The Evolution of Artificial Intelligence: Implications for Cybersecurity and Hybrid Warfare

Haleema Zia

Abstract

Artificial intelligence (AI) systems have been part of military technology since World War II, but evolution of AI and advancement in the field of machine learning, particularly deep learning created a paradigm shift in national security. Deep learning is a form of machine learning that enables computers to make intelligent decisions on its own by learning from experience. The emergence and increased dependence on smart machines capable of thinking and working like humans; has transformative influence on strategic competition, military and information superiority. With the rise of modern terrorism, the terrorist networks started adapting to emerging technologies in order to spread propaganda, extremist activities and cyber-attacks. Therefore, it is crucial for counter terrorism organizations to use AI techniques that are beneficial to disrupt terrorist propaganda and to counter hybrid warfare. Profound understanding and true implementation of AI techniques could help in improving cybersecurity, as it provides improved security performance against sophisticated cyber threats. AI combined with human insight has significant potential for national security and to mitigate the related concerns and risks. This paper has adopted qualitative research approach to provide a brief understanding of AI-enabled systems and its implications on cybersecurity and hybrid warfare in order to disrupt terrorist attacks. It gives an insight on how AI evolution and progress has potential to become a transformative national security tool, at par with aircrafts, computer systems, bio-tech, and nuclear weapons.

Keywords: Artificial Intelligence (AI), evolution, cybersecurity, modern warfare, hybrid warfare

Introduction

Terrorism recurs throughout the human history, as the waves of terrorism keeps on transforming. In the earlier globalization era (1878-1914), the anarchists steered a terrorist campaign that crested in World War I [1]. Since the last third of the twentieth century to the present-day fundamentalists and leftists functioned transnational terrorism - crossing borders and staging terrorist attacks in foreign capitals, in order to capture world attention on their cause[2]. The recent wave of transnational terrorism has given rise to the evolution of dynamics and social structures of terrorist organizations and counter-terrorism institutes. Both terrorist networks and counter-terrorism organizations have continued to adapt to changing environments and emerging innovative technologies. With the rise of transnational terrorism, social network analysis has become a key utility for the counter-terror organizations for assessing and understanding perspectives of terror networks, and for the development of strategies to neutralize and disrupt terror attacks[3]. Conventionally, the term terrorism is often used for the criminal activities of non-state actors and groups including bombings, kidnappings, and assassinations. Terrorist groups have their own ideologies and are generally composed of non-state actors; some of these are created on the basis of religious fanaticism while some

[1] Sandler, Todd, Daniel G. Arce, and Walter Enders. "Transnational terrorism," *Global crises, global solutions* 2 (2009): 516-62.

[2] Sandler, Todd, Daniel G. Arce, and Walter Enders. "Transnational terrorism." *Global crises, global solutions* 2 (2009): 516-62.

[3] Michael Aondona, Chiangi, "A Theoretical Conception of Modern Terrorism: David Rapoport's Four Waves Theory," *Available at SSRN 3498569* (2019).

are on political a ground, which ultimately ends up producing hatred and terror.

The definition of terrorism is still blur and dialectical[4]. As there is no consensus on the definition of terrorism and all terrorist groups are having their own justifications and ideologies which they keep on disseminating, for instance, a person may be considered as a terrorist by some people and a freedom fighter by others. Therefore, it is crucial to consider the fact that terrorists use illegal means often violently in order to hasten the political change process, as their actions are effective and justifiable to them. Even in the absence of a clear definition of terrorism, researchers have figured out three important factors in the concept of terrorism. Firstly, terrorists are generally non-state actors that try to influence public through violence and terror. Secondly, terrorists are aimed to make a political change by attracting attention of general public and to stimulate responses. Thirdly, terrorists purposefully attack the innocent people in order to spread fear, anxiety and terror to make a narrative[5].

Modern terrorism evolved near the end of 18th century after the French Revolution[6]. There are two significant factors that influenced the expansion of terrorism i.e., evolution of modes of communication and invention of new methods of transportation[7]. This has eventually shaped the new global dimension of the modern terrorism, as the information

[4] Jean E. Rosenfeld, ed. "*Terrorism, identity, and legitimacy: the four waves theory and political violence*. Routledge", 2010.

[5] Bruce Hoffman, "Inside Terrorism New York," *NY: Columbia University Press [Google Scholar]* (1998).

[6] Walls, Erin, "Waves of Modern Terrorism: Examining the Past and Predicting the Future," PhD diss., Georgetown University, 2017.

