# The Ethics of Early Crisis Detection - Big Data, AI, and Algorithms in the German Military

Lea Buchhorn,
lbuch@protonmail.com

**Abstract.** Technological developments have and will continue to influence our everyday lives. One of them, AI, promises many benefits in various fields, such as medicine, agriculture, or the military. On the other hand, AI advancement encompasses multifaceted risks and challenges, such as data privacy concerns, opaque decision-making, or discrimination against groups or individuals. AI and Big Data have gained more and more importance in military operations all over the globe. The German military has been trailing different approaches to AI-based early crisis detection applications. However, the more insights are gained about AI and the harm human errors in designing algorithms can cause, the more ethical concerns arise. Thus, this paper investigates which ethical challenges the German military is facing while testing and trying to implement AI-based early crisis detection systems.

**Keywords:** AI ethics, early crisis detection, data ethics, data ethics,



## 1 Introduction

Technological developments have and will continue to influence our everyday lives. One of them, AI, promises many benefits in various fields. AI can support in making medical diagnoses more precise, increasing farming efficiency, or improving the security of citizens (European Commission, 2020). At the same time, AI advancement encompasses multifaceted risks and challenges, such as data privacy concerns, opaque decision-making, or discrimination against groups or individuals [1].

It remains highly difficult to predict the reach and impact new technologies have on society, politics, and security [2]. AI-based systems are increasingly becoming part of our everyday lives, chatbots answer questions on websites, Instagram algorithms show us posts of people we interact with most first, but these systems also change the way militaries across the world are operating. AI and Big Data have gained more and more importance in Military and Defense policies and operations all over the globe, as well as in Germany [3]. Weapon and defense systems have become increasingly complex with the advancing digitalization of the industry. However, governments take quite different stances on how to properly legislate and approach AI utilization in a military context. Germany made it clear that autonomous weapon systems should be pre-emptively banned [5] but utilizing Big Data and AI for predictive purposes such as early crisis detection is a path Germany wants to take.

As our world becomes more and more interconnected, national destabilization due to crisis and war on the other side of the globe can often be felt all over the world [5]. Therefore, the German federal government adopted guiding principles on how to respond to crises and armed conflicts

which are summarized under the theme of "*crisis prevention, conflict resolution, peace promotion"* in 2017. These goals are to be reached with the utilization of AI, big data, and clear guidelines on the ethical use of this data. In the past years, the German military has been trailing and developing different approaches to software- and AI-based early crisis detection applications. These systems are to support the German military in preventing wars, supporting those in need quicker, and stabilizing governments. Many countries, such as the US, have tried or are currently introducing early crisis detection systems that could support and improve early responses. Nevertheless, potential pitfalls around the topic fuel the debate in Germany. Crises often develop due to extremely rapid and often unstructured outbreaks of violent conflicts, the sudden deaths of crucial leaders, and other countless human variables must be considered [6]. This makes it difficult to design algorithms that can account for those quickly changing situations.

Ethical concerns regarding the employment of AI-based early crisis detection systems are also becoming louder. Questions regarding privacy, biased data, unfair outcomes due to discrimination, but also misuse of these technologies will need to be addressed before the systems can be employed. Researchers from Oxford University, such as Floridi, Taddeo, Mittelstadt, Wachter, or Allo have become a leading figure in the quest for data ethics and ethical use of technologies [7] [8]. According to Floridi and Taddeo, data ethics can be seen as an 'evolution' from the information-centric approach to a more abstract data-centric approach of defining ethics [7]. Mittelstadt et al., [8] explore the distinct lines of research in data ethics divided into 'ethics of data', 'ethics of algorithms' and 'ethics of practices'. These research streams are intertwined as all mentioned lines will need to be considered since ethical issues that can arise out of either one of them [7].

Since the ethics of AI in early crisis detection in the German context is a under researched topic, the purpose of this paper is to unravel some of these intertwined lines of research and thus unravel the ethical challenges Germany and its military is facing while aiming for the utilization of AI and big data in their early crisis detection missions. The ethical challenges are manifold and current research might just scratch the surface. The more insights are gained about AI and what harm human errors in designing algorithms can cause, the more ethical concerns arise. Therefore, this paper aims to answer the questions: *which ethical challenges the German military is facing while testing and trying to implement AI-based early crisis detection systems?* First, important terms and concepts will be defined, and the conceptual foundation of the ethics debate in AI will be mapped. A special emphasis will be placed on ethics of data, algorithms, and practices, by Mittelstadt et al. [8] combined with Floridi and Taddeo's research [7]. As this will be the umbrella under which AI supported early crisis detection will be investigated. This section is followed by a thorough literature review to assess the current core trends. Afterward, some technological approaches will be explained in the context of early crisis detection and how the German military is testing its usefulness. Further, the ethical challenges which this process poses will be analyzed by applying the conceptual framework to the case of Germany. Lastly, the conclusion will summarize the main findings and give a possible outlook into the future.



