (UAVs) and their lethal use, mass usage of the precise weapon, special operations, and new technologies (microwave weapon and laser of directional energy),machine-learning services which are platforms that analyse the existing data and last but not least autonomous weapons, constitute some of the most fundamental, recent and perchance risky ways of AI's "rewiring" warfare.[74]

8. Conclusion

Considering all the aforementioned details it becomes crystal clear that Artificial Intelligence and Big Data can be used as autonomous weapons, occasionally lethal, or as a modern and effective, undetectable means of spying. Heavily dependent on technological development and research, they may be a privilege of a closed number of states with economic power to support and conduct relative programs. Taking into consideration the problems and dangers lurking due to their use and proliferation it is high time for international community to take the appropriate measures to prevent a future catastrophe, to regulate their proliferation, to formulate international norms concerning their use and of course to deter their spread into dangerous hands such as terrorist groups or radical militia. It is just a matter of time for an AI or Big Data incident to become a casus belli and to trigger new international security. As a matter of fact, dangers arousing from the use and proliferation of both Big Data and Artificial Intelligence affect international security and stability. Such imminent risks should be eliminated with the appropriate regulation in advance before the danger occurs.

9. Questions to be addressed

- How could each and every State control the Evolution of the Types of Artificial Intelligence as they exist nowadays, in a way that could tackle dangerous weaponisation of them?
- How can we reduce the exploitation of Big Data for the purposes of terrorist attacks and the spread of fear and fake news throughout them?
- What measures should be taken in order to prevent the exploitation of social media by terrorist groups?
- In what way could states' actions be monitored in the field of Artificial Intelligence and Big Data?
- What should be done in order to protect states from cyber-attacks? In addition, how could we reduce and control espionage methods in the cyber world?
- Should there be any limits on the use of AI and BD in hybrid warfare?
- How the proliferation of drones, military and commercial, can be more transparent and should there be any restrictions during transactions involving them?
- What measures have to be taken in order to prevent the acquisition of the necessary know-how and means for the weaponisation of drones by terrorist groups or paramilitary movements?

[74] Chathamhouse.org. (2017). [online] Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf [Accessed 10 Jan. 2019].

