SECURITY AS SIMULACRA:

Surveilling Gendered Bodies and Constructing Security out of Computation

July 2022
UG#: 2481986S
DCU#: 20109911
CU#: 60106041

Presented in partial fulfilment of the requirements for the Degree of
International Master in Security, Intelligence and Strategic Studies
Word Count: 20246
Supervisor: Marcin Kaczmarski
Date of Submission: July 25, 2022

Acknowledgements

I would like to Acknowledge my Dissertation supervisor Dr. Marcin Kaczmarski, my professors at the University of Glasgow, Dublin City University, and Charles University and Dr. Saskia Stachowitsch at the Austrian Institute of International Affairs, for all their guidance through the writing of this dissertation. I would also like to thank my friends for being ride or die, and my family for their love and support.

Table of Contents

Abstract

Artificial Intelligence has become ubiquitous across the field of security and defence, especially in applications alongside surveillance. In this Dissertation I interrogate the question of how, through application and out of discourse AI impacts the securitization of Muslim women's veiling practices within the EU. I argue that the discourse constructed around the use of AI, through official documents written and commissioned by the various EU bodies, forms a cohesive body. Using discourse analysis, I trace the patterns throughout the documents and connect them to manifestations in rhetoric on the wearing of veils in public at the EU institutional level. Through this method, I conclude that the discourses of AI surveillance manifest in the way laws are applied to women who wear Islamic veils, and their identification as a security threat to *Europe* as a both a political and conceptual unit. Furthermore, finding that the discourses of security and science intermingle to form a rigid notion of *risk* which further corners women who are already marginalized by European security frameworks.

Introduction

> *"He had wondered, as had most people at one time or another, precisely why an android bounced helplessly about when confronted by an empathy-measuring test. Empathy, evidently, existed only within the human community, whereas intelligence to some degree could be found throughout every phylum and order including the arachnida. For one thing, the empathic faculty probably required an unimpaired group instinct; a solitary organism, such as a spider, would have no use for it; in fact it would tend to abort a spider's ability to survive… Because, ultimately, the empathic gift blurred the boundaries between hunter and victim, between the successful and the defeated… As long as some creature experienced joy, then the condition for all other creatures included a fragment of joy. However, if any living being suffered, then for all the rest the shadow could not be entirely cast off.*
>
> *Evidently the humanoid robot constituted a solitary predator." (Do Androids Dream of Electric Sheep, Dick, 2007, pp. 26)*

What does intelligence constitute, and how important is it when making social decisions? These are questions humans have grappled with since machines began performing human functions, and since computers have become enmeshed in our daily lives. What is the value of intelligence in the face of humanity's other needs and functions? Artificial Intelligence needs to answer these questions as it becomes part of the daily fabric of social relations. First, AI is a dynamic and important series of technological advances that have been developing for at least a century, aimed at what the father of modern AI John McCarthy describes as "the science and engineering of making intelligent machines, especially intelligent computer programs." (2007, pp. 1). It is a group of technologies that the European Union has described as **"**systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or

unstructured data, reasoning on the knowledge derived from this data and *deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal*." (2018). The U.S. Department of Defense says that "AI refers to the ability of machines to perform tasks that normally require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or *taking action – whether digitally or as the smart software behind autonomous physical systems.*" (2018, pp. 5). Intelligence cannot be decoupled from its situation within people, and thus it's an innately human characteristic. How do we understand a machine to which we, imbue this quality**? A**nd is it intelligence that governs human reasoning and decision making ultimately, or something else?

It is impossible to discuss current international relations and the security arena without accidentally wandering off into discussions surrounding the sphere of AI. Like the implementation of gunpowder, tanks, or the nuclear bomb, AI is a technology that has fundamentally changed the landscape of conflict. We are likely only in the early stages of its development, and yet governments and activists across the globe have realized its potential to either reshape or maintain the status quo. Yet unlike another game changer, the nuclear bomb, AI is to be involved in almost every sphere of life, if one were to accept at face value the claims of its proponents. This means that the ontological considerations of AI can be sourced from a wide variety of disciplines and that conversations around AI can be sourced from a rich historical legacy. The arts, politics, and science all have something to contribute to negotiating the space AI will occupy in the future.

