CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Competition between Public and Private AI: Is either at an Advantage?

Master's thesis

Author: Bc. Tomáš Kosub

Study programme: Security Studies

Supervisor: Mgr. Vojtěch Bahenský

Year of the defence: 2021

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on May 4th Bc. Tomáš Kosub

References

KOSUB, Tomáš. *Competition between Public and Private AI: Is either at an Advantage?* Praha, 2021. 78 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Studies. Department of International Relations. Supervisor Mgr. Vojtěch Bahenský

Length of the thesis: 151,610 characters

Abstract

This paper is discussing the latest development of Artificial Intelligence and puts into perspective two major players in the field of AI development – states and private companies. The premise is, that private companies are leading the development of AI technologies and together with their growing impact on states and international relations as such, they are becoming more important and more powerful. We, therefore, research, whether the AI may be to any extend used by these private actors against states. Starting with its dual-use capabilities, we are showing the current threats enabled by AI technology.

We then illustrate specific cases, when Artificial Intelligence was involved in elections in Brazil and the United States and elaborate the argument, that AI may be misused and eventually possess an advantage over the adversary, in these cases private companies. Debating what AI is, what is the current position of major private actors is towards the state, and revealing the potentials of AI, we build up the argument that AI-enabled technologies may indeed be an advantage.

Abstrakt

Tato práce se věnuje aktuálnímu vývoji v oblastni umělé inteligence a srovnává dva nejvýznamější hráče na tomto poli – státy a soukromé společnosti. Předpokladem je, že soukromé společnosti v současné chvíli vedou na poli výzkumu a vývoje technologií založených na umělé inteligenci a s rostoucí úlohou soukromých společností a jejich významem pro státy a mezinárodní vztahy jako takové roste jejich role a význam. Z toho důvodu se věnujeme výzkumu tématu umělé inteligence a tomu, jestli mohou být tyto technologie do nějaké míry využity soukromými společnostmi proti státům. Od argumentace ohledně možného dvojího využití („dual-use“) těchto technologií ilustrujeme hrozby, které umělá inteligence přináší.

Následně na praktických příkladech ilustrujeme, jak byla umělá inteligence využita při volbách v Brazílii a Spojených státech a rozvádíme argument, že umělá inteligence může být zneužita a přinášet tím výhodu potenciálnímu protivníkovi, v tomto případě soukromým společnostem. Vysvětlením pojmu „umělá inteligence“, analýzou současného postavení soukromých společností a nových hrozeb umožněných umělou inteligencí stavíme argument, že tyto technologie mohou představovat výhodu pro potenciálního útočníka.

Keywords

AI, technology, dual-use, conflict, advantage

Klíčová slova

AI, technologie, dual-use, konflikt, výhoda

Název práce

Soukromá AI a stát - potenciál pro konflikt

Acknowledgement

I would like to express my gratitude to the supervisor, Vojta Bahenský, who patiently advised me through the whole process of researching and writing this paper and without whom such result would not be imaginable. I am convinced that thanks to the dedication and interest, Vojta led me to create the best paper I am capable of writing.

I would also like to thank to the members of my family for their support. Lastly, I would like to thank my roommates, Petra, and Lukas, who patiently listened to my complaints for almost a year, most intensively during the never-ending war with Microsoft Word.

Table of Contents

Introduction

The topic of Artificial Intelligence is not new. It was first debated a long time ago, yet its potential was revealed much later, with the development of modern technologies interconnecting people, states, and continents within a fraction of a second. AI is mostly being pictured as a nefarious robot destroying humankind, yet the reality is slightly problematical. Artificial Intelligence is a complex science, incorporating such fields as machine learning, deep learning, and neural networks. The key thing to know about AI is the fact, that it is nothing precise, nothing with a mass or physical existence (we of course exclude the hardware of the system training the AI algorithm). AI is a piece of software, capable of analysing vast amounts of data, capable of finding common aspects, follow patterns, creating a flow of conclusions, and probability-based outputs.

The AI is employing significant research capacity of IT experts, whose task is to develop these systems and train models. Yet these people do not have sufficient time to provide any larger details of such complex topics. Even academics are often short in this field on explaining the potential of an AI system. Despite many papers are related to Artificial Intelligence, only a small portion of them debated its potential for misuse from the side of private companies. We may hear about biases, cases in the past that were enabled by AI, yet the potential is being excluded from the literature. This has a simple reason. AI is in its infancy, we partially understand the "narrow" AI, but that is only the beginning. We do not know, what will further development bring, yet we may elaborate what we know about the potential for misuse of the known AI.

This paper will be spinning about several topics to answer the research question, which is whether the development of Artificial Intelligence by private companies gives them an advantage over states in a conflict? To provide a satisfactory answer to this question, we need to answer several questions first. Such as whether is Artificial Intelligence a dual-use technology? May Artificial Intelligence be used in a conflict with the state? And how may the private companies use Artificial Intelligence against the state? These particular questions shall provide us with sufficient ground to answer the main question of the paper.

This is the ambition of the paper in front of you. Artificial Intelligence is being developed by states, companies and may be also developed by an individual. The boundaries are rather low as for the demands for AI development, yet the power might be devastating. The better model we create and train, the better is the performance. And by performance, we

mean the "enabling potential". AI does not create many new things, but it accelerates and enables many. There are already fields widely using AI in its daily processes. It optimizes food and goods delivery, manages homes, recognizes faces, answers questions, and much more. But it is also used in weapons control systems, aircraft, and rockets. This puts Artificial Intelligence on the edge of dual use.

The primary aim is to answer, whether may Artificial Intelligence or any AI-enabled technology used against the state by a private company. Before approaching the topic of Artificial Intelligence as such, we firstly must demonstrate the hypothesis, that private companies are actively developing Artificial Intelligence systems and the volume of investments is dominantly in the private sector. We will also discuss the historical evolution of the relationship between states and private companies and touch upon the shift in roles of states and private companies as actors. The premise is, that private companies are significant players within international relations and aspire for even more significant positions.

We then explore the meaning of Artificial Intelligence as a dual use technology, explain how it fits the brackets and demonstrate several examples supporting the conclusions. This discussion was made by many researchers before, yet the argumentation was often rather unconvincing and bordering with speculations. Explaining the potential supported by actual cases shall reveal how may the AI be used in civilian and military uses. This chapter further enhances the necessity for discussion upon the Artificial Intelligence future development and perspectives.

The next chapter will be dedicated to practical threats and their assessment by a panel of experts. It contains insights from the private sector, academia, governmental bodies, and other people with insight into the security field and technology. This shall encourage the argument, that many threats previously evaluated as inefficient or not significant rose in their significance and the level of danger due to the development of AI. The cases shall demonstrate two things. Firstly, threats considered mediocre and not damaging are now enabled to target more precisely, perform trustworthy actions, and manage to exponentially increase its reach. The second is more straightforward and shows the variety of threats. From bias and bullying to deep fakes and video impersonation.

The final analytical chapter will deep dive into three cases when was Artificial Intelligence used against states and shows the potential of AI as a dual use technology. These cases demonstrate several features such as the importance of data and privacy or the novelty

of attacks, which further empower the argument that AI is an emerging threat. The argumentation is mostly based on articles and news reports.

The overall story behind the paper is, that private companies are the main engine driving the development of Artificial Intelligence, which is nowadays rather under-regulated. Due to the changes within the international system, where companies are more often considered as actors delivering trust and confidence, their role compared to the state is more and more significant. This creates friction between the corporate power and the state power and leads to a conflict where private actors use Artificial Intelligence empowered systems to gain an advantage over them.

This hypothesis will be thoroughly discussed and advocated. AI, despite not being a new technology per se, is a powerful tool that, if misused, may have significant consequences. The author believes that this topic deserves to be debated deeper, more practically and the consequences must be demonstrated.

Since much information that needs to be researched is not usually covered by academic literature or publicly available articles, I tried to reach roughly 50 institutions to get input directly from the experts. Unfortunately, the response rate was minimal and the same was the rate for the online questionnaires. In total 2 live interviews were conducted, and 2 written inputs were received. Despite such a low number of interviews, the discussions culminated in a slightly different approach to the topic revealing better opportunities for argumentation without changing the aim of the paper. The list of questions and topics discussed may be found in the appendix, just as the list of institutions contacted. Respondents were selected by the industry they were active in / the focus of their research, which was AI, Machine Learning, and Technology. The interviews were addressing questions in the appendix, elaborating them individually based on the interest or importance for the interviewer or interviewee to maximise the added value. The duration was approximately one hour for each.

1 Introduction to the Artificial Intelligence

Before we take a leap into the question in the topic of this paper, we shall understand what is being meant by the term "Artificial Intelligence" since we will work with it on a regular basis. Defining the term is not an easy task, since there does not exist a universal, internationally agreed definition. Even in the academic sphere, the opinions differ, and the private sector provides no clue in this regard either. We shall therefore investigate several definitions, that are closest to the understanding we will be applying in this paper.

A rather straightforward, yet misleading definition is provided by Robert Dilworth in his paper. "Artificial intelligence is the ultimate replication of what the human mind can do" (Dilworth 1988, p. 124). This definition is however so specific, that it cannot be true. If there is any central information or skill other authors point out and this definition is not containing, it is the lack of empathy. Humans are capable of empathy, understanding a difficult situation of another being and take it into consideration. This is one of the reasons why specific crimes are not being punished equally. We may set a lower sentence to a criminal who did his crime out of desperation while having no mercy with someone not expressing regrets whatsoever. Machines are (as of the time of writing this paper) unable to consider these circumstances at all.

Peter Groumpos also tried to define the term Artificial Intelligence. Keywords he used were "nothing precise", "machines capable of human-like thinking" and "based on the information obtained" (Groumpos 2019). This however is not exactly the interpretation we are looking for either. Despite agreeing AI is nothing precise, we may not relate to the term "human-like thinking". The broadness is what is the problem here since people are unique in the ways of how they think. People act based on data most of the time yet when they feel something is not right, they may change the course of action. Machines, however, are not capable (as of the time of writing this paper) of not acting according to the data.

A definition used by RAND in one of their papers focusing on Artificial Intelligence states, „we use the term artificial agents to refer to devices and decision-making aids that rely on automated, data-driven or algorithmic learning procedures" (Osoba & Wesler 2017). This definition addresses the primary difference. It is a device. A machine creating some outcomes, or we may say outputs, to be precise. We defined that it is nothing alive, nothing that may breathe. The form is purely metaphysical, or in the case of the hardware, physical. By hardware we can imagine CPUs (processing units), memory cards, or wires all put

together. But the AI as such may not be touched. The second part of the definition is related to the core of AI – an automated, data-driven processing unit. That is what defines AI as we shall understand it. Despite this definition is broad, I will further below explain, why this approach is necessary to grasp the topic appropriately.

Artificial Intelligence as one term involves to a large degree other technological fields, namely Machine Learning, Deep Learning, and Neural Networks. The inclusion is even more special when we, as IBM describes it, think of them as "[…] Russian nesting dolls. Each is essentially a component of the prior term" (Kavlakogu 2020). These all make up Artificial Intelligence. In accordance with building up our understanding of the matters discussed, I would like to briefly introduce the terms above and explain, how are they related to AI.

1.1 Neural Networks

"Neural networks reflect the behavior of the human brain, allowing computer programs to recognize patterns and solve common problems" (IBM Cloud Education 2020a). Their role is essentially similar to the human brain. The network comprises neurons, called nodes or artificial neurons connected to each other. Each neuron has attributed specific weight determining its importance, and a threshold. To process any data (move them further), the threshold value has to be reached or exceeded, otherwise, the neuron does not send the data to the next layer. Data flow from one layer to the next, output of the previous neuron is input for the current one and this process is being repeated until the data reach the last, output layer. The input is being evaluated under certain criteria, usually to reach the desired goal such as prioritizing the data or storing them. This is due to the fact, that neural nets are being trained for a specific use. In determining whether acquire some company, the neural net has to process huge quantities of data about the company, the market and create a model of the future market to reach an answer. We may create a training dataset obtaining all companies in the World and make the neural net deciding upon acquiring each of them by any other company to train it in decision making or, more accurately, in providing the desired, probability-based output. The more training data we have and use, the more accurate and faster is the output delivered (IBM Cloud Education 2020a).

1.2 Deep Learning

"Deep learning simulates the human brain, enabling systems that learn to identify objects and perform complex tasks with increasing accuracy—all without human intervention" (IBM Cloud Education 2020b). The main purpose of this layer is to constantly improve the learning time and perform calculations more effectively. It is expected that no human input or action is involved in this process. The machine processes the data streams and uses prior results to improve its performance. Analysing inputs from several different sources in real-time, performing calculations, and creating predictions is the main objective of this field. This technology is already vastly used in consumer services. Digital assistants and chatbots are for example products of deep learning. The more we interact (by more we mean thousands or millions of inputs), the better and precise answers we receive.

One specific sub-field of deep learning is called federated learning. The premise is the same. Analytical unit crunching a large amount of data constantly improving in speed, creating the most efficient and thorough patterns to follow. Yet in some cases, the training set of data might just not be sufficient, and the process is, therefore, slower, and the model is trained for much longer. These systems however are used in many situations across multiple companies that are training their own models and collect their own training datasets. Federated learning represents an approach, where all these data are decentralized, saved in a global pool in one location (server for example). Individual units take results of previously analysed data by a different unit and build on the prior results obtained elsewhere.

To better demonstrate what federated learning is, we may use the example of autonomous driving. This activity is considered complex, and full of uncertain situations in which even human actors fail to respond correctly. Each car is collecting data about the road, signs, weather conditions, other cars, and objects on or next to the road and predicts what might happen in the near future to adjust the car to the situation. Despite the vehicle is capable of collecting millions of data points and analyse them within a second, the learning process is not so quick or simple. It requires years of driving a car to get the skill for humans, and the same goes for the car. Federated learning would allow collecting data from all such cars and provide it to the rest of the cars to use for their learning. Some drivers are more active and experience many dangerous road situations from which the car learns whether it is better to slow down or speed up, turn left, or brake. Other cars benefit from this experience and add further data points. This creates a large pool of information about autonomous

driving that every system connected to it may use. Federated learning collects data from multiple vendors to maximize the training dataset and improve the learning curve of the system (Rieke 2019).

1.3 Machine Learning

Lastly, I would like to mention Machine Learning. From the Neural Network data processing to Deep Learning efficiency boost we got to the level when machines use experience from the past to assess and predict the near future. “Machine learning is focused on building applications that learn from data and improve their accuracy over time without being programmed to do so” (IBM Cloud Education 2020c). There are algorithms looking for patterns in huge datasets according to which to act or decide. I shall better demonstrate on recommendation engines. When we use our favorite music application, it is rather likely it has some type of Machine Learning system inside. Every video we watch, every song we listen to is somehow categorized. Whether we listen to metal or watch videos about cats, there are labels describing the content. What the video includes, how are individual topics significant, how many similar videos we watched before. These systems see a pattern containing the major criteria we looked for and presents to us new recommendations on the landing page. The system tries to replicate our thinking processes when deciding upon the music or video and using its vast insight into the app, it puts forward what it believes has the highest probability of our likeliness. It learns constantly and when you use its recommendation, the system monitors it and enforces the pattern. We may say it gets “treated” for doing a good job.

1.4 Is it all about the data then?

Learning processes are always dependent on data. We may create hypotheses, yet to prove them we need data. Artificial Intelligence as an “ability of a computer or machine mimicking the capabilities of the human mind” (IBM Cloud Education 2020d), is certainly not an exception. As people, we may never be even close to the processing capabilities of machines. Artificial Intelligence is the ultimate enabler regarding working with unimaginable amounts of data. Not only are the machines capable of taking such a huge input, but they also process it and come up with a result significantly quicker than humans. Data are all that matters to the AI. “[AI] is completely dependent on the dataset” (Comiter 2019).

Having the data as such is, as I wrote before, a rather untrivial task to fulfill. People receive inputs all their lives and do their best to analyse them properly. Machines may process the data quickly, yet they need those inputs in huge amounts. There is always something to learn or to improve. That is the reason why any AI has not eradicated humanity yet. It is limited in its abilities and every learning takes months, years, or decades. Nowadays Artificial Intelligence may be classified as narrow AI. More on the classification we will be using follows. For now, we must understand the limitations of AI, which lie in the data. Important is not only the quantity but also the quality of the dataset since it comprises the "ultimate knowledge book" of the AI. The data are a truthful source on which are the algorithms trained (Comiter 2019). One rather catchy and valid quote is, that "algorithms are only as good as the data it trains on" (Kozyulin 2019).

Since data collection, its use, and misuse have been a subject of big debate over the past years, I believe that the importance and understanding of data management is one of the key parts of the paper. I shall illustrate several examples of data management from the private sector further in the paper. Some data are openly shared (anonymized such as statistical data – number of phones bought in 2020, cars sold in America, or average income of the household), some are confidential. We see that there are countries openly advocating for privacy rights and confidentiality – such as the General Data Protection Regulation by European Union (EU), but other countries do very little to protect personal data.

1.5 Classification of Artificial Intelligence

The division of AI into classes may be done according to several lines. As we focus on its abilities and possibilities, we shall stick to the one focusing on the maturity level of AI. We will briefly introduce three types of Artificial Intelligence. Artificial narrow intelligence (ANI), Artificial general intelligence (AGI), and Artificial superintelligence (ASI).

In the majority of countries, people are daily in touch with narrow AI. Starting with search engines that are recommending you top pages fitting your criteria, Siri, Alexa, or Cortana – virtual assistants by Apple, Amazon, and Microsoft to image recognition systems and self-driving cars. The fact that we do not see it does not mean it is not there. Narrow AI is very limited in its abilities, it is goal-oriented (meaning it is usually designed to perform one specific task) such as to recognize a face, drive a car, recommend a product. The main distinction is that this form of AI simulates brain processes only within a certain field.

Despite it may seem intelligent, it is only the first step. On the other hand, it is the only AI we were (up to date) capable to develop.

Artificial general intelligence (AGI) is what we may see as a human brain capability machine. The algorithms may learn and apply new knowledge in solving the problem. It is expected that despite "copying" people, the decisions made will be delivered faster, more precisely, and probability-based, not emotional, or sympathetic (O'Carroll 2017).