## 2 Literature Review and Conceptual Framework

### 2.1 Big Data, AI, and Algorithms

Both concepts, Big Data and AI do not have a commonly agreed-upon definition. Big Data can be considered as an overarching term for large and complex data sets that are derived from one or multiple sources. Processing these datasets requires the support of new technologies as they are too large to be processed through traditional systems [9], [10]. Thus, bluntly put, big data is concerned with all data sets that conventional technology cannot save, analyze, search, distribute, or visualize as they are too large [11].

For example, De Spiegeleire, Maas, and Sweijs [12] define *AI* as "*the study of the computations that make it possible to perceive, reason and act, or the automation of intelligent behavior, which is driven by a general study of intelligent agents both biological and artificial*." (p. 27). More concretely, however, AI can replicate human mental skills, such as adaptive learning from experience, strategizing, or pattern recognition [12]. Furthermore, AI is characterized by being an intelligent agent that can "act upon a task, determine the level of success at completion, learn from that experience and alter future behavior to improve future performance on the task" [13, p.1].

*Algorithms* are simply put a set of instructions that 'tell' the AI how to make decisions, on what to base decisions, and trains its intelligence. Hill in Mittelstadt et al. [8] define algorithms as mathematical constructs that take action and have effects when they are implemented (p. 2). According to Emad, the key difference between an algorithm and AI is that the "algorithm(s) define the process through which a decision is made" [14, Slide 18]. AI, on the other hand, uses training data to learn how to make such decisions and to establish patterns and draw conclusions from them [14], [12]. An algorithm works by processing a given input, either under supervision or by making sense of it by itself, and then producing output. If it is the case that the algorithm can make sense of the data itself, this means that it is 'equipped' with learning capabilities. Thus, the AI can make sense of the gathered data on its own and provide recommendations based on its analysis, and if desired, induce actions [15].

Through the combination of big data, AI, and algorithms it becomes possible to jump on the bandwagon of other technologies developments that have been designed for different purposes [14], [12]. For example, data and algorithms that have been mined and developed for traffic divergence purposes could prove equally suitable for military and defense purposes.

### 4th Industrial Revolution

The 4th industrial revolution has first been coined in by Klaus Schwab the founder of the World Economic Forum. The phrase frames the impact emerging technologies, such as AI have on social norms, national political attitudes, economic development or international relations [16] [17]. Luciano Floridi, the Director of the Digital Ethics Lab at the Oxford Internet Institute describes the concept of the fourth revolution from a philosophical and ethical standpoint [18]. This revolution is based on seeing the world as a network and places great emphasis on connections, relationships, and links between the data nodes [18]. Furthermore, Floridi [18] distinguishes between two groups of ethical concerns that must be considered during this fourth industrial revolution.

The first group has been part of debates for some time now: privacy, data, and the right to be forgotten. These issues have entered mainstream discussions already. The second group, which has been less visible and is also considered to be more long-term, is our interaction with technology [16]. Therefore, the crucial question that arises is how technological developments will be influencing us and our interactions over time. The big risk which arises is that we, as humans, will be adapting to the technologies rather than the other way around [16], i.e., that we will make decisions influenced by the technological environment we find ourselves in. This can range from basic advertisements we see while online shopping to deciding to intervene in a crisis region.

**Data Ethics**

Floridi and Taddeo, being pioneer thinkers in the field of data ethics, published a paper [7] on what data ethics is, and how it impacts data science. Data ethics does not only consider computer and information ethics but shifts towards a more abstract level to being *data-centric* [7]. This shift emphasizes the complexities and different moral dimensions by shedding light on the interactions among hardware, software, and data [7, p.1]. This aspect connects with what Floridi [18] considers to be the crucial part of moving towards a fourth industrial revolution, nodes, networks, and relationships which affect data use. Here, Floridi considers nodes as 'persons' that are dependent on links between the nodes, meaning the link between them is the crucial part of "what makes them what they are" [18].

The hardware does not cause ethical issues but the relationship between the hardware and software and the data which poses new difficulties [7, p. 3]. The increasing use of algorithms and AI and their potential interconnectedness pose many new ethical challenges. Especially ethical issues by algorithmic decision-making are fueling the academic debate. According to Mittelstadt et al. [8], the key to keeping AI and algorithms ethical is for them to be transparent. However, this is highly challenging considering the elaborative analysis and decision-making process of algorithms and AI [8]. Transparency can range from people being aware that they are communicating with a chatbot and not an actual human being to providing open-source tools gain insights about where the data comes from and how it is being analyzed or processed [18], [20]. Operations, choices, and decision-making that previously have been performed by humans are increasingly assigned to be executed by algorithms. Mittelstadt et al., [8] and Floridi and Taddeo [7] share the understanding that there is a shift from the *information-centered ethics* approach towards a *data-centric* approach. This means that moral problems related to data, algorithms, and practices need to be studied to formulate and support morally good solutions [7, p.1], [8, p. 6].

