Centre for Economics and Foreign Policy Studies

edam

Foreign Policy & Security 2019/8

May 2019

WARS OF NONE: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CONFLICT

Can Kasapoğlu, Ph.D. | Director, EDAM Security and Defense Studies Program

Barış Kırdemir, M.Phil. | EDAM - Bosch Cyber Fellow

WARS OF NONE: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CONFLICT

Can Kasapoğlu, Ph.D. | Director, EDAM Security and Defense Studies Program
Barış Kırdemir, M.Phil. | EDAM - Bosch Cyber Fellow

Key Takeaways

Hundreds of millions of years ago, during the Paleozoic era, Planet Earth witnessed the most intense and incredible burst of evolution that sparked off an immense bio-diversity including the emergence of vertebrates to which humans belong. This period is called the Cambrian Explosion. Today, we use the Cambrian Explosion analogy to depict what AI and robotics are about to accomplish, namely, bringing a new ecosystem to the world.

In essence, artificial intelligence and robotics resemble many characteristics of the nature, and 'life' in its biological meaning. Machine-learning, especially artificial neural networks, mimic the human brain to a certain extent. Advances in computational neuroscience and cognitive neuroscience continue to enable new technological leaps such as human-machine teaming and increased levels of autonomy in military systems.

Any sci-fi fashion future warfare scene, in which AI-controlled killer robots fight each other in organized formations using networked-centric concept of operations, would be inspired by the evolutionary biological roots of swarming living things that could be found in the nature.

Large-scale applications still require substantial investment. However, reaching vast amounts of data is now easier. Besides, costs of cutting-edge machine learning engines and computing power are decreasing. High-tech companies like Google, Amazon, and Microsoft offer their infrastructure and software engines to many other users. Cooperation between academia and industry, along with the ongoing scientific momentum, offer lucrative funding opportunities for entrepreneurs. In result, almost on daily basis, artificial intelligence and machine learning algorithms are solving task-specific problems that were unsolvable before.

The US, at present, remains the leading power in the AI-driven geopolitical competition, while China is emerging as an aspirant challenger. Russia, as yet, has not managed to be a part of the top tier in artificial intelligence, autonomy, and robotics. However, the Putin administration pays utmost importance to gaining a know how, since the Kremlin considers AI to be the focal point of the next great power competition.

Network-centric warfare of the 21st century is centered on an unprecedented connectivity between and within the three categorical battlefields – physical, informational, and cognitive – which, all together, build complex battle-spaces. Each battlefield has different interactions with AI-enabled applications. Combination of AI and robotics is likely to cause a drastic shift in the characteristic of armed conflicts.

One should not confuse a lethal autonomous military system with a sole, lone-wolf type killer machine. On the contrary, these systems are the products of the age of network-centric warfare. Thus, an AI-driven, warfighting

This research has been made possible by funding obtained from the North Atlantic Treaty Organization (NATO) for the project "New Perspectives on Shared Security: NATO's Next 70 Years".

robot would act as a part of a larger force under a unified C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance) architecture.

Future air warfare and air power will center on information dominance through a network of air, space, and cyber-space based sensors augmented by contributions across all domains of the battle-space. AI-based technologies will manifest their revolutionary skills mostly in the 6th generation aircraft, which remains a concept at present. Next generation aircraft, which will probably be optionally-manned, will operate alongside with their autonomous unmanned wingmen, and be able to launch drone swarms and carry directed energy weapons.

AI-enabled systems are likely to be weaponized and used in the cyberspace for both defensive and offensive purposes. For the time being, its implications for the strategic balance of power are yet to be fully understood.

NATO nations will need to adapt to the AI-driven transformation and reach a level of consensus. AI is likely to cause major economic and workforce shifts. More critically, it can change how the geopolitical competition is played out. It will also equip authoritarian states, some of which are NATO nations' current and future competitors, with new oppressive and discriminatory tools. Besides, AI can offer increasingly smart autonomous weapons systems to state and non-state actors.

Introduction

This report is a part of EDAM's contribution to the New Perspectives on Shared Security: NATO's Next 70 Years events.The first part of the report explains why the current artificial intelligence (AI) and robotics developments are likely to exacerbate a 'Cambrian Explosion' that brought about an unprecedented bio-diversity to the Earth millions of years ago. The second part assesses near-term policy implications of the AI revolution. The third part sheds light on 'geopolitics of artificial intelligence' and the new great power competition in this respect.

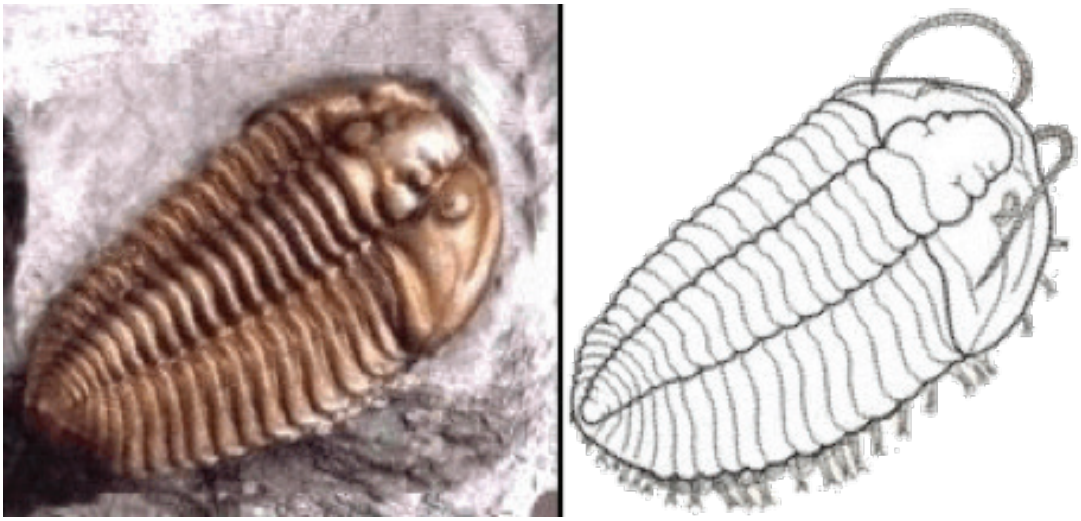
The fourth part presents an in-depth analysis of the evolving characteristics of armed conflicts and the future of warfare precipitated by AI-enabled technologies and concepts. This section divides the battle-space of network-centric warfare into physical, informational, and cognitive battlefields, and explores each part's interaction with artificial intelligence.

The fifth part focuses on the transatlantic alliance's AI agenda and future security environment in which allied leaders will have to operate. Finally, the study will conclude its findings and policy recommendations.

1. A New Cambrian Explosion: AI & Robotics and Political - Military Affairs

Hundreds of millions of years ago, during the Paleozoic era, Planet Earth witnessed the most intense and incredible burst of evolution. Then, life gained an impressive diversity including the emergence of vertebrates to which humans belong. This period is called the Cambrian Explosion[1]. Today, we use the Cambrian Explosion analogy to depict what AI and robotics are about to accomplish[2].

The ongoing techno-scientific revolution, still being in its relative infancy, will lead to the emergence of a new ecosystem. A drastic change in that scale would inevitably bring about an immense geopolitical transformation. Notably, in his famous 2018 Davos speech, bestselling author Yoval Noah Harari told that the present humanity could well be the last generations of the Homo Sapiens. According to Harari, the forthcoming dominant species will be more different from us than we were different from the Neanderthals[3].



Trilobite Arthropods from the Cambrian Period[4]

1 The National Geographic, https://www.nationalgeographic.com/science/prehistoric-world/cambrian/, Accessed on: April 18, 2019.

2 Greg, Allen and Taniel Chan. Intelligence and National Security, Harvard Belfer Center, 2017, p.15.

3 For Harari's speech, https://www.youtube.com/watch?v=hL9uk4hKyg4, Accessed on: May 05, 2019.

4 https://www.trilobites.info/trilobite.htm, Accessed on: April 18, 2019.

Boston Dynamics' Atlas humanoid robot taking a walk in the woods[5]

There is no great difference between AI-driven robotics and biology. *"Every type of animal, whether insect, fish, bird, or mammal has a suite of sensors, tools for interacting with its environment, and a high-speed data processing and decision-making center. Humans do not yet know how to replicate all the technologies and capabilities of nature, but the fact that these capabilities exist in nature proves that they are indeed possible"*[6]. Osborne Wilson, one of the most influential biologists of the modern history, argues that the continuous communication between the fields of evolutionary biology, paleontology, scientific understanding of brain functions, robotics, and artificial intelligence not only drives the progress in each of these fields but also enables a greater understanding of "life"[7].

In essence, artificial intelligence and robotics resemble many characteristics of nature, and 'life' in its biological meaning. Machine-learning, especially artificial neural networks, mimic the human brain to a certain extent. Advances in computational neuroscience and cognitive neuroscience continue to enable new technological leaps such as human-machine teaming and increased levels of autonomy in military systems[8]. Daily life solutions, such as facial or voice recognition, and even smart predictions of Google search functions, owe to artificial intelligence behaving similarly to the human brain in many ways.

Robotic swarms, namely the "collective, cooperative dynamics of a large number of decentralized distributed robots through the use of 'simple' local rules"[9], is another field through which computer science and robotics follow in biology's wake. For example, contemporary research explores behaviors of ant colonies to improve metropolitan transportation systems[10]. Because, at the epicenter of swarm robotics is self-organization, namely, "the emergence of macro-level behavior from non-linear interactions among individual agents, and between systems' components and their environment"[11], be it bio-chemical algorithms or deep learning AI algorithms. Bacteria colonies, bee colonies, bird flocks, termite colonies, and ant colonies all show very advanced swarming behavior[12].

In brief, any sci-fi fashion future warfare scene, in which AI-controlled killer robots fight each other in organized formations using networked-centric concept of operations (CONOPS), will be inspired by the evolutionary biological roots of swarming living things that could be found in the nature.

5 Boston Dynamics, https://www.bostondynamics.com/atlas, April 18, 2019.

6 Greg, Allen and Taniel Chan. Intelligence and National Security, Harvard Belfer Center, 2017, p.17.

7 E.O. Wilson interview, YouTube, https://www.youtube.com/watch?v=lx26k8LTCdI&app=desktop, Accessed on: May 5, 2019.

8 Emerging Cognitive Neuroscience and Related Technologies, National Research Council of the National Academies, 2008.

9 Andrew Ilachinski, AI, Robots, and Swarms, Center for Naval Analyses, 2017.

10 Rami Musa, Jean-Paul Arnaout, and Hosang Jung. "Ant colony optimization algorithm to solve for the transportation problem of cross-docking network." Computers & Industrial Engineering 59, no. 1 (2010): 85-92.

11 Ibid. p.106.

12 Ibid. p.107.

2. The AI Revolution: Exploring Near-Term Policy Implications

It is hard to predict the exact impact and trajectory of AI-enabled technologies. That being said, one can safely argue that these technologies might stimulate a civilizational transformation comparable to the invention of electricity[13]. AI and its applications will change many aspects of the global economy, security, communications, and transportation by altering how humans work, communicate, think, and decide. Intelligent machines will either team up with, or replace, humans in a broad range of activities. Such a drastic shift would boost social, economic, and political influences of those who invent and possess the new, game-changer capabilities, while the losing side could face existential challenges.