10.Bibliography

- Adams, R. (2017). 10 Powerful Examples Of Artificial Intelligence In Use Today. [online] Forbes.com. Available at: https://www.forbes.com/sites/robertadams/2017/01/10/10-powerful-examples-of-artificial-intelligence-in-use-today/#78340bf6420d [Accessed 10 Jan. 2019].
- Aitopics.org. (n.d.). A Brief History of AI. [online] Available at: https://aitopics.org/misc/brief-history [Accessed 5 Jan. 2019].
- Allerin.com. (2019). *Big data and cyber espionage – you've got to know this!*. [online] Available at: https://www.allerin.com/blog/big-data-and-cyber-espionage-youve-got-to-know-this [Accessed 5 Jan. 2019].
- Alyssa Sims, T. (2016). *The Consequences of Global Armed Drone Proliferation*. [online] The Diplomat. Available at: https://thediplomat.com/2016/07/the-consequences-of-global-armed-drone-proliferation/ [Accessed 5 Jan. 2019].
- Arxiv.org. (n.d.). [online] Available at: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf [Accessed 10 Jan. 2019].
- BBC News. (n.d.). Facebook's AI wipes terrorism-related posts. [online] Available at: https://www.bbc.com/news/technology-42158045 [Accessed 10 Jan. 2019].
- Berger, J. (2015). *The Evolution of Terrorist Propaganda: The Paris Attack and Social Media*. [online] Brookings. Available at: https://www.brookings.edu/testimonies/the-evolution-of-terrorist-propaganda-the-paris-attack-and-social-media/ [Accessed 8 Jan. 2019].
- Bulletin of the Atomic Scientists. (2017). *Militant groups have drones. Now what? - Bulletin of the Atomic Scientists*. [online] Available at: https://thebulletin.org/2017/09/militant-groups-have-drones-now-what/ [Accessed 5 Jan. 2019].
- Chathamhouse.org. (2017). [online] Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf [Accessed 10 Jan. 2019].
- CNN.gr. (n.d.). Υβριδικός πόλεμος. [online] Available at: https://www.cnn.gr/news/politiki/story/26822/yvridikos-polemos [Accessed 10 Jan. 2019].
- CNRS News. (n.d.). *A Guide to Lethal Autonomous Weapons Systems*. [online] Available at: https://news.cnrs.fr/opinions/a-guide-to-lethal-autonomous-weapons-systems [Accessed 8 Jan. 2019].
- Cress, M. (2018). HISTORY OF THE AI WORLD – Artificial Intelligence Mania. [online] Artificial Intelligence Mania. Available at: http://artificialintelligencemania.com/2018/06/11/a-history-of-the-ai-world/ [Accessed 10 Jan. 2019].
- Csis.org. (n.d.). [online] Available at: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity [Accessed 9 Jan. 2019].
- DATAVERSITY. (n.d.). A Brief History of Big Data - DATAVERSITY. [online] Available at: https://www.dataversity.net/brief-history-big-data/# [Accessed 10 Jan. 2019].
- Defense One. (2018). AI Experts List the Real Dangers of Artificial Intelligence. [online] Available at: https://www.defenseone.com/technology/2018/02/ai-experts-list-real-dangers-artificial-intelligence/146291/ [Accessed 10 Jan. 2019].
- Definitions.net. (n.d.). *What does militarization mean?* [online] Available at: https://www.definitions.net/definition/militarization [Accessed 5 Jan. 2019].
- Digital Trends. (2019). *Killer Drones: How We Can Detect Them And Defend Ourselves | Digital Trends*. [online] Available at: https://www.digitaltrends.com/cool-tech/weaponized-drone-defense-tech/ [Accessed 5 Jan. 2019].

- Division, U. (n.d.). — *UN GWG for Big Data*. [online] Unstats.un.org. Available at: https://unstats.un.org/bigdata/ [Accessed 8 Jan. 2019].
- Division, U. (n.d.). *Meetings on Big Data for Official Statistics — UN GWG for Big Data*. [online] Unstats.un.org. Available at: https://unstats.un.org/bigdata/meetings.cshtml [Accessed 8 Jan. 2019].
- Dni.gov. (n.d.). [online] Available at: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf [Accessed 10 Jan. 2019].
- Easa.europa.eu. (2015). [online] Available at: https://www.easa.europa.eu/sites/default/files/dfu/A-NPA%202015-10.pdf [Accessed 8 Jan. 2019].
- Ec.europa.eu. (n.d.). [online] Available at: https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf [Accessed 7 Jan. 2019].
- Europarl.europa.eu. (2015). Understanding hybrid threats. [online] Available at: http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf [Accessed 5 Jan. 2019].
- Files.ethz.ch. (n.d.). [online] Available at: https://www.files.ethz.ch/isn/191911/CNAS%20World%20of%20Drones_052115.pdf [Accessed 5 Jan. 2019].
- Forbes.com. (2009). [online] Available at: https://www.forbes.com/2009/06/18/ai-terrorism-interfor-opinions-contributors-artificial-intelligence-09-juval-aviv.html#3d3504e855a0 [Accessed 10 Jan. 2019].
- Forbes.com. (2013). A Very Short History Of Big Data. [online] Available at: https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#612725f065a1 [Accessed 10 Jan. 2019].
- Forbes.com. (2018). Weaponizing Artificial Intelligence: The Scary Prospect Of AI-Enabled Terrorism. [online] Available at: https://www.forbes.com/sites/bernardmarr/2018/04/23/weaponizing-artificial-intelligence-the-scary-prospect-of-ai-enabled-terrorism/#3d9243477b6d [Accessed 10 Jan. 2019].
- Future of Life Institute. (n.d.). *Benefits & Risks of Artificial Intelligence - Future of Life Institute*. [online] Available at: https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/ [Accessed 8 Jan. 2019].
- Ggim.un.org. (2016). [online] Available at: http://ggim.un.org/meetings/2016-3rd_Mtg_EG_ISGI_Paris/documents/UN%20GWG%20Big%20Data%20presentation.pdf [Accessed 8 Jan. 2019].
- Greene, T. (2018). *A beginner's guide to AI: Algorithms*. [online] The Next Web. Available at: https://thenextweb.com/artificial-intelligence/2018/08/02/a-beginners-guide-to-ai-algorithms/ [Accessed 8 Jan. 2019].
- Hrlibrary.umn.edu. (2019). *Charter of the United Nations: Chapter IV the General Assembly*. [online] Available at: http://hrlibrary.umn.edu/peace/docs/chapter4.html [Accessed 5 Jan. 2019].
- Ifpa.org. (n.d.). [online] Available at: http://www.ifpa.org/pdf/USAFreportweb.pdf [Accessed 9 Jan. 2019].
- Inss.org.il. (n.d.). [online] Available at: http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/2_Iasiello.pdf [Accessed 9 Jan. 2019].
- Itgovernance.co.uk. (n.d.). *What is Cyber Security? | IT Governance UK*. [online] Available at: https://www.itgovernance.co.uk/what-is-cybersecurity [Accessed 9 Jan. 2019].
- Medium. (2018). *A Brief History of Hacking Internet-Connected Cars – New World Crime – Medium*. [online] Available at: https://medium.com/s/new-world-crime/a-brief-history-of-hacking-internet-connected-cars-and-where-we-go-from-here-5c00f3c8825a [Accessed 9 Jan. 2019].