Algorithms that are employed to execute classification tasks usually hold two components: a ‘learner’ which in turn produces a ‘classifier’ [8, p. 3]. This process is intended to produce classifications so that the AI can generalize from the data it is being fed. The algorithm places new input into the ‘classifier’ to learn from it and to determine how this input may be classified and what should be done with this information [8]. This suggests that the learning capabilities provide the algorithm with some autonomy. From this follows the difficulty to predict the AI’s recommendations, which poses new ethical challenges. Mittelstadt et al. [8] find six types of ethical concerns raised by algorithms and divide them into *Epistemic concerns*, which are

drawing from the algorithms' evidence; *Normative concerns* which are related to outcomes; and lastly the algorithms' *traceability*.

Ethical problems can arise from *how* data is collected and analyzed. Data can be highly sensitive as assumptions about individuals can be made through connecting data points, meaning it is possible to re-identify people through data mining, - linking, and -merging [7]. This can cause privacy issues. However, in a military and intelligence context this is also a great opportunity to identify key figures in emerging crises. Nevertheless, through the re-identification process certain groups (based on age, gender, ethnic background) to become more transparent [21]. From this, group discrimination can arise [7]. Furthermore, the way of data acquisition is important to consider. How did the actors gain access to the data and who else might be able to access it? According to Hasselbalch, Kofod Olsen, and Tranenberg [22] the rationale that holds, is that every individual should be in control of their data.

Mittelstadt et al., [8], Hasselbalch, Kofod Olsen, and Tranberg [22], and Floridi and Taddeo [7] all place great value on transparency of data to keep it ethical. The purpose and outcomes of data processing must be clear and transparent to trace the process and account for any decisions taken [22]. Overall, transparency is crucial for ethical 'control' in AI data use, which is highly difficult to achieve in a military context where sensitive data is handled.



**Ethics of Algorithms**

The increasing complexity and autonomy of algorithms can cause ethical issues as well. Ethics of algorithms is a concept that is thoroughly discussed by Mittelstadt et al. [8]. The increasing reliance on learning capabilities of algorithms can prove to be problematic and is described as transformative effects by Mittelstadt et al. [8]. Transformative effects emerge from ethical failures stemming from the reliance on (semi-)autonomous decision-making AI. This can also occur even if the algorithm was not designed to purposefully inflict harm.

As aforementioned, Mittelstadt et al. [8] define six ethical concerns stemming from the use of algorithms. Epistemic concerns point to the algorithms' evidence, meaning that evidence can be inconclusive, inscrutable, or misguided. *Inconclusive evidence* can emerge when algorithms draw conclusions from data and produce uncertain knowledge through machine learning techniques or inferential statistics [8]. *Inscrutable evidence* arises from a lack of knowledge about the utilized data but also relates to the difficulty of the interpretation of how many data points are being utilized by the algorithm to provide the conclusions it draws [8]. As algorithms process data they are directly subject to data processing limitations. What they produce as the 'outcome' to classify, make recommendations, or make decisions, can never exceed the input that they have been provided in the first place. This limitation is linked to the concept of *misguided evidence* [8].

The normative concerns Mittelstadt et al. [8] mention are to unfair outcomes and transformative effects. *Transformative effects* emerge from ethical failures coming from the reliance on (semi-) autonomous decision-making AI. This does not necessarily mean that the algorithm was meant to cause harm, but it can alter how people conceptualize the world. Therefore, ethical considerations, especially in a military context are crucial. Evaluating algorithms ethically can also be focused on the action executed by them. Those actions can be discriminatory and have unfair outcomes even if they are based on well-founded and conclusive evidence [8]. Lastly, the traceability of algorithms must be considered. This concept leads back to the design and

availability of new technologies and how these can manipulate large sets of personal and other data [8]. When harm is caused by an algorithm it usually is very difficult to find the cause and debug it and further. Thus, tracing the error. Another point of concern arises here, accountability, who will and can be held responsible for harm caused by an AI.

**Ethics of Practices**

The people and organizations processing data and developing strategies and policies can pose ethical issues. Thus, raising the question of accountability and liability [7]. The goal is to define an ethical framework in which ethical practices foster progress in data science, but also protect the rights of groups and individuals. It is crucial to create an environment that shapes professional codes on how to be responsible and innovative at the same time [7]. Only when such an environment is creates, guidelines on responsibilities, liabilities, and accountability can be addressed. Organizations and people authoritative for developing strategies, policies, and processes can then be guided by the principles and analyze their performances in line with the central points of consent, user privacy, and secondary use [7].



## 3 Software-Based Early Crisis Detection in the German Military

The process of early crisis detection describes the early identification of political, economic, and social developments that have the potential of turning into conflicts, in societies or countries [5, p. 110]. Making use of early crisis detection provides other countries, but also the affected states, with the opportunity to act accordingly by, for example, de-escalating through peacekeeping missions or mediation. Furthermore, early detection allows accounting for avoidable political 'surprises' to be mitigated and reduced [5]. Early crisis detection is a crucial part of Germany's guiding principles to "*crisis prevention, conflict resolution, peace promotion*" and to what the federal government calls Germany's "ethical obligation" towards the world [5, p. 11]. Therefore, Germany plans to further invest in its early crisis detection program by utilizing current AI and big data developments [6], [23], [24]. This is part of the so-called "digital initiative" [24] of the German military.