Artificial intelligence promises significant improvements in terms of efficiency, productivity as well as human lives' longevity and quality. For one, machine learning applications are becoming increasingly capable of solving complex problems in medical services. Systems supported with deep learning algorithms can identify thousands of characteristics in a given dataset and determine which characteristics are the important ones for timely, accurate, and reliable diagnostics. From different types of cancer to Alzheimer's and even very rare diseases, artificial intelligence will help to prolong human life by enabling early diagnosis, deciding on best treatment options, and matching transplant donors with receiver patients very quickly. Modern machine learning algorithms have already started to reduce human error in the most challenging tasks of medicine[14].

Large-scale applications still require substantial investment. However, reaching vast amounts of data is now easier. Besides, the costs of cutting-edge machine learning engines and computing power are decreasing. High-tech companies like Google, Amazon, and Microsoft offer their infrastructure and software engines to many other users. Cooperation between academia and industry, along with the ongoing scientific momentum, offer lucrative funding opportunities for entrepreneurs around the globe. In result, almost on a daily basis, AI and machine learning algorithms are solving task-specific problems that were unsolvable before.

However, the ongoing progress will also disrupt long-lived social, economic, political, and security parameters about how the world functions. This immense change in the basic rules of the game –often compared to previous industrial revolutions and biggest civilizational inventions– require a careful, responsible, and coordinated policy adaptation[15]. For example, AI-enabled systems will continue to reduce labor requirements, ranging from less complex and repetitive tasks to larger workflows. This trend can exacerbate profound fluctuations in the economic eco-system, affecting both the quantity and quality of jobs available for humans. Within the existing economic models, one particular risk would be the diminishing share of growth for large groups of people. Although the job market transformation is already unfolding, the potential effects are still hard to predict. Moreover, the effectiveness of recommended solutions, such as universal basic income, remains unknown[16].

A recent OECD report surveys 32 countries for automation-job transformation dynamics. The findings suggest that automation would significantly impact nearly half of the existing jobs with different risk degrees. Among all surveyed occupations, "highly automatable" jobs in the given countries make only 14%. However, this rate of risk differs between countries. For example, while the abovementioned figure marks 33% in Slovakia, it is only 6 % in Norway[17]. Notably, the OECD analysis concentrates on tasks that will be automated in each occupation, rather than entire sectors or jobs. Thus, while automation will impact tens of millions of people in the surveyed countries, it does not necessarily mean the replacement of entire occupations by machines. Instead, new levels of human-machine interaction and a new set of human-centric tasks are likely to emerge[18].

13 Andrew Ng, https://twitter.com/andrewyng/status/735874952008589312?lang=en, Accessed on: April 21, 2019.

14 Ben Buchanan and Taylor Miller. Machine Learning for Policymakers: What it is and Why it Matters, Belfer Center, 2017.

15 Wired, https://www.wired.com/story/guide-artificial-intelligence/ , Accessed on: April 20, 2019.

16 Osonde A. Osoba and William Welser. The Risks of Artificial Intelligence to Security and the Future of Work, RAND, 2017.

17 Ljubica Nedelkoska and Glenda Quintini. Automation, Skills Use and Training, OECD, 2018.

18 Ibid.

3. Geopolitics of Artificial Intelligence

The US, at present, is the leading power in the AI-driven geopolitical showdown, while China is emerging as an aspirant challenger. Russia, as yet, has not managed to be a part of the top tier in artificial intelligence, autonomy, and robotics. However, the Putin administration pays utmost importance to gain relevant know how since the Kremlin perceives AI as the focal point of the next great power competition. In the meanwhile, ambitious small and mid-size states that can punch above their weights thanks to their techno-scientific know-how, like South Korea, Israel, and Singapore, enjoy promising potentials that should not be underestimated.

Computing power, data availability, and infrastructure are the core pillars of AI geopolitics. Notably, a fierce competition in finding, recruiting, training, and retaining a highly qualified expert workforce has already dominated the ongoing international race for algorithmic dominance[19]. Among the key enablers of the AI industries, data, computing power, and semiconductors will potentially be decisive in tipping the balance of power between major actors. Chinese government and companies, for example, dedicated major investments to expand their computing power and semiconductor capabilities[20] to narrow the gap with other actors in the West, and to develop an "independent" national industrial base.

The abovementioned factors will probably lead to the emergence of even larger strategic gaps between nations. Besides, the new political-economic transformation may widen social inequalities in the world. Such concerns add to other risks such as discriminatory and authoritarian use of AI. Thus, both national endeavors and international partnerships will play key roles to avoid challenges associated with the development and use of artificial intelligence[21].

Technological superiority, particularly at times of scientific breakthrough, is not given for any actor, including the innovator nations. Tech industries and research institutions of the West have invented most of the major leaps in contemporary AI know-how. However, China's ambitious investments could become a game-changer[22]. A recent study by the Allen Institute for Artificial Intelligence shows that the number and quality of research papers generated by Chinese academics will soon go beyond their peers in the US. The study projects that the Chinese scholars would "overtake the US in the most-cited 50% of research papers this year, the top 10% of research papers in 2020, and the top 1% in 2025"[23].

China's strategy to become an AI superpower is aligned with its previously announced "Made in China 2025" program to transform into an innovative economic and technological stronghold. China's Next Generation Artificial Intelligence Development Plan was announced by the State Council in 2017. According to the document, in AI technology, China aims to overtake the West by 2025 and become a global leader by 2030. The plan lays out an overarching agenda for coordinating and encouraging large-scale national and international investments, research and development programs, educating, training, and acquiring a highly skilled labor base, and continuous inter-sectoral collaboration. China's AI strategy has been accompanied by multiple action plans of other entities. Chinese universities, the tech industry, and security sector actively pursue investment and employment programs. China's industrial base and AI sector are expanding globally[24]. Overall, Beijing considers the AI and robotics technologies to be silver bullets in altering the strategic balance of power.

China's ambitious strategy relies on the "military-civil fusion" which focuses on the dual-use nature of new transformative technologies and coordinating all elements of national power. China's ongoing military modernization seeks to

19 Osonde A. Osoba and William Welser IV. An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence Rand, 2017.

20 Paul Triolo and Graham Webster. China's Efforts to Build the Semiconductors at AI's Core, New America, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-efforts-to-build-the-semiconductors-at-ais-core/, Accessed on: April 22, 2019.

21 Cummings, M. L., Heather Roff, Kenneth Cukier, Jacob Parakilas, and Hannah Bryce. Artificial Intelligence and International Affairs: Disruption Anticipated, Chatham House, 2018.

22 Will Knight. China's AI Awakening, MIT Technology Review, https://www.technologyreview.com/s/609038/chinas-ai-awakening/ , Accessed on: April 19, 2019.

23 Will Knight. China May Overtake the US with the Best AI Research in Just Two Years, MIT Technology Review, https://www.technologyreview.com/s/613117/china-may-overtake-the-us-with-the-best-ai-research-in-just-two-years/ , Accessed on: April 19, 2019.

24 Sophie-Charlotte Fischer. Artificial Intelligence: China's High-Tech Ambitions, CSS, ETH Zurich, 2018.

exploit the technological leap and sees "intelligentized" warfare as the new military revolution. The future warfare will be utterly different, particularly in comparison to the current/previous concepts that have been enabled by the information technology. Apart from the research and development initiatives and programs of the private sector, the Chinese Ministry of Defense runs research institutes for artificial intelligence and robotics[25].

In the hands of authoritarian states and malicious actors, AI can be used to severely harm human rights. Some experts suggest that, for at least a decade, China and Gulf states would remain as primary concerns. This is due to the fact that despite the proliferation, large-scale utilization of AI will still require infrastructure investments. In a report for the US House Foreign Affairs Committee, Font-Reaulx suggests that use of AI in these countries may further diminish the space for political opposition. In addition, governments can move "towards totalitarian traits". In the short term, the report recommends mainly technological counter-measures that can limit or prevent totalitarian, oppressive, and discriminatory use of AI-enabled systems. Notably, the report foresees threat scenarios such as "high precision algorithms for identifying dissidents", use of "social credit systems" to ensure regimes' desired behavior, "distortion of public discourse", and even use of autonomous "drones for assassinations"[26].

China is already using AI systems for racial profiling. Chinese authorities use facial recognition technology on a giant network of surveillance cameras to search for, detect, and record the Turkic Uighur population. This capability adds to China's long-lasting surveillance activities such as keeping and tracking the DNA records of its minorities. The latest facial recognition systems are used by multiple law enforcement agencies specifically for "identifying Uighur/non-Uighur attributes"[27]. Major tech companies in China have involved in the development of the system, and they openly advertise its advanced "detection" capabilities. Once available in international markets, such dual-use products can attract 'enthusiastic' customers worldwide[28].

When it comes to the US, we observe a very different approach to the AI-enabled techno-scientific and techno-political agendas. American private sector and academia drive the development of AI. US-based tech companies and researchers have achieved most of the AI breakthroughs to date. However, unlike China, government support and coordination are limited in Washington[29]. To fill this gap, the Trump Administration unveiled the "American AI Initiative" executive order in February 2019[30]. The initiative lays out key pillars of a nation-wide strategy, ranging from access to federal data to infrastructure improvements, workforce, and financial support for research. Yet, most of the US government agencies still lack mechanisms and plans for its implementation[31].

The Department of Defense (DoD) has the most comprehensive strategy across the US government[32]. The DoD's new Artificial Intelligence Strategy was announced shortly after the White House's executive order. The document primarily focuses on delivering AI-enabled capabilities to all forces and key missions, acquiring and retaining a highly skilled workforce, constantly "engaging with commercial, academic, and international allies and partners", while prioritizing ethics and safety measures[33]. The US DoD also runs the Joint Artificial Intelligence Center (JAIC) as a key capability and concept development hub.

On the military R&D angle, Defense Advanced Research

25 Gregory C. Allen. Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security, CNAS, 2019.

26 Paul de Font-Reaulx. AI: The Consequences for Human Rights, House Foreign Affairs Committee Tom Lantos Human Rights Commission Hearing, 2018.

27 "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", The New York Times, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html , Accessed on: April 19, 2019.

28 Ibid.

29 Darrell M. West. Assessing Trump's Artificial Intelligence Executive Order, Brookings Institution, 2019.

30 Accelerating America's Leadership in Artificial Intelligence, White House, https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/ , Accessed on: April 15, 2019.

31 Darrell M. West. Assessing Trump's Artificial Intelligence Executive Order, Brookings Institution, 2019.

32 Ibid.

32 Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity, The U.S. Department of Defense, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF , Accessed on: April 15, 2019.

Projects Agency (DARPA) pursues multiple AI-related R&D programs, and supports other actors in commercial sectors and academia. DARPA's "Next AI" campaign, reportedly worth two billion dollars, is one of the most prominent programs in the US. In addition, the agency also concentrates on "third wave" AI research, envisioning next generation AI systems[34]. Also, the Defense Innovation Unit (DIU) collaborates with the commercial sector through venture capital funding. Currently, the DIU programs primarily cover computer vision, large dataset analytics and predictions, and strategic reasoning[35].