- Medium. (2018). *Data Weaponization and the Future of Privacy – RE: Write – Medium*. [online] Available at: https://medium.com/re-write/data-weaponization-and-the-future-of-privacy-d45a402048c6?fbclid=IwAR347sdJFs4uG5pqVNGfJLIEweXKLjEc2Y7W7B90ccC5dFdI6r789th9k54[Accessed 5 Jan. 2019].
- Merriam-webster.com. (n.d.). *Definition of ESPIONAGE*. [online] Available at: https://www.merriam-webster.com/dictionary/espionage [Accessed 5 Jan. 2019].
- Osce.org. (n.d.). [online] Available at: https://www.osce.org/library/14127?download=true [Accessed 7 Jan. 2019].
- Pew Research Center: Internet, Science & Tech. (2018). *Social Media Use 2018: Demographics and Statistics*. [online] Available at: http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/ [Accessed 8 Jan. 2019].
- Richardson, J. (n.d.). Three Ways Artificial Intelligence is Good for Society - iQ by Intel. [online] iQ by Intel. Available at: https://iq.intel.com/artificial-intelligence-is-good-for-society/ [Accessed 10 Jan. 2019].
- Rohde, Walt, Traub and Cook (2012). *The Obama Doctrine*. [online] Foreign Policy. Available at: https://foreignpolicy.com/2012/02/27/the-obama-doctrine/ [Accessed 8 Jan. 2019].
- Sas.com. (n.d.). *What is Big Data and why it matters*. [online] Available at: https://www.sas.com/en_gb/insights/big-data/what-is-big-data.html?fbclid=IwAR1NJOvHwxL6IMCC0tqWKz1xB-TQysQqLUVC1MbxUrcVBR12l1yqMactZ-c#dmhistory [Accessed 5 Jan. 2019].
- Stratfor. (2016). *The Unstoppable Spread of Armed Drones*. [online] Available at: https://worldview.stratfor.com/article/unstoppable-spread-armed-drones [Accessed 5 Jan. 2019].
- Tat, E. (2017). The Strategic Race for "Algorithmic Warfare" and AI Development. [online] NAOC. Available at: http://natoassociation.ca/strategic-race-algorithmic-warfare-ai-development/ [Accessed 11 Jan. 2019].
- Theses.ubn.ru.nl. (2014). [online] Available at: https://theses.ubn.ru.nl/bitstream/handle/123456789/1178/Westerburger%2C_Steffen_1.pdf?sequence=1 [Accessed 9 Jan. 2019].
- Tienhoven, M. (2016). IDENTIFYING 'HYBRID WARFARE'. [ebook] Leiden: Leiden University. Available at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/53645/2016_Tienhoven_van_CSM.pdf?sequence=1 [Accessed 5 Jan. 2019].
- Un.org. (2015). *Discussing Drones at the UN Headquarters – UNODA*. [online] Available at: https://www.un.org/disarmament/update/discussing-drones-at-the-un-headquarters-2/ [Accessed10 Jan. 2019].
- Un.org. (2019). *Chapter IV*. [online] Available at: http://www.un.org/en/sections/un-charter/chapter-iv/index.htm l [Accessed 5 Jan. 2019].
- Un.org. (2019). *UN General Assembly - First Committee - Disarmament and International Security*. [online] Available at: http://www.un.org/en/ga/first/ [Accessed 5 Jan. 2019].
- Un.org. (2019). *UN General Assembly - Functions and Powers of the General Assembly*. [online] Available at: http://www.un.org/ga/about/background.shtml [Accessed 5 Jan. 2019].
- Un.org. (n.d.). *The Drone Dialogues: New challenges for States on Armed Drones Use and Proliferation – UNODA*. [online] Available at: https://www.un.org/disarmament/update/the-drone-dialogues-new-challenges-for-states-on-armed-drones-use-and-proliferation/ [Accessed 5 Jan. 2019].
- Unece.org. (2015). [online] Available at: https://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.44/2015/mtg1/WP18-Wirthmann_AD.pdf [Accessed 5 Jan. 2019].