The goal of the program is to collectively (together with other EU member states) stand against conflicts and Germany, being a credible leader and having influence in the international political environment, plays a crucial part in this effort [5]. Using advancing technologies by applying AI-based systems can support these efforts. AI systems can aid in unraveling patterns that help to identify emerging crises. In those situations, purposive actions taken by Germany can help to sustainably de-escalate intra- or inter-state altercations or identify critical developments in an early stage [12]. The programs are intended to detect crisis developments up to 18 months in advance by gathering data on new developments and reading data from various databases and sources [6]. Since 2014, the German military already uses software systems called 'Textrapic' and 'Brandwatch' to monitor social media channels to analyze the general mood and opinion of societies [19].

Germany has been researching and exploring various software-based instruments to support its early crisis detection efforts [18]. Programs such as IBM Watson analyze big data and use AI to allow the user to "predict and shape future outcomes" and "automate complex processes" [25]. Watson is a self-learning AI that first was built as a high-performance search engine [6]

and has since been applied in medical diagnosis [20]. This shows how versatile AI has become and it can be adapted to new learning environments. Until mid-2019, IBM Watson has been in a trailing phase in the German military [19], [6]. IBM Watson was built to identify patterns in large data sets and is supposed to detect tendencies of emerging crises that are relevant for Germany in the time frame of six to 18 months [26], [11].

Watson evaluates data from various sources and databases such as the Armed Conflict Location and Event Data Project (ACLED) which has been collecting real-time data from key actors and the number of victims in Africa since the late 1990s [6]. Furthermore, the Global Terrorist Database and the Global Database of Events, Language, and Tone are being monitored as well [19]. Based on this data, developments can be calculated and help predict escalations in similar settings. Not only IBM Watson is being trialed and considered to be beneficial for early crisis detection. The software company SAP also supports the German military by assessing possible equipment and supply bottlenecks [11]. SAP "Analytics" is being tested for predictive maintenance [11] and SAP "Hana" is supposed to process and analyze open data from the world wide web [19]. SAP Hana works with a 'predictive analytics library' which is expected to give insights into economic areas [19]. However, a clear-cut decision on which IT systems will be implemented has not been taken yet.

Naturally, critique is voiced as well. Critics are concerned that extremely rapid and often unstructured outbreaks of violent conflicts, the sudden deaths of crucial leaders, and the countless human variables are impossible to predict [6]. Various ethical concerns are raised as to how data is being acquired, how is it analyzed, and whether there will be an open-source option included for transparency [6]. Another considerable critique that is regularly voiced is the extreme budget this program devours. Around three to four million euros are estimated to be spent annually in the next 15 years on software-based early crisis detection [6]. Worrying here is also a lack of expertise in military staff [23]. Here, correctly gathering data is one obstacle, but handling the AI properly is another. Currently, the German military is lacking appropriately trained and educated IT, staff, at a scale that would be needed to properly handle such advanced AI programs. At present, the analysis task is handled by Deloitte Consultants, but the Center for Intelligence and Security Studies at the German Military University in Munich will have the task of retraining and educating military officers [6].



## 4 Putting the pieces together

In September 1961, the former German chancellor Willy Brandt addressed the UN with his famous words "*Peace is not everything, but without peace, everything is nothing.*" Since then, Germany has made it one of their main priorities to support the United Nations and other allies with peace-keeping missions. As a part of this, early crisis detection has become crucial to fulfilling this goal. However, with the advancement of technologies, Germany also needs to adjust its military operations. In the course of a digital initiative of the German Ministry of Defense, the government, and the military are considering various IT-based systems [24]. Nonetheless, most of these systems have been around for a long time already, such as IBM Watson which has been introduced as a high-performing search engine, in 2010 [11]. According to the federal budget plan [27, p. 60–64], around 1,04% of the defense budget is aimed to be invested in the 'innovative application of AI'. However, this budget needs to be distributed

between all AI initiatives and not only be spend on early crisis detection. Considering that AI ethics is still a rather niche concern in the military context, the limited budget and attention received, it appears unlikely that ethical research initiatives will receive funding soon.

The German military budget has been shrinking since the 1990s. The German military does not only need to uphold ethical standards in their daily routines and deployments, but also the increasingly more important digital space. Transparency considerations, a core component in keeping AI and algorithms ethical, suggest that it should be comprehensible where the gathered data is coming from. The answer of the Bundesregierung [11] to the question of what kind of data will be processed remains rather untransparent as it states that they will access information from "unstructured and structured data from open but also from classified sources" (p. 10). However, they are being more transparent when it comes to disclosing databases that have been attached to the event databases that will be utilized to gather appropriate data and how the sources will be evaluated. The Armed Conflict Location & Event Data, Global Database of Events, Language and Tone, and the Global Terrorism Database have been attached and are continuously validated by the University of the German Military in Munich but also other data from sources that cannot be disclosed will be used [11, p. 10].