Lastly, dis-utopian, Artificial Superintelligence (ASI). "ASI is where machines become self-aware and surpass the capacity of human intelligence and ability" (O'Carroll 2017). This form of AI is believed, will outperform humans in every way without any problems. The ability to recognize, discover, follow, and adopt new patterns shall be ultimate. This is one of the reasons why many people are sceptical of AI. At the beginning of 2015, dozens of AI experts signed a document called "An Open Letter on Artificial Intelligence". Between those belong Elon Musk, the late Stephen Hawking, or Steve Wozniak. They warn before the misuse of the technology and recommend approaching the research with caution and rationality (An Open Letter on AI 2015). Musk, one of the founders of Open AI, is frequently warning the public, that AI shall be under the supervision and strictly controlled (Etherington 2020). Stephen Hawking and 3 AI specialists even stated, that the "commercially driven creation of intelligent machines may be our worst mistake in history" (Groumpos 2019, p. 28).

1.6 What is AI for international institutions?

During one of the interviews with the representative of the Artificial Intelligence Policy Development and Coordination Unit within the European Committee, I was advised to take into consideration transnational bodies and their impact and stance towards Artificial Intelligence and data management. When talking about AI on the state and corporate level, we get the needed insight. Yet to understand the dynamism, shortly mentioning the stands of the European Committee may be useful regarding the attitude towards AI development and its use.

At the beginning of 2020, the EC released a White Paper focusing on Artificial Intelligence and its approach towards AI. The European Committee sees AI as a power that unlocks the further potential to grow. Its use in health care, agriculture, effective farming, contribution to climate change mitigation and adaptation, and help in achieving Sustainable

Development Goals are highlighted. Europe would like to be an AI hub, since it has significant potential and importantly, data resources. There are public and industrial data that are under-used. Europe is also a hub in software development and is a producer of a significant amount of industrial and professional service robots. It plans on investing billions of euros into the development of institutions and talent.

Despite the EC is open and positive regarding AI development, it also raises concerns regarding its need for data. “The volume of data produced in the world is growing rapidly, from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025” (European Commission 2020b, p. 4). This is incredible growth in data produced, and the vast majority may be used for learning algorithms. While in countries like China or Russia the concern over private data does not raise any interest, the European Committee and European Union itself debate these concerns. The GDPR limited the collection of data in general, offering online users options to decide upon the use of their data.

Google recently announced that it will stop selling data from the Chrome browser application to third parties. While it may seem like an unimportant announcement, the implications are significant. Instead of selling individual´s data, that are anonymized only slightly, Google introduced a new format, that will enhance the protection more. During its 2019 initiative called „Privacy Sandbox“, Google attempted to sell the browsing and purchasing habits of customers, while preserving their privacy. They then came up with the Federated Learning of Cohorts concept, or FLoC. FLoC still tracks users and monitors their behavior, but it creates so-called cohorts. These cohorts are groups of users with similar browsing habits. This „group anonymization“ does indeed preserve individuals´ data and creates a new concept of approaching the customer´s data protection. Instead of getting inputs about the behavior of every individual, the third party receives the habit patterns of groups of users and their trends (Morrison 2021).

A step similar to the GDPR did the California Consumer Privacy Act of 2018 (CCPA). The consumer has „the right to know about the personal information a business collects about them and how it is used and shared, the right to delete personal information collected from them (with some exceptions), the right to opt-out and the right on non-discrimination for exercising their rights under the CCPA“ (California Consumer Privacy Act 2018).

1.7 Concluding the chapter

Having discussed the approach to the term of AI, its definitions, individual parts, and categorization and explaining why data are key for the use of AI, we shall explain what can be understood as a common understanding of Artificial Intelligence. At its core, it is algorithmic learning. As for now, learning stands for educating the algorithm from data, looking at what patterns work in a certain field. Whether it is a chatbot, a virtual assistant, or a system for driving a car. AI is not an autonomous technology in a way it may reproduce itself. Not now and not without human intervention. Artificial Intelligence as being apparent from the academic and public literature, just as from several interviews is an ultimate enabler. It is, as described by Horowitz in his paper, "[…] electricity. It is an enabling technology" (Horowitz 2018). Therefore, we may not narrow the definition posed at the beginning.

Artificial Intelligence in its narrow form will be used for the purpose of this paper as a default understanding of the term AI. While its potential, wildly debated, is still unknown, it makes processes more efficient, speeds up the data analysis, and discovers patterns not seen before. Yet this AI is not capable of deciding by itself what steps shall it take to extend its knowledge out of the specific field we programmed it for. AI creates probability-based predictions, delivers the value of smart, fast, and accurate data processing.

2 Companies and States in AI Development

With the emergence of Artificial Intelligence, states became intrigued by its potential applications across many fields, including the military. Systems capable of recognizing patterns across the vast amounts of data, coming up with unseen and innovative solutions, and outperforming current standards are obviously of great interest not only to states themselves but also to private companies that envision more effective and efficient processes, lower costs, and precision. Despite these are not the only actors in the arena, the development and use of AI by non-state actors, international organizations or other subjects are beyond the scope of this paper. The primary focus of this paper is to explain, whether there are grounds to believe private actors may misuse Artificial Intelligence against states and whether the use of AI would bring them an advantage. Answering the question of whether AI provides any advantage in a conflict is, therefore, the core of this paper. In the following chapter, we will deep dive into AI funding and research as an indicator of where the current center of the development is. Besides funding, we will focus on the actual technologies developed and debate the processes and dynamism of the whole AI market and its primary driving forces.

The situation is however slightly complicated due to differences in the approach of states to the market and subjects on it. Specifically, we talk about China and Russia (as some of the largest players on the field) and their relation to private companies. When we briefly consider the issue of the word “private” in the context of China, we hear about transparency issues connected to many key business players in the Chinese market. The shareholder´s structure is difficult to be mapped and most often we are unable to tell, whether there is any involvement from the government. Chinese government however has been rather transparent in its goals and ambitions. “The objective is to establish a 'united front' between business and government and facilitate the 'enhancement of the party’s leadership over the private economy. ' According to the plan, 'private economic figures are to be more closely united around the party, ' thereby achieving ' a high degree of consistency with the Party Central Committee on the political stand, political direction, political principles, and political roads' (Olson 2020). From this, we may assume, that private companies in China are private to the degree, when there is no interest of the governing party to control the business activity.

Reading the statements, we may not consider Chinese private companies as strictly private as we do in the case of the United States or the United Kingdom. The concept of

"privateness" is different, emphasizing the fact, that a private company is a subject without a direct connection to the state, meaning that the state has no power in directing the policy or goals of the private actor from the inside. The only tool the state has is legislative, which is being called regulation.

Despite this, we may compare the investments of the governments into Artificial Intelligence. Just as China invests in companies in China devoting their work to the Research & Development of Artificial Intelligence, or AI-related technologies, so do other countries.

2.1 R&D Investments among the Global Players

Government spending on Artificial Intelligence in China, as estimated by the Center for Security and Emerging Technology (CSET). Using data from China´s 2018 Ministry of Finance national expenditure report shows that in total, AI R&D investments are between 2 and 8,4 billion USD (Acharya & Arnold 2019). Despite proclaimed low certainty, these data are rather close to the estimation from 2017 shared by Lieutenant General VeraLinn Jamieson of the US Air Force, stating "[w]e estimate the total spending on artificial intelligence systems in China in 2017 was $12 billion. We also estimate that it will grow to at least $70 billion by 2020" (Pawlyk 2018). In total, China plans to create an industry of AI that shall be worth about 150 billion USD to its economy by 2030 (Metz 2018). On the other hand, we have the United States that invested roughly 5,5 billion USD in 2017 but 16,5 billion USD in 2019 creating a massive growth of 300% (Liu 2020a). Both countries are therefore highly interested in AI applications. From this, we may not however reliably differentiate the flow to development of civilian or to military applications. We only can show the investments at this high level.

Apart from the government spending and investments into Artificial Intelligence, there are private investments (Venture Capital investments or Private Equity funds) that create the major financial income of private actors developing AI. In 2019, the United states VC investments accounted for massive 114 billion dollars heading to technology. China, in second place gained over 45 billion dollars, the UK about 14 billion USD, Germany around 7,5 billion, and France in fifth place with investments about 5,5 billion USD (Tech Nation Report 2020).

If we focus on AI exclusively, the United States dominates private investments with approximately 56% of global AI investments over the last 5 years. The United States alone

raised about 15,7 billion USD in 2019, China accounted for 4,7 billion USD, the United Kingdom in third place with over 1,83 billion, Canada with 1,16 billion, and France with 0,84 billion USD. China was however the only of these five countries recording a fall from the 2018 numbers (Tech Nation Report 2020).

Except for China and the US, one more player is aspiring for domination. The Russian Federation. In 2017 Vladimir Putin, the president of the Russian Federation stated, "[a]rtificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world" (Vincent 2017). The Russian research model is standing alone. The state research institutions account for 72% of domestic R&D and employ approximately 80% of Russian researchers. There is minimal transfer of knowledge and technology between the private and public sectors (Kozyulin 2019). The state is concentrating the research power under the control of the government, and despite investing just a fraction of the US´s R&D budget (estimation of approximately 700 million USD investments into R&D in Russia in 2017), some believe, that the Kremlin has secret expenses reaching up to 3 trillion roubles (over 40,5 billion USD) (Kozyulin 2019). This may mean that the research programs are more significant than we expect.

We see that the amount of money invested in AI is significant. The reason I argue private companies receive much more money than the governments however stands on the ground, that countries do not necessarily invest all their money in government research. Over the last couple of years, governments started to announce joint ventures with private actors in AI development. France, for example, created in 2019 a fund of 5,5 billion dollars that supports the cooperation between the private sphere and the state (CNBC 2019). Canada created an AI-hub called CIFAR (Canadian Institute For Advanced Research), hosting research labs for Facebook, Google, or Uber (Falcon 2018). Some authors agree, that investing in civilian technology development is the better way, reducing the potential of duplicating already developed technology and without any necessity for the state to look for human capacity (Taylor 2019).

Among already mentioned countries, the State of Israel is another vital player on the AI scene with estimated start-up investments of about 2 billion USD in 2017 (which is 60% growth compared to 2016), largely due to the direct involvement of the Israeli government

trying to establish a close connection between the military and the private sector (Slijper, Beck and Kayser 2019).

Between the main application areas of AI, to which the most publicly disclosed funding was aimed between 2015-2019 in the US belongs transportation (17,3%), business services and analysis (15,5%), and sales, retail, and customer relations (12,6%). In China, transportation accounts for 46,5%, arts, leisure, sports, travel, and lifestyle makes 14,3% and security and biometrics were 13,1%. Military and public safety created 0,8% and 0,1% respectively (Arnold, Rakhovsky & Huang 2020).

A portion of the money invested by states does go through funding to private companies – Amazon for example cooperates with the US government on their projects (Sayler, 2020). Private companies can mobilize large amounts of capital. Many authors agree that the private sector is the primary engine for AI developments and advances (Kania 2018). "[…] private sector companies are the leaders in tech invention, not governments" (Horowitz et al. 2018).

2.2 Comparing the investments of state and private actors

If we break up the incomes into the budget for research and development activities for state and for private actors, we have to mention the main issue states face. State entities are, regarding the R&D activities, rather secretive. Despite some works are contracted, the only source of funding them is the budget of the state itself. This may have several reasons yet the main is due to national security concerns. Any involvement of other sources might be considered as a threat to the national security, compromising the research, and states only outsource the work, which is partial and not endangering the security concerns. Usually assuring the security by requiring clearances for the employees.

Private actors however are not limited by the inflow of financial resources. Not only that companies invest huge proportions of their revenues back into R&D, but they may also receive funding in multiple ways. First is the direct way, when states invest in companies, pay them for their services, etc. An example may be the contract between the National Aeronautics and Space Administration (NASA) and company SpaceX for building a Moon Lander. SpaceX specializes in high-tech, space-focused equipment, and delivery systems to the orbit (among many other things) and to other celestial bodies, most notably the Starship project aiming for Mars or now the lunar lander aiming for the Moon. The main activity of

SpaceX is of course research and development. Winning the 2,9-billion-dollar contract with NASA incentivizes their development and pushes their abilities regarding further space exploration (Davenport 2021). Given the unique technology of recovering boosters and fairing systems, SpaceX can save millions of dollars, that may be invested elsewhere. The Falcon 9 project used for delivering the payload to the Low Earth Orbit and to the ISS is the current money-maker of the company. Now, SpaceX is launching boosters for the ninth time. This reliability causes significant savings. If SpaceX uses the booster ten times out of which only four are for a commercial client, the company has all costs paid for 6 more launches. This means that from the fifth launch on, SpaceX operates essentially "for free" and may launch its own Starlink satellites to the orbit (ElonX Net 2020).

Just as direct investments may come from the "home state" (meaning the state where the company has its HQ), it may come from abroad. As mentioned before, the United States attracted most foreign direct investments into technology and AI, globally estimated to 15,7 billion dollars in 2019. The most popular source is the Private Equity (PE) or Venture Capital (VC) funds. These amounted in the US to over 114 billion dollars. (Tech Nation Report 2020). The sources in the case of private companies are many and the volume is increasing each year.

Investments into Artificial Intelligence, which is a part of R&D expenses are very difficult to track. Such detailed data are not always published even in states, that at least require public access to the financial reporting of private companies. The strongest argument we may provide after researching the topic is comparing the strength of sources funding R&D activities within state and private companies and support it by showing the sums invested. Since one of the hubs of AI development certainly is in the United States, I would like to illustrate the situation there due to several reasons. The government is open about its investments into Research & Development, private companies are reporting these expenses as well and we may create a picture of the situation. As for China and Russia, we are unable to do so on the level of reliability that would be beneficial. That is the reason why I focus on the United States alone.

When comparing the R&D budgets, we need to understand that we have no clear idea, how much are individual departments investing purely into AI. We focus on providing the base understanding of R&D investment flow assuming the portion of R&D budgets within state institutions and within private companies are comparable in proportion, not in

volume. We may not be able to determine the exact investments into the AI, yet we may provide a rationale why private actors may be leading the way.

On a very high level, we may assume that from the whole bunch of US institutions, the primary driving forces of R&D are the Department of Defense, and NASA. For these two institutions was requested the funding in total the volume of 70,7 billion USD (Sargent 2020, p. 5). The leading 4 US technological companies – Google (Alphabet), Apple, Facebook, and Microsoft invested in the same year in a total 84 billion. More information on the investments may be found in Table 1 in the Appendix. The overall argument however stands, that private companies pursue R&D activities financially as much as possible, growing in the volume of investments much faster, than the government. Private companies have one more advantage over the state, and that is the possibility to monetize the technology developed. All these small but significant details support the argument of private companies having better grounds for larger investments into AI. Not to mention that we compared only the 4 largest technological companies in the US, omitting other companies and start-ups and discussing only their own investments.

2.3 Role of underdogs regarding the AI development: resources for delivery

Artificial Intelligence is a kind of technology, that may be developed by many. States, private actors, or even non-state actors and individuals. Basically, everyone may start doing AI research. The initial financial input is not large, considering you own a laptop and have access to the Internet, your possibilities in today´s world are seemingly unlimited. However, developing Artificial Intelligence on the level, it is possible to adjust the trajectory of a missile due to atmospheric changes and defence systems is not trivial, nor doable without sufficient funding and programming background. There are a few conditions, that support the endeavors of creating good AI systems.

Despite AI´s promise is “without human”, the development is exceptionally labor-intensive. The need for AI experts is apparent across all markets, across all sectors and fields. The shortage of talent may be demonstrated by the salaries offered. According to The New York Times, “[t]ypical A.I. specialists, including both Ph. D.s fresh out of school and people with less education and just a few years of experience, can be paid from $300,000 to $500,000 a year or more in salary and company stock. Costs at an A.I. lab called DeepMind,

acquired by Google for a reported $650 million in 2014 when it employed about 50 people, illustrates the issue. Last year, according to the company's recently released annual financial accounts in Britain, the lab's "staff costs" as it expanded to 400 employees totaled $138 million. That comes out to $345,000 an employee" (Metz 2017). Highly educated, trained people capable of working on AI development are a scarce resource, further underlining the more common partnerships between universities, states, and private companies in the process.

A 2017 survey by Teradata company showed, that 91% of respondents chosen from 260 global companies perceive "the lack of access to talent and understanding" as one of the main barriers to implementing AI solutions in their companies. A slightly lower number of companies stated that the issue is also budgetary (Bourne 2017). When developing AI, a huge amount of money is invested into people and their salaries, but the second-largest expense is the technology itself. The need for computers, servers, and computational power is unimaginably expensive, not considering the electricity bills.

One more requirement is data. Since AI is an algorithm capable of crunching vast amounts of data looking for patterns and logic behind them, the more data we have, the better the AI may become. We may describe this on a baby. When growing up, it learns by perceiving the world around it, looking for patterns, and gaining experience. Firstly, it learns via the attempt-fail method and gains first datapoints according to which it reasons further. The knowledge is then stored in the brain and when used regularly, it becomes automatic. The advantage of the code is, it may go through years of data within minutes and most importantly, it can remember all the outcomes and use them whenever required. If uncertain, it performs a step that has the highest probability of success (Taylor 2019).

We discussed three main requirements for developing and researching AI – talents, sufficient financial support, and data. A common misperception is that only global leaders can develop Artificial Intelligence. Countries like the US, China, France, and Israel certainly are capable of developing AI. They have a high-quality education, vital support from the government, and via private funding and can provide sufficient data to the algorithm to improve its processing and reasoning capacities. But these are only predispositions. No one is eliminated from the AI competition when not having these resources. Having best-in-class education and funding eases the development of AI. But does not determine, who may be

developing the AI. And just like that, the Democratic People´s Republic Korea (DPRK) started its own AI projects.

As Tai Wei Lim (2019) wrote in his article, Artificial Intelligence may, contrary to expectations, be developed in poor countries. The DPRK was behind the algorithm called Eunbyul (Song 2016) that can play the game GO, one of the most complex games invented. A similar algorithm, called AlphaGo, defeated the world champion Lee Se-dol in 2016 (Deepmind 2016). Even though the software is not the same, the capability of creating an algorithm able to play such a complicated game is stunning. Even more if we consider the origin of the algorithm. North Korea might be considered as underdog in AI development, yet the education system is not necessarily one of the worst. The DPRK has a high-quality university from which graduated some of the highest-ranking members of the Chinese Communist Party. North Korean hackers are being largely covered by the media and are blamed responsible for ransomware attacks and frauds. Given the ability to educate its people, mobilize the whole country and use hackers in its AI R&D missions may mean, that the DPRK might be on a solid level of AI maturity (Lim, 2019).