While China pursues an ambitious national AI strategy which has a solid financial backing and government-led coordination, and the US still enjoys a global commercial and academic leadership, Russia seems to lack both these pillars to become a first-tier AI power. After all, the Russian spending on AI technology remains very low compared to the US and China. Besides, the present state and anticipated trajectory of the national economy do not help President Putin in materializing his AI vision. Russia's problematic GDP and stagnant characteristics of Russian political and economic system seem to lack the capacity to produce influential technology hubs and most cited research institutions[36]. Moscow's national AI strategy document, which is expected to be announced in June 2019, will probably aim to fill these gaps as much as possible. Nevertheless, Moscow could well succeed in conducting AI-enabled information operations and political warfare.

4. AI and the Future of Warfare: Exploring the Physical, Informational and Cognitive Battle-Spaces

Network-centric warfare of the 21st century is based on unprecedented connectivity between and within the three categorical battlefields which, all together, builds complex battle-spaces. The first one remains the physical battlefield in which ballistic missiles, main battle tanks, stealth aircraft, the rifle of a ground infantry, and other military 'hardware' are fielded. This is where one could observe the direct, brute physical impact, such as destroying a bridge with explosives or hunting down an armored vehicle with air-ground missiles.

Secondly, there is the informational battlefield. In this segment, information superiority-related activities take place such as military systems and platforms sharing their inputs through datalink connectivity, space-based intelligence is harvested by satellites and conveyed to weapon systems, the trajectory of an incoming ballistic missile is cued to the battle management hubs, electronic warfare assets attempting to blind the adversary's acquisition radars before an airstrike among many other informational tasks.

Thirdly and finally, the cognitive battlefield completes the network-centric trinity. The cognitive battlefield is where information operations and political warfare take place, such as disinformation activities through spreading fake news about an ongoing conflict or revealing an adversary's hostile buildup by disseminating open-source intelligence output. The cyber-space, being the fifth domain of warfare, is shared between the informational battlefield and cognitive battlefield. Clearly, both the F-35 5th generation aircraft's off-board connectivity through ground-breaking ALIS system, and Russia's information operations on the internet use the cyber-space.

This chapter will focus on each of the abovementioned battlefields with a specific focus on the effects of AI and robotics. By doing so, we aim to come up with a precise forecast about how the future battlespace will be shaped by the ongoing techno-scientific breakthrough.

33 Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity, The U.S. Department of Defense, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF , Accessed on: April 15, 2019.

34 Statement of Dr. Peter Highnam Deputy Director Defense Advanced Research Projects Agency (DARPA) Before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, https://www.armed-services.senate.gov/imo/media/doc/Highnam_03-12-19.pdf , Accessed on May 1, 2019.

35 Statement by Michael Brown Director of Defense Innovation Unit Before the Senate Armed Services Committee Subcommittee on Emerging Threats and Capabilities, https://www.armed-services.senate.gov/imo/media/doc/Brown_03-12-19.pdf , Accessed on: May 1, 2019.

36 Alina Polyakova. Weapons of the Weak: Russia and AI-driven Asymmetric Warfare, Brooking Institution, 2019.

4.1. How the New 'Cambrian Explosion' will Change Warfare?

The adaptation and integration of information communication technologies (ICT) into weapon systems and military capabilities have already been changing the character of armed conflicts. Some experts believe that ICT-enabled information has already become the "most consequential trend" in warfare and could become the "dominant factor in deciding the outcomes of battles, operations, and ever wars"[37].

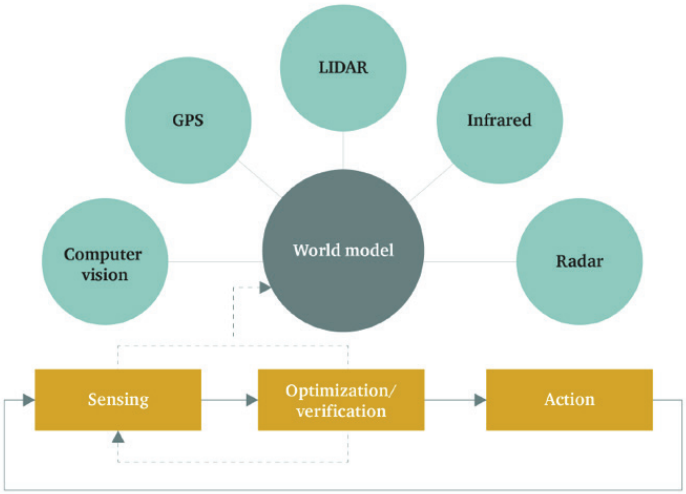
As the US Joint Operating Environment 2035 Report suggests:

> *"Very powerful information technologies will be widely available around the world by 2035, including wireless handheld or even brain-interfaced devices with advanced levels of connectivity. More modern developing states will continue to construct comprehensive national information technology infrastructures consisting of fiber-optic and cellular networks that far exceed the current state of the art. Potential competitors will have access to huge volumes of commercially-available geospatial and other geophysical data that once cost billions and was available to only to the richest and most technically-competent countries"[38].*

Analytical projections for next decades of war suggest that deep-learning and human-machine collaboration are likely to bring about faster and better decision-making by enabling enhanced management of large data streams. In the meanwhile, social networking, digital media, and instantaneous reporting from war zones have already added a 'battle of narratives' dimension to modern warfare in the cyber domain[39].

AI, filling the cognitive systems of robots and robotic warfare, follows a similar pattern with human intelligence in sensing the world and acting in it. Clearly, AI decides its actions by processing the incoming information through verification and optimization algorithms. In other words, an autonomous system (including a warfighting robot that can take decisions) has to construct a world model to act in and interact with. Moreover, this world model (be it the traffic in rush hour or a battlefield) would be extremely dynamic with changing parameters each second. In result, the authenticity of the constructed world model and timely precision of its updates are key to an advanced autonomous system[40].

At this point, one should not confuse a lethal autonomous military system with a sole, lone-wolf type killer machine. On the contrary, these systems are the products of the age of network-centric warfare and unprecedented interoperability. Thus, an AI-driven, warfighting robot would act as a part of a larger force under a unified C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance) architecture. A lethal autonomous system has to be provided with key information such as a visual mapping of the environment (i.e. Forward Line of Own Troops, humanitarian and protected sites like hospitals, and adversary locations), mission guidance (i.e. rule of engagement and the commander's intent), and dynamic de-confliction information (i.e. last minute changes in the protected entities' locations)[41].



An Autonomous System's Key Technical Feature: A Dynamic World Model[42]

37 Jennifer, McArdle, Victory Over and Accross Domains: Training for Tomorrow's Battlefields, CSBA, 2019.

38 The US Joint Chiefs of Staff, Joint Operating Environment 2035, 2016, p.18.

39 Australia, Future Operating Environment 2035, 2016.

40 Mary, 'Missy' L. Cummings, Artificial Intelligence and the Future of Warfare, Chatham House, 2017, pp.2-3.

41 Larry, Lewis. Insights for the Third Offset: Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations, CAN, 2017, p.29.

42 The Illustration was retrieved from: Mary, 'Missy' L. Cummings, Artificial Intelligence and the Future of Warfare, Chatham House, 2017, p.3.

The 2000s, especially the War on Terror era following the 9/11 attacks, witnessed how ISR platforms, the UAVs, turned into strike assets. Now, due to the pressing threats and casualties emanating from hybrid warfare and urban operations, defense planners need to use more unmanned ground vehicles (UGV) with smarter solutions. This paradigm stems from the strategic thinking of delegating 'dull, dirty, and dangerous' jobs to robots to relieve humans. In the battlefield, such a shift would boil down to standoff (to keep humans away) and precision (to conduct sharp military operations) functions. To do so, 'robots' should be able to sense, plan, and execute missions with high level of autonomy, and should be equipped with the expanding sensors technology (such as hyper-spectral imagery, sonar, and light detection and ranging – LIDAR)[43]. Electronic miniaturization, telecommunications, and global positioning remain essential factors for a viable robotic warfare plan. Notably, Moore's Law, namely the idea that transistor density and computing power doubles every two years, suggest a steady growth in micro-electronic mechanical (MEM) based sensors which pave the ground for robotics[44].

4.2. Into the Future: AI and Robotics Dominated Warfighting in Urban Battlefields

Parameters of contemporary military conflicts differ from the Cold War-type force-on-force military balance and warfighting. Today, asymmetric conflicts take place in complex battlefields with more dynamism, smarter weapon systems, dispersed combatants, and non-linear CONOPS. Decision-making process and requirements are incredibly faster, and distinguishing fighters from civilians is harder than ever[45]. By 2030, it is estimated that some 4.9 billion people, nearly 60% of the world's population, will be living in urban areas. Back in the 1950s, for example, 30 % of the world's 2.5 billion people were in urban areas[46]. Urban warfare offers 360 degrees battlegrounds with restricted mobility, very high operational tempo, serious casualty risk, increased subterranean activity, blurring distinctions between combatants and non-combatants, along with a dynamic conflict trajectory[47].

Inevitably, the risks associated with the urbanization of the battlefield has kicked-off a debate on future killer robots that will be based on today's unmanned ground vehicles. Open-source writings estimate that one-fourth of the US combat troops will be replaced by UGVs[48]. Likewise, the Russian Military Industrial Committee plans to generate 30% of the Russian combat power in 2030 from a pool of remotely-controlled and autonomous military robotic platforms[49]. These trends in armament could change the traditional understanding of manpower forever. Many open-source defense surveys, for example, report available manpower and demographics as a core element of military power. As robots dominate the battlefield gradually, our understanding of population and even casualties could radically change[50]. Would this make politicians more aggressive and bolder when deciding to wage war? We don't know yet. But one thing is clear, the decision-making parameters (probably even the decision-making tools and algorithms) will differ.

However, one should understand that the UGV revolution is still well behind the UAV revolution at the time being. Let us

43 Simon, Monckton. "Current and Emerging Technology in Military Robotics" in Robotics and Military Operations, William G. Braun et.al. [ed.], Kingston Conference on International Security Series, US Army War College SSI, 2018, pp.30-31.

44 Simon, Monckton. "Current and Emerging Technology in Military Robotics" in Robotics and Military Operations, William G. Braun et.al. [ed.], Kingston Conference on International Security Series, US Army War College SSI, 2018, pp.35-37.

45 Zdzislaw, Sliwa. "The Tendencies of Unmanned Ground Vehicles Development in the Context of Future Warfare" in Digital Infantry Battlefield Solutions: Introduction to Ground Robotics, Part I, joint study of Milrem, Estonian National Defence College, Latvian National Defence Academy, Latvian Institute of International Affairs, Riga Technical University, University of Tartu, 2016, p.33.

46 For a detailed projection, see: The US National Intelligence Directorate, Global Trends 2030, 2012.

47 For a good reading on urban warfare, see:The US Army Asymeetric Warfare Group, Lessons Learned from Urban Operations from 1980 to the Present, 2016.