Naturally, in a national security domain, full transparency is impossible to achieve and also not desirable. Much of the data is classified and cannot be shared as then also enemies could access it [28]. However, there needs to be a middle ground where clear guidelines can be shared on how data is gathered, what is considered crucial, and what actions were taken based on the analysis. The issues that arise with the use of classified and red data, (data that cannot be collected through openly accessible databases) [6], cannot be left unmentioned. Especially red data makes a hard case against transparency. Nevertheless, EU and national values must also be upheld when utilizing AI. The first steps are being taken with peace ethics workshops for the military in which 'ethics and digitalization and AI' are being addressed [29].

Another issue that ties in here, is that the German military is still developing guidelines on how to use data ethically and not infringe on any privacy laws [30], [31]. Here the concept of transformative effects comes into play. Clear guidelines need to be developed to assure that the algorithm of Watson does not exclude data or triggers inappropriate actions by its analysis [8]. The Bundesregierung [30] states that early crisis detection specialized staff will develop a response. However, this is where some members of the Bundestag fear misuse of technology that cannot be monitored without clear guidelines [23]. The quality of the gathered data is often unclear as well as how the algorithms weigh the individual pieces of data. Therefore, it is crucial to develop guidelines that keep the technology and staff in check to avoid misuse. The new technology could be turned into a surveillance tool that could potentially be misused in accessing online communications or even be used to repel refugees when it falls into the wrong hands [23].



**Algorithms**

The output that algorithms, such as Watson, generate is derived from inferential statistics and/or machine learning techniques [8]. This means that the conclusions being drawn from the output are probable but also uncertain since (important) information can still be missed if it does not fit into the algorithm's computation. This potential bottleneck is defined by Mittelstadt et al, [8] as inconclusive evidence. Especially in the context of the military's use of AI early crisis

detection, ethical issues can arise by potentially missing events that might not be included in the algorithm. Specifically, in early crisis detection sudden events such as the death of a key actor can play a crucial role and change the dynamics quickly. If the algorithm misses an event or does not weigh it appropriately, as it has not been programmed to do so, it might suggest an incorrect response. Here the question of ethical responsibility and accountability becomes pressing.

The German military [11] states there will always be a human component at the end of the decision-making chain, who will make the final decision to either act or not to. However, in the case of inconclusive evidence, it could happen that something might not be flagged, leading the staff to not even reviewing it and trusting the AI. Therefore, the ethics of AI construction and ethics of AI use are crucial to handling AI and algorithms ethically and transparently. By making sense of information by itself through learning capabilities, the algorithm can provide recommendations. This suggests that the learning capabilities provide the algorithm with some degree of autonomy, which makes it difficult to predict the AI recommendations. Furthermore, this also complicates the traceability and transparency of the automated decision-making process that leads to the recommendations. This, in turn, makes ethical design and use crucial so that it is possible to account for the output generated through the algorithms learning capabilities [19], [20].

Nevertheless, the impact of this autonomy remains uncertain to some. As a result, tasks performed by machine learning are difficult to predict. On the one hand, the data used by these prediction systems is gathered from worldwide databases and building models [6]. On the other hand, a great obstacle for early crisis detection is the inaccessibility of so-called *red data*. This can lead to a situation where all openly accessible data points to "no emerging crisis" in a scenario but one secret source reports that they hold governmental intelligence about a planned strike that will cause a crisis [6]. This unbalanced information input can cause issues in generating balanced outcomes. Thus, the AI might not know that the one secret source should be weighed much higher than the other openly accessible sources and the generated outcome will not reflect reality.



### The 4th Industrial Revolution in the Military Context

According to Floridi's [18] understanding, the 4th industrial revolution focuses on the interaction between people and technology. Not only can technologies steer us into directions to buy something or to behave in a certain way, but they can also influence us to such an extent that people will behave differently around certain technologies. For example, while driving one can use apps to detect where there are speed cameras are, or sometimes people know their locations from experience. At those locations, people will adhere to the speed limit to avoid being fined. The same logic holds for more profound topics such as early crisis detection. There will be a very thin line to walk to use the AI systems for crisis prevention and not let them turn into a surveillance machine.

Andrej Hunko, a member of the German Bundestag for the Left Party, criticizes the early crisis detection initiatives. In an interview with Brühl [23], he voiced concerns over the "civil-military glance into a crystal ball that is supposed to help repel refugees, prepare interventions or help winning wars". This is a rather dark view on early crisis detection, but one that should be considered. If these crisis detection technologies fall into wrong hands, a lot of harm can be

caused, especially considering the ethical problems the German military has been fighting for a long time [32]. Racism and discrimination are issues that continuously cause issues in the military ‘s structure. They will not suddenly disappear and can possibly even be elevated by AI through enhancing biased views. These are ethical issues that need to be considered as they could increase structural discrimination and legal and ethical frameworks that could account for this are still far from well-established.

