Military and Security Aspects of Artificial Intelligence

22 Jun 2020

Summary
This paper presents military and security aspects of Artificial Intelligence (AI) as a new area of security policy. AI is commonly understood as the ability of machines to perform tasks that normally require human intelligence and is a key area of advanced computing. Important AI-related techniques include neural networks, deep learning, machine learning, Edge computing and robotics. The concepts and definitions of AI and its impact on engineering are presented. The United States and China compete for technology leadership in AI, followed by Europe. The AI strategies of these actors are presented, with a focus on military projects which include a large variety of unmanned and autonomous vehicles, but also C2 (Command and Control) and Intelligence, Surveillance, and Reconnaissance (ISR) programs.
AI systems have a specific cybersecurity profile, they can serve in cyber-attack detection and automated cyber defense, but have also complex vulnerabilities which can be exploited with new attack types such as data poisoning and adversarial images. AI systems are also of growing importance for information warfare.
Finally, the challenging field of machine logic and ethics is briefly presented.

Contents

1. Fundamentals

1.1 Introduction

Artificial Intelligence (AI) is commonly understood as the ability of machines to perform tasks that normally require human intelligence and is a key area of advanced computing. Important AI-related techniques include neural networks, deep learning, machine learning, Edge computing and robotics. This paper presents military and security aspects of Artificial Intelligence (AI) as a new area of security policy.

1.2 What is Artificial Intelligence?

1.2.1 The DoD Working Definition

Even for human intelligence, there is no standard definition. However, the core of human intelligence definitions includes the mental capacity to recognize, analyze and solve problems, and a human being is then more intelligent if this can be done faster and/or for more complex problems.
Historically, the concept of Artificial Intelligence (AI) focused on machines could be used to simulate human intelligence. A practical definition which covers the common understanding of AI was made by the US *Department of Defense (DoD)*.
The summary of the 2018 DoD AI strategy states that "*AI refers to the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action— whether digitally or as the smart software behind autonomous physical systems*."[1]

Many definitions focus on activities that require human intelligence, but strictly spoken, already the simple pocket calculators of the 1970ies made something that normally requires human intelligence. However, it is evident from literature, the AI researchers mean advanced and autonomous computing when they talk about AI. Therefore, **intelligent agents** are all devices that can perceive the environment and maximize the chance of goal achievement. When a computing application becomes normality, it is typically not considered as AI anymore (**AI effect**), past examples are e.g. pocket calculators, translation computers and chess computers, current examples are navigation systems and home assistant systems like *Alexa, Siri* etc.

The FY2019 National Defense Authorization Act (NDAA) provides a formal definition of AI with 5 types of AI systems[2]:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action

[1] DOD 2018, p.5
[2] NDAA 2019, Section 238

3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.

1.2.2 'Strong' and 'Weak' AI

The so-called 'weak' AI can reproduce an observed behavior and can carry out tasks after training[3], i.e. systems that use machine learning, pattern recognition, data mining or natural language processing. Intelligent systems based on 'weak' AI include e.g. spam filters, self-driving cars, and industrial robots. In contrast, 'strong' AI would be an intelligent system with real consciousness and the ability to think.
The current AI of 2020 is still 'weak' AI with programmed machines that do fast calculations, which allows them to interpret, mimic or predict actions by using data bases and statistical models, but still have no idea of itself and cannot reflect, i.e. they cannot really think or say "I" and "why".

On the other hand, human actions include a lot of repetitive and routine activities which can be standardized and are thus accessible for AI already now. Furthermore, decision making is often only the choice between standard options. Even things that human beings perceive as complex activity, e.g. driving a car from town A to town B, are mostly long sequences of routine activities and standard decisions, for example: The car comes to a traffic light: stop or go?, ….then driving…. a crossing comes: turn left or right?...then driving again… and so on…
This is in a similar way also applicable for industry production and machine activities.

In summary, already current AI systems are able to support or replace human activities in significant parts of daily life, communication, commerce, industry etc. and to support or control all kinds of machine use which explains the massive growth of AI and its enormous potential.

1.2.3 AI-related Techniques

Important AI-related techniques are **neural networks, deep learning, machine learning Edge computing** and **robotics.**

Neural networks: The human brain is processing input with interlinked nodes of nerve cells, the neurons. The processing includes signal transfer, but also filtering by inhibitory neurons. Finally, incoming input patterns can be compared with known patterns to create a reaction. As a simplified example, when the eyes see on the street an object with four wheels, signals are transferred from the eyes' retina to the optical cortex in the posterior

[3] Perez at al 2019, p.6

brain and from there to the neighbored interpretative cortex and memory areas in the Hippocampus region which finally allows to classify the object as ‘car’, even if the specific car model was never seen before.
The same principle is used in AI applications: The input is transferred and filtered through multiple hidden layers of computer areas (nodes), before the output (e.g. object classification, decision) is given.
Neural networks can be acyclic or **feedforward neural networks** where the signal passes in only one direction and **recurrent neural networks** with feedback signals and short-term memories of previous input events.
Deep learning means learning of long chain of causalities based on neural networks while the related concept of **Machine learning (ML)** is focusing on memory (experience) by developing computer algorithms that improve automatically through experience. **Fuzzy logic** focuses on the manipulation of information that is often imprecise, e.g. “put it a bit higher” where algorithm help to transform it into a more precise information.
Natural language processing includes algorithms to understand human language by systematic analysis of the language elements and their relations. A related area is **voice processing**.

A new AI area are **Bio-Inspired Computation Methods** which uses collections of intelligent algorithms and methods that adopt bio-inspired behaviors and characteristics such as genetic algorithms (GA =mutation, recombination and selection of algorithms), evolution strategies (ES), ant colony optimization (ACO), particle swarm optimization (PSO), and artificial immune systems (AIS)[4].

Edge computing is a layer of distributed computers between clouds and users that brings computation and data storage closer to the location where it is needed, to improve response times.

The key concept of **AI and Robotics** tries to optimize the robots’ level of autonomy through learning to enhance the ability to manipulate, navigate and collaborate. Robots can sense the environment by integrated sensors or computer vision which is also a field of AI[5].
In practice, a rise of **co-bots** (co-worker robots) can be observed which support human beings e.g. by taking over repetitive activities such as sorting or carrying things, room disinfection etc.[6].

Historically, AI, machine learning, pattern recognition, robotics etc. were relatively independent research areas, but meanwhile they are increasingly confluent, so a wider understanding of AI includes these areas into the discussion.
The modern concept of automated systems thus includes the originally separate, but now overlapping concepts of autonomy, robotics and AI[7].

[4] Truong/Diep/Celinka 2020, p.24
[5] Perez et al. 2019, p.24
[6] Jung 2020, p.70-71
[7] Hoadley/Sayler 2019, p.4

1.2.4 AI-driven Engineering

1.2.4.1 Computers and Machines

Currently, the typical construction process of larger machines is to embed various computing elements and to connect them to control the machine. A *Eurofighter* Jet has more than 80 computers and 100 kilometers wires[8].
However, this construction leads to a very complex computing environment with a lot of interfaces which increases the risk for communication and compatibility problems as well as software problems, makes it difficult to keep all systems up to date and offers a lot of vulnerabilities for cyber-attacks.

A NATO country decomposed a jet to secure all components against cyber-attacks and re-assembled everything thereafter, but due to the costs it was suggested that component security should be requested from component providers instead[9]. However, this would mean to delegate the IT security to multiple suppliers. Similar checks were done in car hacking and the **walled garden concept** that believes that a system of multiple components can be secured externally as a whole did not stand intrusion tests, i.e. each component would need to be secured individually[10].