The same logic can go to any other country in the World. We may not expect the programs to be the top-of-the-class quality given the essential condition is to have the brains. This field is highly competitive and AI experts are demanding as of their salaries. Yet no state is excluded from the activities in the AI field. Private companies may significantly improve the position of the state, as they concentrate such experts and are often willing to participate with states on the development of AI-based technologies. This is connected with the education quality since companies tend to concentrate in cities and states producing highly educated people, who understand the basics of AI and push the company forwards to higher revenues.

2.4 Breakthroughs and the driving forces

Investing money without any significant return is not reasonable. Just as would be investing in technologies and institutions, that do not make any breakthrough or advancement in the particular field. Therefore, the next topic addressed is the origin of major AI breakthroughs. During the 1990s, DARPA (Defence Advanced Research Projects Agency) and the National Institute of Standards and Technology (NIST) began working on a project called Face Recognition Technology (FERET) (NEC New Zealand 2020). The testing began in the 2000s and since then, private actors just as states are using this

technology and mastering the software. Despite this technology has been developed by a state actor, further advances were catalysed by private companies, using it in their own devices such as phones or smart homes (Charlton 2019).

This application is incredibly spread and vastly used by many states and companies. The majority of phones have facial recognition systems included as a safety measure when accessing the phone or when confirming payment. This technology has non-trivial requirements on the AI being able to recognize the human face under different light, with make-up or with a new moustache or a beard. And despite this technology is out for over 20 years, further updates and improvements are going on. Cameras with facial recognition are used for crime prevention and identification and although these systems are not 100%, AI is providing the user with probability with which is the identification performed.

Another industry experiencing a significant inflow of money regarding AI development is Healthcare. In 2019, over 4 billion USD were raised by AI start-ups focusing on healthcare (Landi 2020). Apart from the COVID-19 pandemic, the most notable AI use is in "hyper-personalized medicine". The short definition says that hyper-personalized medicine uses AI to develop new classes of drugs tailored to a person´s genes (Regalado 2020). The concept was originally invented on academic soil in cooperation with hospitals, nowadays these technologies are primarily developed by private companies (Welcome To The Future With Jay Allen 2020).

In 2019, OpenAI introduced the GPT-2 model, capable of generating original texts on its own. The ability to connect words to full sentences providing the reader with a full message is an incredibly time-consuming process. Similar algorithms may one day write books, articles based on the observation or be used further in AI development (Yadav 2019).

These examples show that the development core is decentralized. Private companies, states and academia – all of these are at the epicentre of AI development. Private actors, due to their active interest in generating revenue seek possible acquisitions and technology applications, that may help them achieve that goal. State´s, if not included, are then purchasing these technologies or, if included, invest into the development on a yearly basis. The third way leads via acquisition. Mergers and acquisitions in the US regarding the disclosed AI deals made 25% of all investments. Compared to China that invested less than 1% into M&A (Arnold, Rakhovsky & Huang 2020, p. 18). Such a difference between the acquisition share of investments may indicate, that there is either a very little overlap of

interests of actors, or it is regulated by some central authority, having insight into all these processes.

Despite some companies (namely Google) refused to cooperate on specific AI projects (Statt 2018), other companies such as Raytheon, IBM or Oracle collaborate with the US government (Gershgorn & Rohlrich 2018). The cleavage here is however not financial, but moral. When Google was leaving the US government contract, the reason was ethical, as "[a]bout 4,000 Google employees signed a petition demanding 'a clear policy stating that neither Google nor its contractors will ever build warfare technology.' A handful of employees also resigned in protest" (Wakabayashi & Shane 2018).

There are multiple companies in the United States, in or outside the Silicon Valley eager to cooperate with the government. Some of them are owned by former military members. "I'm an Army retiree after 24 years and a half-dozen combat tours, so I have an obligation to provide this technology. I'm not a guy out on the west coast who's made a lot of money like Google. All of my engineers have security clearances, so we're pretty bought in on trying to help the military in this area" (Gershgorn & Rohlrich 2018).

Private companies are the key driver in AI development mainly for civilian, but also for military-related use. The number of investments from private equity funds and other non-state sponsors is only hardly comparable to the expenses of states. The position of the United States is different compared to China´s due to transparency. American companies declare their owners and shareholders so the direct involvement of the state in private actors' decisions would be revealed. While in China, the structure of owners is invisible or only partially declared.

The Chinese market is saturated by large AI players, that are cooperating with the central government, receiving funding, and developing technology in collaboration with the government. Actors in the US show, that the interest may be low considering the use of the technology and therefore may decide to step back. In the case of China, we may not make any conclusions except the one, that large companies developing AI are cooperating with the state. We also found that just as there are companies openly distancing from the governmental projects, there are those, that perceive it as a duty and privilege to serve their country.

We saw that countries investing most heavily are, apart from the US, secretive in disclosing any detailed information. The United States increased their volume of investments

into R&D and AI as well. The pace of growth however is not comparable to the one of private actors. The top 4 companies we mentioned above grow their R&D investments by about 17% a year. The state however grows by about 5,5% per annum. Even if my assumptions are incorrect here, and the shares of AI on the budget is lower in the private sector, the pace indicates that private actors are closing the gap or increasing the difference of the investments.

The primary aim of this chapter was to shed a light on the money, and investments regarding the AI and R&D sector. Despite trying to narrow the numbers to AI as such, we could not create comparable examples from the state and private sphere. The argumentation over the volume of R&D investments is important due to the AI definition we posed above. It is an enabler and therefore not limited to only one application. Instead, it may assist the state and private companies across all major activities, creating significant added value to the actor and be further improved.

The primary engine to AI development lies in brains and dollars. Acquiring people capable of understanding, programming, and fine-tuning the algorithms are a scarce resource and their education takes some time and money. Capable engineers and programmers not only create the systems considerably quicker, but they are delivering quality to the job. And high-quality codes are the ones desired. Private companies are winning the battle for brains and as demonstrated, even the money. Private actors are in the lead in key attributes and are essentially limited by the quality and quantity of data which is one of the reasons cooperation with states makes sense.

3 Companies versus States

Over the last century, it became more and more standard, that private actors are present within international relations and negotiations. Private organizations are a vital part of such relations, often as contracting parties for delivering certain solutions, goods, or services. Corporations are very important for international relations since they tend to strengthen the relation and help to develop common dialogue (Friedmann 1957).

In the beginning, I would like to dedicate several lines to properly explain what we mean by state and private actors. A state is a "human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory" (Weber 1918). State in our understanding is indeed a community of people, that occupies some territory, has a governing body, is recognized by other states, and executes an effective control over the citizens living within it. The state shall have authority over everyone within its sphere of power (meaning territory).

Private actors on the other hand are subjects created by people, that are not under the direct control of the state. They are created and run by individuals with a certain goal, such as enhancing technological advances or generating money. It is important, that every matter regarding the functioning of the private subject is discussed by the individuals running the company within the rules set by the state. The company may not violate the state by its actions, just as it must respect the rules set for private actors by the state authority.

Private companies and corporations have a significant impact on the society and state as well. Manufacturing plants, research & development centers, or offices, all these projects and venues have a positive impact on the state and society regarding such phenomenon as employment, tax income, and lower prices of the goods manufactured on the domestic market. "Manufacturing is essential to the health of an economy. It both fuels and results from innovation. It is natural in the course of economic activity that "factory jobs" are tradable on international labour markets" (Heskett 2012). Corporations are employing a comparable amount of people to the largest public institutions. In 2017, the largest employer was the US Department of Defence with 2,9 million employees, followed by the People´s Liberation Army in China with 2,4 million people, third was Walmart accounting for 2,3 million employees followed by China National Petroleum Corporation with 1,5 million employees and McDonald´s with roughly 1,5 million employees (Shendruk 2020; The

world´s 30 biggest employers 2017). The tax incomes from these jobs are undeniably indispensable for the state.

One example of how private actors are significant for states may be demonstrated in discussions between Tesla and the Government of Germany. At the end of 2019, the German government and Tesla Inc. agreed on building a Tesla factory in Germany. ¨Tesla is known for its electric-powered vehicles, capable of driving the longest out of all electric vehicles in sale at this time (Siddiqui 2020). "German Economy Minister Peter Altmaier called the announcement a "glorious success" for the country's attractiveness to the auto industry, especially in the race to develop and produce electric cars and batteries" (Moulson 2019). Preparing for increased volume of electric vehicles (EV) sold in the future years, "the government and industry agreed to aim for 50,000 publicly accessible charging stations nationwide by 2022" (Moulson 2019). Increasing the share of EVs and building a denser network of chargers is a step in the right direction, given the adopted EU policy of decreasing the CO_2 emissions from cars in and after 2020 (European Commission 2020). "This is good news for VW, Daimler, and BMW," said Dudenhoeffer, who heads the Center Automotive Research" (Moulson 2019).

In this case, Tesla serves as the accelerator of changes. The European Union is heading towards sustainability and carbon neutrality, focusing on reducing car emissions. Opening a factory of an electric-car producer, building thousands of new public chargers, and having lower prices on new cars coming out of the production plant is a strong motivator for other European car manufacturers to pursue projects aimed at sustainability and effectivity. Tesla in this case helped not only Germany but to the European Union in enhancing one of their goals.

Companies are nowadays international, extending their reach to more markets, opening new sources of income. The location of their production plants is, due to the reasons mentioned above, of significant importance. Corporations are adaptive, profit-motivated, and efficient in coordinating production within the international system. States rely on corporations since the movement of their main production sites has a huge impact on the state, therefore they enhance tax cuts and create good conditions for investments (Kapfer 2006). Samsung for example is considering building a new site in Austin, Texas worth over 17 billion dollars. About 1,800 new jobs will be created and the state is planning tax breaks in the value of over 800 million dollars (Nellin & Jin 2021).

One of the first examples of such partnership may be found in the context of the United States when the JP Morgan Chase bank, a private actor invested in the railroad during the 1800s (Martin 2018). These projects grew by size and volume of investments and are nowadays called the "Public-Private Partnership" or PPP, describing the cooperation between states (or public area) and the corporate (private) area. And in the 20th and 21st centuries, this tool is being actively used. As Kobrin (2009) wrote in his paper, "[corporations] have the resources and capabilities necessary to supply public goods in the absence of effective international alternatives and the ability to provide private governance where public regimes are lacking". Private companies are now fulfilling multiple roles – distribution of energy, fuel, arming, technical solutions, supply of water even public transportation is not always provided by state per se, but by a contracted private actor. States stepped down from fulfilling some public responsibilities that were outsourced to private actors. Within the states as well as outside the states.

The wealth of private companies may be illustrated in the 2016 ranking of revenues of states and largest private companies. Unsurprisingly, the first place holds the United States, followed by China, Japan, Germany, and France. The first non-state actor is the US company Walmart with revenue roughly seven times lower than the leading US. Despite this, the ranking of 100 subjects contains only 29 countries. Fourteen of the remaining private subjects are Chinese, 27 are American. Just to illustrate the greatness of some corporations, Ford Motor had the same revenue, as Saudi Arabia and Sweden was only slightly ahead of Exxon Mobil (de Freitas 2018).

Private actors affect international relations more and more. They are being used in negotiations or may be contracted as providers of certain services. Further is provided essential distinction of engagement of private actors in the international negotiation processes as outlined by The Oslo Forum Network of Mediators that differentiate three basic forms of engagement. Direct participation, Indirect participation, and Providing Knowledge and Research.

Direct engagement of private actors was explained in the case of El Salvador during an armed conflict at the end of the 1980s. The economy was rebuilding and business as such emerged from the previous systems based on land and agriculture. Emerging young businesspeople understood that the conflict is damaging this transformation and formed a business-centric political party called Alianza Republicana Nacional (ARENA) that won in

1989. After the end of the conflict, governmental negotiations led "to the reform of the police, the military and the judiciary, and demobilisation of armed combatants. Cristiani guaranteed businesses access to government decision-making processes. His advisory team included individuals from FUSADES[1] and business executives. The business was engaged in conflict-related research and dedicated resources to support former FMLN (Farabundo Martí National Liberation Front) combatants' attendance at graduate schools to improve their managerial and other skills" (Tripathi & Gündüz 2008). The bond between business and state grew stronger changing the environment of the country, leading to the development and public-private partnership.

The private partnership is however rather often within international relations. Over 150 companies are directly involved in a project called Power Africa. The commitment is to invest over 40 billion USD in the African Energy markets. These companies range across the whole value chain, capable of executing such initiatives (USAID 2021).

Second, indirect participation of private actors in international relations may be demonstrated in the case of Colombia in the mid-1990s. The state was in crisis, at the edge of significant recession and violence. This situation led businesses to support protest marches and formed the Citizens´ Mandate for Peace, Life, and Freedom (CMPLF), mobilizing a significant part of society against the violence. Businesses pushed for stability and for the creation of an environment suitable for peace negotiations between the government and Fuerzas Armadas Revolucionarias de Colombia (known as FARC). The businesses contacted the guerrilla directly. They negotiated in Germany and despite the talks between the government and FARC did not solve the situation definitively, the overall conditions in Colombia were improved, emphasizing the importance of private actors in peace talks (Tripathi & Gündüz 2008). Private companies tend to be considered as authorities due to their expertise, they are credible providers supported by customers, capable of compiling, organizing, and analysing difficultly obtainable information (Bruce 2002).

Private companies may also perform the function of a knowledge provider. "In 1994, the Northern Ireland CBI produced a landmark publication, Peace – A Challenging New Era. Better known as the 'peace dividend paper', the document spelled out the economic rationale for peace and soon became the reference point for the peace process. […] The CBI paper identified several inhibitors to economic development, including increased security costs for

[1] US-funded organization, the Salvadoran Foundation for Development

the private sector, damage to the tourism industry, and emigration" (Tripathi & Gündüz 2008).

The concepts introduced contained direct involvement of private actors when the main initiative and delivery is provided by them. Explicitly we talk about delivering tools and equipment, installing it, and even operating in the near future before it is transited to the accepting state. Indirectly, companies may serve as neutral actors, developing international economic relations or act as intermediaries. Representatives of private subjects are regularly present during international visits, participating in the negotiation. They may also serve as knowledge providers and enlightening forces. Assisting governments during crisis situations, such as advising them during the COVID-19 pandemic, researching for international best practices, or supporting certain points of view to stabilize or improve the economic situation.

As visible from the examples above, private companies can act collectively and pursue stability and prosperity. And despite the de jure power remains to the states, the de facto power is moving towards corporations. They are growing in power at the expense of national states, thanks to a significant role in international relations (Kapfer 2006). Some authors mention this in the context of the "two system" perspective. The premise is that even states are aware companies may have insight into the foreign countries and try to use them for their own good, for example by the politicization of foreign investments (Babic, Fichtner & Heemskerk 2017). Other authors go even further, stating "[w]e find it telling that at the beginning of 21st century there are so many examples of sites or locations of authority that are neither states, state-based nor state-created. The state is no longer the sole, or in some instances, even principal, source of authority, in either the domestic arena or in the international system […] companies are in charge of economy" (Bruce 2002). They further argue that globalization of liberalism and the privatization of economic processes involves the relocation of regulatory function from public to private authorities (Babic, Fichtner & Heemskerk 2017).

Corporations and private actors are indispensable in the international field. Their role in international negotiations has many different forms, yet their contribution and importance are unique. They are used as proxies in international relations, but just as well there may be those who misuse the situation. Many companies demonstrate their power by hiding in tax heavens and avoid the payments and states may not execute their power on them. The role

and involvement of private actors in international politics grew in size just as in volume and their services are being used without any larger notice from the rest of the World.

3.1 Approach of states to private actors

States significantly vary in their relation to private actors. Some argue that the United States even lacks in Artificial Intelligence due to the liberal attitude, compared to China (Horowitz et al. 2018). As mentioned before, companies in the United States have a choice whether or not to work with governmental agencies. And as in the case of Google who stopped governmental contracts in all its companies, including the recently acquired Boston Dynamics company or Schaft (Sayler 2020), the US Government respects this decision. China on the other hand openly wants deep civil-military fusion, including AI technology (Kania 2018). Baidu, Alibaba, or Tencent are some of the most significant Chinese companies with large AI hubs across the country, supplying and cooperating with the government on big technological projects. China is also lowering the bar between what is private and where the state may collect the data. It was emphasized, that the datasets and data, in general, are the primary and major training material of AI systems. According to the Congressional Research Service, in 2020 over 20% of all data collected were obtained by China with a prediction it will be 30% in 2030 (Sayler 2020, p. 22). China is often criticised for using its surveillance system for „rating" its citizens. This requires an advanced AI system in facial recognition, capable of high-efficiency monitoring and identifying individual people on the street (Jing 2017).

The main issue is the connection between the private and military spheres (Horowitz et al. 2018). Since the connection between private companies and the government in China is either forced or very strong, and the United States relies on generous contracting policy, the difference is significant. The US on the other hand tends to use more regulatory powers of the state, hosting discussions and forums on AI-enabled biases and errors that must be prevented. Some argue that the regulatory power is exercised only on one side, targeting the private sector only, leaving the governmental agencies and projects untouched (Brainard 2020). Apart from regulation, the state holds one ultimate tool – acquisition. Certain technologies developed in the private sphere may be considered for the government threatening and shall not be distributed to everyone. That is when the acquisition comes to action. However problematic these steps are, the US established the Joint Artificial Intelligence Center (JAIC), which „may use a consortium of companies and academic

institutions to procure technologies and services needed to make AI a ubiquitous force within the military" (Maucione 2020). The main rationale is mentioned in the Congressional Research Service´s report saying that company technologies may be up to 90% used in military applications (Sayler 2020).

3.2 Technological Advantage of Private Companies & their Power

We already know the investments into AI are primarily concentrated in the private sector, delivering and improving most known AI systems and technologies. People are daily in touch with AI-based systems in form of phone facial recognition for access and payments, at the airports during passport scan, or in form of chatbots. In fact, over 85% of customer services are operated by chatbots. We daily use our computers and Internet that is covered by the advertisement. These ads are becoming more and more predictive and based on the history of our browser, they are capable of recommending you fashion, electronics, vacations, and other products you are likely to be interested in. Predictive advertisement can attract new customers and boost the revenue of the store. In 2020, about 57% of buyers were influenced by these ads (Groumpos 2019).