Another issue that is aligned with the 4th industrial revolution is the possible adaption of people, which has been mentioned earlier. When the early crisis detection application is spread out more and more with the continuous development of the technology, it is likely that the public views is as a surveillance instrument. Is it ethical to track everyone’s phone GPS data, simply because someone has maybe been in proximity to a key actor of a social uprising without them knowing? This question needs investigation as well as whether people might adjust their behavior so that they cannot be traced even if they are not planning an uprising or engaging in another critical action. People might lose trust and the little trust that is left in privacy in digital communication could be lost completely [23]. Ethical boundaries will need to be established and communicated to the public so that people will not feel subjected to unnecessary surveillance.



**Unfair Outcomes, Biases, and Gaps in Data**

Another crucial ethical consideration is: where does the training data from which the AI learns come from? Regardless of which program will be implemented, the data acquisition will affect the outcome [8]. The normative concern of unfair outcomes is crucial to consider in the context of ethical early crisis detection AI applications. A popular example of the importance of balanced and unbiased data has been shown by Amazon’s recruitment practices. Amazon’s employed a recruitment AI that was favoring male applicants over female applicants for technical positions. The reason for that was that the AI was programmed to detect patterns in resumes that have been received during the past ten years, and most of those came from male applicants [33]. Thus, the self-learning program taught itself to favor men since their resumes have been successful in the past. This trained the AI to implement the patterns into its future calculations and decision making leading to unfair outcomes.

However, when we place this error into the early crisis detection context, the issue that arises goes far beyond gender discrimination in the workplace. Human lives, economies, social structures, and governments are at stake. The AI produces suggestions based on what it is being fed and this ultimately reflects imperfect human history. The question, therefore, is not, does this data also include biases, but rather: which biases are embedded in the data? The AI’s algorithms are programmed in a way that it learns from past events and mirrors decisions and responses that have been taken [22].

Nevertheless, there are invisible gaps in the data. For example, unconscious biases of researchers that investigate the emergence of crises are not uncommon, especially regarding the role of women in conflict. Nevertheless, women are a crucial component in understanding the unfolding of crises, whether this concerns the disappearance of women but also how “radicalization processes for women bring them into the fold of insurgency” [34]. Those gaps in research and biased data can cause various ethical issues. Racial or ethnic profiling is another one that has gained more attention in a post-September 11 world. Especially in the United States, these issues have caused upstir when it has been discovered that racial profiling is implicit in

some machine learning algorithms [35]. Thus, the algorithms employed by the early crisis detection system could possibly flag people incorrectly based on their skin color, religion, or other characteristics. This ethical issue needs attention when legal frameworks will be established to guide the early crisis detection operations.

Crises are emerging much quicker than in the past and have different dynamics. For instance, the Arab Spring emerged through people connecting on Twitter [36]. This has been the first time a social uprising has been organized via social media on such a scale. Nowadays the AI has been programmed to recognize those patterns and can indeed screen for certain buzzwords, interactions between known key actors or people who are becoming more and more active on social media and other online platforms. But what happens when a new platform is build or people are starting to connect through offline channels again? This will be something new for the AI and has many unknown variables, that might not be programmed into the algorithms [15], [12].

Ethical and Legal frameworks that govern data acquisition, data processing, and data tracking, are crucial in stepping forward with early crisis detection AI. Even if the technology is still far from being completely where we would like it to be, in the defense sphere it is extremely important to already consider legal and ethical implications and thus, recognize measures for responsible supervision, regulation, and governance [12]. De Spiegeleire, Maas, and Sweijs [12] also indicate, however, that this is not a zero-sum game and if the AI application is balanced and handled properly it can come with innumerable positive implications. Along with these considerations, it also needs to be examined to what extent the AI is being planned to be self-learning. Little information about the German military's intentions has been made available to the public on this matter.

**Transparency**

The ethical analysis of the early crisis detection system offers a compass for governance regulations. This 'governance compass' provides direction for legislators to align with Germany's values and social expectations of how the country should implement the new early crisis detection system [14] to account for transparency, of the decisions taken, the roles of the system, and the responsibilities that need to be taken. The legislation, regulations, and general rules and procedures need to be clearly established and transparently communicated before the employment of the AI early crisis detection systems. Furthermore, the question of accountability is still a pressing issue that needs much more attention in future research [12]. Especially, an EU-wide initiative on how to assure and organize accountability would be beneficial.

Transparency also needs to be considered with the application of AI algorithms in different contexts. Watson, for example, has been proven to be highly versatile as it first was intended as a high-performance search engine, and has since been applied in weather forecasting and medical diagnosis [20]. This variety and adaptably shows how capable it is to function in different environments to deliver new output. However, these adaption processes will also need to be taken under investigation and happen transparently. Screening for possible emerging crises is a much more sensitive topic compared to how the weather might be tomorrow.