[7] Gerard Chaliand, and Arnaud Blin, eds. "*The history of terrorism: from antiquity to al Qaeda*. Univ of California Press," 2007.

spread was much faster through media and other innovative technologies and people were able to travel beyond national borders through modern ways of transportation. In the late 19th century, spreading propaganda through pamphlets became a tool of Russian anarchists to change mindset of people in order to achieve ideological objectives[8]. Vietnam War triggered off the New Left wave, as the role of United States in the war induced an increased hatred for the US especially among the developing countries[9]. After this New Leftists wave, there was drawn a clear distinction line between West and East, vindicating the Soviet support in the form of intelligence, aid, logistics, and other resources to violent terrorism organizations in Europe, Asia and also in the Middle East. In the same era, Cold War characterized by ideological conflicts and state sponsored terrorism started spreading widely. In the New Left Wave ideology of radicalism was combined with nationalism that spread rapidly because of the advanced media, communication and technological development[10]. The world today is experiencing terrorism in the name of religion. The misinterpretation of Jihad and the fusion of terrorist ideologies with the religious beliefs are distressing[11].

The Iranian revolution along with the Afghan invasion is seen as a precursor to Islamist radicalization in the decades to come. This motivated Muslims to defend their faith and has also stimulated fourth religious wave

[8] Walls, Erin, "Waves of Modern Terrorism: Examining the Past and Predicting the Future," PhD diss., Georgetown University, 2017.

[9] Walls, Erin, "Waves of Modern Terrorism: Examining the Past and Predicting the Future," PhD diss., Georgetown University, 2017.

[10] Michael Aondona Chiangi, "A Theoretical Conception of Modern Terrorism: David Rapoport's Four Waves Theory," *Available at SSRN 3498569* (2019).

[11] Gerard Chaliand, and Arnaud Blin, eds. "*The history of terrorism: from antiquity to al Qaeda*. Univ of California Press," 2007.

of terrorism[12]. This wave of terrorism is very unique and different from all other waves of terrorism because its methods and operations appear in different manifestations. The uses of religion in violence, fundamentalism and spread of ideologically extremist organizations especially Al-Qaeda and ISIS (Islamic State of Iraq and Syria) have grabbed special attention across the global affairs. In future, this could become one of the prominent and important features of international terrorism. These radical groups and organizations have fully equipped themselves with technology and advanced intelligence systems in order to create a greater impact[13].

The distinction between peace and war has become blurred due to the extensive usage of innovative technologies and AI. The term hybrid warfare became common since 2010, which includes the blended methods of war i.e. conventional, unconventional, and irregular war. Hybrid warfare is a combination of intelligence systems along with new technologies and fanatical fighting style, irrespective of the state structures or compliance to the armed related conflict laws. Both state and non-state actors are involved in conducting hybrid warfare. State actors in this kind of warfare employ proxies in order to evade detection. Hybrid warfare also incorporates undiscriminating violence, felonious disorder, terrorist acts, and cyber warfare -which are attempts to damage and or completely destroy computer systems and information networks of another nation through cyber-attacks, computer viruses, and denial-of-service attacks[14].

[12] Denys Proshyn, "Breaking the Waves: How the Phenomenon of European Jihadism Militates Against the Wave Theory of Terrorism," *International Studies. Interdisciplinary Political and Cultural Journal* 17, no. 1 (2015): 91-107.

[13] Michael Aondona, Chiangi, "A Theoretical Conception of Modern Terrorism: David Rapoport's Four Waves Theory," *Available at SSRN 3498569* (2019).

[14] Farman Kakar, “Hybrid Warfare and Pakistan,” *The News International,* January 13, 2019.

The hybrid warfare has a far-reaching impact across national governments, societies, and multinational corporations and institutions. Artificial Intelligence (AI) related technological advancements and innovations could have unpretentious consequences for military applications and operations, which includes tactical battlefield as well as strategic perspectives. AI related technologies broadly include big data, quantum computing, and the 'internet of things', robotics, miniaturization, and autonomy[15].

AI has the potential to bring military power along with the repercussions of re-ordering the power balance[16]. The geopolitical competition between different countries especially, China and the U.S. have forced them to construct AI related capabilities, as it has become a precarious element of national security[17]. A series of studies were conducted by the U.S. Department of Defense (DoD) and it released a report titled National Artificial Intelligence Research and Development Strategic Plan in 2016, describing the AI potential to reinvigorate U.S. military dominance[18]. In the quest to become technologically equipped superpower, a national level Artificial Intelligence agenda was launched by Beijing for "civil-military

[15] James Johnson, "Artificial intelligence & future warfare: implications for international security," *Defense & Security Analysis* 35, no. 2 (2019): 147-169.

[16] Kareem Ayoub, and Kenneth Payne. "Strategy in the age of artificial intelligence." *Journal of strategic studies* 39, no. 5-6 (2016): 793-819.

[17] Robert O. Work, "Remarks by defense deputy secretary Robert work at the CNAS inaugural national security forum," *Center for a New American Security* 14 (2015).

[18] "The National Artificial Intelligence Research and Development Strategic Plan," *National Science and Technology Council,* (Washington: Executive Office of the President of the United States), October, 2016, https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf (accessed February 5, 2021).

fusion" with Chinese characteristics.[19] Russia has also triggered 35% of the structure of its military forces to become robotic by 2025.