The trend is now going forward to create a fully integrated computing system with embedded artificial intelligence elements first and then to align and adapt the machine environment to this as e.g. done in the latest *Tesla* car models[11].
This allows a significant simplification of the IT environment combined with larger data flows and may be an option for other machines as well as e.g. military machines and air planes which are meanwhile (over)loaded with complex computed elements.

1.2.4.2 Computers and Biologic Systems

The embedding of computers is also an issue for biologic organisms. In strict definitions, a **cyborg** (cybernetic organism) is a biologic organism with integrated machine elements. Retinal and cochlear implants as well as pacemakers fulfill this definition already. Note that cyborg development is going much slower than expected, because this approach has a very limited potential. Among other problems, the interfaces between living and computer sections are challenging. Another issue is the energy supply for the machine parts as any heat or radiation would damage the surrounding tissue. The immune system and the surrounding tissue tend to react against the implants with inflammation, rejection and fibrosis. Maintenance and repair requirements are already used as backdoors for cyberattacks. In summary, the amount of machine parts that an organism may be able to carry seems to be quite limited.

Compared to this, **autonomous biohybrids**, free combinations of biological and synthetic materials seem to have a much larger potential. Here, tailor-made biologic material is

[8] Köpke/Demmer 2016, p.2
[9] Leithäuser 2016, p.8
[10] Mahaffey 2016, p. V6
[11] Floemer 2020

composed around computed machines elements and artificial intelligence could provide the autonomy to this system.

In 2016, a swimming robot that mimicked a ray fish was constructed with a microfabricated gold skeleton and a rubber body powered by 200,000 rat heart muscle cells[12]. The cells were genetically modified so that speed and direction of the ray was controlled by modulating light. However, the biohybrid was still dependent from the presence of a physiologic salt solution.

Currently, three key technologies are in development which may enable advanced biohybrids, these are **artificial cells**, **organoids** and **synthetic/artificial genomes**.

Since 2010, a **minimal genome** cell is developed, this is the smallest possible genome that allows autonomous life and replication[13]. In 2016, a new cell, called *Syn 3.0*, was created by replacing the genome of *Mycoplasma capricolum* with the genome of *Mycoplasma mycoides*, with removal of unessential DNA[14]. After it was found that a slightly larger genome than the smallest possible leads to improved cell growth, a modified minimal cell was created which allowed to reduce the number of genes with unknown function to 30 in the year 2019[15]. If the function of these 30 genes could be clarified, the basic mechanisms of living cells are identified and could then be used to create freely **designable artificial cells**.

Also, the control of cell differentiation has made substantial progress: **Organoids** are small **artificial organs** created by targeted application of growth factors and hormones to stem cells with many functionalities of the original organ, e.g. lungs and airways[16] for studies of coronavirus infections, but also other organoids like small brains.

The other matter is **synthetic genomes**[17]. The rapid technical progress of DNA synthesis allows meanwhile a synthesis of **artificial chromosomes** for *Yeast (S. cerevisiae)*. Together with designable cells this technology may allow large-scale genomic variation and optimization.

2. AI Strategies

2.1 Introduction

The United States and China compete for technology leadership in AI, followed by Europe as third largest actor.

As for other advanced technologies, research is done by three groups, i.e. state, private companies and academic research. In complex projects, these groups cooperate with each other and the state tries to coordinate and fund the AI projects of highest strategic value. In the security sectors, this means those applications with highest impact on military and intelligence capabilities.

[12] Park et al. 2016
[13] Kastilan 2010
[14] Danchin/Fang 2016
[15] Lachance et al. 2019
[16] Elbadawi/Efferth 2020, Heide/Huttner/Mora-Bermudez 2018
[17] Wang/Zhang 2019, p.23

The key strategic challenge is to identify these strategic AI applications and to ensure coordination for rapid development and deployment.

2.2 The AI Strategy of the United States

The *Presidential Executive Order on Maintaining American Leadership in AI*[18] was signed on 11 February 2019. The executive order emphasized the importance of continued American leadership in AI for its economic and national security and for shaping the global evolution of AI in a manner consistent with its values, principles, and priorities. At the same time, the DoD released an unclassified summary of its AI strategy with a clear focus on the *Joint Artificial Intelligence Center (JAIC)* for strategy implementation[19].

Note that a primary strategic direction for the future is the cooperation with the Intelligence Services (here meaning secret services) of the *Five Eyes*-Group (US, UK, CDN, AUS, NZ) and then secondary within the NATO[20].

In June 2019, the *White House Office of Science and Technology Policy's National Science and Technology Council* released the National *AI R&D Strategic Plan* which defined key strategies for Federal AI R&D investments[21].

The United States systematically expanded the institutional framework for AI research and funding[22].

[18] Trump 2019
[19] DoD 2018, p.9
[20] NSCAI 2020, p.4
[21] OSTP 2020, p.6
[22] Hoadley/Sayler 2019, p.9-10, RAND 2019, DoD 2018, OSTP 2020, NSCAI 2020

Sector/Administration	**Institution**	**AI impact**
Military		
Department of Defense DoD	Joint Artificial Intelligence Center (JAIC) since 2019	coordinates the efforts to develop, mature, and transition artificial intelligence technologies into operational use
	National Security Commission on Artificial Intelligence (NSCAI) since 2019	assessment of militarily relevant AI technologies and provides recommendations
	Defense Advanced Research Projects Agency (DARPA) for 60 years	Currently over 20 AI programs
	Defense Innovation Unit DIU since 2016	DIU works with companies to prototype commercial solutions against DoD problems. Contracts are typically awarded in less than 90 days
Intelligence		
Office of the Director of National Intelligence ODNI	Intelligence Advanced Research Projects Agency (IARPA) since 2007, integrated precursor agencies from NSA, NGA and CIA	Similar purpose like DARPA, but with focus on intelligence. Initiated the Algorithmic Warfare Cross-Functional Team (Project Maven) which will be transferred to JAIC. *Project Maven*: since 2017 for automating intelligence processing with computer vision and machine learning algorithms for target identification from drone data Other AI programs include developing algorithms for multilingual speech recognition and translation in noisy environments, geo-locating images without the associated metadata, fusing 2-D images to create 3-D models, and analysis tools to infer a building's function based on pattern-of-life analysis
Central Intelligence Agency CIA	[has own firm In-Q-Tel for cooperation with start-ups]	Around 140 projects focusing on AI e.g. for image recognition and predictive analytics
Civil Sector		
Department of Energy DOE	Artificial Intelligence and Technology Office	to accelerate DOE's AI capabilities, ensuring the national and economic security
Government		
National Science and Technology Council NSTC	The Select Committee on AI since 2018	Consists of heads of departments and agencies principally responsible for the government's AI R&D (Research and Development) under the Information Technology R&D (NITRD) Subcommittee
	The Machine Learning and Artificial Intelligence (MLAI) Subcommittee	The MLAI Subcommittee monitors the state of the art in machine learning (ML) and artificial intelligence (AI) and reports to the NSTC Committee on Technology and the Select Committee on AI
	The AI R&D Interagency Working Group	It operates under the NSTC's NITRD Subcommittee and consists of research program managers and technical experts from across the Federal Government and reports to the MLAI and NITRD Subcommittees

2.3 The AI Strategy of China

According to the 2017 *New Generation AI Development Plan*, China is aiming to become the global AI leader and develop a domestic AI market worth USD 150 billion by 2030[23]. The Chinese government views AI as an opportunity to "leapfrog" the United States by focusing on AI for enhanced battlefield decision-making, cyber capabilities, cruise missiles, and autonomous vehicles in all military domains[24].

In 2017, a civilian Chinese university demonstrated an AI-enabled swarm of 1,000 uninhabited aerial vehicles at an airshow. To accelerate the transfer of AI technology from commercial companies and research institutions to the military as *Civil-Military Integration (CMI)*, the Chinese government created a *Military-Civil Fusion Development Commission* in 2017[25].