48 Janis, Berzins. "Unmanned Ground Systems in Future Warfare" in Digital Infantry Battlefield Solutions: Introduction to Ground Robotics, Part I, joint study of Milrem, Estonian National Defence College, Latvian National Defence Academy, Latvian Institute of International Affairs, Riga Technical University, University of Tartu, 2016, p.24.

49 Greg, Allen and Taniel Chan. Intelligence and National Security, Harvard Belfer Center, 2017, p.21.

50 Ibid. p.23.

examine the Russian experience with their unmanned beast, Uran-9, in Syria to explore the unmanned ground warfare environment.

Uran-9 is a remote-controlled (up to 3 km), robotic-tank with *a 30mm Shipunov 2A72 automatic cannon, four ready-to-launch 9M120-1 Ataka (Spiral-2) ATGMs, four Igla-V surface-to-air missiles, and a 7.62mm Kalashnikov PKT/PKTM machine gun.* It can also mount a Shmel-M reactive flame thrower[51]. In May 2018, Russian military planners deployed the robotic tank to Syria to test its warfighting capabilities and combat readiness. While some sources praised Uran-9 for its "high performance in an operational environment"[52], some others reported fairly poor results in thermal and electro-optical sensors (the platform could spot enemy targets beyond 1.25 miles, as claimed) and lack of weapons stabilization[53].

The Uran-9 [54]

Without a doubt, remote-controlled UGVs, unlike UAVs, suffer from disrupted control signals due to topographical features and buildings in urbanized areas[55]. This is why autonomy and cross-domain capabilities could make a real difference in unmanned ground CONOPS. Notably, it is not a coincidence that Russia's Uran-9 experimental combat debut in Syria overlapped with the Russian inter-branch efforts to boost AI-based military solutions, including playing wargames to explore the impacts of artificial intelligence based models in tactical, operational and strategic levels[56].

Increasing a UGV system's autonomy could reduce its dependence on remotely-controlled links, and thereby, would allow it to operate in hostile environments with more freedom of action. Another key aspect of augmenting robotic ground systems on the battlefield is to foster their resiliency against cyber and electronic warfare[57]. Finally, one should not consider ground robotics to be an isolated segment. Military robots are designed to, and will, operate as an essential element of network-centric warfare[58].

51 Congressional Research Service, US Ground Forces Robotics and Autonomus Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress, November 2018, p.12.

52 IHS Jane's, https://www.janes.com/article/83252/russia-upgrades-uran-9-combat-ugv, Accessed on: April 17, 2019.

53 Sebastien, Roblin. "Russia's Uran-9 Robot Tank Went to War in Syria (It Didn't Go Very Well), The National Interest, January 2019, https://nationalinterest.org/blog/buzz/russias-uran-9-robot-tank-went-war-syria-it-didnt-go-very-well-40677, Accessed on: April 17, 2019.

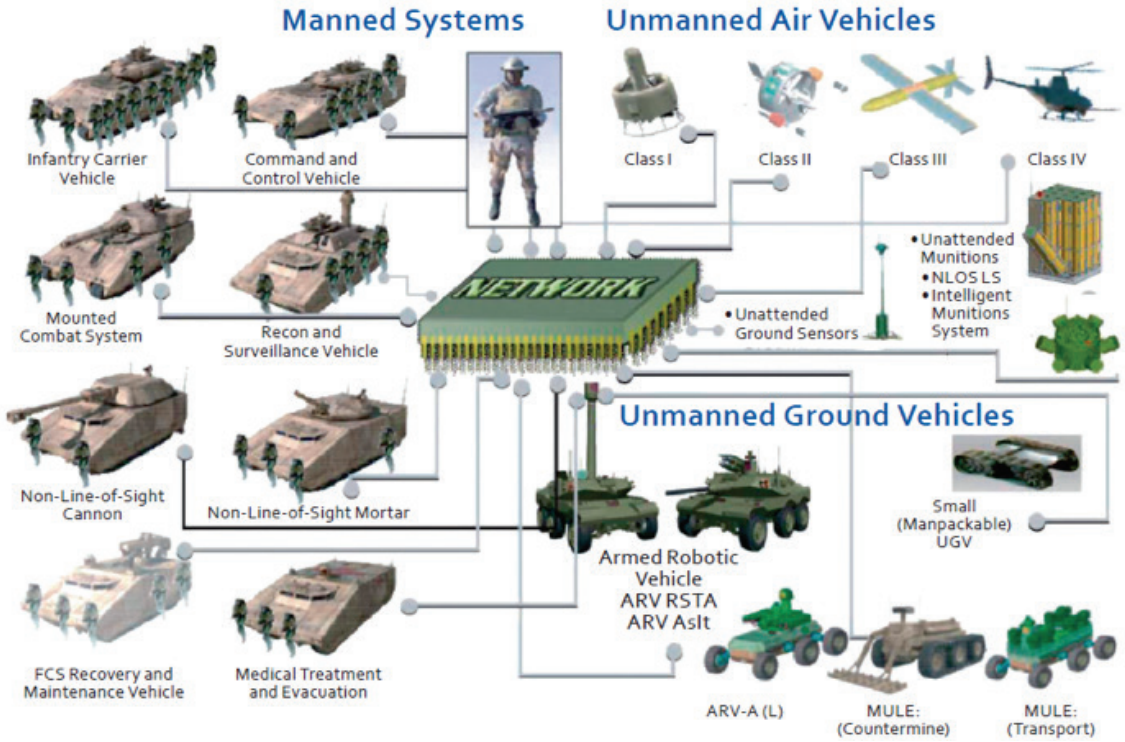
54 Business Insider, https://www.businessinsider.de/russias-uran-9-robot-tank-performed-horribly-in-syria-2018-7?r=US&IR=T, Accessed on: April 17, 2019.

55 Sebastien, Roblin. "Russia's Uran-9 Robot Tank Went to War in Syria (It Didn't Go Very Well), The National Interest, January 2019, https://nationalinterest.org/blog/buzz/russias-uran-9-robot-tank-went-war-syria-it-didnt-go-very-well-40677, Accessed on: April 17, 2019.

56 For the official text, see: http://mil.ru/conferences/is-intellekt.htm, Accessed on: April 17, 2019.

57 Janis, Berzins. "Unmanned Ground Systems in Future Warfare" in Digital Infantry Battlefield Solutions: Introduction to Ground Robotics, Part I, joint study of Milrem, Estonian National Defence College, Latvian National Defence Academy, Latvian Institute of International Affairs, Riga Technical University, University of Tartu, 2016, pp.24-25.

58 Zdzislaw, Sliwa. "The Tendencies of Unmanned Ground Vehicles Development in the Context of Future Warfare" in Digital Infantry Battlefield Solutions: Introduction to Ground Robotics, Part I, joint study of Milrem, Estonian National Defence College, Latvian National Defence Academy, Latvian Institute of International Affairs, Riga Technical University, University of Tartu, 2016, p.42.



Ground Robotics and UGVs as an Essential Component of Future Combat Systems and next Generation Network-Centric Warfare [59]

UGS	Capability Class	Potential Applications
Small robotic building and tunnel searcher	Tele-operated ground vehicle	Mine detection, mine clearing, engineer construction, explosive ordnance disposal/unexploded ordnance materials handling, soldier-portable reconnaissance/ surveillance
Small-unit logistics mover	Semi-autonomous preceder/ follower	Supply convoy, medical evacuation, smoke laying, indirect fire, reconnaissance/ surveillance, physical security
Unmanned wingman ground vehicle	Platform-centric autonomous ground vehicle	Remote sensor, counter-sniper, counter-reconnaissance/infiltration, indirect fire, single outpost/scout, chemical/ biological agent detection, battle damage assessment
Autonomous hunter-killer team	Network-centric autonomous ground vehicle	Deep reconnaissance, surveillance, and target acquisition, combined arms (lethal direct fire/reconnaissance/indirect fire for small unit defense or offense), static area defense, military operations in urban terrain reconnaissance

Combat Mission Portfolio of Unmanned Ground Vehicles [60]

[59] Zdzislaw, Sliwa. "The Tendencies of Unmanned Ground Vehicles Development in the Context of Future Warfare" in Digital Infantry Battlefield Solutions: Introduction to Ground Robotics, Part I, joint study of Milrem, Estonian National Defence College, Latvian National Defence Academy, Latvian Institute of International Affairs, Riga Technical University, University of Tartu, 2016, p.42.

[60] Retrieved from: Janis, Berzins. "Unmanned Ground Systems in Future Warfare" in Digital Infantry Battlefield Solutions: Introduction to Ground Robotics, Part I, joint study of Milrem, Estonian National Defence College, Latvian National Defence Academy, Latvian Institute of International Affairs, Riga Technical University, University of Tartu, 2016, p.25.

4.3. Controlling the Outcome: Techno-Ethics of Autonomous Robotic Warfare

Contextually, UGVs can accomplish a broad array of tasks including, but not limited to, operating in CBRN (chemical, biological, radiological, and nuclear) contaminated battlefields, transportation and military logistics, counter-mine operations, disaster response, ISR (intelligence, surveillance, and reconnaissance), and counter-IED (improvised explosive devices) tasks.

But still, if nations are to fight wars by using robots, then they will have to control the outcome. This necessity makes an emerging field, probabilistic robotics, vital to building reliable robotic warfare capabilities[61]. Robotics, in essence, "is the science of perceiving and manipulating the physical world through computer-controlled devices"[62]. Robots are real-time systems and behavior remains uncertain to some extent due to many reasons such as software, algorithmic approximations, or mechanical failure. Probabilistic Robotics, a new field of larger robotics studies, rely on probabilistic algorithms to compute a robot's momentary uncertainty, as well as to anticipate its future uncertainty[63].

At the heart of robotics debates, there lays the autonomy and its unpredictability. By definition, an autonomous weapon system (AWS) refers to *"a weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation"*[64]. The level of uncertainty in AI-based systems' behaviors, especially when it comes to military purposes, is related to the complexity of the sensed world. In a world containing some 1,000 categories of objects, a machine learning algorithm can score 60 – 70 % identification record, while in a world of 22,000 categories of objects, the accurate identification rate could decrease to less than 16%[65].

The world model, or the constructed reality by an AI-empowered brain, would differ between an UAV operation and navigation of a driverless car. While the former's world model is relatively straightforward thanks to the GPS-based systems, radar support, terrain mapping, and advanced mapping; the latter has to deal with very swiftly changing dynamics like pedestrians, nearby vehicles, and even changing routes due to an instantaneous roadblock or demonstration[66].

All in all, the real impact of the AI and robotics driven breakthroughs on ground warfare remains to be seen. Many ethical, technical, and CONOPS issues are unclear at the time being. However, human-machine teaming, along with a qualitative and quantitative increase in unmanned ground platforms will continue with exponential growth.

61 Simon, Monckton. "Current and Emerging Technology in Military Robotics" in Robotics and Military Operations, William G. Braun et.al. [ed.], Kingston Conference on International Security Series, US Army War College SSI, 2018, p.38.