It is not only the metaphysical world of the Internet, we use AI-based systems as well, starting with robotic vacuum cleaners. The number of industrial robots supplied grew from 121 thousand in 2010 to over 250 thousand in 2015 and for personal and domestic use the number was 5,4 million units. This includes robots on the ground, naval, and aerial. Just, for example, the number of registered drones in the US culminated at 865 thousand in March 2021 (Vailshery 2021).

The media industry is also hugely affected by AI and its potential. Dependence on media, sensationalism and click baits play role in affecting the opinions and tendencies in society. Media were the main tool of propaganda and with the literally massive reach of these days' media, the risks are serious. Media provide tools for dictators and authorities to manipulate the news environment and to control the main message (Brundage et al. 2018).

When we mention security topics, the outsourcing of certain tasks to a private supplier is common. Private companies were contracted in 1995 to rebuild the Bosnian army (Avant 2004) or we may mention the company Blackwater that was contracted for security services in Iraq (Apuzzo 2014). Despite the outsourcing is not new, the growth is apparent. Private actors have better insight into many modern industries, attract professionals and

experienced people from the private and public sphere on high salaries and invest heavily into R&D. Even private actors may hire a private actor for certain services, such as in the case of British Petroleum company using a contractor to secure its pipelines in Colombia. Transnational actors have more and more power in security and in certain situations, they have even control over violence, which is one of the basic definitions of a state (Avant 2004). Kobrin (2009, p. 12) in his paper says, that transnational corporations "[…] have the resources and capabilities necessary to supply public goods in the absence of effective international alternatives and the ability to provide private governance where public regimes are lacking." In these situations, private companies may aspire to replace failing states in control of the territory or industry.

Authors such as Crawford and Schultz discuss specifically Artificial Intelligence that is being used in areas believed to be still exclusive to a state such as certain judiciary decisions. They are concerned primarily about the understanding of decisions made by the software, "[…] governments are turning to third-party vendors with increasing frequency to provide the algorithmic architectures for public services, including welfare benefits and criminal risk assessments. As such, when challenged, many state governments have disclaimed any knowledge or ability to understand, explain, or remedy problems created by AI systems that they have procured from third parties" (Crawford & Schultz 2019, p. 1941). Their arguments are also moral, pointing that each case of bail release or loan request shall be decided on an individual basis, taking into account things that machines are not yet capable to work with, such as empathy or humanity (Crawford & Schultz 2019, p. 1945-52). They believe that governments still have the most powerful, yet the situation is shifting. Despite private actors are being subjects of regulations (Crawford & Schultz 2019, p. 1957).

The most sceptical opinion was written by Susan George in her paper saying that „It's not just their size, their enormous wealth and assets that make the TNCs dangerous to democracy. It's also their concentration, their capacity to influence, and often infiltrate, governments and their ability to act as a genuine international social class in order to defend their commercial interests against the common good" (George 2014). And despite the motives and aspirations of these actors shall be debated later, many sources and data point out, that private actors are being more and more important in the functions previously exclusive to states.

This chapter focused on explaining, why are private actors vital within the international system. Their roles range from supporting, to actively engaging another state. They are envisioned as guarantors, confident partners verified by customers, and trustworthy partners in providing smart and innovative solutions. The economic development would be significantly slower without private actors in the system. As their role grows, more and more services are outsourced and contracted, even within the security industry. They possess the unwritten, yet respected authority of capable providers and effective bodies. And with the growing financial potential and services they deliver, these actors are players within the international system states must count with.

It does not only have to be their role within the international system, but the solutions they deliver to the governments. If judiciary algorithms are fully implemented and not sufficiently reasoned, states may face unsatisfied citizens. The strongest tools these companies have at the moment against states are those actively interacting with society. Demonstrating the point on the bail system, AI is learned on a specific dataset. In this case, it would be the list of a court rulings in previous cases including specific details about the cases such as the race of the person. From that, we may create AI that is reliably ruling upon the cases of White people, yet it may be harsh and seemingly unjust against Afro Americans or Asians due to the dataset that was ethnically biased. Again, given the United States, this topic is these days very actual and may lead to riots and protests damaging the state.

Any act of the private company causing harm to the public shall be perceived as dangerous. The role of states is to protect their citizens and whenever is this violated by a private actor, they shall be punished. Private actors stand below the sovereign state; therefore, they must respect its decisions and processes. Any acts against this are endangering the public and the state itself.

The chapter illustrates, that private companies are on many levels capable of replacing the state. Many companies are having sufficient financial resources to compete with states and their ability to respond quickly puts them into an interesting position against states. Being capable of challenging the state, however, does not necessarily mean companies will do so. Therefore, we need to go deeper to understand in what situations may private actors benefit from such situation and evaluate whether the AI may play any role.

4 Is AI dual-use technology?

Before we debate the role of Artificial Intelligence as a dual-use technology, we shall firstly understand, what dual-use technology is. There are multiple definitions available online, such as the European Union´s document, that defines the dual-use as follows: „Dual-use products, services, and technologies can address the needs of both defence and civil communities. A large and increasing number of technologies are generic and not specific to single civil or military applications. Advanced materials, nanoelectronics, information and communication technologies (ICT), unmanned systems and automation or photonics are just a few examples of fields in which research, technology development, and manufacturing can be used for multiple applications“ (EU funding for Dual Use 2015, p. 8). We may understand it as a modern definition, yet in 1992 report by the US Department of Defence came up with one of the very first ones. “Dual-Use, with respect to products, services, standards, processes, or acquisition practices, means products, services, standards, processes, or acquisition practices, respectively, that are capable of meeting requirements for military and nonmilitary application” (Gray et al. 1996).

These definitions may seem vague, free, and including all possible emerging technologies. And in most cases, these definitions are correct. Just as nuclear energy may be used to power cities, it may be used to destroy them. Dual-use technology is simply any technology, that may serve to development and prosperity in the civilian sector just as to the military applications and misuses in the civilian sector. And despite there is nothing wrong with providing technology to the military, we shall be careful not to create any weapon or tool, that may put civilians in harm. Nuclear weapons are sadly an example where we failed to do so, and we witnessed the consequences.

In the following paragraphs I would like to introduce Artificial Intelligence in more detail to assess its fit into the definition of „dual-use“. We shall understand what creates the arguments to believe it is a mis-usable technology. We will investigate several papers arguing about this particular problem and determine what key aspects is the AI missing to be a dual-use weapon.

4.1 Literature overview

Among the authors rules opinion, that AI is indeed dual-use technology. They even argue that its “quick development and employment in weapon systems to gain an advantage

over the opponent, leads to AI arms race incentivizing speed over safety and ethics" (Slijper, Beck & Kayser 2019). The Congressional Research Service states, that many applications of modern technology, such as AI are dual-use technologies. They also argue, however, that technology developed by private companies may be in up to 90% of cases used in military applications (Sayler 2020).

Understanding Artificial Intelligence as dual-use technology has some rather obvious consequences, and that is an arms race. States go on at emphasizing the importance of AI in their military development projects and policies, each wishing to become the hub of AI. In 2019, President Donald Trump signed an executive order that prioritized Artificial Intelligence, its research, and development (Brody 2019). Two years before that, Russian President Vladimir Putin stated, that "whoever becomes the leader in this sphere [meaning the AI] will become the ruler of the world" (Vincent 2017). China has been rather open in its intentions wishing "military-civil fusion in innovation. […] Tsinghua University launched the Military-Civil Fusion National Defense Peak Technologies Laboratory to create a platform for the pursuit of dual-use applications of emerging technologies, particularly AI" (Slijper, Beck & Kayser 2019).

These countries actively explore opportunities and ways how to implement AI in their military. In the Russian federation, a Russian counterpart to the American DARPA (Defense Advanced Research Projects Agency) called Foundation for Advanced Research Projects was established. Given the fact, that the Russian government employs the vast majority of researchers and the information exchange is at the necessary minimum (Kozyulin 2019), this centre is another step further to the advanced development of AI and potentially its implementation into the military. Russia takes this matter seriously. They started building a brand-new city called Era, which shall be devoted to military innovation research in the field of Artificial Intelligence and supporting technologies (Slijper, Beck & Kayser 2019).

The United Kingdom also does not wish to stay at the back. In 2019 the UK established DASA (Defense and Security Accelerator) that shall be funding exploitable innovation to support UK defence and security (Slijper, Beck & Kayser 2019). The State of Israel has the C4i directorate, that´s main objectives are "to initiate, develop, exploit and strengthen the IDF's technological integration system" (C4I and Cyber Defense Directorate 2021). The Republic of Korea announced in 2018 the establishment of a research institute

focusing on Artificial Intelligence, which shall become the "next-generation combat control tower" (Slijper, Beck & Kayser 2019).

The fact, that many countries started investing a large amount of money into AI research centres and try linking it with the military creates a situation that may threaten many. The Congressional Research Service report mentions that some countries try to push ethics further for the possibility of using AI-based machines and tools. They are being fed by large volumes of data. These systems are used in analysing pictures and videos and there is evidence suggesting the existence of lethal autonomous weapons systems (LAWS). In 2003 the US Patriot Air Defence System operating in automated mode shot down a British Royal Air Force plane that killed the pilot. The automated mode authorizes the system itself to decide upon using the weapon with no human interaction or oversight (Kozyulin 2019). This happened due to an error called "false positive" which will be discussed further below.

Artificial Intelligence may therefore be easily categorized as dual-use. I would like to take a closer look and demonstrate some exact uses of AI before going deep dive in the next chapter. As we explained at the beginning, Artificial Intelligence is an enabler. A tool that analyses vast amounts of data within several seconds or minutes and provides probability-based recommendations and predictions. It is very useful in battlefield analysis taking as input thousands of variables and ending by recommendation of the likely-to-succeed strategies (Sayler 2020). And despite it is not one technology per se (such as nuclear weapons but rather a level up of many technologies), the dual-use threat lies in enabling other technologies to be more dangerous and threatening.

Artificial Intelligence in the current, narrow form as we specified at the beginning can perform only one specific task. Determining the best outcome of a battle or playing a hand of poker. The AI learns through performing computations, simulations and it can create a thousand of times more scenarios within one second than we can in a year. The scope of speed is crucial in understanding the added value of such a machine. AI system capable of playing poker might not be so innovative given that bots may do so as well. AI in poker can calculate probabilities instead of blindly betting. And it may go even further.

Artificial Intelligence system performed a specific strategy called "bluffing". The system analysed the situations so perfectly it performed a successful bluff and won a game. Performing such action requires either luck or incredibly well analysed players, in this case, the researchers agreed it was the second latter as the system performed it several times. And

the use does not end here, as it is also capable of managing multiple devices at once. For example, drones in order not to crash to each other. People are not capable of managing more than two drones at a time. These systems may operate hundreds of them, performing stunts and even light shows (Pohler et al. 2018).

As this topic was already mentioned, I would like to talk a bit about lethal autonomous weapons systems, that are also present in our lives. These may be semi-autonomous, requiring human oversight and approval of using a weapon (majority of rocket launchers, rockets, or cyber systems) or autonomous, such as the US Patriot system. These systems provide the ability of finer targeting, higher efficiency and effectiveness, the ability to quick respond to the change of conditions and naturally attract the attention of many militaries. But as in the Patriot case, there may come situations when the system evaluates the situation incorrectly. We call these mistakes by “false-positive” and “false-negative”. Despite the names are straightforward, a short explanation is in order. We say the system evaluated the situation as false positive when the situation did not fulfill the requirements to be responded to, yet the system conducted the action. False negative is the opposite when the system should have acted, but it did not.

4.2 Comparing AI to other dual-use technologies

There is however one more difference that causes AI to stand out of the traditional group of dual-use technologies. And that is the development potential. If we compare nuclear weapons to AI, the differences are apparent. To develop a nuclear weapon, you must have sufficient financial background, blueprints, research capacities, and the ability to obtain weapons-grade radioactive material (plutonium or uranium) by enrichment in centrifuges. Apart from the financial background, all remaining points are closely supervised and monitored, potentially raising alarm when someone tries to gather all the necessary components (Kozyulin 2019).

Chemical and biological weapons are much harder to watch yet the AI might not raise any alarm whatsoever. Artificial Intelligence is more hidden, subtle, the requirements are much lower since all you need is a computer and access to the Internet. Necessary to say, however, that computational power is vital in processing the data and training a suitable algorithm. The more complex task is required to be done, the more time, training data, and finances we must invest into the project. This may increase the costs due to technical equipment, energy bills, and personnel. Despite that, the availability of technology and all

components, limited availability of training data, and access to the Internet provide the individual or group of individuals (non-state actors, private companies) with all necessary tools to build a capable AI system. The level of maturity is to a high degree dependent on the skills and data the model was trained on.

At the end of this chapter, I would like to briefly discuss an example of dual use of an Artificial Intelligence empowered system. AI-empowered systems are used in stock trade. They are quick, predictive, and efficient. Their learning, just as in the case of every AI system, is based on data. Historical values, growth, reaction to a crisis or certain situation, connections, etc. All these factors are relevant for the AI and it needs to be given these data points to grasp the basics of trading. Upon this the AI can create patterns, finding common behavior under certain conditions, and determine the probability of certain behavior of the stocks in the near future. These systems are being delivered by private companies, trusted by banks, financial institutions, and traders (Thomas 2020). These private actors, if interested, may change the dataset of gathered data to support certain thinking at the expense of another and benefit in long term. Data infection and manipulation just as data insufficiency are the primary issues of trust in the AI systems. Just like that, we might cause a second financial crisis within a century, as was the first one in 2007-2008. Artificially changing prices of shares to create financial bubbles that may go off is perhaps nowadays the largest nightmare of all traders. Despite this example does not demonstrate military use, it shows dual and malicious use in the private sphere, caused by affected training data as this is vital for these systems. Not to mention that the potential outcome in form of a crisis would damage states as well. The probability and feasibility of such an act are low, yet Artificial Intelligence enabled this application that would cause major financial losses to individuals, companies, and states. The advantage here may be to a certain degree orchestrated, benefiting for example companies focusing on specific industries. Such as technological companies thrive during the pandemic since most of the activities are held online, states are depleting their savings to support damaged economies. It is necessary to emphasize, however, that such an event has a very low level of feasibility.

Demonstrating the ultimate technology military and private sector are currently very interested in is facial recognition. Modern platforms such as phones, laptops, and smart home systems are working on the same model as are the AI systems in cameras on the street. The only difference is in its purpose. Facial recognition is nowadays more common than any

other AI-empowered system apart from already mentioned virtual assistants and recommendation engines. In 2019, the facial recognition market amounted to 3,2 billion USD and is expected to grow to 7 billion USD in revenue by 2024 according to Statista (Liu 2020b). This indicates that wherever we are now, the pace and the facial recognition technology are not going to slow down.

On one hand, this is a safety feature. By 2025, as many as 72% of hotel operators shall implement the facial recognition systems (Xie 2018) and as much as 49% of people agree, „that facial recognition should be used in stores if it catches shoplifters“ (Calvello 2019). All of us will be in touch with this technology on a regular basis, as „97% of airports will roll out facial recognition technology by 2023“ (Facial Recognition Airports Survey 2018).

There is however the other use of facial recognition system – target recognition. Facial recognition systems do increase the accuracy of target recognition on the battlefield. These systems are even capable of analysing the behavior and predict (with a certain probability) the future development of weather or assess the best approaches to the target. We talk about recommending the type of weapon to minimize the civilian losses, predicting atmospheric conditions, or verifying that the target is the desired one and not anyone else. “DARPA’s Target Recognition and Adaption in Contested Environments (TRACE) program uses machine learning techniques to automatically locate and identify targets with the help of Synthetic-Aperture Radar (SAR) images” (Singh & Gulhane 2018).

As discussed during several interviews with representatives from the European Committee and a Ph.D. student from the Cambridge University, the Artificial Intelligence empowered technologies are seen as dual-use due to their ability to scale up the pace of analysing vast amounts of data, understand the patterns and create a recommendation, how to proceed further. Most notable mentions include the Cambridge Analytica incident, the social media influencing but also the use of AI in net traffic analyses, drone attacks, image recognition, and satellite analyses. AI is being implemented in new detection devices capable of locating and tracking submarines (Kozyulin 2019).

To sum up the chapter, it is important to mention that there is no narrow definition of dual use technology or service. Any technology or service that may be used for civilian just as for military / nefarious civilian use may be under the definitions above understood as dual use. The definitions used were selected due to the prestige of institutions publishing

them just as they demonstrate the uniqueness of Artificial Intelligence within the dual-use brackets. AI is an enabler. It is not physical; you may not touch it. This technology works on improving the others by increasing their speed and efficiency by analysing data from the input. It always needs its use case. However, there are just as many fields in which the AI helps just like those, where the AI incentivizes and improves weapons systems. Artificial Intelligence shall and will be considered as dual use technology within this paper.

The problematic thing is, that in a majority of cases we may not determine, who shall benefit from the misuse of AI. The applications are widened by using AI, but that does not necessarily mean the one creating the AI will benefit. There are many unknowns that affect the algorithms in real life such as already mentioned false positives and false negatives mistakes. The system may be in many situations unpredictable in the sense that we do not know how it will respond to a new situation. Due to that, the systems are rigorously tested, tuned, and checked. After reviewing the topic, I am at the moment convinced of only one application of AI where private actors may directly benefit, and that is manipulation with the society and public opinion.

5 May the AI be used in a conflict with a state?

Demonstrating the abilities of Artificial Intelligence as an enabler and a dual-use technology, we will be elaborating the discussion on the research question we posed at the beginning. The potential for misuse relates to every technology and answering whether it will ever be used may not be easy. We, therefore, explore a couple of threats emerging with the development of AI and discuss in detail, what are the odds this case might happen in the future. In this chapter, we will be building on the research of Caldwel, Andrews, Tanay, and Griffin, discussing with a large group of field experts across the academia, private sector, and the state.