The concept as given in the *Defense White Paper (DWP)* from 2019, it the development of warfare from mechanization to informationisation and now with A.I. to 'intelligentisation'. Thus, for the Chinese army PLA, AI is essential for "**intelligentised warfare**"[26]. The practical strategic approach is to provide directions and resources centrally, but to implement locally, so that competition between Chinese cities and regions for AI-research is activated. To strengthen academic capabilities, hundreds of new AI professorships were established.

The military AI research focus is on Command and Control and on a broad spectrum of unmanned vehicles.

China is further investing in U.S. companies working on militarily relevant AI applications, potentially granting it lawful access to technology and intellectual property, but U.S. is still concerned that industrial and cyber espionage may be conducted also[27].

The largest AI project at the moment is the civilian **China Social Score System**, where health data, financial data (which includes consumption habits), digital data, mobile data and surveillance camera pictures are combined to create behavior, movement and content profiles. Based on output, lower interest rates, easier travel and other advantages (promotions, job offers, better positions in dating platforms thus improving the chance to reproduce) are granted for people with good score, with corresponding disadvantages for people with low scores. The idea is the automated management of a large society[28].

2.4 The Cross-Dependence of the United States and China

Both states are linked to each other with respect to human and technical resources. A cold war-like split into two separate cyber and AI worlds may cause significant problems for both states and the progress of AI as well[29].

Currently, many top Chinese researchers, i.e. those who delivered top papers at AI conferences, work in the US instead of China, even if they made their first academic degree in China. China tries to attract AI researchers with very good job offers, as even after the

[23] Hoadley/Sayler 2019, p.1, NATO 2019, p.10

[24] NATO 2019, p.10

[25] Hoadley/Sayler 2019, p.20-22

[26] Bommakanti 2020, p.3-4

[27] Hoadley/Sayler 2019, p.22-23

[28] Westerheide 2020

[29] Mozur/Metz 2020

Doctorate many Chinese researchers stay for a longer time in US instead of returning to China.
The DoD A.I. key *Project Maven* was developed with the help of a dozen *Google* engineers, many of them Chinese citizens. In particular, oversight was done by the Stanford Professor Dr. Fei-Fei Li. The Pentagon said that they were only working with unclassified data and were the best qualified to do this[30].

Both states are major cyber powers: China is the main producer of physical electronics in computers and smartphones, even US firms outsource their production often to China. This is logic as China is the main owner of computer metals. Digital technologies, such as cell phones and computers, contain rare metals such as niobium, germanium, indium, palladium, cobalt, and tantalum. The US has identified 35 raw materials as critical, for 14 of these raw materials they have no own production. For rare metals, China has 71% market share and 37% of reserves in 2019.[31] A shortage would have a huge impact because recycling could not compensate for the losses. China's very large share of rare metals, which are irreplaceable for the IT industry, is therefore strategically significant.
On the other hand, US dominates the level of central servers and of deep-sea cables. In the physical world, the internet is finally bound to a physical network with a significant level of centralization. The US-based company *Equinix* controls according to their website with their own IXPs and co-location of client computers in their data centers roughly 90% (!) of the data volume transfer of the internet.
China has the impression that US dominates the cyberspace while US feels threatened by Chinas actions in cyberspace, see 5G and *Huawei* dispute in 2019[32].
Also, the NSCAI believes that US has still no credible alternative to the Chinese provider *Huawei* use in 5G[33] which is a major security problem because 5G networks will be a kind of “connective tissue” between AI applications.[34]

2.5 The Balance between Cyber and Physical Power

Computing and AI can support and replace human activities and by this leverage the intelligence and military capacities of a country. This method allows high-tech nations with large economies to consolidate and expand their power.

[30] Mozur/Metz 2020
[31] FAZ 2019, p.17
[32] Security concerns against the Chinese company *Huawei* were expressed by Western countries, as this is meanwhile one of the largest global smartphone producers and also one of the largest infrastructure providers, in particular radio masts for smartphones and other data traffic. The next Internet communication generation **5G** is coming which will allow the first time a broad implementation of **the Internet of Things** and of smart home and smart city solutions, in particular by much higher data flows, real-time transfer massively reduced latency times (transmission delays) under 1 millisecond and also reduced energy need for transfer per bit, refer to Giesen/Mascolo/Tanriverdi 2018
[33] NSCAI 2020, p.54
[34] NSCAI 2020, p.55

But in 2017, the Pentagon, more specifically, the *Strategic Studies Institute (SSI) of* the *U.S. Army War College*, a study based on the so-called **post-primacy scenario**[35], in which the US is still the largest economic and military power, but is no longer able to shape world order due to rising competitors such as China. Thus, geostrategy now has to be re-thought for an unstable, multipolar world that is not necessarily dominated by Western values anymore.
An Australian military study on the US capabilities[36] showed that America's capacity to enforce the liberal order has declined, as the US and its allies accounted for 80% of world defense spending in 1995, which is now down to 52%[37]. The military equipment is overused and overaged with increased accidents due to near-continuous combat in the Near and Middle East region and budget instability caused by debt crisis and parliamentary disputes, training cuts[38]. There is a growing mismatch between strategy and resources.
The conclusion is that this *"...requires hard strategic choices which the United States may be unwilling or unable to make. In an era of constrained budgets and multiplying geopolitical flashpoints, prioritizing great power competition with China means America's armed forces must scale back other global responsibilities. A growing number of defense planners understand this trade-off. But political leaders and much of the foreign policy establishment remain wedded to a superpower mindset that regards America's role in the world as defending an expansive liberal order."* [39] Trade-off means to reduce the burden in dealing with multiple secondary priorities to achieve the primary goal.

In summary, the focus on cyber and AI activities will only expand the power of a state, if also the physical capabilities are maintained and aligned, otherwise the freedom of action is in danger despite improved knowledge and technology.
Also, there is an ongoing discussion, whether cyber intelligence may be a less risky, remote and cheaper way to do the espionage, but cyber espionage can only complement conventional espionage work and cannot replace the presence of local agents.

2.6 The AI Strategy of the European Union

The European Commission recently released a *White Paper on Artificial Intelligence* and supports a regulatory and investment-oriented approach with the objectives of promoting AI and of addressing the associated risks against (citation) "a background of fierce global competition".[40]

[35] Lovelace 2017 writes in his foreword: *"The U.S. Department of Defense (DoD) faces persistent fundamental change in its strategic and operating environments. This report suggests this reality is the product of the United States entering or being in the midst of a new, more competitive, post-U.S. primacy environment. Post-primacy conditions promise far-reaching impacts on U.S. national security and defense strategy. Consequently, there is an urgent requirement for DoD to examine and adapt how it develops strategy and describes, identifies, assesses, and communicates corporate-level risk"*
[36] United States Studies Centre 2019
[37] United States Studies Centre 2019, p.11
[38] United States Studies Centre 2019, e.g. p.47-48 amongst others
[39] United States Studies Centre 2019, p.9
[40] EC 2020

The aim is to become a global leader in innovation in the data economy and its applications, but with a regulatory **ecosystem of trust** into these rapidly evolving technologies.
To achieve this, the Commission established a *High-Level Expert Group* that published Guidelines on trustworthy AI in April 2019 with seven key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental wellbeing, and accountability. Further, a *Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics* was prepared. However, the EU has so far no clear strategy for the military dimension of AI[41].
The European Union permanently improves funding, but emphasizes the need to enhance efforts, as some €3.2 billion were invested in AI in Europe in 2016, compared to around €12.1 billion in North America and €6.5 billion in Asia[42].