AI technologies have a greater potential to enable and multiply the wide-ranging range military applications, but it also poses security threats for the LEAs (Law Enforcement Agencies) because of the enhanced AI - technologies being used by the extremist organizations and terrorist groups. AI is very important methodology to counter cyber terrorism and cybersecurity threats in the present era. According to defense experts AI will be having an evolutionary, if not revolutionary, influence on future warfare and autonomy. Advances in AI technologies and robotics have the tendency to intensify the absolute power of all types of actors, but the relative power balance might remain with the leading nation states[20]. National level initiatives and objectives are demonstrating acknowledgment by global security community of military-technical technical upheaval and transformative potential of AI technologies for national security as well as strategic calculus of nations[21].

Artificial Intelligence (AI) and Countering Hybrid Warfare

Artificial Intelligence (AI) is defined as the digital technology usage in order to construct such systems which are proficient enough to perform

[19] The State Council Information Office of the People"s Republic of China, „State Council Notice on the Issuance of the New Generation AI Development Plan", July 20 2017, http://www.gov.cn/zhengce/content/2017 -07/20/content_5211996.htm.(accessed February 5, 2021).

[20] Daniel S. Hadley and Lucas J. Nathan, "Artificial intelligence and national security," Congressional Research Service, Washington, November 10, 2020, https://fas.org/sgp/crs/natsec/R45178.pdf, (accessed February 5, 2021).

[21] James Johnson, "Artificial intelligence & future warfare: implications for international security," *Defense & Security Analysis* 35, no. 2 (2019): 147-169.

various complex tasks which require intelligence[22]. Multi Capability Development Campaign (MCDC)'s project document titled Countering Hybrid Warfare defined the hybrid warfare as the orchestrated use of multiple power instruments that are tailored to explicit vulnerabilities across the broad-ranging societal functions in order to achieve synergic effects[23]. The impact of AI on hybrid warfare can be explained by studying the stages of AI development. The Artificial Intelligence development usually involves three tiers. Firstly, Artificial Narrow Intelligence (ANI) – which denotes machine intelligence that is considered equal to and in some instances, exceeds human intelligence to perform specific tasks. Secondly, Artificial General Intelligence (AGI) – which discusses machine intelligence meeting the full range of human intelligence across any kind of task. Thirdly, Artificial Super Intelligence (ASI) – denotes machine-based intelligence that has capacity to exceed human intelligence across any task. Currently, only ANI technologies are widely available and have significant implications on hybrid warfare[24].

The term warfare intends to signify the adversarial, serious, enduring, and hostile nature of the challenge. It also describes hybrid aggressor's ability to create war-like effects and outcomes through weaponization of non-military means that the hybrid warfare might be employed to set such conditions in order to accelerate future conventional aggression in a more effective way. The challenge for LEAs (Law Enforcement Agencies) and

[22] Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe et al.,"The malicious use of artificial intelligence: Forecasting, prevention, and mitigation," *arXiv preprint arXiv:1802.07228* (2018).

[23] Farman Kakar, "Hybrid Warfare and Pakistan," *The News International,* January 13, 2019.

[24] Spiegeleire De Stephan, Matthijs Maas, and Tim Sweijs. *Artificial intelligence and the future of defense: strategic implications for small-and medium-sized force providers*. The Hague Centre for Strategic Studies, 2017.

other military and Intelligence organizations and think tanks is to detect the hybrid threat in order to introduce relevant operational methodologies and make strategies to neutralize it. The actions taken in order to counter hybrid warfare should be of specific nature, degree, and type of the threat or attack. In order to make efforts to counter hybrid warfare, it is important to set realistic strategic goals – in order to disrupt hybrid aggression, identify appropriate thresholds – which could vary according to the type of aggression and vulnerability to get targeted and also according to the counter action capacity, and design and implement a relevant strategy. The design and strategy could be based on three components including detection, deterrence, and response[25].

Implications of Artificial Intelligence (AI)

Artificial Intelligence and advanced machine learning techniques play a vital role in detection of possible hybrid threats. It also requires updating warning intelligence through anticipation and pattern recognition. Deterring hybrid aggressors require building exclusively on traditional deterrence approaches in order to pursue reliable measures with the help of horizontal escalation, which is communicated and tailored to the aggressors. These are usually balanced between deterrence by denial, which includes punishment and resilience. Responding to hybrid aggressors, threats, and attacks could be done by implementation of appropriate arrangements and measures at any stage of the cycle of hybrid threats. The hybrid threat cycle includes processes from identification of potential vulnerabilities to resilience building activity, in response to a hybrid attack.

[25] MCDC, (2017), Information Note, "What is Hybrid Warfare? sets out the wider understanding which forms the baseline assessment for this handbook", (see Chapter 3).

Developing institutional machinery and AI technologies is very important for implementation of these measures to counter hybrid threats, through government and multinational institutions. The advancements in technology and trends in power and interdependence have caused growing trends in the use of hybrid warfare[26]. Rapid and advanced developments in AI provide innovative capabilities to military as well as non-military domains. Consequently, not only war hardware will be transformed but it will also affect human dimension in warfare. The impact of AI applications on hybrid warfare can be described and explained through synergic use of five different instruments and means of power called MPECI - Military, Political, Economic, Civil and Informational, which are used to exploit enemies' vulnerabilities.