The following part will be to a significant degree a combination of two major articles discussing this very topic. It is important to mention, that we are discussing any misuse of AI by anyone against the state. This chapter is an overview of the AI potential in a conflict in general. The emergence of Artificial Intelligence in the field of security not only means a more efficient security system, but it also signals an "expansion of existing threats" (Pohler et al. 2018). This technology is available to a wide group of potential adversaries and as mentioned before, it is not all so expensive to develop. Of course, the more money we invest into the system (time of people, obtaining high-quality datasets, investing in state-of-the-art equipment), the more we may get regarding the precision and trust in the algorithm. Some companies even provide open source codes, meaning that anyone with access to the Internet may download the piece of code and may apply it as they wish without understanding it. An example may be a quote from one article, that "in 2019, Chinese researchers published open-source code for AI missile systems controlled by deep reinforcement learning algorithms" (Haney 2020, p. 61).

Attacks are much more difficult to counter and provide a significant degree of anonymity. The attribution problem in cyberspace is well known and there still are no multilaterally binding legislations how to attribute any kind of cyber misuse. AI is fast in its development, available and efficient in its tasks. It is natural, that someone might want to find out what is going to happen if the AI is not used the way it was originally intended. What may be disputable is the fact, that Artificial Intelligence is still in its infancy. Is the narrow AI therefore capable of threatening anyone?

As a matter of fact, we answered this question before. It is and the fact we talk about narrow AI changes nothing. All processes relying on data (vital majority) are affectable by

AI by increasing the speed of analysis, improving efficiency, and bringing new ways of conducting the job. Whether civilian such as in the healthcare industry or in the military, AI does work towards all technologies. In this place, it is important to say that AI as such is only a term. Artificial Intelligence is not a specific thing or a computer. It is an algorithm, a metaphysical thing working within already existing systems.

In 2020, an article by Caldwell, Andrews, Tanay, and Griffin called *AI-enabled Future Crime* collected examples of crimes and assessed their threat levels. After this exercise, the team organized a two day workshop with representatives from academia, government, private sector, police, and defence forces to "catalogue potential criminal and terror threats arising from increasing adoption and power of artificial intelligence, and to rank these threats in terms of expected victim harm, criminal profit, criminal achievability and difficulty to defeat" (Caldwell et al. 2020, p. 1).

The outcome was a classification of AI-enabled threats into three groups according to several criteria such as the harm done, profit for the attacker, achievability regarding the technical requirements and costs, and defeat-ability, standing for the difficulty of repairing the damage done by such a threat. Since this discussion was incorporating people from across the AI-related fields, it is important to show the threats and explain how the experts rated them.

5.1 Low risk threats

The bottom in all categories is represented by forgery and bias exploitation. Forgery, meaning a generation of fake content in art or music was rated as unprofitable, minimally harming, easy to defeat and, tough to achieve. "There has been some success producing digital images that broadly mimic the visual style of great painters, that is a very different proposition from creating actual physical objects that would pass muster in a gallery or auction house" (Caldwell et al. 2020, p. 11). These threats are not expected to be dangerous since the disproportionate imbalance between gains and costs. In this case, we also believe that potential private adversary would not benefit over the state.

Bias exploitation was found low in profit and minimal in harm. Taking the advantage of biases any AI learned may mean strengthening opinions of an individual or group of people by recommending certain Google pages or YouTube videos but again, despite these threats are real as we will see below, there are threats much more vital to the system. This

point is strictly related to bias. Recommendation systems will be thoroughly debated in a different context, but as for bias on the internet, the experts agreed it is not beneficial compared to the costs.

AI-authored fake reviews and AI-assisted stalking were rated as easily achievable since there are tools enabling to oversee the activity of people or an individual. Other fields are however low in profit and rather easy to defeat. Stalking is considered damaging on the level of an individual but does not possess a wider issue. Fake reviews lack persuasive power and are therefore not considered so risky.

As for the last interesting example from this category, I would mention burglar bots. "Small autonomous robots that could be delivered into premises through small access points, such as letterboxes or cat faps, to retrieve keys or to open doors allowing ingress for human burglars" (Caldwell et al. 2020, p. 10). The only threat evaluated as "profitable" within this category of low risk threats, yet the crimes are rather harmless and compared to the profit, highly technically demanding.

None of the threats in this category were aimed against the state to the level when would the private actor gain any significant advantage or reason to conduct such an act. These cases are however present and thank for their existence to the AI. Their low damage rises from the impact on individuals or very small groups of people. They are also much easier to fight against than the following threats and cause relatively minor damage.

5.2 Medium risk threats

In this category, we start with crimes rated as primarily neutral across the criteria. Online eviction, tricking face recognition, and autonomous attack drones. The face recognition problem is rather hard to achieve since for example, Apple claims, that the "false-positive rate is just 0,001%" (Knibbs 2017). This threat is demanding in technical skills yet causes rather minimal harm and is therefore not considered as vital. Even more so if we include the fact, that the attacker must be lucky every time countering facial recognition system.

Online eviction in fact stands for much more. For example, the denial of access to any service required or in general disabling access to all online activities. As for an example, I illustrate ransomware called WannaCry that encrypted a user´s hard drive requiring payment in Bitcoin to gain the encryption key. Here I would not agree with the assessment

claiming that these attacks are low profit since the WannaCry bill culminated on about 4 billion USD globally (Kaspersky 2017). And this is one of the largest we saw, many others, smaller might just disappear in the media. Ransomware might also be a tool private companies may endanger the state. The attribution is difficult, if even possible and the need for governmental systems to function is vital. The potential gain might be a contract for antivirus software or simply a demonstration of power and vulnerability. I personally believe that companies have very little interest in these types of acts, as it represents an act of aggression. A lower level of such threat is a DDoS (Distributed Denial of Service) attack, that overloads the receiving platform, forcing it to collapse.

There is a known case that piloted drone delivered drugs to a prison (BBC 2018). Autonomous drones are expected to perform even finer operations, such as being weaponized and attack aircraft engines. "They were rated highly for potential harms, but low for defeat ability since in many contexts protection may be provided using physical barriers" (Caldwell et al. 2020, p. 9). Such smuggling might have interesting implications, yet it is believed private companies have different interests than smuggling drugs or using such technology against a state.

Learning-based cyber-attacks are rather profitable and harmful, yet their capabilities are still low. Finer targeting, higher efficiency is yet not sufficient to consider this kind of threat as significant. Despite there is a huge potential for change due to the expansion of online systems and development in reinforced learning in AI.

Data poisoning is as mentioned a rather problematic issue since the algorithm creates all its processes and "thinking" upon the dataset. Injecting data that are not objective (meaning changed purposefully to change the output) has significant consequences and even more so if such dataset is distributed. Experts however agreed that trusted sources are difficult to infect and despite the threat is significant, difficult to defeat, and profitable, the feasibility is an issue here. Systems are rigorously checked in edge situations and on multiple occasions. The rules in place are ensuring a high level of trust to the implemented system.

Market manipulation such as AI-enabled change of trading algorithms, damage to competition or currencies is damaging, but also profitable and tricky to defeat. Yet again, "Achievability was rated low, because of the extreme difficulty of accurately simulating market behaviour and the very high cost of entry to engage in large scale trading" (Caldwell et al. 2020, p. 10). We discussed this higher above, such algorithms are certainly possible to

develop, but to implement them, we would have to demonstrate high precision that shall not be possible when checking these systems.

The most harmful in this category are military robots. Any leak of information here is significant and threatening. Despite the experts again agreed, that the military has access to explosives and other edge technologies, they are kept secret and therefore difficult to obtain any knowledge about them. Here I would be a bit sceptical and cautious since human errors are known to exploit many secrets. We may mention the infection by Stuxnet in Iran from a flash drive of one of the plant workers (unintentional, yet demonstrating the point) or the case of Edward Snowden who uncovered the monitoring of people and violation of privacy rights under the argument of state security and protection of human lives.

5.3 High risk threats

The top 6 threats discussed will be divided here into two parts. Firstly, I will take a closer look at those having some downsides for the criminals, such as the disruption of AI-controlled systems, driverless vehicles as weapons, and AI-authored fake news. Then we will talk about the rest in a detail to see what makes them so dangerous.

Artificial Intelligence has proven to compose a text that is to a large degree indistinguishable from the one written by a human being (Simonite 2020). The AI advantage in creating fake news and conspiracies lies in the ability to put together multiple sources quickly and efficiently, generating many versions and improve the visibility of the articles created. Against AI-created fake news is much more difficult to defend, yet the profitability is not so high compared to other threats. A potential boost to this ability may be the recommendation engine implemented on the search websites. Spreading artificially created fake news might have a significant impact on society and might destabilize the situation in a country. This threat shall be not taken lightly. The primary gain would be political, which may benefit certain private actors.

We already discussed that the use of AI extends the potential attack space for an adversary. More and more companies and governments are using systems based on Artificial Intelligence so there is a significant level of harm that may be done by disrupting it. On the other hand, these systems are difficult to obtain and train. Despite this, disrupting AI-controlled systems remains to be a big challenge requiring computational capacities as well

as highly educated people. Questionable is also the matter of benefit, which in this case is not apparent.

Driverless vehicles are significantly updating the potential for attacks focused on soft targets. Over the last years, we witnessed multiple cases involving a vehicle. „Autonomous vehicles would potentially allow expansion of vehicular terrorism by reducing the need for driver recruitment, enabling single perpetrators to perform multiple attacks, even coordinating large numbers of vehicles at once“ (Caldwell et al. 2020, p. 7). Despite these vehicles are still in development and rely on human being behind the wheel, experts believe that it is a matter of time since such an attack takes place. This technology might be however more used by non-state actors, notably terrorists. Private actors as such would not directly benefit from the misuse of autonomous vehicles.

Large-scale blackmailing is one of the AI applications that has, thanks to AI technology much wider impact than ever before. Usual blackmailing messages include threats such as publishing intimate pictures and videos unless paying a certain amount to the adversary. Despite there are many who understand these e-mails, some are still willing to pay. Education can help prevent this from happening. Therefore, the risks are high, just because composing these e-mails is simple and available.

High profitability, minimal need for advanced systems, and hard defence are specific for tailored phishing. This „social engineering“ threat is another ultimate use case of AI systems. The system may collect publicly available data about an individual including a phone number or an e-mail and adjust every single message making it a highly reliable source but containing malicious content. Nowadays these attacks are focused on width more than depth meaning the reach is significant, yet the profit or response rate is very low. AI-adjusted emails might be a game-changer. Even more when we consider the automation of the process thanks to the AI.

Perhaps the most damaging threat is audio and video impersonation. We tend to obtain hard evidence of speculation before making any judgment, so audio and video sources are highly relevant. The content is being called “deep fake”, representing not only artificial creation but also a difficult process of revelation of the fake. It is even more difficult to convince society that it was a lie. There are some ways of revealing fake content, but these are not possible to be preserved for much longer due to issues in controlling the origin of the

fakes. The possible advantages for private companies are in manipulation with public opinion.

The following examples are the main tools and technologies in which the Artificial Intelligence plays role. They demonstrate specific issues and in multiple dimensions illustrate reasons why anyone might be interested in doing so. It is even more concerning, that the uses of AI-enabled technology rated the highest (military robots, driverless vehicles as weapons, tailored phishing, and audio/video impersonation) are those potentially threatening states by corporations. Despite some of the examples were rated as low in achievability, it is mostly so due to the narrow AI. With its development, we may expect this value to be much in favor of the adversaries. Only a small portion however might be used by private companies. We expect, that due to their position, companies will have to rely on plausible deniability of conducting any kind of attack. Therefore, any threats listed, that do not offer this attribute are out of consideration.

Artificial Intelligence enables many technologies for a possible misuse against a state. The consequences might be seemingly marginal, yet in some cases, the threats are significant and call for caution and awareness. Not many can be done by private companies as explained above, but some may be tempting for other potential adversaries, such as terrorists, extremists, or foreign adversaries.

Out of all the above-mentioned threats, only a few are considered plausible threats to the state from the side of private companies. All of them are concentrating on society, more specifically influencing, and mobilizing people. Others are considered and meaningless or threatening to the companies themselves. Therefore, if companies ever decide to use any technology against the state, it will most likely be similar to information warfare on steroids thanks to the use of video and audio deep fakes or AI-created documents and statements. The following chapter shall elaborate several cases into a bit more detail, discussing the misuse of AI against the state.

6 How may the AI be used against the state?

Following the specific threats arising with the emergence of AI, we proceed to several examples, when were the AI algorithms used against states. This is the most important part as it demonstrates real events that happened in the past. All of them took place after the 2000s, more specifically after 2015 demonstrating the novelty of practical AI misuse. We will deep dive into all these cases, to understand the context and the importance of AI algorithms. Firstly, we will investigate Brazil shortly before the presidential election in 2018, then debate the National Health Service in the United Kingdom and finish strongly with Cambridge Analytica / Facebook incident.

6.1 YouTube and its influence on presidential election in Brazil

One of the key target groups for the AI learning process is a customer, user, or literally any human being interacting online. Observing them, analysing their steps and decisions is a core feature allowing Artificial Intelligence to do what it excels at. Seeking patterns and understanding its audience to that degree it proposes products the users wish or are tempted to buy. Such recommending algorithm was launched by YouTube some years ago. This algorithm "learned from user behavior and paired videos with recommendations for others" (Fisher & Taub 2019).

Despite this technology allows us easier access to the information we might potentially look for, there is one big downside. These recommendation engines are doing their job so well, that if you watch 5 videos labeled as "far-right" or "conspiracy", it starts showing you more and more videos with the same or similar content. If we for example wish to see an interview with Jeff Bezos or Elon Musk, we find hundreds of videos. And the more we watch it, the more similar results are pinned to our YouTube homepage.

In many cases, this behavior is considered as desired. Yet, watching radicalising or extremist videos might be an example of undesired behavior, due to the nature of the content. The main issue is however that YouTube will be recommending you more and more videos so there is no simple escape from this. The other is the issue of creating so-called "echo chambers".

"YouTube´s recommendation system is engineered to maximize watch time, among other factors, the company says, but not to favor any political ideology. The system suggests what to watch next, often playing the videos automatically, in a never-ending quest to keep

us glued to our screens. […] As the system suggests more provocative videos to keep users watching, it can direct them toward extreme content they might otherwise never find" (Fisher & Taub 2019). These engines are now very common. Google uses it to ease the searching, translating, and filtering relevant results. Regarding the YouTube, "the system now drives 70 percent of total time on the platform, the company says" (Fisher & Taub 2019). This is a stunning result. Only 30% is, therefore, the organic search, meaning we type something into the YouTube search bar. The rest is only clicking on what YouTube suggests from the main page or the recommendation bar on the side.

Jair Bolsonaro, in 2018 presidential candidate and now the president of Brasilia was very active on social media platforms, most notably on YouTube. His videos influenced many people to vote for him, as do any other spots or election videos. Yet in this case, the circumstances differ. A team of researchers at the Federal University of Minas Gerais in Brazil tried to replicate the recommending algorithm of YouTube. "The team analysed transcripts from thousands of videos, as well as comments beneath them. Right-wing channels in Brazil had seen their audiences expand much faster than others did and seemed to be tilting the site´s overall political content. In the months after YouTube changed its algorithm, positive mentions of Mr. Bolsonaro ballooned. So, did mentions of conspiracy theories that he had floated. This began as polls still showed him to be deeply unpopular, suggesting that the platform was doing more than merely reflecting political trends" (Fisher & Taub 2019).

This conclusion means that YouTube had significant power in shaping the people´s opinions, influencing a vast amount of society and extending the reach of the campaign. This behavior is the reason, why many politicians became more active on social media. The issue here lies in several facts. Firstly, we are talking about elections for the highest office in a sovereign state. Second, the recommendation engine was introduced during the campaign, inverting the public opinion about a candidate from one side to another. Lastly, as mentioned above, algorithms maximise the watch time and recommend videos of similar topics eventually creating an environment where is one opinion only.

Another team at Harvard decided to test if the rapid growth of far-right in Brazil was caused by the new YouTube engine. "By repeating this thousands of times, the researchers tracked how the platform moved users from one video to the next. They found that after users watched a video about politics or even entertainment, YouTube's recommendations

often favoured right-wing, conspiracy-filled channels" (Fisher & Taub 2019). The audience of Brazilian far-right channels grew and so did the preferences for the election. "YouTube challenged the researchers' methodology and said its internal data contradicted their findings. But the company declined the Times' requests for that data, as well as requests for certain statistics that would reveal whether the researchers' findings were accurate" (Fisher & Taub 2019).

Harvard team not only confirmed the Brazilian team, but also elaborated the argument further, by revealing a pattern in the recommendation system that favored conspiracy and far-right channels and videos. In the first round on the 7th of October 2018, Bolsonaro gained 46% of the votes, winning the general election 3 weeks later with over 55% of the popular vote.

A similar influence on the public by YouTube was spotted during the Zika virus in Brazil during 2015-2016. "Many Brazilians searching YouTube for health care information found videos that terrified them: some said Zika was spread by vaccines, or by the insecticides meant to curb the spread of the mosquito-borne disease that has ravaged northeastern Brazil" (Fisher & Taub 2019). During that time, a decision was made to distribute larvicides that were supposed to fight the mosquitos spreading the virus. When YouTube launched its recommendation engine, more and more people started to refuse the medicine. "They say, 'No, I've researched it on Google, I've seen it on YouTube" (Fisher & Taub 2019) said Dr. Auriene Oliviera, an infectious disease specialist. "Brazil's medical community had reason to feel outmatched. The Harvard researchers found that YouTube's systems frequently directed users who searched for information on Zika, or even those who watched a reputable video on health issues, toward conspiracy channels. A spokesman for YouTube confirmed the Times' findings, calling them unintended, and said the company would change how its search tool surfaced videos related to Zika" (Fisher & Taub 2019).

We usually see these engines offering us similar products to those we searched for shortly before. Yet the same system is rather dangerous regarding any trending topic. People tend to look for information, that is easily understandable, quick, and straightforward. Videos are therefore preferable choices and Google usually offers several videos regarding the topic you searched. They are quick and comfortable to the vast majority of the population. The research conducted by Statista in the first half of 2020 showed, that in Brazil, 71% of people consider social media as the primary source of information. Similar is for

example the situation in India (82% of respondents), and Nigeria (78% of respondents) (Watson 2021).

6.2 National Health Service and the data privacy

The following example illustrates the importance of data, as we discussed before. The National Health Service, or the NHS, is an umbrella term for all health and medical services for people living in the United Kingdom. European countries usually have private insurance companies, but the UK embodies it within one government funded company. The services are comparable, clients enjoy for their regular payment common services of the medical institutions without charge. More importantly, the NHS collects the medical and personal data of over 55 million people in the UK, making a huge dataset of private information. Given the fact it is the only institution administering such data in the UK, its reach and access are ultimate.