3. Military Aspects

3.1 An Introductory Case Study: The Eurosur Project

This project was for not for military purposes, but it shows very clearly the vision of fully integrated autonomous control systems. In the European Union, various research projects are evaluating the use of drones which are not steered by a human operator, but by a server for daily routine operations. Relevant projects are INDECT for the internal EU security since 2009[43] and certain others as part of the *European Border Surveillance System (EUROSUR)* which took place between 2008 and 2012.

The *Eurosur* projects were in particular[44]:

- OPARUS (Open Architecture for UAV-based Surveillance Systems) for border surveillance by drones that also intends to ensure integration into civil airspace
- TALOS (Transportable autonomous patrol for land border surveillance) with patrol machines
- WIMAAS (Wide Maritime area airborne surveillance*)* for use of UAVs for maritime control

The concept to conduct daily routine operations of these devices by a control server (*Unmanned Units Command Center UUCC*) was presented as part of these projects, but from a cyber war perspective this server would be the key vulnerability and would need to be maximum secure and resilient.

[41] Franke 2019
[42] EC 2020, p.4
[43] Welchering 2013, p. T6. The research for automatic threat detection focuses on scenarios like the following one. If a camera observes abnormal behavior of an individual, the combination of automatically activated observation drones, microphones and automated face recognition may help to identify the individual and its intentions. If necessary, it is planned to utilize data from Facebook, Twitter, Google plus, credit card data etc. to identify and prevent dangerous activities.
[44] Oparus 2010, SEC 2011, p.7, Talos Cooperation 2012

3.2 Practical Applications

3.2.1 Unmanned Aerial Vehicles (UAVs, Drones)

Drones aka **Unmanned Aerial Vehicles (UAVs)** are meanwhile advanced weapons with growing system autonomy. On the other hand, the defense against drones has also made significant progress.

Drones are not only used for reconnaissance, but also for active fighting. Drones are used for all kinds of operations that are „dull, dirty, dangerous or difficult“[45].

Drones allow observation and/or targeted killing of adversaries as *Lethal Autonomous Weapons Systems (LAWS)*[46]. However, the technical progress allows more and more **assistance functions**, i.e. the human decision making is increasingly supported and influenced by computers[47]. Meanwhile, the creation of a legal '**machine liability**' is now under discussion[48]. Any progress to fully automated drones would require enhanced cyber security efforts to avoid that machines are taken over by adversary hackers[49]. Autonomous drones can avoid detection by communication with control station, so this is part of stealth drone concepts such as the **Lijan** drone tested in 2013 by China[50].

The *Drone Databook* from 2019 summarizes the drone availability and research of 101 countries and uses the *NATO Standardization Agreement 4670* classification ranging from I to III based largely on their maximum take-off weight: Class I (less than 150 kilograms, typically Micro, Mini, and Small Drones), Class II (150 to 600 kilograms, typically "tactical" UAVs), and Class III (more than 600 kilograms as *"medium-altitude long-endurance" (MALE)* or *"high-altitude long-endurance" (HALE)* UAVs) [51].

Most importantly, at least 24 countries are currently developing new military unmanned aircraft (10 Class I systems, 12 Class II systems, and 36 Class III systems). At least seven countries are exploring next-generation drones, including stealthy aircraft (US, China, Russia, and France), high-altitude pseudo-satellites (US, China, UK), swarms (US, China, UK), and manned-unmanned teaming systems (Australia, Japan, UK, China, and the U.S.) [52].

Swarms are AI-based drones which are autonomous (not under centralized control) capable of sensing their local environment and other nearby swarm participants, able to communicate locally with others in the swarm and able to cooperate to perform a given task[53].

[45] Jahn 2011, p.26

[46] Thiel 2012, p. Z2

[47] However, a possible future with fully automated killing decisions remains speculative. The research on **lethal autonomous robots (LARs)** is in progress, Klüver 2013, p.2

[48] In the civil sector, this is discussed in US for self-driving cars (i.e., cars with autopilot functions), Burianski 2012, p.21

[49] The largest drones are meanwhile able to replace conventional airplanes, i.e. an intrusion could create major security risks. The European drone project *Neuron* is an unmanned aerial combat vehicle (UACV) with stealth technology which may be able to execute larger air attacks than current drones (Bittner/Ladurner 2012, p.3; Hanke 2012, p.14).

[50] Gettinger 2019, p.IV

[51] Gettinger 2019, p.IV

[52] Gettinger 2019, p.XV

[53] Hoadley/Sayler 2019, p.14

Chinas drone development focus is on a large variety of Class III drones[54]. Three current US projects for AI drones are *Valkyrie, Skyborg* and *Gremlins*[55].

- The XQ-58A *Valkyrie* is a jet-powered Class III UAV of the Air Force's *Low-Cost Attritable Strike Demonstrator (LCASD)* aka *Loyal Wingman* which can accompany manned aircrafts into combat and e.g. attack enemy air defenses. The first flight took place in 2019.
- *Skyborg* is an Air Force concept for an autonomous low-cost strike drone that could serve as a vessel for testing different artificial intelligence technologies that would enable complex, autonomous operations. A future *Skyborg* UAV could operate alongside the *Valkyrie*, tests fights with manned aircrafts are expected for 2021.
- *Gremlins* is a DARPA program to develop a swarm of low-cost, reusable Class I UAVs which could e.g. used for reconnaissance or electronic warfare.

The functioning of autonomous devices is dependent on the underlying programs which can result in ethical and practical dilemmas[56]. If the programmed habit is known, e.g. drones (like cars) could be intentionally misled, captured or destroyed by mimicking certain situations or objects.

The most important ways to attack drones are:

- **Drone hacking**: by using the **Battle Management Language** commands which are sent on predefined frequencies. The limited costs and efforts needed for such attacks are a key security concern for militaries[57].
- **GPS-spoofing of drones:** sending false coordinates to the drones may mislead them or even urge to do an emergency landing
- **Jamming of drones:** Flooding with electromagnetic signals can induce an emergency landing which allows destruction or even capture of the attacked drones.
- **Physical attacks:** Shooting of drones, but also capturing of drones, even by trained animals, is a growing market for security firms. Also, laser defense is under development.
- **Loss of Communication:** The *EuroHawk* drone combined drone technology derived from the *Global Hawk* drone provided by *Northrop Grumann* and a new advanced reconnaissance technology called *ISIS (Integrated Signal Intelligence System)* from the EADS affiliate *Cassidian*. During a flight to Europe, this drone showed temporary losses of communication for a few minutes which constitute potential windows of opportunity for (cyber) attacks from adversaries. In general, loss of communication can enforce the unplanned landing and require destruction, if there is a relevant danger of takeover by adversaries.

[54] Gettinger 2019, p.16

[55] Gettinger 2019, p.245

[56] Hevelke/Nida-Rümelin 2015, p.82

[57] Welchering 2017

Iraqi insurgents were able to use commercially available software to intrude U.S. drones which allowed them to view the videos of these drones[58]. In 2011, the *Creech Air Force Base* in Nevada that serves as control unit for *Predator*- and *Reaper*- drones reported a computer virus infection; but the US Air Force denied any impact on the availability of the drones[59]. Also, Iran was able to capture a US drone (type RQ-170) in 2011[60]. The vulnerability of drones depends also on the drone type with can have different control modes and grades of system autonomy[61].

The drone technology itself could cause losses of relevant number of drones. So far, most drone losses were caused by handling errors and conventional technical problems.

A systematic analysis by the *Washington Post* revealed 418 drone crashes from 2001 to 2014, main causes were limited capabilities of camera and sensors to avoid collision, pilot errors, mechanical defects and unreliable communication links[62].