The military dimension includes using such military systems that are AI-enabled, which includes aquatic, aerial and ground robots. Although these AI-enabled technologies provide great autonomy and expert reasoning in the warfare but they cannot operate without human insight. Great progress is made on the use of AI based weapons and technologies, for instance; Israel has deployed fully automatic self-driving military automobiles to patrol the border along Gaza strip and has future plans to fully equip these autonomous robots with military weaponries for deployment along the borders of Egypt, Jordan, Syria, and Lebanon[27].

The Centre for a New American Security and Bard College, collected a database according to which there are almost 150 Unmanned Aerial Vehicles (UVAs) being used by 48 countries by 2017, ranging from

[26] Global Strategic Trends – The Future Starts Today, UK Ministry of Defence (2018), page 125-147, https://www.gov.uk/government/publications/global -strategic-trends (accessed February 5, 2021).
[27] Elie Perot, "The blurring of war and peace," *Survival* 61, no. 2 (2019): 101-110.

hummingbird size i.e. Black Hornet mini-copter to the massive size of RQ-4 Global Hawk i.e. 15,000 pound[28]. Other than robotics and autonomous weaponry, AI-enabled command and control systems have shown immense potential and utility in dealing with information overload, refining situational alertness, disrupting and neutralizing enemy propaganda, and recommending and formulating certain strategies and courses of action. The advanced and automatic deep learning machine systems have capacity to view the patterns of hybrid warfare in order to give early warnings to the military and state actors that something suspicious is going to happen in the grey zone conflict areas. In this way, these AI based command and control systems are also capable to respond to such events rapidly and under briskly shrinking engagement windows. There are an increasing number of companies that are making predictions while claiming to analyse big online data through machine learning algorithms and to detect events 1-10 days ahead. Predata – a U.S. consulting firm claims that they are using smart AI-enabled metadata to predict any possible events of geographical, market-moving, or security nature[29]. Because of the surveillance and reconnaissance through the use of AI based drone systems, it is easy to detect potential threats and lead to greater stability of states through enhanced monitoring of grey zone or trouble areas, thereby reducing covert or hybrid operations.

While considering the political dimension, it is evident that AI-enabled technologies and tools e.g., bots (automated accounts) and impression accounts on social media platforms are used to conduct disinformation

[28] Jon Walker, "Unmanned Aerial Vehicles (Uavs) –Comparing the USA, Israel, and China," (2017).

[29] Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare," *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917.

campaigns by different countries in order to destabilize political narrative of west, sow divisions within different countries and also to blur the distinction line between fact and fiction. Machine intelligence was also actively used in U.S. election campaigns e.g., according to Cambridge Analytica – a data science firm claims that during the U.S. presidential elections 2016, an extensive advertising campaign was launched in order to influence voters on the basis psychology of each individual. Similarly, in 2017 general elections in the UK massive groups of political bots were used for spreading fake news and misinformation on social media, which helped building public opinion in a certain way[30].

The economic dimension of AI can be explained in the context of hybrid warfare, when the states are targeted, they tend to counter attack by economic coercion e.g., economic isolation and financial cut-off become the ultimate choice of states. AI based tools are used for optimizing capital investment, assessing credit quality, regulatory compliance, trading transaction, and fraud detection purposes.

As far as civil dimension is concerned, there are certain AI-enabled tools that distort public opinion and spread digital propaganda. AI have great utility in the information domain, as it is an important domain for shaping political discourse, influencing perceptions of people, and changing the political outcome through manipulation of information availability. In the age of narrow AI, the hybrid warfare can be depicted in one picture by combining all the five dimensions. The inclusion of Artificial Intelligence

[30] Polonski, Vyacheslav W. Polonski, "How Artificial Intelligence Conquered Democracy," August 2017, https://www.independent.co.uk/news/long_reads/artificial-intelligence-democracy-elections-trump-brexit-clinton-a7883911.html (accessed February 21, 2021)

in the hybrid warfare will not obsolete the traditional ways of fighting the wars because the term 'hybrid' itself implies that there is a significant role of both low-end techniques and methods i.e., suicide bombings, IEDs (Improvised Explosive Devices), pistol and dagger, as well as AI-enabled high-end tools and techniques[31].

Hybrid Warfare: the blurring of War and Peace

The ambiguity related to hybrid warfare has blurred the war and peace boundary[32]. The cold war concerning the United States of America and the Soviet Union and hybrid warfare –which is considered as post-Cold War phenomenon, has made it clear to the International Relations practitioners and other experts that politics of the world can not only be seen and studied separately through the peace and war lens. According to a recent NATO summit declaration, increased pressure and challenge from state and non-state actors is being faced by different nations. These state as well as non-state actions are using hybrid activities in order to create ambiguity and to distort the distinction line between peace, conflict, and crisis[33]. Hybrid Warfare is becoming a very popular term but also a controversial one in the military and academic discourse. The term hybrid warfare is not yet clearly defined, as it is given certain meanings and definitions by different International Relations experts, academicians, observers, and military practitioners through the observation of enemies' activities. With changing circumstances, the competitors also change their tactics of

[31] Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare," *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917.