When the United Kingdom closed a deal with the United States on Trade, one of the articles of the agreement discussed access to the NHS information that was supposed to be available to the US. The price of this dataset is estimated to over 10 billion pounds a year (Nikolic 2020). "Washington has already made clear it wants unrestricted access to Britain´s 55 million health records [..] as part of any post-Brexit trade agreement" (Helm 2020). These data are being fed to AI algorithms, estimating the probability of certain medical complications, the likeliness of injuries, or speeding up diagnoses of certain diseases (Helm 2020). And as one of the leaders in the pharmaceutic industry, the United States needs an excessive amount of data. This dataset is unique in its nature, size, and data quality. All these attributes matter when creating a high-efficiency algorithm capable of evaluating the probability of diseases of future clients to the insurance company. Such technology would save millions of dollars to insurance companies since they might tailor insurance contracts to the specific client based on the AI analysis from the data obtained in the UK.

The NHS also got a lot of criticism for selling "anonymized" data about General Practice (GP) surgeries to some of the drug giants in the US. It does even sell licenses for access to the database. Many argue that patients do not know how these data are processed and many others expressed their doubts about anonymity. Firstly, patients that wish not to submit their data must actively opt-out, meaning you must explicitly express your will not to be contained in the dataset open for sale. And secondly, there is the argument of traceability. "[…] patient data compiled from GP surgeries and hospitals – and then sold for

huge sums for research – can routinely be linked back to individual patients´ medical records via their GP surgeries. […] there is clear evidence this is already being done by companies and organizations that have bought data from the DHSC (Department of Health and Social Care), having identified individuals whose medical histories are of particular interest" (Helm 2020).

The issue is problematic from many angles. Data privacy is one of the most discussed human rights now, yet in many countries very little has been done to protect them. Artificial Intelligence algorithms may be a very useful tool in analysing millions of records of operations, diagnoses, and treatments and their success rates, creating a model, where, if information about the client is inserted, may estimate the risks of diseases. Given the vast dataset with detailed information, family history, and your own medical report, the algorithm may, of course with some error margin, estimate, how likely are you to suffer from certain diseases such as cancer, diabetes, Parkinson´s disease, etc. (Helm 2020). At the moment, the insurance companies play the "game of guess", where their estimates of your costs regarding GP, operations, or other medical expenses is lower than the costs you pay for the service. This data selling of so many people and accessed by drug and medical companies might empower the algorithms to predict the health of further millions of people and allowing tailoring of insurance payment towards the customer.

This case demonstrates a different approach to the issue. The monopolistic position of NHS regarding the medical data collection was misused and data provided by individuals were misused. The aim is to build AI algorithms upon this dataset, enhancing the "modernization" of the insurance industry. But such an act damages the government of the UK. Despite the link between AI and its use against a state is weaker than in the remaining two cases, the rationale remains. The UK government exchanged private information with the US that uses them in creating AI models. Such a step discredits the government and opens active debate about the degree of privacy and data protection. It threatened the state as trust is important in the state-citizen relationship.

6.3 Facebook and the Cambridge Analytica incident

The Cambridge Analytica case is certainly the most famous incident from all of those already mentioned. Cambridge Analytica is a company focusing on political data-analysis. It cooperated with the former president of the United States, Donald Trump´s campaign in 2016. Their tools consist of analysing huge datasets and advising the party strategists what

topics shall be mentioned or not mentioned, what is the current trend and prevailing opinion in the society, and how it should be addressed. Before the 2016 election in the United States, Cambridge Analytica “built extensive personality profiles, which its clients can leverage for 'psychological targeting' of ads” (Wired 2018).

The major problem is that Cambridge Analytica had to gain the data from somewhere. And the source was Facebook. “The firm is being accused of using and secretly keeping data on 50 million Facebook users without their permission” (Wired 2018). At the end of 2019, “the Federal Trade Commission has officially ruled that Cambridge Analytica deceived consumers through its data-gathering practices” (Lecher 2019).

The way of getting access to the data was revealing. A third-party application called “thisisyourdigitallife” created by the Cambridge University´s Psychometrics Centre and was downloaded by nearly 300 thousand people. Users log into the app using their Facebook credentials. The application´s Terms of Use however stated that not only their data will be used by the third-party, but it will also use the data of their friends (Wired 2018).

The scandal is connected to the 2016 US Presidential election, where Donald Trump´s campaign relied on a targeted advertisement. They were using the services of Cambridge Analytica, highly likely using outputs of illegally obtained data from Facebook. Mark Zuckerberg, the CEO of Facebook appeared in front of many Congressional committees, testifying upon the misuse of the data Facebook is gathering.

The 2016 Presidential election in the United States was, as usual, one of the most watched events that year. Donald Trump, a businessman, and a billionaire won the election over Democrat Hillary Clinton. Immediately after the election, many started to speculate how did Donald Trump win. We now know that Trump´s campaign cooperated with Cambridge Analytica, that after the election “both denied and embraced the idea that they had played a pivotal role in the outcome” (Bump 2018).

We shall firstly understand, what happened between Facebook, Cambridge Analytica and how is it related to AI. “Cambridge Analytica harvested information from over 87 million Facebook users through an external app in 2015. The data came from a personality quiz, which around 270,000 people were paid to take. The quiz — "thisisyourdigitallife" — in turn, pulled data from their friends' profiles as well, ending in the enormous data stash” (Ma & Gilbert 2019). Among the data harvested was a variety of personality points and

information such as “openness, conscientiousness, agreeableness, IQ, gender, age, political views, and religion” (Weis 2018).

The Trump digital campaign, run by Theresa Hong, was however even more detailed, trying to understand voters in depth. The details contained such information as to when was the last time they voted, who did they vote for, what car they drive etc. This further helped to shape the campaign regarding topics to address, what state to travel to next, where not to travel or what to develop further on the agenda. All ads created were tailored to a specific group, targeted to the audience with the largest voting potential (‘The digital guru who helped Donald Trump to the presidency’ 2017).

The personality prediction app was developed by Aleksandr Kogan, who worked at the Cambridge University. Facebook used his app and Kogan claimed the data are collected for academic purposes. Yet his research was handed to Cambridge Analytica that used it in political campaigns (Weis 2018). Facebook then released a statement that Kogan “lied to us and violated our Platform Policies by passing data from an app that was using Facebook Login to SCL/Cambridge Analytica, a firm that does political, government and military work around the globe" (Grewal 2018).

„During the 2016 US presidential race, Cambridge performed a variety of tasks for the Trump campaign, including profiling voters, purchasing TV ads, and suggesting where Trump should travel to best appeal to voters, according to The Times. Several news outlets reported in 2016 that the Trump campaign paid Cambridge Analytica $5 million for its services in September alone that year, a significant increase from the $250,000 it paid one month earlier“ (Weis 2018).

In 2018, one of the former Facebook employees, Mark Zuckerberg´s speechwriter, gave an interview in which she described the internal attitude of the company towards the state. Kate Losse described her worries at the beginning, when Facebook was just a small social network, yet as it grew in size and popularity, her concerns upscaled. “My worry began to deepen when Zuckerberg began using the language of states to talk about Facebook’s burgeoning power. 'Companies over countries,' he told me once, as we discussed a blog post about Facebook’s goals. 'If you want to change the world, the best thing to do is to build a company,' he added” (Losse 2018).

“Facebook employees are often brilliant and technically gifted. But the atmosphere we inhabited did not encourage asking questions about power, at least publicly. Instead,

internal conversations stayed focused on technical and growth questions; questions that can be answered with metrics — how fast are we growing and what technical roadblocks can we remove — rather than introspection" (Losse 2018).

Mark Zuckerberg´s attitude towards privacy might be illustrated in this part of the conversation. "When asked about people who thought Apple was better at privacy, Zuckerberg claimed those customers had 'Stockholm syndrome.'" The further statements are even more surprising, as the Cambridge Analytica incident occurred. "Revelations that the company worked with the Trump campaign and the Brexit campaign in the United Kingdom to use shadily harvested data from Facebook to target political ads has shaken the company's public image. But Cambridge Analytica is a scandal that isn't a scandal: Everyone who has ever worked on or with the Facebook platform knew that for several years, the platform made data available to third-party developers by design. The scandal is that the world finally understands the ramifications of that state of affairs" (Losse 2018)

Kate estimates, that there still is only a minimal reflection within the company. Despite the company has taken steps to "make anonymized data sets available to researchers to understand how election interference happens on Facebook" (Losse 2018). As a speechwriter, Kate got the chance to understand the company from a different side – the one represented to the outside, and the one creating its growth and development. "In the early days of Facebook, it was easy to dream big and hope for the best even while "moving fast and breaking things"; in many ways, we were more successful than anyone who worked there back then could have imagined. But now that market dominance has been achieved and its risks are readily apparent, it's time to set real limits on Facebook's power" (Losse 2018).

To conclude upon the topic of Facebook, the AI was used largely in political data-analysis company assisting the campaign of the US president. At the beginning of 2020, Andrew Bosworth, a Vice-President at Facebook App released a statement commenting a leaked internal memo. Upon the 2016 campaign mentioned the following. "So, was Facebook responsible for Donald Trump getting elected? I think the answer is yes, but not for the reasons anyone thinks. He didn't get elected because of Russia or misinformation or Cambridge Analytica. He got elected because he ran the single best digital ad campaign I've ever seen from any advertiser. Period" (Bosworth 2020). Theresa Hong even stated in her interview with the BBC, that "Without Facebook, we would not have won. I mean Facebook

really and truly put us over the edge" ('The digital guru who helped Donald Trump to the presidency' 2017).

We demonstrated that Artificial Intelligence may be and was used against states. Most notably during the Brazilian presidential election in 2018, but also in 2016 targeting the voters for the former US President Donald Trump. The data used are becoming a tool that private giants use against states and may participate on their destabilization. Just as in the NHS case, selling the personal data of millions of people allowing private companies to take advantage of them or the states is exactly what happened in these three cases. The data are an important resource, but we see that for some they are available in a huge quantity. Unless states issue stronger legislative frameworks on data protection, their use, and price, these situations may happen again in various forms and intensities.

We discussed the relations between state and private actors in chapter three and one of the key points was, that private actors must respect the processes and decisions made by the state. Elections are a key process for democratic states and any attempt to manipulate the outcome shall be considered an attack on the state. All three cases demonstrated a different angle of data misuse. In the case of the NHS, there was no direct involvement of private entities in the trade agreement. The only harm done is a result of poor judgment of the UK Government to hand data about its citizens to a foreign country. In this regard, any private actor did not endanger the state directly. The potential for misuse comes with the use of data by private companies in the US. The targeted audience is the people that may face uneven conditions when dealing with insurance companies, likely biasing due to the evaluation conducted by an AI algorithm.

The case of Facebook and Cambridge Analytica is slightly ambiguous, yet the main point remains. Cambridge Analytica misused personal information to create models based on which the Trump campaign addressed the constituents. This is based on the understanding in this paper considered as influencing the outcome of the democratic process. It is a step over the line where companies may operate to the sphere where it endangers essential pillars of the state. It remains to be slightly ambiguous due to the fact, that social media are means to deliver a message to the people. It corresponds with what social media may do during election time. In other words, Facebook is a means to influence the electorate. But it may not be a tool we pay in order to know what certain groups of people want us to say in order

to get the vote. That shall be considered as an attack against the state, since you may "buy" a vote.

Similarly, we may think about the events in Brazil. YouTube launched new technological tools that were enhancing the company´s policy. And regardless of the intentions, the algorithm worked unreliably, against the policy of the company, and encouraged certain topics and ideologies to the detriment of the other. These events led to the growth of far-right thinking of users and influenced the elections in a democratic state. As in the previous case, such technology affecting the outcome of state crucial processes shall be considered as threatening and dangerous to the state.

After researching these three cases, we have strong grounds to believe that without Artificial Intelligence, such situations would be unthinkable and most likely would not be possible. Artificial Intelligence, therefore, opened new threats and is an enabler in this regard. But one more question remains. Would private companies benefit from these acts? Researching this question is not trivial, if even possible. We may assume, that in the United States, Republican representatives might be more open towards limited regulation of technological giants and their taxation, as Donald Trump was declaring (Jagoda & Birnbaum 2019). These tendencies might be slightly different on the Democratic side as new president Joe Biden took the office earlier this year (Wiseman 2021).

7 Findings

The paper followed the logical process outlined in the introduction. We discussed what does the term Artificial Intelligence mean, how it works and where may it be found. After the theoretical introduction, we explained where the primary core of AI development is and how are some countries approaching this technology. We then debated the role of private actors within the international system and why are they important for states as well. Given the AI´s nature, the next chapter discussed the dual-use technologies and tried to fit the AI to it. We have also talked about some new threats the AI enabled and lastly, we mentioned several cases when we believe the AI played a significant role in damaging the state.

Artificial Intelligence, just as all emerging technologies requires significant investments to be developed to a degree it may assist us. As the financial question is important to finding the main centres of research and development of AI, we looked at this area as well. States invest untrivial amounts of money in research and development, they collaborate on research projects, acquire companies with interesting research potentials, and are active not only home but also abroad. Their main limitation is however the source of money – the state budget. Private actors are more independent regarding cash management since they may obtain the finances in multiple ways. We mentioned direct investments from home and foreign countries, their own R&D investments, PE funds, and VC funds. The resources are not only richer in number, but also generous in volume. The primary core of AI R&D, therefore, lies in the private sector and companies acquire more highly educated people in this regard, as they offer higher salaries and benefits. States often participate in research and development, actively involving with the private sector and academia to be a part of the development. Some countries are however approaching this differently. For example, China, that is believed to be highly involved and controlling the R&D of Chinese companies. It pursues its national strategy to incorporate these actors to fulfilling national goals and become the leader in AI. The same goes for the Russian Federation, which concentrates the most of AI capacities in the state sphere and any private research is not so significant. Due to these reasons, we decided to focus on more open countries, respecting privateness.

Private companies are very active not only within the state but also in the international environment. They participate in negotiations, secure deliveries of technology

and goods or even services and are used as “soft approach “in international relations. Their presence during international visits is regular and desired, as they help to develop technological and economic exchange and common dialogue. Their role grew over the decades and are now significant players that must be respected. Financially, some are equal to the states, they represent huge groups of people as they belong to the largest employers, and their reliability, to prosper and survive in the long term must be supported by satisfied customers. They made up large bodies potentially challenging states since in some key areas, like security, delivery of strategic goods, and other services, may be asked to replace the state. There are at least reasonable grounds to assume that private companies may eventually aspire for similar roles states have these days. And is the AI a tool that may help them get there?

Artificial Intelligence is being compared to electricity. It enables a light bulb to shine, a washing machine to do the laundry, and computers to work. AI is the same. It enhances the speed and effectiveness of processes, resulting in the growth of work done within the same timeframe, quality, and originality. It is however something, that may help adjust the public transportation system just as increase the accuracy of ICBM missiles. It may be used for recommending us products we are looking for or lock us in an echo chamber when deciding who to cast a vote. Artificial Intelligence enables and reveals a wide spectrum of applications. Some are civilian, some military. But in both cases, they may be used in a safe manner, or maliciously. That is what makes AI a dual use technology. And the more capital we mobilise, the better conditions we must develop a high-quality AI capable of conducting assigned tasks precisely.

Despite AI enables a significant amount of potential threats, private companies would not benefit from most of them. These institutions need to maintain plausible deniability. Otherwise, their name would suffer, and states would most likely take steps to avoid any such event from happening in the future. Therefore, the remaining cases are mostly focusing on influencing the people and their opinions. Many threats we illustrated had either a low level of achievability or were not financially beneficial. Private companies already concentrate significant financial resources, so financial motivation is not believed to be their primary aim. Yet the power over the people is significant. These companies compile huge datasets of information about almost every individual and have them “at the disposal”.

Three cases, illustrating primarily the importance of data were introduced and rigorously explained. At their core, there were private companies who either knowingly or not created algorithms threatening states during their most important moments – the elections. We examined two specific approaches – algorithmic persuasion in the case of Brazil, where certain videos were preferred at the expense of others, or algorithmic tailoring in the case of Facebook and Cambridge Analytica. These threats are enabled by Artificial Intelligence, more specifically, privately developed AI. They are used on a regular basis and proved to be correct as they boost the revenue of fashion stores and other consumer appliance industries. People are in touch with it daily and may be influenced. It is precisely those moments when people decide upon something and these algorithms may influence them. Whether during shopping online or on election day. Such cases that happened in Brazil and the US are showing us, that algorithms may interfere with the most important processes of states, possibly influencing the outcome. And states are certainly not those who benefit. What more, if such influence is found, the results are questioned, and the reliability of states is shaken. We have seen no such thing in case of Cambridge Analytica or YouTube, yet it is certain, that their power is not trivial and must be considered.

In answering the research question as introduced in the project, we will summarize all the key findings to prepare the ground for the final argument. Artificial Intelligence is being pursued by both, states, and private companies. The investments are significant and both states and companies are increasing the volume of money spent to accelerate the development of AI. Private companies have the advantage of multiple ways of where the money comes from, they can acquire specialists and experts and monetize their research. Their role is constantly growing, and, in many cases, they supply countries in delivering services and goods.

Artificial Intelligence opened doors to many new threats and opportunities that actors developing AI may enjoy. We have seen that private actors do possess tools and technology to use and misuse AI algorithms against states. Influencing elections via targeted advertising and tailored campaigning, or by recommending videos with politically unbalanced algorithms outlines the maliciousness of such AI use. As for the benefits, we mentioned that such significant companies may be politically interested in elections and all cases we discussed were focusing on that matter. Any further benefits would be unsupported by evidence and are therefore not mentioned. The key takeaway is, that Artificial Intelligence

is a dual-use technology, it may be used against the state and provides an advantage to the adversary in the very nature of the attack, that would be without this technology unimaginable or disproportionately more difficult to perform.