Conflict and crisis hold a highly unpredictable human component, which is impossible to control and makes early crisis detection extremely difficult. However, it is crucial in increasing a

nation's bargaining power [24], [3]. The unstructured outbreaks or rapidly changing emerging events due to social media usage, make early crisis detection so difficult. Therefore, IBM Watson and the other systems still must prove that they indeed are valuable platforms for early crisis detection and are versatile enough to be re-designed for their intended purposes.

## 5 Conclusion

The ethical challenges stemming from introducing AI-based early crisis detection applications are multifaceted and call for equally versatile solutions. Much more needs to be done regarding ethical responsibility and military AI usage. The German military holds great responsibility to gather and use data ethically before deploying such systems. Therefore, this paper examined some of the ethical challenges the government will be facing when implementing AI-based early crisis detection systems, by applying concepts defined by Floridi and Taddeo [7] and Mittelstadt et al. [8]. Data ethics is still a developing field and has gained more attention in the past but will also need much more debate and awareness in the future since it is impacting almost everyone's lives.

The relevance of data ethics in the context of military use is supported by the theoretical framework since the actions either taken by the AI or the recommendations provided by it have an impact on human lives. The analysis has shown that there are gaps in crisis development research, biases in data collection, and harmful algorithm design, which all can lead to unfair outcomes. AI is already impacting most people's lives and employing more and more AI applications in the military will have even greater impacts on our lives. Great opportunities such as preventing wars, supporting those in need quicker, and stabilizing governments can come from the advancements; but the risks are not to be undermined. The impact this development might eventually have on our behavior can only be speculated.

Transparency which is one of the key factors to keeping technology and AI ethical is extremely difficult to achieve in a military and defense context. It will not be possible to make the codes and algorithms completely open-source as classified sensitive data will be handled, and it will also not be in Germany's interest to disclose this information. Further challenges will be the training and education of the staff that is supposed to operate the early crisis detection applications. More challenges lie ahead ss the German military currently is lacking qualified staff to execute the operations and also will need to implement ethics training to ensure ethical compliance.

There are many more ethical challenges that require attention and further research will need to be conducted to gain greater insight into the potential bottlenecks and pitfalls. Therefore, it is of utmost importance for the German government to establish guidelines and frameworks that govern the AI and big data utilization of early crisis detection systems to account for ethical challenges. Even with the existence of an extensive legal basis, it will be highly difficult to account for accountability when harm is caused due to the utilization of AI. More research and initiatives will be needed to advance the ethics research and avoid the AI being turned into a surveillance tool, or cause harm and eventually cost human lives.

## References


[1] European Commission: On Artificial Intelligence-A European approach to excellence and trust White Paper on Artificial Intelligence A European approach to excellence and trust. Retrieved November 17, 2021, from https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (2020)
[2] Bausum, Heinemann, Schuler: Die Welt im Jahr 2035 gesehen von der CIA und dem National Intelligence Service – Das Paradox des Fortschritts. [Übersetzung des Reports des National Intelligence Council (NIC): Global Trends: Paradox of Progress.] München. (2017)
[3] Turchin, A., & David, D.: Military AI as a convergent goal of self-improving AI (2018)
[4] Hasselbach G., Kofod Olsen B, Tranberg P.: White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions. https://dataethics.eu/wp-content/uploads/dataethics-whitepaper-april-2020.pdf (2020)
[5] Bundesregierung: Krisen verhindern, Konflikte bewältigen, Frieden fördern. Leitlinien der Bundesregierung. (2017)
[6] Müller, B.: Die Krisen von Morgen erkennen. Retrieved from https://www.faz.net/aktuell/politik/inland/bundeswehr-die-krisen-von-morgen-erkennen-15670056-p2.html (2018)
[7] Floridi L, Taddeo M. 2016 What is data ethics? Phil. Trans. R. Soc. A 374: 20160360. http://dx.doi.org/10.1098/rsta.2016.0360
[8] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L.: The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2) (2016)
[9] Provost, F., & Fawcett, T.: Data science and its relationship to big data and data-driven decision making. *Big data*, *1*(1), 51-59. (2013)
[10] Giest, S.: Big data for policymaking: fad or fasttrack?. Policy Sciences, 50(3), 367-382. (2017)
[11] Bundeswehr: Blick in die Zukunft: Big-Data-Software für die Bundeswehr. Retrieved from http://www.bundeswehr-journal.de/2018/blick-in-die-zukunft-big-data-software-fuer-die-bundeswehr/ (2018)
[12] De Spiegeleire, S., Maas, M., & Sweijs, T.: Artificial intelligence and the future of defense: strategic implications for small-and medium-sized force providers. The Hague Centre for Strategic Studies. (2017)
[13] Mancini, P., & Jenkins, M.: Ethics of Artificial Intelligence in the Legal Field. Academia. edu (2017)
[14] Morris S.: The importance of Governance – Data Science and Artificial Intelligence [PowerPoint slides]. Retrieved from https://armanyc.org/images/downloads/2020_Conference/confirm2020_sharon_morrisfinal.pdf (2020)
[15] Krüger, P.: Wie künstliche Intelligenz Kriegsführung verändern kann. Retrieved May 11, 2020, from https://www.sueddeutsche.de/digital/kuenstliche-intelligenz-militaer-waffen-kriegsfuehrung-muenchner-sicherheitskonferenz-1.4791986-2 (2020)
[16] Philbeck, Thomas, and Nicholas Davis. "The fourth industrial revolution." Journal of International Affairs 72.1 (2018): 17-22.
[17] Schuller, K.: The Fourth Revolution and the Ethics of Information. Retrieved May 15, 2020, from https://medium.com/digitalpolicysalon/the-fourth-revolution-and-the-ethics-of-information-3eebc0d2ced8 (2020)
[18] Floridi, L.: The fourth revolution in our self-understanding. (2014).
[19] Krempl, S.: Bundeswehr will Krisen mit Maschinenlernen voraussagen.