62 Sebastian, Thrun. et.al. Probabilistic Robotics, Massachusetts Institute of Technology, 2006, p.3.

63 Ibid.

64 Congressional Research Service, US Ground Forces Robotics and Autonomus Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress, November 2018, p.3.

65 Mary, 'Missy' L. Cummings, Artificial Intelligence and the Future of Warfare, Chatham House, 2017, p.8.

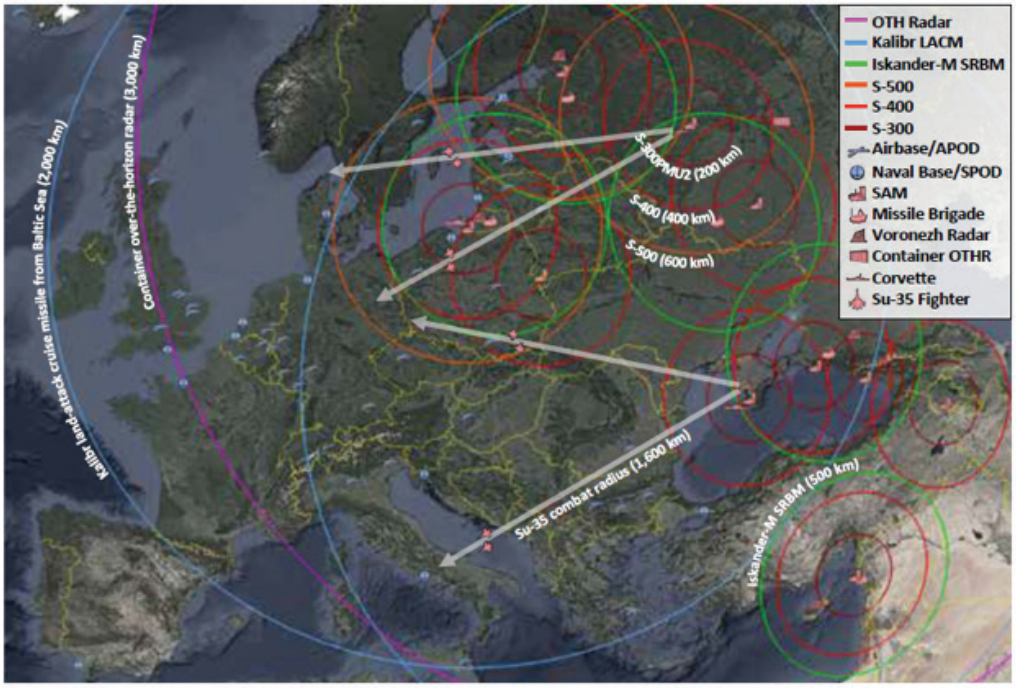
66 Mary, 'Missy' L. Cummings, Artificial Intelligence and the Future of Warfare, Chatham House, 2017, p.4.

4.4. Future Air Warfare and AI

Next generation air power assets will have to overcome certain threats in their operations. Firstly, anti-access / area denial (A2/AD) challenges are on the rise through advanced SAM systems (surface-to-air missile) and electronic warfare (EW) capabilities. Secondly, critical enablers, such as aircraft carriers and air bases, are to face pressing risks stemming from both kinetic and non-kinetic attacks. And thirdly, as sensors are getting more dense and powerful, none-stealth aircraft are to face drastically diminishing survivability when penetrating hostile airspace[67].

The 5th generation aircraft is a conceptual response to these challenges. At the time of writing, approximately 17% of the US Air Force's (USAF) fighter inventory consists of 5th gen. platforms. Within two decades, these platforms will become dominant in the USAF's fighter arsenal[68].

With its powerful sensors, stealth capabilities, open software architecture, unprecedented data fusion and analysis capacity, the F-35 represents a new epoch in air warfare[69]. Italy's air force chief, General Enzo Vecciarelli, rightly considered the F-35 to be an information superiority asset[70]. But what is information superiority in the first place? Briefly, gaining information superiority over an adversary means *"ensuring you have as much accurate information about the battle-space as possible, including ensuring access to one's own networked information systems in all domains in the event of conflict, and denying the adversary the information they need to make rapid and well-informed tactical and operational decisions or to effectively use their military forces"*[71].



Data to build this graphic derived IHS Jane's (2019).

Russian A2/AD Projection in the Baltics and Black Sea Regions (CSBA) [72]

67 For a detailed report, see: Justin, Bronk. Next Generation Combat Aircraft: Threat Outlook and Potential Solutions, RUSI, 2018.

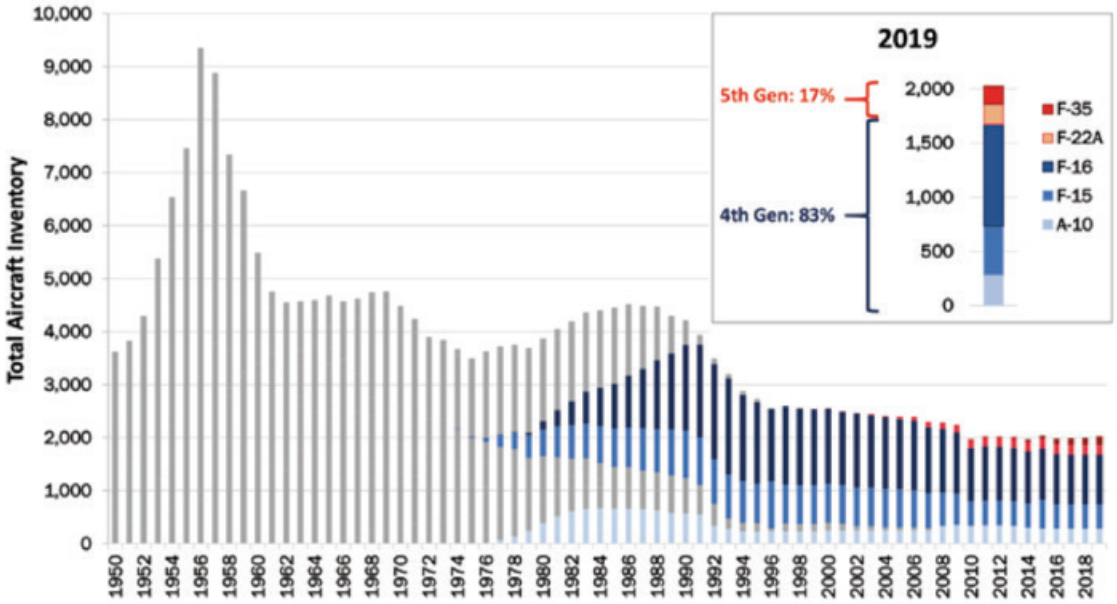
68 For a comprehensive study, see: Mark, Gunzinger et.al. An Air Force for an Era of Great Power Competition, CSBA, 2019.

69 Justin, Bronk. Maximum Value from the F-35: Harnessing Transformational Fifth-Generation Capabilities for the UK Military, 2016, pp.7-8.

70 Tony, Osborne. "Italian Air Force Commander on How F-35 will Transform the Service", Aviation Week & Space Technology, 2018.

71 Thomas, G. Mahnken et.al. Piercing the Fog of Peace: Developing Innovative Operational Concepts for a New Era, CSBA, 2019, p.19.

72 Mark, Gunzinger et.al. An Air Force for an Era of Great Power Competition, CSBA, 2019. p.34



Trends in the US Air Force Fighter Inventory (CSBA) [73]

Future air warfare and air power will center on information dominance through a network of air, space, and cyber-space based sensors augmented by contributions across all domains of the battle-space. As emphasized by the US Air Superiority 2030 Flight Plan, finding the optimum way to fuse data from cloud-based sensors and translating the inputs into weapons-quality information at operational and tactical levels remain key to success[74].

AI-based technologies will manifest their revolutionary skills mostly in the 6th generation aircraft that remains a concept at present. Next generation aircraft, which will probably be optionally-manned, will operate alongside with their autonomous unmanned wingmen, and be able to launch drone swarms and carry directed energy weapons. The 5th generation's impressive connectivity, most visibly observed in the F-35, will ascend to a new level in the 6th generation air warfare through network-centric operational capability with low earth orbit satellites and advanced (possibly stealthy[75]) unmanned aerial systems[76].

The 6th generation systems will probably have state-of-the-art sensors fusion with ground, sea, space, and other air elements. Besides, building on the newly experienced off-board connectivity with the 5th generation F-35's ALIS (Autonomous Logistics Information System) and the aircraft's advanced MADL datalink (Multifunction Advanced Data Link), the 6th generation systems are expected to enjoy unprecedented network-centric battle management and C4ISR architecture. But who will deal with all this real-time intelligence? The third and fourth generation aircraft addressed the growing complexity of the battlefield by adding another seat to the cockpit. Yet, so far, the 5th generation designs are single-seat aircraft. This is where AI, one more time, will play a game-changer role. Futuristic writings estimate that artificial intelligence and machine learning are to assume more intensive workloads in air power in the 2030s and beyond, by determining which data should be presented to the pilot[77]. Of course, such a digital complexity comes at a price. Future, 5th and 6th generation air powers will be more susceptible to cyber and electronic warfare threats[78].

Another field that AI could make a real difference is the

74 For the full text, see: The US Air Superiority 2030, 2016.

75 Kris, Osborn. "RIP F-35: The Air Force's Sixth-generation Fighter could Make Everything Obsolete", The National Interest, January 2019, Accessed on: April 17, 2019.

76 Can, Kasapoglu. "6G Challenge: Can France and Germany Co-Produce Future of Warfare", Anadolu Agency, February 2019, https://www.aa.com.tr/en/analysis-news/6g-challenge-can-france-and-germany-co-produce-future-of-warfare/1395852, Accessed on: April 17, 2019.

77 Sebastien, Roblin. "Here Comes the Revolutin: Why 6th Generation Fighters could Change Everything", The National Interest, February 2019, https://nationalinterest.org/blog/buzz/here-comes-revolution-why-6th-generation-fighters-could-change-everything-45697, Accessed on: April 17, 2019.

78 Ibid.

unmanned aerial warfare and drones. To better understand how UAVs, augmented by more autonomy, could change the characteristics of the conflict, one should focus on the numerical increase in these platforms. In 2001, the Pentagon possessed some 170 unmanned aerial systems. By 2014, the US UAV inventory had risen up to more than 11,000[79]. There is no other asset that was subject to such a boost within only a decade. On the defensive end of the spectrum, counter-drone systems are also on the rise. 2018 studies reveal that more than 150 manufacturers in some 30 countries are producing and designing over 230 counter-drone systems[80].

Unmanned aerial systems (UAS) have gained more competitive edge in air warfare in recent years. At first, these platforms were predominantly ISR (intelligence – surveillance – reconnaissance) assets carrying advanced sensors. The War on Terror, following the 9/11, had witnessed UAS transforming into strike assets for kinetic roles in counterinsurgency and counterterrorism operations. The US military and its allies have increasingly relied on medium and high altitude, long-endurance (MALE) systems in Afghanistan and Iraq. These two theaters showed that networked use of unmanned aerial systems has brought a new way of warfare into existence. As a result, UAVs have become the principal weapon systems in counterterrorism operations in Pakistan, Somalia, Yemen and Libya. In 2009, then CIA Director Leon Panetta stated that using drones in the war on terror was "the only game in town"[81]. Indeed, the ratio of unmanned strikes rose from 5% in 2011 to 56% in 2015, and 61% in the first quarter of 2016[82].