Conclusion

This paper combined many forms of data inputs to put together an overview and start a wider discussion upon the topic of Artificial Intelligence misuse against the state. Despite failing in interviewing enough people across the sectors, their inputs and further sources provided me with sufficient information to conclude the paper and open an even wider debate on this topic. After introducing the topic of Artificial Intelligence, its meaning, essentials of functioning, and its potential, we debated the core of all the development of AI. The majority of funding, the fact that governments compete to fund more private companies focusing on AI development, and the overall situation of these businesses and their applications answered the question, that private companies are behind the AI progress, development, and success. They are profit motivated and therefore invest significant proportions of their revenues back to research and development units focusing on advances in the field the company is interested in the most. We found out, that states tend to participate in the development of technologies they believe they have practical applications for, yet many others are not regulated or restricted. These systems for the training require vast amounts of data, but only a little has been so far done to protect the data from misuse.

The ambition of this paper was to examine whether there are any grounds to believe private companies may misuse an AI-empowered technology against states. We explained how AI works, how does it fit the brackets of dual-use definitions, and explored new threats enabled by AI. We dedicated a significant part to the importance of data and its quality since it is a cornerstone of any AI algorithm. Despite the findings show, that the main core of AI development is in the private sector and that the AI enabled many previously insignificant threats to grow in importance, the argumentation would deserve to be elaborated more.

This paper provided essential grounds to grasp the tendencies of AI development, its main drivers, and potential, yet some topics deserve to be discussed more in depth and most importantly shall be based on interviews with field experts. It set the ground in understanding the AI potential, its enabling power and demonstrate that it may influence major events in democratic states such as the election. The paper reached its goal in proving there is a reason to believe that Artificial Intelligence does provide a strategic advantage to private companies when countering a state, such as what happened in Brazil and the United States. The potential and practical cases are evidence of such a threat.

The further arguments worth discussing are more hidden and could not be researched from open sources to provide any relevant outputs. One such question we tried to answer at a very low level as if the private companies could benefit from such use of AI against the state. This argument was not in the scope of this paper yet proposes the direction of potential further investigation. The benefits we debated were mainly focused on financials and political preferences.

Another big and relevant question arising from this research is, whether private companies even intend to use such power. In all cases presented, private actors defended themselves that the actions were unintended. Given the fact that none of them was as of today held accountable for these events, we need to consider them as not guilty and not speculate upon their intentions. Private actors are, as mentioned, to a large degree cooperating with state agencies, collaborating on projects, and enjoy the benefits of Public-Private Partnerships. This might indicate that it is not in the interest of these companies to change this course of action. Wider debate, discussions, and primarily interviews with representatives of companies focusing on Research and Development in Technology or AI specifically might bring interesting conclusions as to the relation, attitude, and depth of cooperation between states and private actors in this regard.

Actual discussions among states and international organizations are focusing on the added value of this technology, which is enabling us to increase the pace of development of society and improve our wellbeing. They are open to any cooperation that emphasizes these goals and is willing to contribute while preserving the standards to pursue the development with respect to protecting the people and their privacy.

List of References

A brief history of Facial Recognition. *NEC New Zealand*. Available at: https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/ [Accessed March 06, 2021].

Acharya, A. & Arnold, Z., 2019. Chinese Public AI R&D Spending: Provisional Findings. *Center for Security and Emerging Technology*. Available at: https://cset.georgetown.edu/wp-content/uploads/Chinese-Public-AI-RD-Spending-Provisional-Findings-1.pdf [Accessed March 06, 2021].

Alphabet Inc. Form 10-K. In *United States Securities and Exchange Commission*. Delaware 2020. Available at: https://abc.xyz/investor/static/pdf/20210203_alphabet_10K.pdf?cache=b44182d [Accessed May 3, 2021].

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J. & Mané, D., 2016. Concrete problems in AI safety. *arXiv preprint arXiv:1606.06565*.

An Open Letter on AI: Research Priorities for Robust and Beneficial Artificial Intelligence. *Future of Life Institute*. Available at: https://futureoflife.org/ai-open-letter/ [Accessed April 11, 2021].

Apple Inc. Form 10-K. In *United States Securities and Exchange Commission*. California 2020. Available at: https://d18rn0p25nwr6d.cloudfront.net/CIK-0000320193/7b5717ca-6222-48e6-801c-9ea28feeef86.pdf [Accessed May 3, 2021].

Apuzzo, M., 2014. Blackwater Guards Found Guilty in 2007 Iraq Killings. *The New York Times*. Available at: https://www.nytimes.com/2014/10/23/us/blackwater-verdict.html [Accessed March 06, 2021].

Arnold, Z., Rakhovsky, I. & Huang, T., 2020. Tracking AI Investment. In *Center for Security and Emerging Technology*. Available at: https://cset.georgetown.edu/research/tracking-ai-investment/ [Accessed March 06, 2021].

Avant, D., 2004. The privatization of security and change in the control of force. *International Studies Perspectives*, *5*(2), pp.153-157.

Ayoub, K. & Payne, K., 2016. Strategy in the age of artificial intelligence. *Journal of strategic studies*, *39*(5-6), pp.793-819.

Babic, M., Fichtner, J. & Heemskerk, E.M., 2017. States versus corporations: Rethinking the power of business in international politics. *The International Spectator*, *52*(4), pp.20-43.

Baer, W, 2018. Countering the Artificial Intelligence Threat. *Cosmos and History: The Journal of Natural and Social Philosophy*, *14*(1), pp. 17-26. Available at: http://cosmosandhistory.org/index.php/journal/article/view/680

Bosworth, A., 2020. Thoughts for 2020. *Facebook*. Available at: https://www.facebook.com/boz/posts/10111288357877121 [Accessed April 11, 2021].

Bourne, V., 2017. State of Artificial Intelligence for Enterprises. *Teradata*. Available at: https://assets.teradata.com/resourceCenter/downloads/ExecutiveBriefs/EB9867_State_of_Artificial_Intelligence_for_the_Enterprises.pdf [Accessed March 06, 2021].

Brainard, J., 2020. US proposes principles for AI. *SCIENCE*, 367(6474), pp.127-127.

Brody, B., 2019. Trump Signs Order Prioritizing Artificial Intelligence Research. *Industry Week*. Available at: https://www.industryweek.com/technology-and-iiot/article/22027134/trump-signs-order-prioritizing-artificial-intelligence-research [Accessed April 11, 2021].

Bruce, R., 2002. *The emergence of private authority in global governance* (Vol. 85). Cambridge University Press.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. & Anderson, H., 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Buckland, B.S. & Winkler, T.H., 2015. Public Private Cooperation: Challenges and Opportunities in Security Governance. *DCAF Horizon 2015 Working Paper No. 2*. Available at: http://www.cpahq.org/CPAHQ/CMDownload.aspx?ContentKey=f0b3defd-dffb-4a96-a69a-bb36b68b3f38&ContentItemKey=49187091-f7a6-4785-b317-49a5a13e7215 [Accessed April 14, 2021].

Bull, B., Bøås, M. and McNeill, D., 2004. Private sector influence in the multilateral system: A changing structure of world governance?. *Global Governance: A Review of Multilateralism and International Organizations*, *10*(4), pp.481-498.

Bump, P., 2018. All the ways Trump's campaign was aided by Facebook, ranked by importance. *The Washington Post*. Available at: https://www.washingtonpost.com/news/politics/wp/2018/03/22/all-the-ways-trumps-campaign-was-aided-by-facebook-ranked-by-importance/ [Accessed April 11, 2021].

Button, R.W., 2017. Artificial Intelligence and the Military. *RealClear Defense*. Available at: https://www.realcleardefense.com/articles/2017/09/07/artificial_intelligence_and_the_military_112240.html [Accessed March 06, 2021].

C4I and Cyber Defense Directorate. *Israeli Defence Forces*. Available at: https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/ [Accessed April 11, 2021].

Caldwell, M., Andrews, J.T.A., Tanay, T. & Griffin, L.D., 2020. AI-enabled future crime. *Crime Science*, *9*(1), pp.1-13.

California Consumer Privacy Act (CCPA). *Office of the Attorney General*. Available at: https://oag.ca.gov/privacy/ccpa [Accessed April 11, 2021].

Calvello, M., 2019. 22 Eye-Opening Facial Recognition Statistics for 2020. *Learning Hub*. Available at: https://learn.g2.com/facial-recognition-statistics [Accessed April 11, 2021].

Comiter, M., 2019. Attacking Artificial Intelligence. *Belfer Center Paper*.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe, Brussels: European Commission.

Confessore, N., 2018. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [Accessed April 12, 2021].

Crawford, K. & Schultz, J., 2019. AI systems as state actors. *Columbia Law Review*, *119*(7), pp.1941-1972.

Creighton, J., 2017. Making AI Safe in an Unpredictable World: An Interview with Thomas G. Dietterich. *Future of Life Institute*. Available at: https://futureoflife.org/2018/09/17/making-ai-safe-in-an-unpredictable-world-an-interview-with-thomas-g-dietterich/ [Accessed March 06, 2021].

Dafoe, A., 2018. Global Politics and the Governance of Artificial Intelligence. *Journal of International Affairs*, *72*(1), pp.121-126.

Davenport, C., 2021. Elon Musk's SpaceX wins contract to develop spacecraft to land astronauts on the moon. *The Washington Post*. Available at: https://www.washingtonpost.com/technology/2021/04/16/nasa-lunar-lander-contract-spacex/ [Accessed April 23, 2021].

de Freitas, W., 2018. Who is more powerful – states or corporations? *The Conversation*. Available at: https://theconversation.com/who-is-more-powerful-states-or-corporations-99616 [Accessed March 06, 2021].

Diamantis, M.E., 2019. The extended corporate mind: When corporations use AI to break the law. *NCL Rev.*, *98*, p.893.

Dilworth, R.L., 1988. Artificial intelligence: The time is now. *Public Productivity Review*, pp.123-130.

Etherington, D., 2020. Elon Musk says all advanced AI development should be regulated, including at Tesla. *TechCrunch*. Available at: https://techcrunch.com/2020/02/18/elon-musk-says-all-advanced-ai-development-should-be-regulated-including-at-tesla/ [Accessed April 11, 2021].

EU funding for Dual Use. European Committee. Available at: http://ec.europa.eu/DocsRoom/documents/6913/attachments/1/translations/en/renditions/native [Accessed April 11, 2021].

Facebook ad campaign helped Donald Trump win election, claims executive. *BBC*. Available at: https://www.bbc.com/news/technology-51034641 [Accessed April 12, 2021].

Facebook Inc. Form 10-K. In *United States Securities and Exchange Commission*. Delaware 2020. Available at: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/4dd7fa7f-1a51-4ed9-b9df-7f42cc3321eb.pdf [Accessed May 3, 2021].

Facial Recognition Airports Survey. *Reservations*. Available at: https://www.reservations.com/blog/resources/facial-recognition-airports-survey/ [Accessed April 11, 2021].

Falcon, W., 2018. CIFAR - This Is How Canada Funds Its AI Leadership. *Forbes*. Available at: https://www.forbes.com/sites/williamfalcon/2018/12/03/cifar-this-is-how-canada-funds-its-ai-leadership/?sh=51fa5d6da03c [Accessed March 06, 2021].

Fawkes, A.J., 2017. Developments in Artificial Intelligence: Opportunities and Challenges for Military Modeling and Simulation. In *Proceedings of the 2017 NATO M&S Symposium* (pp. 11-1).

Filibeli, T., 2019. Büyük Veri, Yapay Zeka ve Makina Öğrenimi Algoritmalar: Hakikat Ötesi Çağda Dijital Tehditlerin Betimleyici bir Analizi. *Galatasaray Üniversitesi İleti-ş-im Dergisi*, (31), pp.91-110. Available at: https://dergipark.org.tr/tr/doi/10.16878/gsuilet.626260 [Accessed March 06, 2021].

Fisher, M. & Taub, A., 2019. How YouTube Radicalized Brazil. *The New York Times*. Available at: https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html? [Accessed April 11, 2021].

Fischer, S.C., 2018. Artificial Intelligence: China's high-tech ambitions. *CSS Analyses in Security Policy*, *220*.

France's $5.5 billion tech fund 'only the beginning,' French minister says. *CNBC*. Available at: https://www.cnbc.com/video/2019/09/19/frances-5point5-billion-tech-fund-only-the-beginning-says-french-minister.html [Accessed March 06, 2021].

Friedmann, W.G., 1957. Corporate Power, Government by Private Groups, and the Law. *Columbia Law Review*, *57*(2), pp.155-186.

Gang who flew drones carrying drugs into prisons jailed. *BBC*. Available at: https://www.bbc.com/news/uk-england-45980560 [Accessed April 11, 2021].

Geist, E. & Blumenthal, M., 2019. Military Deception: AI′s Killer App? *War on the Rocks*. Available at: https://warontherocks.com/2019/10/military-deception-ais-killer-app/ [Accessed March 06, 2021].

Geist, E. & Lohn, A, 2018. How Might Artificial Intelligence Affect the Risk of Nuclear War? In RAND Corporation, pp. 1-28. Available at: https://www.rand.org/pubs/perspectives/PE296.html [Accessed March 06, 2021].

George, S., 2014. State of corporations: The rise of illegitimate power and the threat to democracy. *Transnational Institute and Occupy. com. State of Power*, *204*.

Gershgorn, D. & Rohlrich, J., 2018. These companies are pitching AI to the US military. *Quartz*. Available at: https://qz.com/1461910/these-companies-are-pitching-ai-to-the-us-military/ [Accessed March 06, 2021].

Goodfellow, I., McDaniel, P. & Papernot, N., 2018. Making machine learning robust against adversarial inputs. *Communications of the ACM*, *61*(7), pp.56-66.

Gray, A. et al., 1996. Dual Use Research project Report. *Potomac Institute for Policy Studies*. Available at: https://potomacinstitute.org/images/dualuse.pdf [Accessed April 11, 2021].

Green, B. & Hu, L., 2018, July. The myth in the methodology: Towards a recontextualization of fairness in machine learning. In *Proceedings of the machine learning: the debates workshop*.

Grewal, P., 2018. Suspending Cambridge Analytica and SCL Group From Facebook. *About Facebook*. Available at: https://about.fb.com/news/2018/03/suspending-cambridge-analytica/ [Accessed April 11, 2021].

Gronlund, K., 2019. State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons. *Future of Life Institute*. Available at: https://futureoflife.org/2019/05/09/state-of-ai/ [Accessed April 14, 2021].

Groumpos, P.P., 2019. Artificial Intelligence: Issues, Challenges, Opportunities and Threats. *Creativity in Intelligent Technologies and Data Science*, pp.19-33. Available at: http://link.springer.com/10.1007/978-3-030-29743-5_2 [Accessed March 06, 2021].

Haney, B.S., 2020. Applied Artificial Intelligence in Modern Warfare and National Security Policy. *Hastings Science and Technology Law Journal*, 11(1), pp.61-100.

Helm, T., 2019. Patient data from GP surgeries sold to US companies. *The Guardian*. Available at: https://www.theguardian.com/politics/2019/dec/07/nhs-medical-data-sales-american-pharma-lack-transparency [Accessed April 12, 2021].

Helm, T., 2020. Revealed: how drugs giants can access your health records. *The Guardian*. Available at: https://www.theguardian.com/technology/2020/feb/08/fears-over-sale-anonymous-nhs-patient-data [Accessed April 11, 2021].

Heskett, J., 2012. Are Factory Jobs Important to the Economy? *Harvard Business School*. Available at: https://hbswk.hbs.edu/item/are-factory-jobs-important-to-the-economy [Accessed March 06, 2021].

Horowitz, M.C., 2018. Artificial intelligence, international competition, and the balance of power (May 2018). *Texas national security review*.

Horowitz, M.C., Allen, G.C., Kania, E.B. & Scharre, P., 2018. *Strategic competition in an era of artificial intelligence*. Center for a New American Security..

Houde, S., Liao, V., Martino, J., Muller, M., Piorkowski, D., Richards, J., Weisz, J. & Zhang, Y., 2020. Business (mis) Use Cases of Generative AI. *arXiv preprint arXiv:2003.07679*.

How much does it cost to launch a reused Falcon 9? Elon Musk explains why reusability is worth it, 2020. *ElonX Net*. Available at: https://www.elonx.net/how-much-does-it-cost-to-launch-a-reused-falcon-9-elon-musk-explains-why-reusability-is-worth-it/ [Accessed May 1, 2021].

Charisi, V., Dennis, L., Fisher, M., Lieck, R., Matthias, A., Slavkovik, M., Sombetzki, J., Winfield, A.F. & Yampolskiy, R., 2017. Towards moral autonomous systems. *arXiv preprint arXiv:1703.04741*.

Charlton, A., 2019. Voice and sensors are key to today's smart home, but could biometrics replace them? *GearBrain*. Available at: https://www.gearbrain.com/smart-home-facial-recognition-2638892005.html [Accessed March 06, 2021].

Cheng, L., Varshney, K.R. & Liu, H., 2021. Socially Responsible AI Algorithms: Issues, Purposes, and Challenges. *arXiv preprint arXiv:2101.02032*.

Church, K.W., 2018. Emerging trends: Artificial Intelligence, China and my new job at Baidu. *Natural Language Engineering*, *24*(4), pp.641-647.

Iansiti, M. & Lakhani, K.R., 2020. Competing in the Age of AI. *Harvard Business Review*. Available at: https://hbr.org/2020/01/competing-in-the-age-of-ai [Accessed April 14, 2021].

Jagoda, N. & Birnbaum, E., 2019. Trump escalates fight over tax on tech giants. *The Hill*. Available at: https://thehill.com/policy/technology/472915-trump-escalates-fight-over-tax-on-tech-giants [Accessed May 4, 2021].

Jing, M., 2017. Baidu offers facial recognition technology to help Beijing airport streamline boarding, traffic. *South China Morning Post*. Available at: https://www.scmp.com/tech/china-tech/article/2108163/baidu-offers-facial-recognition-technology-help-beijing-airport [Accessed March 06, 2021].

Joh, E.E., 2017. Private Security Robots, Artificial Intelligence, and Deadly Force. *UCDL Rev.*, *51*, p.569.

Kania, E.B., 2018. New Frontiers of Chinese Defense Innovation: Artificial Intelligence and Quantum Technologies. *SITC Research Briefs*, (2018-12).

Kapfer, S., 2006. Multinational corporations and the erosion of state sovereignty. *Illinois State University*.

Kavanagh, C., 2019. *New tech, new threats, and new governance challenges: an opportunity to craft smarter responses?*. Carnegie Endowment for International Peace..

Kavlakoglu, E., 2020. AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference? *IBM Blog*. Available at: https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks [Accessed April 11, 2021].