[32] Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare," *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917.

[33] Elie Perot, "The blurring of war and peace," *Survival* 61, no. 2 (2019): 101-110.

fighting in order to adapt to the changing environments. As a result, researchers are continuously in a process of finding novel characteristics and distinctive dimensions of hybrid warfare. In broad terms, it is considered to be a combination of fanatic fighting styles and new technologies which are being used by non-state actors as well as by state actors through covert operations. The differences in training, weapons, equipment, and skills between contemporary regular and irregular tactics created a new environment.

Gray-zone tactics or hybrid warfare has posed incessant challenges to defense area. The state actors use incremental tactics and paramilitary forces for achieving security objectives as well as political aims without stimulating the war response. The combinational military means usage with that of non-military is considered to be the protrusive element of hybrid warfare[34]. According to Alex, usage of technology plays a crucial role in conducting warfare; however, James Mattis and Frank Hoffman downplayed the role of technology in warfare[35]. It is not because technology does not have impact but its fascination by military professionals has blinded them to the importance and preponderance of humans in the warfare. The term hybrid relates to more than blurring and cross-breeding of regular and irregular tactics. Some researchers and experts view hybrid warfare as a conflict which involves a amalgamation of state and non-state actors i.e. conventional military forces as well as irregulars (insurgents, guerrillas, and terrorists), focused to achieve

[34] Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare," *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917.

[35] Alex Ronald, "War and Technology," *Foreign Policy Research Institute*, February 27, 2009. https://www.fpri.org/article/2009/02/war-and-technology/ (accessed February 21, 2021).

political objectives. In the current security environment AI is considered to be the most disruptive technology and its combination with variability of irregular tactics will soon render the cognizance of hybrid warfare obsolete[36].

There are five salient features of hybrid warfare which are as follows;

i. ***Synergy*** - it is the first characteristic of hybrid warfare i.e., synergy involves the synergistic use of various means across MPECI spectrum in order to manipulate the intensity and process of hybrid warfare. The hybrid actors will use all possible means for attainment of desired effects targeting political and psychological domains, which are based on the political goals, enemy weaknesses, and the available capability[37].

ii. ***Ambiguity*** - the second characteristic of hybrid warfare is ambiguity which explains the obscure boundary between war and peace. Although war and peace are traditionally considered to be the opposite manifestations, but hybrid warfare has made this distinction ambiguous by using such features and activities that challenge easy categorization and distinction between the two phenomena[38]. Ambiguity also refers to obscuring combatants' identity in war, as the states may deploy different troops without emblems and also use proxies in order to hide identity of agency.

[36] Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare," *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917.

[37] Elie Perot, "The blurring of war and peace," *Survival* 61, no. 2 (2019): 101-110.

[38] Reichborn-Kjennerud, Erik, and Patrick Cullen. *What is hybrid warfare?.* Norwegian Institute for International Affairs (NUPI), 2016, https://brage. bibsys.no/xmlui/bitstream/id/411369/NUPI_P (accessed on February 21, 2021)

There are several instances when civilians convert to war fighters in disguise.

iii. ***Asymmetry*** **-** the third characteristic of hybrid warfare is asymmetry which denotes that the propensity of state and non-state actors is not equal, as state actors are well-equipped with advanced technological weapons and training skills in comparison with non- state actors. However, there is an advantage to non-state actors as they do not operate under the state law and therefore can launch terrorist attacks by criminal and illegal means. In contrast, state actors are confined by the law and despite a few exceptions; they cannot launch counterattacks, ignoring the legal norms[39]. There are many instances when non-state actors use violent extremist ideologies in order to achieve their objectives, but state actors are confined by war ethics and are always duty-bound.

iv. ***Disruptive Innovation*** - the disruptive innovation is the fourth characteristic of hybrid warfare, which is done at tactical levels or for operations for achieving strategic objectives. State actors ensure this through different activities including rapid mobilization of non-attributable forces and disinformation campaigns in cyber domain as well as media. The non-state actors use disruptive innovation through terrorist attacks, suicide bombings, and repetitive use of modern commercial technology, increased military

[39] Elie Perot, "The blurring of war and peace," *Survival* 61, no. 2 (2019): 101-110.

sophistication e.g., using UAVs and anti -ship, secure communication channels, command and control systems[40].

v. ***Battle Over Psychology*** –which is the fifth important characteristic of hybrid warfare, denotes psychology of target population including the home front population, the conflict zone population, and the population of international community[41]. The state or the non-state actors both attempt to win battle over psychology by presenting their ideologies, loyalties and agendas to population under concern by use of Artificial Intelligence and through various mediums including social media. Therefore, the non-state actors try to make efforts to strike a lethal blow on the enemies and amplify their success through propaganda and disinformation campaigns especially through social media. However, the state actors tend to intimidate but economize the military equipment usage and armaments for psychologically pressurizing the target population.