Now, with AI-enabled technologies on the rise, the UAV revolution could go well beyond the numerical rise and operational intensity. As mentioned, since the 6th generation aircraft will enter into service in the 2030s and the 2040s, "physical teaming between 'manned' and 'unmanned' vehicles, and cognitive teaming that blends automation and human decision-making" will probably form the epicenter of military drone programs[83]. Especially, more autonomous UAVs are likely to be a vital component of penetrating into A2/AD environments. Further development and integration of artificial intelligence technology are expected to enable decision-support for operations while increasing the autonomy of future unmanned aerial systems[84]. More autonomous systems will also reduce bandwidth requirements as they will not have to stay in contact with the human operator constantly. Furthermore, next-generation unmanned aerial systems will be "the key to affordable power projection"[85].

Finally, when it comes to air-to-air warfare, the situation is more complicated. So far, defense studies suggest that no unmanned system has been able to down a manned platform, and it could continue for a certain period of time. However, recently reported simulation tests involving the US Air Force Research Lab suggested that an artificial intelligence system was able to defeat a veteran human pilot "repeatedly and convincingly"[86]. Nevertheless, it still remains to be seen if AI-enabled military applications could help an unmanned system in scoring a clear kill against a manned platform in an air-to-air engagement.

79 Mark, A. Gunzinger and David A. Deptula, Toward a Balanced Combat Air Force, CSBA, 2014.

80 Arthur Holland, Michel. Counter-Drone Systems, the Center for the Study of the Drone, 2018.

81 CNN, http://edition.cnn.com/2009/POLITICS/05/18/cia.pakistan.airstrikes/, May 27, 2018.

82 Reuters, https://www.reuters.com/article/us-afghanistan-drones-exclusive/exclusive-afghan-drone-war-data-show-unmanned-flights-dominate-air-campaign-idUSKCN0XH2UZ, Accessed on: May 6, 2019.

83 Paul Scharre, Yes, Unmanned Combat Aircraft Are the Future, War on the Rocks, 2015, https://warontherocks.com/2015/08/yes-unmanned-combat-aircraft-are-thefuture/ , Accessed on: May 6, 2019.

84 Ibid.

85 Paul Scharre, Yes, Unmanned Combat Aircraft Are the Future, War on the Rocks, 2015, https://warontherocks.com/2015/08/yes-unmanned-combat-aircraft-are-thefuture/ , Accessed on: May 6, 2019.

86 Breaking Defense, https://breakingdefense.com/2016/08/artificial-intelligence-drone-defeats-fighter-pilot-the-future/ , Accessed on: May 6, 2019.

4.5. AI and Naval Warfare

Artificial intelligence and greater levels of autonomy will transform naval operations[87]. In particular, autonomous systems will help operational planning, human-machine interactions, C4ISR missions, operational security, and defense against multi-domain threats that require speed and agility.

Ongoing AI-enabled efforts include programs to improve logistics scheduling, aircraft routing[88], elimination of enemy small boat swarms[89], clearing mined areas, and protecting critical ports and infrastructure[90]. Operators' ability to interact with and supervise large quantities of unmanned platforms is growing.

For naval use of AI-enabled systems, challenges are not rare. Specific difficulties emanate from the characteristics of the naval operational environment and how modern artificial intelligence and machine learning systems function. Modern naval operations take place in an environment with too many moving components and dynamic conditions. Vital AI-enabled systems will rely on the accuracy of "pattern recognition" to detect, track, and eliminate a multitude of threats, or simply to assist human decision makers at all levels. The rate of accuracy would be at risk even though very small and novel changes in data patterns. This "*susceptibility*" can also be exploited by adversaries who seek to manipulate autonomous defenses. Moreover, the costs of data collection and data transmission are significantly higher than regular AI applications[91]. Therefore, across-the-force strategies and in-house AI-centric research institutions are crucial enablers for modern armed forces.

4.6. AI and the Informational Battlefield: Initiation to Algorithmic Warfare

Algorithmic Warfare is centered on three main pillars. The first pillar refers to the exponential growth in computer processing power that enabled a boost in the machine-learning capabilities. Secondly, the sudden growth in big-data, married to very large datasets being available, have led to greater 'training capacity' to support learning machines[92]. As a 2018 Australian defense report underlines, *"digital data is growing at an astonishing rate. In 2013, around the time that intelligent machine technology development quickened, the world produced 4.4 zettabytes of data. (A zettabyte is 10 21 i.e. a one followed by 21 zeros.) By 2020, this annual production rate is expected to be 44 zettabytes and, by 2025, 163 zettabytes"*[93]. Thirdly and finally, cloud-based technologies have allowed data resourcing and off-board processing[94]. On the other hand, as the world witnesses exponential growth in the data available, one cannot say the same for the required manpower to analyze and disseminate the intelligence inputs. Open-source assessments indicate that while the US Air Force generated approximately 1,600 hours of video per day back in 2014, such a large undigested intel needed some 100,000 individuals to process, exploit, and disseminate the data[95].

87 Connor S. McLemore and Hans Lauzen. The Dawn of Artificial Intelligence in Naval Warfare, War on the Rocks, https://warontherocks.com/2018/06/the-dawn-of-artificial-intelligence-in-naval-warfare/ , Accessed on: April 17, 2019.

88 Ertan Yakici et al. Daily Aircraft Routing for Amphibious Ready Groups, Annals of Operations Research, 2018.

89 Navy Could Use AI to Combat Swarms of Enemy Boats, The US Department of Defense, https://www.defense.gov/explore/story/Article/1825907/navy-could-use-ai-to-combat-swarms-of-enemy-boats/ , Accessed on: May 4, 2019.

90 Rob Wittman. US Navy's Unmanned Vehicle Efforts Are the Answer to Deterring Adversaries, Defense News, https://www.defensenews.com/unmanned/2018/04/26/us-navys-unmanned-vehicle-efforts-are-the-answer-to-deterring-adversaries/ , Accessed on: April 15, 2019.

91 Connor S. McLemore and Hans Lauzen. The Dawn of Artificial Intelligence in Naval Warfare, War on the Rocks, https://warontherocks.com/2018/06/the-dawn-of-artificial-intelligence-in-naval-warfare/ , Accessed on: April 17, 2019.

92 For a detailed study on Algorithmic Warfare, enabler technologies and emerging doctrines, see: Peter, Layton. Algorithmic Warfare: Applying Artificial Intelligence to Warfighting, Australian Air Power Development Centre, 2018.

93 Ibid. p.10

94 Ibid. p.5

95 Shaun, Williams and Jacob Hess. "The Combat Cloud Across the Range of Military Operations: Interagency Coordination", OTH, August 2017, https://othjournal.com/2017/08/09/intergovernmental-combat-cloud/, Accessed on: April 17, 2019.

To date, the US Department of Defense's (DoD) Project Maven has been one of the most tangible manifestations of Algorithmic Warfare. According to the US DoD, the project uses biologically inspired neural networks and deep learning to autonomously detect objects of interest from still or moving imagery[96]. The project was designed to address the insufficiency in the available intelligence analyst pool when assessing the massive amount of undigested inputs from global counter-terrorism surveillance. In fact, the rapid growth in the available data harvested from intensive aerial surveillance – for about 95% of the intelligence on ISIS comes from drone imagery – on the ISIS terrorists has hastened the 'experimental combat debut' of Project Maven[97].

Project Maven also revealed how ethical issues in next-generation warfare could play out. Following intensive reactions from its employees who think the company should not be involved in defense projects, Google chose not to seek another contact with Pentagon on this very portfolio[98]. Nevertheless, experts estimated that many other tech companies would be happy to replace Google, having reminded that Amazon, Microsoft, and IBM were among the original bidders of the project tender[99]. Notably, at the time of writing, Microsoft and Amazon were among the last standing competitors in a lucrative, winner-take-all, $10 billion contract for the Pentagon's cloud services[100] (the JEDI-Joint Enterprise Defense Infrastructure), while Google decided not to bid[101].

As AI algorithms assist or even replace human decision making in key social, legal, and economic applications, bias and discrimination in key AI-assisted procedures have become key policy issues. AI misbehavior is deeply rooted in data that train these systems which can have a huge social and political impact through justice, law enforcement, education, recruitment, or credit scoring applications.

Algorithmic errors and biases in simple applications for individuals' daily use may cause minimum impact. Potentially, the significant security risk may emerge in critical infrastructure, defense and military, healthcare, financial system, the justice system and other key pillars of modern governance. The "*scored societies*" concept raises concerns about potential bias and discrimination issues at larger scales, risking the victimization of certain groups of people[102].

There are many applications and promising features that would diminish the risk of social bias on a daily basis. However, concerns about unfairness, injustice, and discrimination emanate from the core characteristics of modern machine learning techniques. Notably, such risks exist regardless of the initial intention and objective of a given application[103]. Design of modern artificial intelligence and machine learning algorithms rely on the accuracy of their learned behavior. These algorithms depend on training data that are either given and labeled by the programmer or extracted from their environment through various mechanisms and complex procedures. The "black box" aspects of machine learning as well as the variety and veracity of data sometimes cause algorithmic systems' misbehavior. Moreover, the underlying mechanisms in learning agents' workflow cause significant vulnerabilities and security risks that malign actors could exploit[104]. Without technical and policy-level solutions, one

96 The US Department of Defense, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End", July 2017, https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/, Accessed on: April 16, 2019.

97 Defense One, https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/, Accessed on: April 16, 2019.

98 Scott, Shane. et.al. "How a Pentagon Contract Became an Identity Crisis for Google, The New York Times, March 2018, https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html, Accessed on: April 16, 2019.

99 Lara, Seligman. "Pentagon's AI Surge on Track, Despite Google Protest", June 2018, https://foreignpolicy.com/2018/06/29/google-protest-wont-stop-pentagons-a-i-revolution/, Accessed on: April 16, 2019.

100 Fortune, http://fortune.com/2019/04/10/pentagon-jedi-project-amazon-microsoft-cloud-services/, Accessed on: April 16, 2019.

101 Nextgov, https://www.nextgov.com/it-modernization/2018/10/microsoft-amazon-ceos-standby-defense-work-after-google-bails-jedi/152047/, Accessed on: April 16, 2019.

102 Osonde A. Osoba and William Welser IV. An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, Rand, 2017.

103 Ben Buchanan and Taylor Miller, Machine Learning for Policymakers: What it is and Why it Matters, Belfer Center, 2017.

104 Osonde A. Osoba and William Welser IV. An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence Rand, 2017.

cannot consider AI-enabled systems to be the ultimate remedy to prevent bias in decision-making processes[105].

One of the key differences in how machines and humans learn, in many tasks, is the amount of data used by the learner. More often than not, machine learning needs vast amounts of data to perform well and gain accuracy. In contrast, humans are usually overwhelmed by large amounts of data. Human learning rather includes inter-contextual understanding, interpretation, and knowledge transfer. Such a human-like way of intelligence would be the greatest leap in the progress of artificial intelligence. However, many AI experts think that it may take decades to reach that point[106].