Knibbs, K., 2017. The Questionable Benefits to Apple's Facial-Recognition Phone Unlocking. *The Ringer*. Available at:

https://www.theringer.com/tech/2017/9/12/16293096/apple-iphone-x-facial-recognition-unlocking [Accessed April 11, 2021].

Kobrin, S.J., 2009. Private political authority and public responsibility: Transnational politics, transnational firms, and human rights. *Business Ethics Quarterly*, pp.349-374.

Kozyulin, V., 2019. *Militarization of AI.* Russian Center for Policy Research.

Landi, H., 2020. Investors poured $4B into healthcare AI startups in 2019. *Fierce Healthcare*. Available at: https://www.fiercehealthcare.com/tech/investors-poured-4b-into-healthcare-ai-startups-2019 [Accessed March 06, 2021].

LeCun, Y., Bengio, Y. & Hinton, G., 2015. Deep learning. *Nature*, 521(7553), pp.436-444. Available at: http://www.nature.com/articles/nature14539 [Accessed March 06, 2021].

Lecher, C., FTC officially rules that Cambridge Analytica deceived Facebook users. *The Verge*. Available at: https://www.theverge.com/2019/12/6/20999078/ftc-cambridge-analytica-facebook-users-official-ruling-privacy-scandal [Accessed April 11, 2021].

Lempert, R., 2019. Bezos World Or Levelers: Can We Choose Our Scenario?.

Lim, T.W., 2019. North Korea's Artificial Intelligence (A.I.) Program. *North Korean Review*, 15(2), p.97. Available at: https://www.jstor.org/stable/26915828?seq=1 [Accessed March 06, 2021].

Lin, P. & Allhoff, F., 2019. Arctic 2.0: How Artificial Intelligence Can Help Develop a Frontier. , 33(02), pp.193-205. Available at: https://www.cambridge.org/core/product/identifier/S0892679419000108/type/journal_article [Accessed March 06, 2021].

Liu, S., 2020a. Artificial Intelligence funding United States 2011-2019. *Statista*. Available at: https://www.statista.com/statistics/672712/ai-funding-united-states/ [Accessed March 06, 2021].

Liu, S., 2020b. Facial recognition market size worldwide in 2019 and 2024. *Statista*. Available at: https://www.statista.com/statistics/1153970/worldwide-facial-recognition-revenue/ [Accessed April 11, 2021].

Lohn, A., Parasiliti, A. & Welser IV, W., 2016. Should We Fear an AI Arms Race? *Defense One*. Available at: https://www.defenseone.com/ideas/2016/02/should-we-fear-ai-arms-race/125670/ [Accessed March 06, 2021].

Losse, K., 2018. I was Zuckerberg's speechwriter. "Companies over countries" was his early motto. *Vox*. Available at: https://www.vox.com/first-person/2018/4/11/17221344/mark-zuckerberg-facebook-cambridge-analytica [Accessed April 11, 2021].

Ma, A. & Gilbert, B., 2019. Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened up until now. *Business Insider*. Available at: https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-

firm-that-harvested-50-million-facebook-profiles-2018-3#what-did-cambridge-analytica-do-1 [Accessed April 11, 2021].

Marchant, G., 2019. “Soft Law” Governance of Artificial Intelligence.

Martin, M., 2018. Founded When? America's Oldest Companies. *Business News Daily*. Available at: https://www.businessnewsdaily.com/8122-oldest-companies-in-america.html [Accessed March 06, 2021].

Maucione, S., 2020. DoD’s AI center setting itself up to be a more agile buyer, use of OTAs. *Federal News Network*. Available at: https://federalnewsnetwork.com/defense-main/2020/09/dods-ai-center-setting-itself-up-to-be-a-more-agile-buyer-use-of-otas/ [Accessed March 06, 2021].

Meadway, J., 2019. NHS data is a goldmine. It must be saved from big tech. *The Guardian*. Available at: https://www.theguardian.com/commentisfree/2019/dec/09/nhs-data-goldmine-value-private-companies [Accessed April 12, 2021].

Metz, C., 2017. Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent. *The New York Times*. Available at: https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html [Accessed March 06, 2021].

Metz, C., 2018. As China Marches Forward on A.I., the White House Is Silent. *The New York Times*. Available at: https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html [Accessed March 06, 2021].

Microsoft Corporation Form 10-K. In *United States Securities and Exchange Commission*. Washington 2020. Available at: https://microsoft.gcs-web.com/static-files/4e7064ed-bbf7-4140-a8cb-79aba77421b9 [Accessed May 3, 2021].

Morrison, S., 2021. Google is done with cookies, but that doesn’t mean it’s done tracking you. *Vox*. Available at: https://www.vox.com/recode/2021/3/3/22311460/google-cookie-ban-search-ads-tracking [Accessed April 11, 2021].

Moulson, G., 2019. Tesla to build factory in Germany after subsidies announced. *AP News*. Available at: https://apnews.com/article/c9fe791cacbf405cbb9c88e1bd52ae9f [Accessed March 06, 2021].

Nellis, S. & Jin, H., 2021. Samsung considers Austin for $17 billion chip plant, eyes tax breaks of at least $806 million - documents. *Reuters*. Available at: https://www.reuters.com/article/us-usa-semiconductors-samsung-elec/samsung-considers-austin-for-17-billion-chip-plant-documents-idUKKBN2A433B [Accessed March 06, 2021].

Nikolic, I., 2020. UK Government sells millions of NHS patients’ medical data to US drugs giants after wrongly stating it would be ‘anonymous’, experts claim. *Daily Mail*.

O'Carroll, B., 2017. What are the 3 types of AI? A guide to narrow, general, and super artificial intelligence. *CodeBots*. Available at: https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible [Accessed April 11, 2021].

Olson, S., 2020. Are Private Chinese Companies Really Private? *The Diplomat*. Available at: https://thediplomat.com/2020/09/are-private-chinese-companies-really-private/ [Accessed March 06, 2021].

Osoba, O.A., & Wesler IV, W., 2017. The Risks of Artificial Intelligence to Security and the Future of Work. *RAND Corporation*. Available at: https://www.rand.org/pubs/perspectives/PE237.html [Accessed April 11, 2021].

Pawlyk, O., 2018. China Leaving US Behind on Artificial Intelligence: Air Force General. *Military.com*. Available at: https://www.military.com/defensetech/2018/07/30/china-leaving-us-behind-artificial-intelligence-air-force-general.html [Accessed March 06, 2021].

Pohler, L. et al., 2018. A Technological Perspective on Misuse of Available AI. *Conscious Coders*. Available at: https://www.consciouscoders.io/wp-content/uploads/2018/08/A_Technological-Perspective_on_Misuse_of_Available_AI-1.pdf [Accessed March 06, 2021].

Poon, M., 2016. Corporate capitalism and the growing power of big data: Review essay. *Science, Technology, & Human Values*, *41*(6), pp.1088-1108.

'Power Africa' 2021, USAID. Available at: https://www.usaid.gov/powerafrica/privatesector [Accessed May 2, 2021].

Ramesh, R., 2014. NHS patient data to be made available for sale to drug and insurance firms. *The Guardian*. Available at: https://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy [Accessed April 12, 2021].

Reducing CO2 emissions from passenger cars - before 2020, European Commission. Available at: https://ec.europa.eu/clima/policies/transport/vehicles/cars_en.

Regalado, A., 2020. Hyper-personalized medicine. *MIT Technology Review*. Available at: https://www.technologyreview.com/technology/hyper-personalized-medicine/ [Accessed March 06, 2021].

Regulation (EU) 2019/452 of the European Parliament and of the Council establishing a framework for the screening of foreign direct investments into the Union, Brussels: Official Journal of the European Union.

Response to Guardian story "NHS patient data to be made available for sale". *NHS England*. Available at: https://www.england.nhs.uk/2014/01/guardian-story/ [Accessed April 12, 2021].

Rieke, N., 2019. What Is Federated Learning. *The NVIDIA Blog*. Available at: https://blogs.nvidia.com/blog/2019/10/13/what-is-federated-learning/ [Accessed April 11, 2021].

Roberts, C., 2016. Killer Robots: Moral Concerns Vs. Military Advantages. *The National Interest*. Available at: https://nationalinterest.org/blog/the-buzz/killer-robots-moral-concerns-vs-military-advantages-18277?nopaging=1 [Accessed March 06, 2021].

Roberts, P.S., 2019. AI for Peace. *War on the Rocks*. Available at: https://warontherocks.com/2019/12/ai-for-peace/ [Accessed March 06, 2021].

Sargent, J.F., 2020. Federal Research and Development (R&D) Funding: FY2020. In *Congressional Research Service*. Available at: https://fas.org/sgp/crs/misc/R45715.pdf [Accessed April 23, 2021].

Sayler, K.M., 2020. Artificial intelligence and national security. *Congressional research service report R45178*.

Shendruk, A., 2020. Amazon has become the world's fifth largest employer. *World Economic Forum*. Available at: https://www.weforum.org/agenda/2020/12/amazon-employers-online-retail-covid-pandemic-coronavirus [Accessed March 06, 2021].

Siddiqui, F., 2020. Teslas still go much farther on a single charge than their competitors. But the strategy carries risks. *The Washington Post*. Available at: washingtonpost.com/technology/2020/01/10/tesla-battery-range/ [Accessed March 06, 2021].

Simonite, T., 2020. Did a Person Write This Headline, or a Machine? *Wired*. Available at: https://www.wired.com/story/ai-text-generator-gpt-3-learning-language-fitfully/ [Accessed April 11, 2021].

Singh, T. & Gulhane, A., 2018. 8 Key Military Applications for Artificial Intelligence in 2018. *Market Research*. Available at: https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018 [Accessed April 11, 2021].

Slijper, F., Beck, A. & Kayser, D., 2019. State of AI. Available at: https://www.paxforpeace.nl/media/files/state-of-artificial-intelligence--pax-report.pdf [Accessed March 06, 2021].

Song, J., 2016. Before AlphaGo, there was North Korea's Eunbyul. *NK News*. Available at: https://www.nknews.org/2016/03/before-alphago-there-was-north-koreas-eunbyul/ [Accessed March 06, 2021].

Spelda, P. & Stritecky, V., 2020. The future of human-artificial intelligence nexus and its environmental costs. *Futures*, *117*, p.102531.

Statt, N., 2018. Google reportedly leaving Project Maven military AI program after 2019. *The Verge*. Available at: https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire [Accessed March 06, 2021].

Sylvester, J. & Raff, E., 2018. What about applied fairness?. *arXiv preprint arXiv:1806.05250*.

Taylor, T., 2019. Artificial Intelligence in Defence: When AI Meets Defence Acquisition Processes and Behaviours. *RUSI Journal*, 164(5-6), pp.72 - 81.

Tech Nation Report 2020. Available at: https://technation.io/report2020/ [Accessed March 06, 2021].

The Cambridge Analytica Story, Explained. *Wired*. Available at: https://www.wired.com/amp-stories/cambridge-analytica-explainer/ [Accessed April 11, 2021].

'The digital guru who helped Donald Trump to the presidency' 2017, BBC, television interview, BBC London.

The Google DeepMind challenge match. *DeepMind*. Available at: https://deepmind.com/alphago-korea [Accessed March 06, 2021]

The world's 30 biggest employers. *Love Money*. Available at: https://www.lovemoney.com/gallerylist/67573/the-worlds-30-biggest-employers [Accessed March 06, 2021].

Thomas, M., 2020. How AI Trading Technology is Making Stock Market Investors Smarter. *BuiltIn*. Available at: https://builtin.com/artificial-intelligence/ai-trading-stock-market-tech [Accessed April 11, 2021].

Tripathi, S. & Gündüz, C., 2008. A role for the private sector in peace processes? Examples, and implications for third-party mediation. *Centre for Humanitarian Dialogue*. Available at: https://www.files.ethz.ch/isn/90802/Private_Sector_Peace_06_08.pdf [Accessed March 06, 2021].

Vailshery, L.S., 2021. Unmanned aircraft systems (UAS)/drones registered in the United States as of March 2021. In Statista. Available at: https://www.statista.com/statistics/1221517/uas-drone-registrations-united-states/#:~:text=The%20number%20of%20drones%20in,stand%20at%20around%20372%20thousand. [Accessed May 2, 2021].

Vincent, J., 2017. Putin says the nation that leads in AI 'will be the ruler of the world'. *The Verge*. Available at: https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world [Accessed March 06, 2021].

Wakabayashi, D. & Shane, S., 2018. Google Will Not Renew Pentagon Contract That Upset Employees. *The New York Times*. Available at: https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html [Accessed March 06, 2021].

Waldrop, M.M., 2019. News Feature: What are the limits of deep learning?. *Proceedings of the National Academy of Sciences*, *116*(4), pp.1074-1077.

Watson, A., 2021. Main source of information about news and current affairs in selected countries worldwide as of June 2020. *Statista*. Available at: https://www.statista.com/statistics/198765/main-source-of-international-news-in-selected-countries/ [Accessed April 11, 2021].

Weber, M., 1918. *Politics as Vocation.* Munich University.

Weis, B., 2018. Trump-linked firm Cambridge Analytica collected personal information from 50 million Facebook users without permission. *Business Insider*. Available at:

https://www.businessinsider.com/cambridge-analytica-trump-firm-facebook-data-50-million-users-2018-3 [Accessed April 11, 2021].

Welcome To The Future With Jay Allen: Hyper-Personalized Medicine, 2020, *Mornings with Rebecca & Burns*, 90.9 KCBI FM

What Are Neural Networks. *IBM Cloud Education (a)*. Available at: https://www.ibm.com/cloud/learn/neural-networks [Accessed April 11, 2021].

What Is Deep Learning. *IBM Cloud Education (b)*. Available at: https://www.ibm.com/cloud/learn/deep-learning [Accessed April 11, 2021].

What Is Machine Learning. *IBM Cloud Education (c)*. Available at: https://www.ibm.com/cloud/learn/machine-learning#toc-what-is-ma-qhM6PX35 [Accessed April 11, 2021].

What Is Artificial Intelligence. *IBM Cloud Education* (*d*). Available at: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence [Accessed April 11, 2021].

What is WannaCry ransomware? *Kaspersky*. Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry [Accessed April 11, 2021].

White Paper: On Artificial Intelligence - A European approach to excellence and trust, Brussels: European Commission. Available at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

Wiseman, P., 2021. Biden's corporate tax plan takes aim at income inequality. *AP News*. Available at: https://apnews.com/article/personal-taxes-government-and-politics-business-dcd7a48bcf82a8d5a734d9ea7a7dc4c4 [Accessed May 4, 2021].

Wulf, H., 2011. The privatization of violence: a challenge to state-building and the monopoly on force. *The Brown Journal of World Affairs*, *18*(1), pp.137-149.

Xie, M., 2018. The Future Of Biometric Facial Recognition. *Forbes*. Available at: https://www.forbes.com/sites/forbestechcouncil/2018/09/19/the-future-of-biometric-facial-recognition/?sh=4991f01e3c74 [Accessed April 11, 2021].

Yadav, R., 2019. Top 7 Artificial Intelligence Breakthroughs We Saw In 2019. *Analytics India Magazine*. Available at: https://analyticsindiamag.com/top-7-artificial-intelligence-breakthroughs-we-saw-in-2019/ [Accessed March 06, 2021].

Yu, R. & Alì, G.S., 2019. What's inside the Black Box? AI Challenges for Lawyers and Researchers. *Legal Information Management*, *19*(1), pp.2-13.

Zwetsloot, R. & Dafoe, A., 2019. Thinking About Risks From AI: Accidents, Misuse and Structure. *Lawfare*. Available at: https://www.lawfareblog.com/thinking-about-risks-ai-accidents-misuse-and-structure [Accessed March 06, 2021].

List of Appendices

Appendix no. 1: Research & Development spending of selected institutions

Source: Annual reports (listed in references), own calculations

R&D expenses (*in millions USD*)	**2018**	**2019**	**2020**	**CAGR 18-20 (%)**	**% of revenue (2020)**
Department of Defense	52 386	55 832	59 463	6,5 %	n.a.
NASA	11 755	n.a.	11 280	-2,0 %	n.a.
STATE ENTITIES	**64 141**	n.a.	**70 743**	**5,0 %**	
Alphabet (Google)	21 419	26 018	27 573	13,5 %	16,1 %
Apple	14 236	16 217	18 752	14,8 %	7,0 %
Facebook	10 273	13 600	18 447	34,0 %	21,0 %
Microsoft	14 726	16 876	19 269	14,4 %	13,0 %
PRIVATE ENTITIES	**60 654**	**72 711**	**84 041**	**17,7 %**	

Appendix no. 2: List of institutions and companies contacted with request for an interview

Advisory Council on AI, Canada	Huawei
AirBrain	IBM
Apple	IMDA Singapore
Armorblox	Imperial College London
Banjo	Intel
Berkeley University	Lilt
BIS (Security Information Service)	Microsoft
Caltech University	MIT
Cambricon	NATO
Cambridge University	NUKIB (National Cyber and Information Security Agency)
Carnegie Mellon University	NVIDIA
CIIRC (Czech Institute of Informatics, Robotics and Cybernetics)	Office for Artificial Intelligence, UK
CloudMinds	OpenAI
CloudWalk	Oxford University
Cornell University	Royal Institute of Technology, Sweden
Czech Technical University	Sense Time
Deep 6	Stanford University
Deep Mind	Technical University Munich
DJI	Tesla
European Committee	Ubtech Robotics
Facebook	UNICRI (Centre for AI and Robotics)
Faculty of Mathematics and Physics, UK	University of Birmingham
Good AI	UZSI (Office for Foreign Relations and Information)
Google	Yale University
Harvard University	ZTE

Appendix no. 3: List of questions for interviews

- What do you understand as "Artificial Intelligence"?
- Do you consider AI to be a dual-use technology?
- Is there a visible difference between the AI development of states and of AI developed by private actors? Focusing on the pace of development, the volume of investments, number of patents, etc.
- Do you know of any examples, when was the AI or AI-enabled technology used against a state? If so, could you please provide more details?
- Do you consider the AI to have any advantages when used against the state by a private sector?
- Is there, now, any reason to be afraid that private companies may use the AI or AI-empowered technology against a state?
- Do you believe private actors may have any benefits from such actions as using the AI against a state?
- Do you believe this situation might change over the following years?
- What steps may state (individually or collectively – EU, NATO, etc.) do to limit the potential threat?