All the above-mentioned factors are very crucial in defining the victory or defeat of certain state or non-state actors in the hybrid warfare. The use of AI means, hybrid warfare characteristics, and information revolution using social media applications. Thus, it is evident that the success or failure in hybrid warfare depends less on military gain or loss and more on perceived psychological win or loss.

[40] Vladimir I. Batyuk, "The US concept and practice of hybrid warfare," *Strategic Analysis* 41, no. 5 (2017): 464-477.

[41] Elie Perot, "The blurring of war and peace," *Survival* 61, no. 2 (2019): 101-110.

Information Revolution and Cybersecurity

The internet relies too much on communication infrastructure just like that of telephone system which was an important communication tool a century ago. The information revolution and technological underpinnings of the internet are varied in nature from that of any other telecommunication network or infrastructure. Because of information revolution and increased use of social media, the spread of fake news and reports have become faster. The terrorist organizations that are using hybrid methods to spread terrorism and extremism have been launching successful operations with the help of educated civilians and social media users, as they unintentionally spread their agenda in the form of social media news, pamphlets and twitter trends. In this way, the social media users become the voice of hybrid terrorist groups against the state actors without actually realizing or knowing the agenda behind it. As the world is becoming more digitalized day by day and data is stored on digital and electronic devices, therefore, the nature of attacks or threats is also transforming. There is a need to secure cyberspace and ensure reliable services in order to protect sensitive data and information.

The War against Truth: Understanding Deepfake

The advent of Artificial Intelligence has offered advanced tools and technologies of spreading disinformation and digital propaganda in order to influence the civil society. AI can be used to make real like fabricated video and audio messages to create short-term effect and chaos in public. For instance, such fake news and videos can create shock and cause panic, disorder and intense damage to the public. Most of the times, such messages are created to spread a short-term wave, as public will eventually find out the truth behind the propaganda. The Deepfake technology emerged in 2017, when members of a community developed software to insert facial images from one video to another and then released the edited content through social media platforms. Initially, this was done for entertainment purposes but from 2018 to 2019, several organizations also started adopting deepfake technology in order to release thousands of multimedia texts on Facebook, YouTube, Twitter, and Telegram etc. which attracted quite a large number of public [42]. The rapid spread of tools and services has lowered the barriers for non-experts to create deepfake by using voice audio of non-existent people to enhance social engineering against their target groups. In 2016, Afghan Taliban started using camera - equipped commercial drones in order to film such propaganda footage to misguide pubic and gain their sympathies. In the recent times, video and audio are no more considered as reliable records of reality[43].

The text and video messages created through deepfake technology affected public figures, politicians and others involved in conventional, role-related conduct. Through deepfake technology it has become easy to create fake content showing public officials taking bribe, uttering racial epithets, and engaging in adultery[44]. False videos can also affect the morale of armed forces, as forces can be seen killing innocent civilians in the war zone, which could lead to unrest or violence in the society. There are several instances when false audio messages were circulated in order to create

[42] Ajder, Henry, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen. "The state of deepfakes: Landscape, threats, and impact." *Amsterdam: Deeptrace* (2019).

[43] Franz J. Marty, “Fire from the Sky: The Afghan Taliban‟s Drones”. December 22, 2020. https://thediplomat.com/2020/12/fire-from-the-sky-the-afghan-talibans-drones/ (accessed on April 29, 2021).

[44] Bryan C. Taylor, "Defending the state from digital Decei t: the reflexive securitization of deepfake," *Critical Studies in Media Communication* (2020): 1-17.

chaos and disturbance in the country. Deepfake has also made significant impact on the political arena. For instance, two ground-breaking cases from Malaysia and Gabon proved that deepfake was linked to a political smear campaign and an alleged government cover-up. One of the two cases was associated with an attempted military coup while the other one has continued to threaten a high-profile politician with imprisonment[45]. Social media acts as a catalyst for several prevalent movements to degenerate into political upheaval and social unrest in societies that are already suffering from unemployment, poverty, corruption, poor political leadership, and social discontent.

AI based bots can be used for denial-of-information attacks as well as information flooding attacks, in order to swamp the information channels with noise so that people may not find correct information. Similarly, hybrid actors are capable of producing fake videos of terrorist attacks for creating panic in order to achieve political objectives. AI-enabled technologies are also used to manipulate the information availability, as several search engines give personalized search results for various users as per their likes and dislikes. This particular bias in the algorithm of search engine cannot be easily detected and hence can be used for manipulation of information for creating enduring effects. AI combined with information campaigns offers more massive, autonomous and covert means to carry out psychological warfare and propaganda of political nature in order to change political outcomes and create divisions in the society. The United States Department of Défense (DoD) has defined a new terminology called Active Cyber Defence (ACD), which involves

[45] Ajder, Henry, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen. "The state of deepfakes: Landscape, threats, and impact." *Amsterdam: Deeptrace* (2019).

real-time capability and capacity of discovering, detecting, analysing and mitigating threats and vulnerabilities[46].