Humans and AI systems have very different decision-making mechanisms which result in completely different kinds of errors when they fail. Combining the strengths of humans and machines, as well as eliminating the weaknesses of each other by teaming up these entities, will be key to integrate AI into modern societies. Such teaming trials have already been carried out in the military realm. However, it can eventually extend to other spheres, even top levels of political decision-making which would change the sense of responsibility and accountability. In addition, human-machine interactions will likely take place in operational levels and in a dual-use nature. Thus, "governance" of this transformation is a must to prevent potential pitfalls[107].

As artificial intelligence systems in many areas either replace or team up with humans, the question of how they should make decisions fuels an overarching debate on AI ethics. The extent of human involvement in areas where AI algorithms and autonomous systems would be able to decide even without any human in the loop remains a pressing policy debate. In particular, international non-governmental organizations, scientists, and tech industry figures have been calling for a complete ban on autonomous weapons systems that can choose and engage their targets independently. The increasing availability of smart unmanned systems will amplify the difficulties ahead of potential international regimes, norms, and regulations.

Finally, morality and normative aspects of AI-enabled autonomous decisions can affect not only the security-related applications, but also a variety of areas ranging from self-driving cars to economic, financial, and legal use of intelligent agents. Fitting the AI algorithms with "human moral compass" is inherently difficult[108].

4.7. AI and Cyber Warfare: The Big Ambiguity in Possible Trajectories

Similar to applications in other fields, artificial intelligence will introduce more autonomous systems and quantitatively diminished workforce requirements to cybersecurity and cyber defense. Increasingly intelligent agents will amplify the capabilities of human operators. In particular, AI enhancements will enable timely detection of vulnerabilities and weaknesses in cyber infrastructure. Machine learning algorithms will go beyond extrapolation from previous experiences and become even more capable of identifying anomalies[109]. However, AI-enhanced systems will augment offensive techniques and strategies too. Sophisticated tools are likely to become available in black markets, causing a significant diversification of potential hostile actors[110].

Finally, AI-enabled systems are likely to play increasingly larger roles in modern infrastructures, transportation tools, financial systems, and other areas where they involve in operational tasks and decision-making processes. As a result of highly connected networks, algorithmic errors or hostile attacks can cause significant damage and systemic failure in the absence of preemptive measures[111].

All in all, AI-enabled systems are likely to be weaponized and used in the cyberspace for both defensive and offensive purposes[112]. For the time being, its implications for the strategic balance of power remain to be seen.

104 Osonde A. Osoba and William Welser IV. An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence Rand, 2017.

105 Ben Buchanan and Taylor Miller, Machine Learning for Policymakers: What it is and Why it Matters, Belfer Center, 2017.

106 Ben Buchanan and Taylor Miller. Machine Learning for Policymakers: What it is and Why it Matters, Belfer Center, 2017.

107 M. L. Cummings, Heather Roff, Kenneth Cukier, Jacob Parakilas, and Hannah Bryce. Artificial Intelligence and International Affairs: Disruption Anticipated, Chatham House, The Royal Institute of International Affairs, 2018.

108 Intro to AI for Policy Makers: Understanding the Shift, Brookfield Institute, Policy Innovation Hub, Ontario, 2018.

109 Greg Allen and Taniel Chan. Artificial Intelligence and National Security, Belfer Center for Science and International Affairs, 2017.

110 Ibid.

111 Osonde A. Osoba and William Welser. The Risks of Artificial Intelligence to Security and the Future of Work, RAND, 2017.

112 Ibid.

4.8. AI and the Cognitive Battlefield: Information Operations and Political Warfare

New technologies encourage all types of actors, individuals, groups, and states alike, to conduct influence operations and manipulation at scale. Intelligent algorithms are used to identify susceptible groups of people and also to "measure the response of individuals as well as crowds to influence efforts"[113]. The implementation of "cognitive hacking" takes place on a diverse set of platforms including social media and new forms of traditional news channels. The mediums are also diversified, as distorted and false texts, images, videos, and sounds are weaponized to augment desired psychosocial effects. As Waltzman suggested during a congressional testimony, "cognitive security" is one of the new multi-sectoral fields in which actors engage in "a continual arms race to influence -and protect from influence large groups of people online"[114].

Impact of artificial intelligence systems in each step of the information operations cycle will continue to gain momentum. For example, reconnaissance, surveillance, and espionage activities will employ such systems to either steal aggregated data or to extract and analyze open source information on groups or individuals. Generative Adversarial Networks (GANs), a form of deep neural network algorithms, already produce realistic fake videos and images. On the other hand, artificial intelligence is the only promising means to tackle the given set of threats through technical counter-measures. The tech industry (especially social media platforms), governments, and news organizations will have to employ smart systems to detect, stop, filter out, or debunk sophisticated malicious content, and also to ensure the security of sensitive data. As mentioned earlier, whole-of-government approaches and multi-sectoral partnerships will be crucial to tackle hostile activities in a continuously changing information environment.

Governments and their security apparatuses worldwide aim to adapt to evolving characteristics of information, how it flows, received, and processed. Modern information environment continues to transform, mostly due to the rapid progress in relevant technologies. This transformation covers the entire cyberspace, including human perceptions, cognition, emotions, and decision making. For example, the Joint Concept for Operating in the Information Environment of the U.S. Joint Chiefs of Staff (2018) acknowledges the "rapidly evolving information environment" to be one of the core domains of future military operations. It asserts that both state and non-state adversarial actors would "combine new strategies and new technologies (artificial intelligence, big data, neuro-technological, etc.) with traditional techniques such as violence, propaganda, and deception to support their efforts..."[115]. Enhanced and largely "democratized" capabilities to weaponize realistic fake images, videos, and sounds will add to the existing hybrid threats in the imminent future. Without preventive policy actions and counter-measures, the strengthened hostile information operations will risk the erosion of public trust in legitimate information sources and democratic political systems[116].

Future hostile information operations will include more sophisticated systems that can identify, amplify, and exploit the demographic and political "hypersegmentation"[117]. Such characteristics in information consumption already exist and they emanate from psychosocial susceptibilities such as confirmation bias and homophily. In addition, AI-enabled hostile tactics are already gaining an augmented view of the information networks, expanding their toolkit and effectiveness in identifying the most influential network clusters and relevant impactful content[118].

In the given context and an intensely interconnected cyberspace merging humans with smart machines, adversaries may weaponize artificial intelligence for applying enhanced surveillance and coercion on individuals or larger audiences. Adversaries can use aggregated data and knowledge acquired from a variety of sources to attack individuals, groups, and organization for disrupting

113 Rand Waltzman, The Weaponization of Information: The Need for Cognitive Security, The Senate Armed Services Committee, 2017.

114 Ibid.

115 Joint Concept for Operating in the Information Environment (JCOIE), The US Joint Chiefs of Staff, 2018.

116 Greg Allen and Taniel Chan. Artificial Intelligence and National Security, Belfer Center for Science and International Affairs, 2017.

117 Osonde A. Osoba and William Welser. The Risks of Artificial Intelligence to Security and the Future of Work, RAND, 2017.

118 Ibid.

institutional mechanisms, norms, and threatening national security. AI-enabled reconnaissance and surveillance systems are likely to identify vulnerable targets for coercion. Moreover, coordinated hostile action may detect both physical and human-centric weak points of targeted organizations. Therefore, defensive measures will have to prevent the employment of "hacked" humans, information, and cyber infrastructure by adversaries. Detection and elimination of AI "weapon factories" will be one of the most challenging tasks[119], since the development of such offensive tools can take place in a widely distributed and obscure operational landscape.

5. Nato and AI: Securing the Next 70 Years

The world order is becoming more uncertain and unpredictable than ever. Projections for the next decades suggest growing multi-polarity and conflicting interest in the globe, while NATO is to face a set of pressing challenges to ensure collective defense and cooperative security. Some experts suggest that since artificial intelligence, machine learning, and big data will bring a totally new world, NATO nations should initiate a "NATO-mation" vision to address the emerging challenges and capitalize on their geo-economic and technological advantages[120].

As predicted by the US Armed Forces, some revisionist actors are likely to *"employ a range of coercive activities to advance their national interests through combinations of direct and indirect approaches designed to slow, misdirect, and blunt successful responses by targeted states. These hybrid stratagems will be designed to spread confusion and chaos while simultaneously avoiding attribution and potentially retribution. … Should competitors consolidate a measure of regional primacy, the next logical step will be to invest in the capabilities necessary to assert themselves even farther from their borders both globally and across regions. The leading edge of this new global reach will be investments in more advanced cyber capabilities"*[121].

The core value of China's AI industries is expected to exceed 145 billion dollars by 2030, which would mark some 6% of the Chinese GDP[122]. Current predictions suggest a 15.7 trillion-dollars AI economy globally in the same year[123]. Besides, open-source intelligence pieces of evidence suggest that Beijing has been diligently working on developing AI-enabled weapon systems including microscopic robots, unmanned platforms, and cyber agents[124].

The market size for both military and commercial robotics is increasing. Between the years 2000 and 2015, the global spending on military robotics rose from $2.4 billion to $7.5 billion. Projections for 2025 suggest that the figures could well rise up to $16.5 billion. Besides, the consumer-price index data obtained from personal computers market record between 1998 and 2013 reveal that the average price of a computer dropped by 95%. If we are to witness the same cost curve, then the numerical boost in very capable drones could register a real game-changer. Some experts even claimed that under such a cost curve, a number of actors could field billions of insect-like, high-end 3-D printed mini-drones[125]. Such an uptrend will change the very determining parameters of global security, and NATO should be well prepared for a whole new era.

119 Brian D. Johnson, Natalie Vanatta, Alida Draudt, and Julia R. West. The New Dogs of War: The Future of Weaponized Artificial Intelligence, Arizona State University and Army Cyber Institute West Point, 2017.

120 Andrea, Gilli. Preparing for 'NATO-mation': The Atlantic Alliance toward the Age of Artificial Intelligence, NDC, February 2019.