Retrieved from https://www.heise.de/newsticker/meldung/Bundeswehr-will-Krisen-mit-Maschinenlernen-voraussagen-4118330.html (2018)
[20] Morgan, B.: Ethics and Artificial Intelligence with IBM Watson's Rob High. Retrieved from https://www.forbes.com/sites/blakemorgan/2017/06/13/ethics-and-artificial-intelligence-with-ibm-watsons-rob-high/#4ca155ae260e (2017)
[21] Zwitter, A.: Big data ethics. Big Data & Society, 1(2), 2053951714559253. (2014)
[22] Hasselbalch, G., Kofod Olsen, B., Tranberg, P.: White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions. (2020)
[23] Brühl, J.: Armee will Kriege mit KI und geheimen Infos vorhersagen. Retrieved from https://www.sueddeutsche.de/digital/verteidigung-bundeswehr-will-kriege-mit-kuenstlicher-intelligenz-und-geheimen-infos-vorhersagen-1.4064931 (2018)
[24] Freist, R.: Trade & Invest: Die Bundeswehr will KI-gestützte Lageprognosen. Retrieved from https://www.hannovermesse.de/de/news/news-fachartikel/die-bundeswehr-will-ki-gestuetzte-lageprognosen (2018)
[25] IBM Watson. (n.d.). Retrieved from https://www.ibm.com/watson
[26] Lodwig, E.: Künstliche Intelligenz in digitaler Sicherheitsinfrastruktur – das Cyber Symposium. Retrieved from http://jugendoffizier.eu/kuenstliche-intelligenz-in-digitaler-sicherheitsinfrastruktur-das-cyber-symposium/ (2018)
[27] Bundeshaushaltsplan: Bundeshaushaltsplan 2020 Einzelplan 12 Bundesministerium für Verkehr und digitale Infrastruktur. (2020)
[28] Allen, G., & Chan, T.: Artificial intelligence and national security. Cambridge, MA: Belfer Center for Science and International Affairs. (2017)
[29] Bundeswehr: Friedensethischer Kurs in Hamburg. Retrieved from https://www.bundeswehr.de/de/betreuung-fuersorge/militaerseelsorge/katholische-militaerseelsorge/service/termine-und-veranstaltungen/friedensethischer-kurs-in-hamburg-171476 (2020)
[30] Bundesregierung: Kleine Anfrage der Abgeordneten Andrej Hunko, Dr. Alexander S. Neu u. a. sowie der Fraktion DIE LINKE. vom 13. Juni 2018, eingegangen beim Bundeskanzleramt am 19. Juni 2018 BT-Drucksache 19/2844 vom 19. Juni 2018 „Big Data" und Software zur Vorhersage von „Krisen" bei der Bundeswehr. Bundesministerium für Verteidigung. (2018)
[31] Wille, J., Zimmermann, A., Keller, A., Kutschera, H., Schweingruber, J.: Die Zukunft der deutschen Verteidigungsindustrie. A study performed by strategy& Part of the PwC network (2019)
[32] DPA.: Polizei-Ausbilder sollen Rassismus und AfD thematisieren. Retrieved May 18, 2020, from https://www.wn.de/Welt/Politik/4200972-Menschenrechtsinstitut-Polizei-Ausbilder-sollen-Rassismus-und-AfD-thematisieren (2020)
[33] Dastin, J.: Amazon scraps secret AI recruiting tool that showed bias against women. Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (2018)
[34] Khan, L.: The Women Fighting For ISIS. Retrieved October 12, 2021, from https://www.aspeninstitute.org/blog-posts/the-women-fighting-for-isis/ (2019)
[35] Fast, E., & Horvitz, E.: Long-term trends in the public perception of artificial intelligence. In Thirty-First AAAI Conference on Artificial Intelligence. (2017)
[36] Eltantawy, N., & Wiest, J. B.: The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory. International journal of communication, 5, 18. (2011)