Cybersecurity Management

Non-state actors are also capable of using latest modes of warfare in order to achieve their ideological or political goals. It means there is an ambiguity and fuzziness between criminal behaviour, terrorism, organized violence, and war[47]. Although state actors have an advantage of using modern and advanced AI-based drone systems and technologies, but there are several commercial companies worldwide that are pouring in money for Research & Developmental purposes in the field of Artificial Intelligence (AI). Therefore, state actors are not certain regarding asymmetrical advantage in the hybrid warfare because in future there will be a fundamental shift in technology competence. As a result of this, militaries worldwide could start lagging behind in AI-enabled systems as compared to those of commercial companies. This could also benefit enemy organizations and could create a great security threat[48].

There is an increase in the number of military-grade drones available on internet worldwide for sale. The availability of drone systems and AI-enabled technologies to the terrorist organizations could become extremely destructive as through these technologies they are able to improvise them in order to make lethal weapons by loading explosives[49]. For instance,

[46] Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare," *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917.
[47] Elie Perot, "The blurring of war and peace," *Survival* 61, no. 2 (2019): 101-110.
[48] Guilong Yan, "The impact of Artificial Intelligence on hybrid warfare," *Small Wars & Insurgencies* 31, no. 4 (2020): 898-917.
[49] Tyler Rogoway, "Russia Says January 5th Attack on its Syrian Air Base Was by a Swarm of Drones," January 8, 2018, http://www.thedrive.com/the-war-

Afghan Taliban started using Unmanned Aerial Vehicles (UAVs) in October 2020, and they threaten to demoralize forces of Afghan Government that are perceived to be well-equipped to counter better-equipped enemy. According to a photo shared on Twitter on October 9, 2020, a commercially available quad-copter drone raised Taliban flag in the Southern Afghan province of Helmand[50].

Integration of AI technologies into economic sector has brought maximum benefits but it has also made the economic infrastructure vulnerable. The non-state actors in hybrid warfare may launch cyber-attacks on the networks and financial hubs or physical attacks on the economic infrastructure causing economic disruption, financial breakdown, and social chaos, thereby freezing the whole system at once.

Cybersecurity includes a broad range of tools, applications, and concepts which are closely related to informational and operational defence. It involves the offensive usage of information technology for attacking adversaries. According to technology practitioners the term cybersecurity should only be used for security purposes that involve information or operational technology systems[51]. Cybersecurity is defined as the development, management, governance and use of operations security, information security, and Information Technology security techniques and tools in order to defend assets, compromise the assets of adversaries, and

zone/17493/russiasays-january-5th-attack-on-its-syrian-air-base-was-by-a-swarm-of-drones (accessed February 21, 2021)

[50] Franz J. Marty, “Fire from the Sky: The Afghan Taliban‟s Drones”. December 22, 2020. https://thediplomat.com/2020/12/fire-from-the-sky-the-afghan-talibans-drones/ (accessed on April 29, 2021).

[51] Darko Galinec, Darko Mož nik, and Boris Guberina, "Cybersecurity and cyber defence: national level strategic approach," *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije* 58, no. 3 (2017): 273-286.

achieve regulatory compliance[52]. Cyber defence is a computer-based network defence mechanism that provides responses to certain actions and protection to precarious infrastructure and information assurance for government entities, organizations and other related networks. Cyber defence is very important in order to prevent sensitive data and information and to safeguard assets. It involves prevention, detection, and provision of timely responses to threats or attacks. It provides assurance to work and run different processes and activities without worrying about threats or attacks[53].

Visibility of cyber security status is very important defence mechanism. It indicates having a complete picture with measurements in order to find required and calculated levels of cyber security risks, and to find out the persons responsible for potential threats or attacks. Managing cyber security risks is not possible without measuring cyber security status. Threat intelligence services, data analytics and SIEM (Security Incident and Event Management) can help finding potential or actual compromise on the network, but they just provide overall picture of the possible threats and not the accurate measure of the risk status. Cybersecurity risk management has become a critical real-time facilitator for wining battle against cyber breach. Cybersecurity breaches transpire when some components i.e., people, processes or technology, of the cybersecurity risk management system are absent or they have failed in one way or the other. Therefore, there is a need to understand all the components of

[52] Walls, Andrew, Earl Perkins, and Juergen Weiss. "Definition: Cybersecurity." *Retrieved from Gartner. com website: https://www. gartner. com/doc/2510116/definition-cybersecurity* (2013).

[53] Darko Galinec, Darko Mož nik, and Boris Guberina, "Cybersecurity and cyber defence: national level strategic approach," *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije* 58, no. 3 (2017): 273-286.

cybersecurity risk management system, which is possible by pulling together all the applicable pointers and partial views of cybersecurity threats in order to develop risk-based measurement and prominence of cybersecurity status[54].