Throughout this dissertation, I utilize the term AI to mean simply the array of computational systems that are used to perform functions that a human might otherwise use intellect for. In particular, the technology I am mostly discussing is Machine Learning, a subdiscipline of Artificial Intelligence that has exploded

in productivity and success in the last decade or so, and is responsible for underlying most of the advanced systems used in complex situations today. Most of the high-profile advances in AI, such as autonomous systems and big data analytics, utilize this type of computer system design. However, I will mostly use the term artificial intelligence instead of machine learning (except where to describe the mechanisms of the technology), simply because it covers the discursive category of technology used to assert human power relations in the scientific domain. It is also the term used to cover the degree of technology in most security or defence documents. Also, when I refer to AI, I imply that it is irrevocably intertwined with surveillance, and see the two as operating as a unit. Unfortunately, because official discourse uses the term AI, while obscuring the fusing of the two, I will also mostly reference AI but I hope that readers will understand the subtext of the constant presence of surveillance acts, even when I don't explicitly mention it occurring.

Much of the recent advancements in AI come from the private sector of tech giants and university labs, yet governing bodies still have a massively important role to play in the wide scale utilization of AI. The broad swath of society implicated in the development and deployment of various kinds of AI means that one area cannot be fully considered without taking into account the other. For instance, scholarship on big data analysis by private companies (Zuboff, 2019) is equally as relevant to understanding contemporary AI as a reading of the final report by the United States' National Security Commission on Artificial Intelligence (2021), and in fact, many of the major contributors to this report hail from the private sector. The focus of injecting AI into every facet of society by proponents means that this is a discussion for everyone, and that ideally it should not be confined to "experts". A desire to "optimize" aspects of society should be discussed by those whose industries and lifestyles are affected by it. The effects of AI will be felt by everyone, so the pop-cultural and forum centric discussions about AI are also relevant, even though I do not have the

time or space to properly address them. Luckily politicians, art critics, journalists, and others are bringing AI to the forefront of cultural discussions. AI and the imaginations of the future have played a large role in science fiction literature, a genre that has greatly influenced the academic field of science and technology studies, a group of work that I will consider in my literature review. Such interdisciplinary fields show the strength of multiple viewpoints and traditions in working towards exploring and contextualizing technological developments in history and culture.

The acceleration of AI has also heralded an unprecedented wave of mass surveillance of populations both by governments and corporations. The emergence of an AI that can "learn" from the world around it in order to function has necessitated the conversion of people and things into data. And the only way to do this is to collect that data through surveillance efforts, which in turn relies on AI to render that data meaningful. A ceaselessly reenforcing cycle of surveillance, collection and analysis is currently underway online, and in many physical spaces across the world. Surveillance has always been a category under investigation in security for its centrality to ideas of the enforcement of control, as famously theorized by Foucault. But it has never before been so ubiquitous in all degrees of life. For example, extensive use of AI in surveillance is widespread, where individuals can be tracked for any range of criminal or differences, and their access to basic utilities and movement restricted (Mozur, Xiao, & Liu, 2022). China also employs a hitherto unimaginable degree of surveillance for the purposes of controlling the Turkic population of the Xinjiang Uyghur Autonomous region in the west of the country, and the abuse of technology is well documented by human rights organizations and journalists (HRW, 2019). In democratic countries, surveillance powered by AI is beginning to show its ubiquity as well, with the most surveilled city in the western world, in terms of cameras per person, being London, England. Despite the democratic government of the UK, the effects of widespread surveillance and AI use are

beginning to rear its head, with activities obstructing surveillance becoming grounds for suspicion and questioning by police (Murgia, 2019).

Now is the time to consider how AI-enabled surveillance affects security on both international and domestic fronts. Surveillance and its associated data collection is a chief concern of activist groups, watchdogs, and even democratic governments, and is often discussed in alarmist or sensationalist terms. Still, the refrain from most is "if you aren't doing anything wrong, you don't have anything to worry about", and individuals often return "well, I'm not doing anything wrong, so I'll be fine". The acceptance of facial recognition in smartphones, personal security devices such as the Amazon Ring, and tracking life functions with apps that return data to their makers who in turn sell that information, point to a widescale acceptance of the surveillance of all aspects of life, often for the sake of convenience. But it is in the interest of individuals to question the prevalence of all kinds of surveillance, even types that make their lives a little bit easier. Surveillance is a political as well as a cultural issue (if the two fields can even be unwound) and its security implications and applications are employed to various degrees by different regimes. For example, the degree to which China as an AI superpower employs surveillance differs from the US use of surveillance. Yet, both rely on it to improve their competitive stance, and the power hierarches that are upheld by each regime share similarities.