Tests in New Mexico 2012 have shown that drones are vulnerable for **GPS spoofing**. The same could be shown for *Automatic Dependent Surveillance Broadcast* systems (ADS-B) that allow tracking of the flight route every second. Also, it was observed that drones can be inadvertently irritated by signals that are intended for other drones.[63]

3.2.2 Autonomous Vehicles

Both US and China are working to incorporate AI into **semiautonomous** and **autonomous vehicles**, in US this includes fighter aircraft (such as the Project *Loyal Wingman*), drones, ground vehicles (such as the remote-controlled *Multi-Utility Tactical Transport MUTT* of the Marine Corps), and naval vessels such as the *Anti-Submarine Warfare Continuous Trail Unmanned Vessel* prototype known as *Sea Hunter*[64].

3.2.3 Intelligence, Surveillance, and Reconnaissance (ISR)

AI is expected to be particularly useful in **Intelligence, Surveillance, and Reconnaissance (ISR)** due to the large data sets available for analysis as in the above-mentioned *Project Maven*. But **Imaging Intelligence** is more than target identification or face recognition, the *Defense Intelligence Agency (DIA)* and the CIA for example supervise adversary buildings with restricted access to analyze activities[65]. Satellites for example daily check Chinese hospitals activity by precise counting of the cars on surrounding parking lots. In a recent study, a massive peak was observed in autumn 2019 which may have been an early sign of the Coronavirus pandemic, because an analysis of the Chinese internet in the same study

[58] Ladurner/Pham 2010, p.12

[59] Los Angeles Times 13 October 2011

[60] Bittner/Ladurner 2012, p.3. As intrusion method, the use of a manipulated GPS signal (GPS spoofing) was discussed, but this could not be proven.

[61] Heider 2006, p.9

[62] Whitlock 2014

[63] Humphreys/Wesson 2014, p.82

[64] Hoadley/Sayler 2019, p.14

[65] Folmer/Margolin 2020

showed that Chinese users in Wuhan increasingly searched with *Baidu* for the terms cough and diarrhea.

3.2.4 Command and Control

Command and Control programs with use of AI are evaluated in China and US. The Air Force is developing a system for *Multi-Domain Command and Control (MDC2)* to centralize planning and execution of air-, space-, cyberspace-, sea-, and land-based operations.[66]

3.2.5 Logistics

AI may also support military logistics[67], the *Defense Innovation Unit (DIU)* and the *US Air Force* are working with the JAIC on **Predictive Maintenance** solutions for maintenance needs on equipment, instead of making repairs or to be stuck to standardized maintenance schedules[68]. For the F-35 jet, real-time sensor data embedded in the aircraft's engines and other onboard systems are put into a predictive algorithm to determine when technicians need to inspect the aircraft or replace parts[69].

[66] Hoadley/Sayler 2019, p.12
[67] Hoadley/Sayler 2019, p.10
[68] DoD 2018, p.11
[69] DoD 2018, Hoadley/Sayler 2019

4. Security Aspects

4.1 Brief Introduction

AI-systems can be manipulated, evaded, and misled resulting in profound security implications for applications such as network monitoring tools, financial systems, or autonomous vehicles[70]. AI has to do with computers, hardware and software, so all common threats to digital systems represent common threats for AI systems as well. For a full presentation of cyber threats, please refer to the Cyberwar Paper in Section 7.2.

Beyond this, there are AI-specific threats which need to be presented in more detail. As the complexity of AI systems is rapidly increasing, it is uncertain whether these problems could be resolved or may be even aggravated in future. The software of AI systems can be stolen, i.e. cyber espionage can eliminate the whole advantage by AI systems.

On the other hand, AI can substantially improve the cyber defense up to automated cyber defense and be a weapon in information warfare.

4.2 Cyber Attacks

Cyber attackers are the so-called hackers, who look for vulnerabilities in programs and systems and then take control with their own programs such as *viruses* or *Trojans*. They try to persuade users by social engineering and phishing to open malicious attachments or websites, to disclose passwords and account information.

There are 4 main targets, namely the normal users, the private sector, the state with politics, administration and public institutions, and the critical infrastructures that are needed for life, such as electricity and water supply, hospitals, etc.

Criminals represent the most frequently acting attacker group, then Intelligence Services, while terrorists and cyber armies have so far barely appeared.

Criminal hackers steal data to sell or exploit the victim's account. Or they use screen blockers (ransomware) to request money for the removal. Sometimes they also use the computers to attack other victims or to create digital money (bitcoin or crypto mining).

Intelligence Services can use hacker teams, so-called **Advanced Persistent Threats (APTs)**, which are active in politics, business and technology, including sabotage. The classic definition defines APTs are longer-term attacking groups with defined **techniques, tactics and programs (TTPs)**.

Recent years have shown that an APT is a project group within an intelligence unit that develops and applies its TTPs and targets along the operational goals of the intelligence unit. APTs do not self-evolve, they are formed by putting together appropriate people and aligning their cyber activities to the operational goals.

Foreign governments and administrations are always interesting and under constant espionage pressure, while normal users are less in focus because it is difficult to filter out something useful from the mass (the needle in the haystack).

The hackers of industrial espionage loot research institutions, high-tech and armaments companies. Sabotage hackers attack factories and critical infrastructures, which has already

[70] NSTC 2020, p.1

led to power outages. Among other things, they can disrupt productions, delete data and damage digital devices or directly the computer chips.

4.3 Key Vulnerabilities of AI Systems

4.3.1 General AI Problems

The early AI systems were simple and thus easily explainable. However, meanwhile **Deep Neural Networks** have arisen, which show very good results, but are based on Deep Learning models which combine learning algorithms with up to hundreds of hidden 'neural' layers and millions of parameters, which makes them to opaque black-box systems, this is known as **Explainability** Issue[71].

The types of AI algorithms that have the highest performance are currently unable to explain their processes. For example, *Google* created an effective system to identify cats in movies, but nobody could explain which element of a cat allowed the identification. This lack of so-called "explainability" is common across all such AI algorithms[72]. But there is a discussion that machines sometimes see common patterns or structures in object classes which human beings simply did not note before.

As a result, nobody can predict when and for what reason an error may occur and AI systems have a limited **predictability**.

Systematic errors: AI system failures may create a significant risk if the systems are deployed at scale, i.e. AI systems may fail simultaneously and in the same way, potentially producing large-scale or destructive effects.

Communication issues: 5G networks will be a kind of "connective tissue" between AI applications which means that everyone who can access the 5G networks can influence (alter, disrupt) the communication.[73]

Misuse of Computing Power: the pure speed of AI makes the systems highly attractive for misuse, e.g. for mining of crypto currency which requires a lot of calculations.[74]

4.3.2 Mission Stability

A specific military AI problem is the **mission stability**[75]. Autonomous military systems can improve reconnaissance and intelligence and can speed up decision making and may also allow rapid reaction, but also may destabilize military missions.

Examples:

- An autonomous drone may decide to attack a relevant target, but by this disclose the military presence and jeopardize Special Forces or Intelligence Operations.
- In the *DARPA Cyber Challenge* of 2016, the best computer was a machine that defended itself on the expense of the defense systems.

[71] Arrieta et al. 2020, p.83

[72] Hoadley/Sayler 2019, p.31

[73] NSCAI 2020, p.55

[74] Goddins 2020

[75] Masuhr 2019, Johnson 2020

- A computer may decide that a combat at a certain location may be a waste of resources and withdraw e.g. a drone swarm, but may never understand that sometimes a certain location has a symbolic and psychological value, or is maybe foreseen as anchor point of a new front line or that the fight is only done to distract adversaries from more important areas. The question is: will an advanced military AI really be able to think strategically or only tactical? Context is still very poorly understood by the systems, i.e. they lack common sense[76].
- Mission authority problem: In civil airplanes, pilots already had to fight against defect autopilots which could not be overridden in critical situations[77].
- An AI may decide to fight too quickly, leaving the conventional forces unprepared or closing the door to a peaceful solution.
- An intruded AI system can be turned against its controller or used as double agent (i.e. it sends observations of both sides to both sides)

Conclusion: The more advanced a military AI will be, the higher the risk for mission instability which may suddenly appear in microseconds.