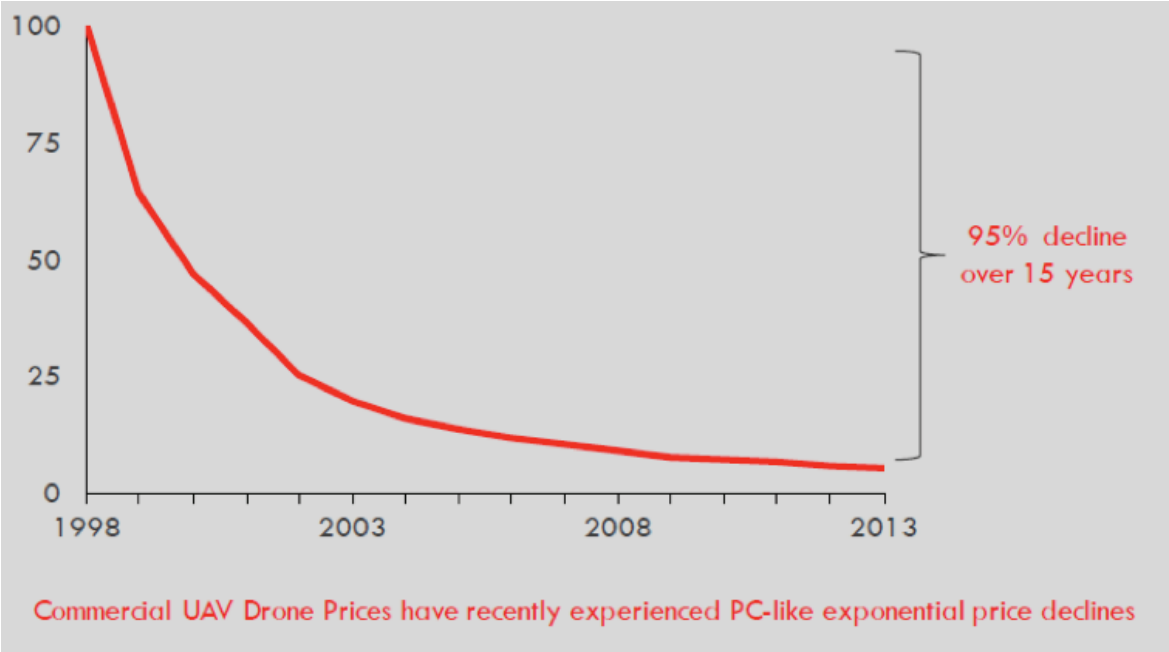
121 The US Joint Chiefs of Staff, Joint Operating Environment 2035, 2016, pp.6-7.

122 Xinhuanet, http://www.xinhuanet.com/english/2018-12/09/c_137660142.htm, Accessed on: May 7, 2019.

123 PWC, https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions/ai-arms-race.html, Accessed on: May 7, 2019.

124 Peter, Apps. "Are China, Russia Winning the AI Arms Race?", Reuters, January 2019, https://www.reuters.com/article/us-apps-ai-commentary/commentary-are-china-russia-winning-the-ai-arms-race-idUSKCN1P91NM, Accessed on: May 7, 2019.

125 Greg, Allen and Taniel Chan. Intelligence and National Security, Harvard Belfer Center, 2017, pp.13-14.



Consumer Price Index for Personal Computers and Peripheral Equipment (Harvard Belfer Center)[126]

One could observe the harbingers of employing AI-related equipment in NATO exercises which is a promising development. But still, the alliance has a long way to go in developing algorithmic warfare capabilities and adopting an AI-led C4ISR architecture[127]. Another issue is that the transatlantic strategic community lacks an ambitious AI vision for the coming decades. Clearly, we do not see something similar to the Chinese strategic thinking on AI and robotics[128] –nor the Russian strategic thinking on information operations– in many NATO capitals. Since most of the innovations in AI and robotics come from outside of the military-industrial complex, some experts have encouraged the alliance to cooperate with GAFA (Google, Amazon, Facebook, Apple) closely, and/or, develop ties with the promising startups[129]. After all, the transatlantic alliance should keep in mind that a disproportional growth in AI and robotics among member nations could inevitably bring about an interoperability gap[130].

Another area of focus would be the values that the North Atlantic Alliance has been defending for decades. Current debates on artificial intelligence are dealing with not only the technological progress, but also bias and discrimination issues in AI systems, management of sensitive personal data, and malicious online behaviors have come on the scene. For instance, the United Kingdom formed an "All-Party Parliamentary Group on Artificial Intelligence", and a "Select Committee on Artificial Intelligence". The United States, during the Obama Administration, adopted the "National Artificial Intelligence Research and Development Strategy", covering important social and economic issues attached to the progress in the AI technology. Recently, a group of lawmakers in the US Congress proposed the "Algorithmic Accountability Act" which would require companies to audit their algorithms. Reportedly, additional bills are also prepared to counter risks of disinformation, and AI-enabled fake content "as a national security threat". Parliamentary groups in the UK and Australia proposed legislative measures to prevent similar harmful use of digital platforms.

126 Greg, Allen and Taniel Chan. Intelligence and National Security, Harvard Belfer Center, 2017, p.14.

127 Defense One, https://www.defenseone.com/technology/2018/05/how-natos-transformation-chief-pushing-alliance-keep-ai/148301/, Accessed on: May 7, 2019.

128 Karlijn, Jans. "NATO Needs to Get Smarter about AI", Atlantic Council, July 2018, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-to-get-smarter-about-ai, Accessed on. May 7, 2019.

129 Martin, Dufour. Will Artificial Intelligence Challenge NATO Interoperability?, NDC, December 2018.

130 Ibid.

EU lawmakers have been actively seeking regulatory action in the midst of emerging digital threats, data privacy issues, and hostile influence campaigns in recent years[131].

In 2018, a consortium of research institutions (including Future of Humanity Institute, University of Oxford, Centre for the Study Existential Risk, University of Cambridge, and OpenAI) published one of the most comprehensive "call for action" reports on "The Malicious Use of Artificial Intelligence"[132]. The report highlights three primary domains in which existing threats are likely to evolve or new threats would emerge. In the digital security domain, the evolving set of threats include potential large-scale and diversified attacks against physical, human, and software vulnerabilities. In addition, AI systems inherit vulnerable structural characteristics that can be attacked "through adversarial examples and data poisoning"[133]. In the physical security domain, availability and weaponization of autonomous systems create major challenges. Also, cyber-physical attacks against autonomous and self-driving systems and swarm attacks are other potential threat scenarios. Finally, there are also significant risks to political security. AI-enabled surveillance, persuasion, deception, and social manipulation threats will be intensified in the near future. The new AI capabilities may strengthen authoritarian and discriminatory political behavior, and "undermine the ability of democracies to sustain truthful public debates"[134].

NATO nations will need to adapt to the AI-driven transformation and develop an acceptable level of consensus in this respect. As mentioned earlier in this paper, artificial intelligence is likely to cause major economic and workforce shifts. More critically, it can change how the geopolitical competition is played out. It will also equip authoritarian states, some of which are NATO nations' current and future competitors, with new oppressive and discriminatory tools. Besides, AI can offer increasingly smart autonomous weapons systems to state and non-state actors. Therefore, in the simplest terms, the transatlantic strategic community's new agenda will have their plate full of tasks, ranging from observing how such dynamics develop in different regions to building international partnerships to ensure common interests and regulatory actions. Diplomatic endeavors that promote peace-building, human rights, and democratic norms may have to deal with ever strengthening toolkit of violent groups and oppressive states, especially those who would employ AI for surveillance, coercion, and hostile information operations. Thus, preventing terrorist groups from seizing lethal autonomous systems and finding ways to deal with digitalized authoritarianism will soon be a top international agenda[135].

Last but not least, AI could also cause drastic changes in hybrid warfare which remains a key concern for NATO. Cyber-enabled information warfare is now a core pillar of modern military campaigns and below-the-threshold-of-war operations. From Ukraine to Syria, Iraq, and other contemporary battle-spaces, the impact of information operations has multiplied. Moreover, both state and non-state actors are now able to use cyberspace to influence large groups of civilians and opposing forces. From reconnaissance activities detecting and profiling target audiences to the weaponization of distorted or fake information and psychological operations, artificial intelligence will enhance offensive capabilities in information warfare. This could bring a new set of significant vulnerabilities for NATO. The AI-driven paradigm shift urges states to adopt whole-of-government approaches to counter such emerging challenges. Furthermore, AI and cyber-enabled information warfare threats exist in a highly dynamic information environment where hostile actors have proven to be tremendously adaptive. Thus, the agility of defensive measures relies on enhanced allied training, exercises, red teaming activities, and constant sharing of lessons learned.

131 Karen Hao, Congress wants to protect you from biased algorithms, deepfakes, and other bad AI, MIT Technology Review, 2019, https://www.technologyreview.com/s/613310/congress-wants-to-protect-you-from-biased-algorithms-deepfakes-and-other-bad-ai/, Accessed on: April 21, 2019.

132 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.

133 Ibid.

134 Ibid.

135 Ben Scott et.al. Artificial Intelligence and Foreign Policy, Stiftung Neue Verantwortung, 2018.

Conclusion and Recommendations

The AI revolution and accompanying technologies are transforming the geopolitical competition. Its wide-ranging impact will continue to occur for the foreseeable future with many unpredictable long-term outcomes.

As AI, machine learning, big data, and autonomous systems development rely on various factors such as data, workforce, computing power, and semiconductors, international disparities may widen in the near future.

International partnerships are key to tackle the challenges outlined in this report. The transatlantic alliance should deal with internal and external AI capability disparities.

NATO needs to increase its readiness levels for emerging security threats by incorporating all member states into the preparatory action. Future AI-powered and highly interconnected world would not tolerate weak links in defense echelons.

AI and robotics are building a new reality with respect to how nations will fight their battles. This change, at large, will bring about a generational gap in grasping the emerging strategic parameters. Thus, the transatlantic alliance needs to empower its new generations, and encourage key posts to be manned by young, bright minds most of whom were born into connected computer societies.

Also, given the sectoral dynamics of AI and defense affairs (considering the fact that commercial projects in the ICT, AI, and robotics are likely to pioneer military modernization programs), we recommend NATO to support young professionals across the allied nations. In doing so, related NATO bodies could provide funding to young startups established by the member state nationals. Multi-national projects, in particular, should be prioritized to boost the allied cohesion and to minimize the interoperability gap mentioned earlier.

NATO needs to establish a multi-disciplinarian researches center of excellence on emerging technologies and their geopolitical impacts. As stated above, while such a center should have direct communication channels with the alliance's leadership positions, it should primarily attract and employ young and bright brains from allied nations. A new international and interdisciplinary research center would enable effective solutions for all the challenges this report mentions. The proposed institution would blend the high-level techno-scientific output from existing NATO bodies such as STO and other centers of excellence with state-of-the-art scientific contributions from member nations and in-house experts.

Comprehensive collective initiatives are known to be effective in nuclear and cybersecurity fields. For instance, the Tallinn Manual provides detailed guidelines on the application of international law to cyber operations. Similar endeavors to unify the governance of normative, legal, and ethical aspects of AI-enabled technologies across the alliance would be a milestone for addressing wide-ranging challenges. Additionally, an AI Planning Group, similar to the Nuclear Planning Group, could be established as a steering committee for the Alliance. Such an initiative would develop a deeper level of strategic planning. Ultimately, it would enable NATO to acquire a more proactive attitude on AI-related matters.

Future battle-spaces will depend on systematic synchronization of physical, informational, and cognitive battlefields augmented by algorithmic warfare. This trilateral structure will re-define key concepts of military sciences such as center of gravity, fog of war, friction, behind the frontline, concentration of forces, and so on. Concept development in the age of AI, big data, and robotics will be more important than ever.

Centre for Economics and Foreign Policy Studies

edam

Foreign Policy & Security 2019/8

May 2019

WARS OF NONE: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CONFLICT

Can Kasapoğlu, Ph.D. | Director, EDAM Security and Defense Studies Program

Barış Kırdemir, M.Phil. | EDAM - Bosch Cyber Fellow