- Unescap.org. (n.d.). [online] Available at: https://www.unescap.org/sites/default/files/ESCAP_Artificial_Intelligence.pdf [Accessed 5 Jan. 2019].
- Unidir.ch. (2018). [online] Available at: http://www.unidir.ch/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-artificial-intelligence-en-700.pdf [Accessed 5 Jan. 2019].
- Unocha.org. (2014). [online] Available at: https://www.unocha.org/sites/unocha/files/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf [Accessed 5 Jan. 2019].
- Unog.ch. (n.d.). *Where global solutions are shaped for you | Disarmament | The Convention on Certain Conventional Weapons*. [online] Available at: https://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B4C1257180004B1B30?OpenDocument [Accessed 7 Jan. 2019].
- Unstats.un.org. (2015). [online] Available at: https://unstats.un.org/unsd/trade/events/2015/abudhabi/presentations/day3/01/2%20Classification%20of%20Big%20Data.pdf [Accessed 5 Jan. 2019].
- Unsystem.org. (n.d.). *Action on Cybercrime and Cyber Security | United Nations System Chief Executives Board for Coordination*. [online] Available at: https://www.unsystem.org/content/action-cybercrime-and-cyber-security [Accessed 9 Jan. 2019].
- Usip.org. (n.d.). [online] Available at: https://www.usip.org/sites/default/files/sr119.pdf [Accessed 8 Jan. 2019].
- Vocabulary.com. (n.d.). *Militarization - Dictionary Definition*. [online] Available at: https://www.vocabulary.com/dictionary/militarization [Accessed 5 Jan. 2019].
- www.tutorialspoint.com. (n.d.). Artificial Intelligence Research Areas. [online] Available at: https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_research_areas.htm [Accessed 10 Jan. 2019].
- Yardley, J. (2012). *Panic Radiates From Indian State of Assam*. [online] Nytimes.com. Available at: https://www.nytimes.com/2012/08/18/world/asia/panic-radiates-from-indian-state-of-assam.html [Accessed 8 Jan. 2019].
- Završnik, A. (2018). Big data, crime and social control. New York: Routledge.