4.3.3 Data Manipulation

- **Manipulated images** can confuse of autonomous systems. Small stickers on the street were enough to drive the autopilot of a *Tesla* vehicle on the opposite lane[78]. Meanwhile, there are pixel-style camouflage paintings on modern Chinese military vehicles, but also on Russian helicopters.
  Already smallest -for human eyes invisible- changes in digital images can cause systematic misinterpretation by AI, a process known as **adversarial machine learning**[79].
- **Data poisoning:** machines can be systematically misled by mislabeled data. This can be done by tapes in stop signs for traffic[80], but maybe the misuse of military flags and symbols could be another option.
- **Object Dummies** would certainly be able to mislead even autonomous combat drones.
- **Spoofing**: misleading of *Global Positioning System (GPS)* controlled systems by sending a false GPS signal which overrides the right signal, e.g. against drones or ships

4.3.4 Hardware (Inside AI)

An advanced AI system may be able to detect and to react to any attack, but has no chance to defend itself against hardware defects that are inside the AI, which may even allow to take over the AI system from outside:

- **Falsified microchips**

[76] Wright 2020, p.7

[77] Voke 2019 wrote in his analysis on page 33: *„Moreover, if AI is showing improper intentions or acting poorly, humans must be able to override its behavior. Although the system did not perform as required, the human must be able to exercise control once recognition of a hazardous situation occurs. Transparency is a requirement for control, and control is a requirement for trust."*

[78] FAS 2019, p.21

[79] Wolff 2020

[80] Wolff 2020

However, the USA is also afraid of backdoors, in particular in hardware, thus the use of Asian chips is avoided for security-relevant technologies. For the same reason, the US State Department avoids use of Chinese computers within their networks. Nevertheless, military and government cannot produce all hard– and software alone, so the use of **commercial off-the-shelf (COTS)** technology cannot be avoided and will be a source of vulnerabilities. The global supply chain of such products is also a potential source of vulnerabilities: a study of the US senate from 2012 reported that up to one million falsified chips were installed in US weapons, 70% of these chips came from China, but a significant amount came from UK and Canada also[81]. To counter this problem, US government has defined strict requirements for microelectronics used in AI systems[82].

- **Modified motherboards**

China produces 75% of the mobile phones and 90% of all PCs, as even US companies outsource this production step to China. According to a disputed *Bloomberg* report, subcontractor companies in China may have been put under pressure by the hardware hacking unit of the Chinese army PLA to insert these additional chips which would allow total background control[83]. The company *Super Micro* is a provider of server motherboards and during an evaluation of the software company *Elemental Technologies* by *Amazon Web Services (AWS),* a tiny microchip was found, a little bit larger than a grain of rice that was not part of the original design[84]. *Elemental Technology*, which is a development partner of CIA's *In-Q-Tel* since 2009, provided servers to the DoD data centers, the CIA's drone operations and to navy warships.

- **Fuzzing:** Perhaps the strongest cyber weapon is fuzzing, the sending of random codes to chips, which can exploit or even destroy them with far-reaching military consequences: the US stopped the use of Chinese chips in the weapons systems around 2007 in fear to be deactivated during combat. Many chips are susceptible to interference by fuzzing due to construction flaws, some of them can be corrected with external updates, but not all of them, i.e. when the chip is built in, it is too late... The chip makers are trying to fill in the gaps, but constantly new errors are found. Thus, chips should be tested intensively in the existing military technology so that the lights do not suddenly go out when they come too close to the enemy. One of these random commands has the name "*halt and catch fire*" which irreversibly shuts down the computer chip. Although this command could only be executed on certain chips and details were understandably kept secret, it shows that a **'digital rescue shot'** is at least technically possible.[85]

[81] Fahrion 2012, p.1

[82] NSCAI 2020, p.60

[83] Robertson/Riley 2018

[84] Robertson/Riley 2018

[85] It should be noted, however, that in Fuzzing research already earlier commands were found that disturbed that affected the chip functions, which was initially more seen as as an annoying test obstacle.

4.4 Cyber Defense

4.4.1 Cyber Attack Detection

Security firms use Threat Intelligence to match attacks with attack pattern databases, but also use **Intrusion Detection** to scan traffic for unusual events and statistical issues. **Threat Intelligence** repositories compare incoming information with known IP-addresses, domain names, websites and also with lists of known malicious attachments. This allows immediate detection and sometimes even attribution of an incoming attack.

The US Government is currently expanding the use of advanced sensor systems[86]: The *Continuous Diagnostics and Mitigation (CDM)* program provides real-time capacity to sense anomalous behavior and to create reports to administrators on a dashboard. *Einstein 3A* is working by installing sensors at Web access points to keep threats out while CDM should identify them when they are inside.

For cyber defense, US researchers have developed **pattern recognition algorithms**, which allow after attack detection the automated deletion of data packages that are part of the cyber-attack. To avoid escalation, retaliation to networks or systems is not yet automated.

AI methods in cyber-attack detection include to detection or categorization of malware, network intrusions, phishing, and spam attacks which may help to counter *Advanced persistent threats (APT)*; and identify domain generated by *domain generation algorithms (DGAs)* [87].

4.4.2 Automated Cyber Defense

The DoD agency *Defense Advanced Research Projects Agency DARPA* conducted the *Cyber Grand Challenge* on 04 Aug 2016 in Las Vegas, where 7 computers were detecting cyber-attacks and creating responses fully automated, i.e. without any human intervention. This procedure went on for 30 rounds over 12 hours. The computers and their programming teams were selected before out of hundred competitors[88].

A machine called *Mayhem* won the Challenge, the success was achieved by being inactive during most of the rounds, while the other computers fought against each other. However, this meant that the machine has won that rescued itself instead of keeping the defense systems permanently active (which in real combat would mean that the computer prioritizes its existence over everything else). Another machine detected a vulnerability, but the automatically created patch slowed down the machine, so the machine decided to remove the patch [89]

DARPA was satisfied with the results; it was a first step forward to an automated defense and response system[90]. As the number of vulnerabilities is meanwhile immense[91], automated systems may stop unknown or overseen vulnerabilities.

[86] Gerstein 2015, p.4-5

[87] Truong/Diep/Celinka 2020, p.24

[88] DARPA 2016

[89] Atherton 2016

[90] DARPA 2016

[91] A US data base collected 75.000 vulnerabilities in 2015, Betschon 2016; in a test 138 security gaps were found in the Pentagon systems, Die Welt online 2016

However, while it may be possible to give routine surveillance to machines, human supervision cannot be removed. Otherwise, a spoofed (misled) machine could decide to attack the own network. Or an attacker may convince the attacked computer to get inactive or mis-constructed patches may slow down the defense system.

4.5 Information Warfare

The concept of information warfare is well established, e.g. in psychological warfare, targeted information or propaganda was released to adversaries to influence their behavior. The modern information warfare is a bit different, as this is the *combined manipulation of digital technologies and information* to influence adversaries.

Bots (automated actors and communicators in internet) are meanwhile a widespread phenomenon and it is possible to create large amounts of fake tweets and fake human communication (**social bots, internet of thingies**)[92].
A new attack variant is **fake traffic**. In a test, fake traffic software could execute 100,000 clicks on a certain website from one computer, but simulate that each of these clicks came from single different computers.

In summer 2017, a study about **computational propaganda** was published by the University of Oxford[93]. The authors define computational propaganda *„as the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks"*. Currently, *Facebook* and *Twitter* are the main platforms for those activities.
The EU has established a task force which should detect **fake news**, to correct them and also should support a positive perception of the EU in Eastern States[94].