Beyond considerations for my use of the term artificial intelligence in place of machine learning or computer learning, I would like to make a specific explanation for my focusing on the securitization of gendered "bodies", instead of using words like people, humans, citizens, individuals, etc. When discussing people who have been marginalised in academic works, "bodies" are often singled out as the focus of oppression, control or marginalisation. It sometimes makes me uncomfortable, a decoupling of the body from the person who

inhabits it. However, in this case, what I observe is that very decoupling through the use of AI technologies. Through the use of AI in surveillance, women become only bodies either recognizable or unrecognizable through sensors and layers of processing. Therefore, my intent is to highlight that dehumanization and decontextualization of the person from her surroundings, and the reinterpretation of the complex individual situated within a socio-cultural environment into points of data from the body. I also want to highlight, through my use of the term gendered bodies, the construction of such a category as an exterior force to the individual. Through governmental legislation, securitization tools, and general cultural forces, the external gendering of a person, who may or may not identify completely with female categories of gender, individual agency is also disregarded. That is to say, simultaneous to the construction of a security paradigm by securitizing actors is the construction of a gender paradigm which supports that actors' securitizing move. The targets of this particular securitization are gendered as "women", but AI, as a tool of power also supports the gendering and securitization of those classed as "men" in other situations and have implications for individuals who evade hegemonic gender paradigms.

Furthermore, my intent with using securitization as the theory of security most relevant to AI, surveillance, and gender is its ability to step outside the dominant ontological assumptions of those who are deploying AI to enforce reified "security" measures. The complete dominance of assumptions based on both scientific and political discourses as objective truth do not sit well with my own understandings or experience of the world, and the process driven, post-modernist adjacent securitization theory offers a pathway to reconsidering security grounded in an interpretation of the world according to the truths of the already powerful.

In this paper I will generally be focusing on the how institutions act, yet, while exploring the effect of AI on a "women's" security issue, I do so with the full knowledge of the side-lining of women as actors in their own security. My analysis does not discuss the myriad of ways women, and Muslim women in this particular instance, are resisting surveillance while taking policy directed against their persons into their own hands and attempting to "de-securitize" their choices in the face of governmental and societal power. That is nevertheless an important part of the story, even though my specific focus and the constraints of a dissertation does not allow me to delve into it.

Ch 1: Literature Review

In order to build a theoretical framework that will enable me to assess the impacts of deep learning in surveillance technology on the securitization of the practices I wish to interrogate in this paper, it is necessary to draw from multiple streams of scholarship. There are multiple fields that deal with both surveillance and the development and effect of technology on society, including surveillance studies within the field of sociology, which has contributed much to my own understanding of the centrality of surveillance in modern life. However, despite my own feeling that a too narrow focus can be reductive when discussing such a wide-reaching issue, in focusing these broader topics on the realm of security, I will narrow in on select streams of scholarship. Furthermore, as mentioned in my introduction, for ease of collective understanding and standardization with the way institutions discuss the technology, I will use the term AI to refer to a collection of technologies designed to replicate or enhance human decision-making capabilities. Many employ a type of machine learning structure known as deep neural networks (DNNs), and their success is responsible for the current ubiquity of artificial intelligence in security frameworks. Machine learning is the thread of applied computer science scholarship I will be drawing from.

First, I will look at securitization scholarship, and particularly those scholars interested in the impact of big data on governance. Then I will examine applied and sociological scholarship on the development and design of machine learning models, and the scholarship which is concerned with how the design of such models interacts with socio-political realities. Finally, I will draw from feminist scholarship, including feminist perspectives from the field of STS, and show how feminist scholars grapple with emergent technologies in gendered security politics. All these areas are intersected by principles of post-modernity; therefore, core literature will also feature from post-modernist philosophy,

particularly the work of Jean Baudrillard on hyperreality, and signs and semiotics. This interdisciplinary approach will allow an analysis of artificially intelligent surveillance to be situated in the specific security contexts of the European Union, while also situating it within a general theoretical canon and the epistemology of artificial intelligence and surveillance as tools of security.