Recommendations

This paper highlights following important recommendations to help state actors and policy makers to take relevant actions in order to neutralize hybrid warfare;

1. Although the initiation of Artificial Intelligence has given rise to technological advancements, but in order to create military-technical upheaval, comprehend large gains in military's effectiveness and revolutionize the hybrid warfare. However, there is still a need of organizational innovations and innovative operational concepts designed to exploit new technologies.

2. The defence sector can get benefit from the advantages brought by the AI era through organizational adaptation. The organizational structures of successful AI-based companies may give some insight to the defence sector in order to adapt AI technologies on organizational level.

3. The spread of fake news, trends and propagandas on social media by the terrorist organizations and groups should be dealt through the implementation of social media regulations and laws.

[54] Simon Marvell, "The real and present threat of a cyber-breach demands real-time risk management," *Acuity Risk Management* (2015): 26-27.

4. There should be a national level cybersecurity policy aimed at leveraging the strengths of government for evolution of standard security practices, which could be used by government, businesses, security agencies, and general public in their use of cyberspace on routine basis.

5. Training sessions, workshops and seminars should be conducted involving cybersecurity stakeholders i.e., public sector, economic and academic sector, AI-based organizations, Multi-National Companies (MNCs), students and other citizens from different walks of life in order to give them a clear understanding of hybrid warfare tools and techniques used by the hybrid actors and terrorist groups through the use of social media platforms.

6. Cybersecurity risk management tools should be developed in order to measure the risk status and achieve cyber resiliency success through well-timed and synchronized actions and operative decision-making process.

7. It is important for military domains and LEAs to focus on human insight along with smart and autonomous systems in order to remain on the winning edge and to neutralize hybrid terrorist groups.

8. The use of innovative ideas, operational innovation, and organizational adaptation should be encouraged in order to build a more resilient, flexible, and intelligent defence organizations to tactically deal with hybrid warfare.

Conclusion

In the recent years, there has been an unprecedented increase in the use of Artificial Intelligence based devices, weapons and autonomous command and control systems and applications, in both military and non-military domains. In future, AI–enabled innovative and fresh new tools and technologies will become more common in fighting hybrid warfare and distorting cybersecurity. This will also create a great competition for control of data of vital importance. The salient features of hybrid warfare will still significantly influence the hybrid actors; therefore, success might not only be in the hands technologically equipped actors. The use of AI-enabled technologies has made the wars slower, bitter and indecisive which is possibly creating more chaos.

State actors use Artificial Intelligence (AI) and autonomous robotics and drone systems in order to detect security threats and to neutralize hybrid terrorist groups and other state enemies. As far as military implications are concerned, AI-enabled autonomous weapons have tendency to free human beings from the kill-chain, as facial recognition technology combined with mini-drones is capable to pin-point and kill the target. AI-enabled systems have significant implications for cyber security and are helpful in creating or distorting particular public opinions. AI-enabled campaign 'aids', based on the political preferences and personal likings, are capable of automatically generating tailored political, religious, or ideological messages in order to target individual voters, interest groups, and general public. It becomes an amplified and widespread tactic for shaping public opinion and distorting particular political or religious sentiments. AI can also track the economic, financial, and trade activities of the target groups or actors and give refined analysis and optimized plans to punish the target actors.

Information warfare and spread of fake news and propaganda has also become decisive factor in determining the victory or defeat in this contemporary warfare. It has become convenient to spread fake audio and video messages through the use AI-enabled technologies. Deployment of computational propaganda with the help of automated accounts as well as impression accounts is being actively used in order to change opinion of people or to spread certain kind of agenda or ideology. General public is also becoming a significant tool in disguise to spread the voice of these hybrid terrorist groups, as in many instances they are unable to filter the right and genuine information. AI-enabled systems are very crucial for deciding and responding to hybrid warfare and there is a dire need for military organizations and LEAs to invest in AI.

Technology based companies are free to pour money to make advanced AI-enabled command and control systems and fully automatic drones in order to commercialize the usage of such technologies to analyse online big data and to detect possible events of geographical, political or security nature. This commercialization of AI-enabled weapons and systems could be beneficial to the terrorist organizations by improvising the same AI-based systems for destructive purposes. Therefore, in this advanced technological era, uncertainty and surprise are still prominent features of the hybrid warfare. Enhanced cybersecurity management and reducing vulnerabilities is crucial for government and agencies and an operation-based approach is necessary to achieve specific results.

Miss Haleema Zia *has done MS (Management Sciences) from Riphah International University, Islamabad. She has extensive professional experience with development sector and is also having several years of experience with the Counter Terrorism Department. She is currently holding position of Director Communications at Adal Foundation. As an independent researcher in the fields of Management Sciences and Counter Terrorism, she is aimed at constructing a significant connotation between the two fields. She can be accessed through* ***haleemazia@gmail.com*****.**