Information can be used as political weapon. In the past, this was called (referring to Russian term) **Kompromat**, which included real and/or fabricated facts about political adversaries to weaken them. AI is enabling increasingly realistic photo, audio, and video fabrications, or "**deep fakes**,"[95]

A modern version are **Leaks**, which can be done by state or non-state actors. While initially leaks were typically released in Internet, meanwhile also intercepted or recorded confidential telephone calls from leading politicians are published.
Artificial intelligence could also be used to create full digital patterns-of-life to create a comprehensive profile of service members, suspected intelligence officers, government officials, or private citizens[96]. An already established approach is the collection and analysis of **user profiles**. In March 2012, *Google* announced that profiles of users can be

[92] Graff 2014, p.13, Brundage et al. 2018, p.43-49
[93] Woolley/Howard 2017
[94] Stabenow 2017, p.3
[95] Hoadley/Sayler 2019, p.11-12
[96] Hoadley/Sayler 2019, p.12

compiled by combining data from search engine usage, *YouTube, Google plus* and Gmail[97]. Similar procedures are also known from social network companies.
Another approach is the **digital dust analysis**. If in Russia or China a new US embassy member is announced, not only the amount, but also the spread of digital information is checked. If the newcomers' digital footprint is too small in social media posts, cell phone calls and debit card payments, then the diplomate is flagged as an undercover CIA officer[98].

5. Ethics and Machine Logic

There are many aspects of AI which may cause ethical problems, e.g. in the military sector, if automated decision-making may end in killing of adversaries. It is common sense that for AI systems a human oversight or at least an emergency override function in case of apparent malfunctions is included.

Another challenge is the **predictability** and **explainability** issue. The specific characteristics of many AI technologies, including opacity ('black box-effect'), complexity, unpredictability and partially autonomous behavior, may make it hard to verify compliance with, and may hamper the effective enforcement of, rules of law to protect fundamental rights[99]. Certain AI algorithms, when exploited, can display gender and racial bias, e.g. for facial analysis. Human decisions can also be biased but, the same bias in widely used AI systems could have a much larger effect, affecting and discriminating many people[100].

While it is possible that AI researchers and their countries are committed to ethical and societal values, it is currently, where AI has limited understanding of situation contexts, very difficult to imagine an AI with embedded values. For example, human beings usually have a clear idea what dignity, justice and fairness means to them, but what are these terms in program code or machine language?
A classic problem of machine ethics and logic is the **collision dilemma** of autonomous cars[101]: a pedestrian may suddenly cross the street and the autonomous car system may be confronted with two options, i.e. dodge and risk the death of the driver or move and risk the death of the pedestrian.

A strong AI system with the ability to ask for the rationale and with an independent understanding of itself (*cogito ergo sum*) may –based on superior knowledge and intelligence- probably not follow human logics and ethics anymore. In the DARPA contest 2016, the machine has won that rescued itself instead of keeping the defense systems permanently active.

[97] Spiegel 2013, p.111
[98] Rohde 2016
[99] EC 2020, page 11-12
[100] EC 2020, page 11-12
[101] Hevelke/Nida-Rümelin 2015

6. Concluding Remarks

This paper presented military and security aspects of Artificial Intelligence (AI) as a new area of security policy. Already current AI systems are able to support or replace human activities in significant parts of daily life, communication, commerce, industry etc. and to support or control all kinds of machine use which explains the massive growth of AI and its enormous potential. The United States and China compete for technology leadership in AI, followed by Europe. The military projects focus on unmanned and autonomous vehicles, C2 (Command and Control) and Intelligence, Surveillance, and Reconnaissance (ISR) programs. China and US are linked to each other with respect to human and technical resources. A cold war-like split into two separate cyber and AI worlds may cause significant problems for both states and the progress of AI as well. It was shown that the focus on cyber and AI activities will only expand the power of a state, if also the physical military capabilities are maintained.

AI systems have a specific cybersecurity profile, they can serve in cyber-attack detection and automated cyber defense, but have also complex vulnerabilities which can be exploited with new attack types such as data poisoning and adversarial images. As the complexity of AI systems is rapidly increasing, it is uncertain whether these problems could be resolved or may be even aggravated in future. AI systems are also of growing importance for information warfare, in particular for deep fakes.

Machine logic and ethics is another challenging issue. A strong AI system with the ability to ask for the rationale and with an independent understanding of itself (cogito ergo sum) may –based on superior knowledge and intelligence- probably not follow human logics and ethics anymore.

7. Literature

7.1 Literature References

Arrieta, A.B. et al. (2020): Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities, and challenges toward responsible AI. Information Fusion 58 (2020), p. 82–111

Atherton, K.D. (2016): DARPA's Cyber Grand Challenge Ends In Triumph. Popular Science 06 Aug 2016, 2 pages

Betschon, S. (2016): Die Crux mit gefälschten Chips. Neue Zürcher Zeitung 31 Aug 2016, p.39

Bittner, J., Ladurner, U. (2012): Die Waffe der Überflieger. Die Zeit No.50/2012, p.2-3

Bommakanti, K. (2020): A.I. in the Chinese Military: Current Initiatives and the Implications for India Observer Research Foundation (ORF) Occasional Paper 234 February 2020

Brundage, M. et al. (2018): The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute University of Oxford/Centre for the Study of Existential Risk University of Cambridge/Center for a New American Security/Electronic Frontier Foundation/OpenAI February 2018

Burianski, M. (2012): Maschinen können nicht haften. Frankfurter Allgemeine Zeitung No. 272/2012, p.21

Danchin A., Fang, G. (2016): Unknown unknowns: essential genes in quest for function. Microb Biotechnol. 2016 Sep;9(5):530-40. doi: 10.1111/1751-7915.12384. Epub 2016 Jul 20

Die Welt online (2016): Pentagon: Hacker finden bei Test 138 Sicherheitslücken. http://www.welt.de/newsticker/news1/article156330187, 1 page

DoD (2018): U.S. Department of Defense, Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity

EC (2020): White Paper On Artificial Intelligence - A European approach to excellence and trust Brussels, 19.2.2020 COM(2020) 65 final

Elbadawi M., Efferth T. (2020): Organoids of human airways to study infectivity and cytopathy of SARS-CoV-2. Lancet Respir Med 2020 Published Online May 21, 2020 https://doi.org/10.1016/S2213-2600(20)30238-1

Fahrion, G. (2012): Pfusch am Gewehr. Financial Times Deutschland, 23 May 2012, p.1

FAS (2019): Sicherheitsexperten manipulieren Teslas Autopiloten. Frankfurter Allgemeine Sonntagszeitung No. 9, 03 April 2019, p.21

FAZ (2019): Amerika will mehr seltene Erden fördern. Frankfurter Allgemeine Zeitung, No.130, p.17

Floemer, A. (2020): Teslas Modell 3 ist VW und Toyota technisch um sechs Jahre voraus. Welt Online 19 Feb 2020

Folmer, K., Margolin, J. (2020): Satellite data suggest Coronavirus may have hit China earlier: Researchers. ABC News online, 08 June 2020

Franke, U.E. (2019): Not smart enough: The poverty of European military thinking on artificial intelligence – ECFR/311 December 2019

Gerstein, D.M. (2015): Strategies for Defending U.S. Government Networks in Cyberspace. RAND Office of External Affairs Document CT-436 June 2015, 7 pages

Gettinger, D. (2019): The Drone Databook. The Center for the Study of The Drone at Bard College, 353 pages

Giesen, C., Mascolo, G. and Tanriverdi, H. (2018): Hört, hört. Süddeutsche Zeitung 14 Dec 2018, p.3

Goddins, D. (2020): Machine-learning clusters in Azure hijacked to mine cryptocurrency. Ars Technica, 11 June 2020

Graff, B. (2014): Sie sind da. Süddeutsche Zeitung No. 107, 10/11 May 2014, p.13

Hanke, T. (2012): Erfolgreicher Probeflug der europäischen Kampfdrohne. Handelsblatt 03 Dec 2012, p.14-15

Heide, M., Huttner W.B. and Mora-Bermudez, F. (2018): Brain organoid models for neocortex development and evolution. Current Opinion in Cell Biology 2018, 55:8–1

Heider, D. (2006): Drohnen im zivilen und militärischen Einsatz. University of Münster 01 Feb 2006, 10 pages

Hevelke, A., Nida-Rümelin, J. (2015): Intelligente Autos im Dilemma. Spektrum der Wissenschaft October 2015, p.82-85

Hoadley D.S., Sayler, K.M. (2019): Artificial Intelligence and National Security Congressional Research Service R45178 Version 6 Updated November 21, 2019

Humphreys, T./Wesson, K. (2014): Drohnen auf Abwegen. Spektrum der Wissenschaft (German Edition of Scientific American) March 2014, p.82-86

Jahn, T. (2011): Das Milliardengeschäft mit den Drohnen. Handelsblatt 25 Nov 2011, p.26

Johnson, J.S. (2020): Artificial Intelligence: A Threat to Strategic Stability. Strategic Studies Quarterly Spring 2020, p.16-39

Jung, A. (2020): Ära der Cobots. Der Spiegel 25/2020, 13 Jun 2020, p.70-71

Kastilan, S. (2010): Vier Flaschen für ein Heureka. Frankfurter Allgemeine Zeitung 21 May 2010, p.33

Klüver, R. (2013): Automaten des Todes. Süddeutsche Zeitung No 187/2013, p.2

Lachance J.C., Rodrigue S., Palsson B.O. (2019): Minimal cells, maximal knowledge. Elife. 2019 Mar 12;8. pii: e45379. doi: 10.7554/eLife.45379.

Ladurner, U., Pham, K. (2010): Iran im Krieg 2.0. Die Zeit No.40, p.12

Los Angeles Times (2011): Air Force says drone computer viruses pose 'no threat'. Los Angeles Times online 13 October 2011, 11:26 am

Lovelace, DC Jr. (2017): in: The Strategic Studies Institute (SSI) and U.S. Army War College Press. At our own peril: DoD risk assessment in a post-primacy world. Principal Author and Project Director: Nathan P. Freier. June 2017

Masuhr, N. (2019): AI in Military Enabling Applications. CSS Analyses in Security Policy No. 251, October 2019

Mozur, P., Metz, C. (2020): A U.S. Secret Weapon in A.I.: Chinese Talent New York Times online 09 June 2020

NATO (2019): Artificial Intelligence: Implications for NATO's Armed Forces. Science and Technology Committee (STC) - Sub-Committee on Technology Trends and Security (STCTTS) Rapporteur: Matej Tonin (Slovenia) 149 STCTTS 19 E rev. 1 fin Original: English 13 October 2019

NDAA (2019): National Defense Authorization Act (NDAA) United States of America 2019

NSCAI (2020): National Security Commission on Artificial Intelligence First quarter Recommendations March 20202, 131 pages

NSTC (2020): Artificial Intelligence and Cybersecurity: Opportunities and Challenges Technical Workshop Summary Report - A report by the Networking & Information Technology Research and Development Subcommittee and the Machine Learning & Artificial Intelligence Subcommittee of the National Science & Technology Council March 2020

Oparus (2010): Oparus Overview and Objectives. Website of the OPARUS project, 3 pages, oparus.eu

OSTP (2020): American Artificial Intelligence Initiative: Year One Annual Report. Prepared by The White House Office of Science and Technology Policy February 2020

Park, S.J. et al. (2016): Phototactic guidance of a tissue-engineered soft-robotic ray. Science 08 Jul 2016: Vol. 353, Issue 6295, pp. 158-162

Perez J.A., Deligianni, F., Ravi D. and Yan G.Z. (2019): Artificial Intelligence and Robotics. The UK-RAS Network

RAND (2019): The Department of Defense Posture for Artificial Intelligence. Rand Corporation Document RR4229 Santa Monica, USA

Robertson, J., Riley, M. (2018): How China used a tiny chip to infiltrate America's top companies. Bloomberg Businessweek 04 Oct 2018

Rohde, D. (2016): Is the CIA ready for the age of Cyberwar? The Atlantic online 02 Nov 2016

SEC (2011): Commission Staff Working Paper. Determining the technical and operational framework of the European Border Surveillance System (EUROSUR) and the actions to be taken for its establishment. Brussels, 28 Jan 2011, SEC (2011) 145 final 11 pages

Spiegel (2013): Verdacht statt Vertrauen, Der Spiegel 26/2013, p.111

Stabenow, M. (2017): Warnung in roten Lettern. Frankfurter Allgemeine Zeitung 25 Jan 2017, p.3

Talos Cooperation (2012): Transportable Autonomous Patrol for Land Border Surveillance D.10.3 4th Workshop 25 May 2012

TAZ online (2013): China testet das "scharfe Schwert". 23 Nov 2013, 4 pages

Thiel, T. (2012): Auf der sicheren Seite. Frankfurter Allgemeine Zeitung No. 281/2012, p.Z1-Z2

Trump, D.J. (2019): Donald J. Trump, Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence, Washington, D.C.: The White House, February 11, 2019.

Truong, T.C., Diep, Q.B. and Zelinka, I: (2020): Artificial Intelligence in the Cyber Domain: Offense and Defense Symmetry 2020, 12, 410; doi:10.3390/sym12030410 www.mdpi.com/journal/symmetry

United States Studies Centre (2019): Townshend A. and Brendan Thomas-Noone with Matilda Steward "Averting crisis: American strategy, military spending and collective defence in the Indo-Pacific," United States Studies Centre at the University of Sydney, August 2019

Voke, M.R. (2019): Artificial Intelligence for Command and Control of Air Power. Wright Flyer Paper No. 72 Air University Press

Wang F., Zhang W. (2019): Synthetic biology: Recent progress, biosafety and biosecurity concerns, and possible solutions. Journal of Biosafety and Biosecurity 1 (2019) 22–30

Welchering, P. (2013): Digitale Überwachungsaugen an jeder Ecke. Frankfurter Allgemeine Zeitung No. 110/2013, p.T6

Welchering, P. (2017): Cyberwar in der Luft - Hacker warnen vor Angriffen. Heute online May 2017

Westerheide, F. (2020): China – The First Artificial Intelligence Superpower. Forbes Cognitive World Contributor Group online 14 Jan 2020

Whitlock, C. (2014): When drones fall from the sky. Washington Post online from 20 June 2014

Wolff, J. (2020): How to Improve Cybersecurity for Artificial Intelligence. Brookings Report 08 June 2020

Woolley, S.C., Howard, P.N. (2017): Computational Propaganda –worldwide– Executive Summary. Working Paper No. 2017.11 University of Oxford, Project on Computational Propaganda 2017, 15 pages

Wright, N.D. (2019): Artificial Intelligence, China, Russia, and the Global Order Technological, Political, Global, and Creative Perspectives. Air University Press in October 2019

7.2 Further Readings

2019 Political Warfare
https://nbn-resolving.org/urn:nbn:de:gbv:700-201909181987

2019 Cyberwar-methods-and-practice
https://repositorium.ub.uni-osnabrueck.de/handle/urn:nbn:de:gbv:700-201907091696

2019 Attribution of Cyber Attacks – Chapter 13 in: Reuter, C. (Hrsg.): Information Technology for Peace and Security, 279-303. ISBN: 9780128117361 Springer Vieweg. Abstract in www.springerprofessional.de/attribution-of-cyber-attacks/16544512