Securitization and Big Data

The original framework for securitization, articulated in Barry Buzan, Ole Wæver and Jaap de Wilde in their text *Security: a New framework for analysis* (1997), outlines a particular discursive origin of the process of constructing security. However, several schools have moved away from a rigid approach rooted in a rigid speech-act approach. Amongst them, Thierry Balzacq (2008) outlines a more flexible approach that **centres** *tools and instruments*, and identifies the need to acknowledge the ambiguous relationship between security actors and audiences. This is an important broadening of the theory and allows for the implementation with more specificity outside of European democratic contexts, where the same kind of actor-audience relationship may not be as cut and dry. This kind of move manifests in Jinghan Zeng's (2021) analysis of the securitization of AI in China, moving towards a focus on the technological dimension of securitization, and technology as a key tool and feature of the modern security landscape.

Claudia Aradau's work on securitization and big data is particularly concerned with the effect of mass computing, and of datafication on governance (Aradau & Blanke, 2017, 2018). The collection, storage, and use of mass amounts of data points is crucial in understanding where the future of security is heading due to the general increasing datafication of all parts of social life. Her critical approach is the most incisive of the smorgasbord of writing on governance and data more broadly and also borrows the most clearly from securitization

scholarship. Many studies focus on individual case applications of the Internet of Things (IoT) without critically examining the underlying justification for the mass collection of data beyond the now universal inclination for such technology to be "more efficient", cheaper, and to deliver nebulously "better" services (Mayer-Schönberger & Cukier, 2013). Aradau and her collaborators also deal with the actual applicability of mass data collection, which goes beyond the privacy/security trade-off, to actually examine whether any measurable security is achieved by expansive and invasive data collection. For instance, many proponents of the proliferation of the IoT and use of mass data in policing take for granted that passive collection is in itself a neutral activity, with no agenda or at least one which only seeks to organize society along neutral lines, and from there proceed to describe the effectiveness of the use of data, without examining *how* and why certain data is collected affect its use. While this angle is considered in critical work such as Aradau's, the preponderance of security scholarship approached the use of big data in governance from this perspective. As such, I hope to contribute to the body of work which interrogates the underlying assumptions of the integration of technology into security, and how the specific nature of the technology use contributes to a specific type of security and governance. Aradau and Mercedes Bunz (2022) incisively note in an article in Radical Philosophy that, "AI may be a new technology, but it emerges from and works upon existing distributions of power. Yet, power has only recently come to feature in critiques of AI, even on the left." Perhaps it is necessary for objects of focus in the social sciences to become central to the study and applications of AI. Many critical scholars explicate the effect of capitalism on the development of artificial intelligence, which opens a pathway toward exploring the underlying assumptions of AI, then applied to security contexts. It is also worth noting how the discourses of risk pervade official documents regarding technology in general from the EU, and the interaction of technology and 'crisis' terminology.

Securitization scholars highlight the centrality of risk management in security and surveillance regimes, and the key role that information and data processing play in these risk regimes. They do not always explore the technical architecture of these regimes beyond datafication, which is what I hope to focus on in my analysis of the securitization of women's veiling practices. Because the specific type of securitizing tool influences the way in which the issue is securitized (Balzacq, 2008) I believe it is important to interrogate exactly how the design of the tool, which is now ubiquitous across various types of surveillance devices, affects the outcome of the securitization. If all you have is a hammer, everything starts to look like a nail. Promoting AI as the end all be all of tools in governance leads to a single-minded approach on how to solve problems and enact governance that is highly data and technology centred.

Applied Artificial Intelligence

As explored in security literature focused on risk and governance, Datafication is a vital step to the effective utilization of machine learning models and algorithms for governance, a fact which securitization scholars grapple with, but which is conspicuously absent in applied machine learning literature. The *meaning* and *significance* of data is less often explored by researchers and designers of deep neural networks in published applied literature. Nevertheless, the question of the meaning of data and specifically, human derived data, is integral to assessing the impacts of technology on society and politics. STS scholars are perhaps the bridge between applied researchers and security scholars in this regard. The (inter)discipline is fruitful for security studies in its flexibility in considering various approaches and viewpoints of one topic, which I hope to integrate into my own analysis.

The Cultural Life of Machine Learning (Roberge & Castelle, 2021) compiles insightful and important works on the social dimensions of what is often presented as a purely mechanical scientific process. Grappling with the history of the computer science development, the volume situates computer science within an epistemological tradition. Datafication is the first step to rendering people governable and managing risk in control regimes (Aradau & Blanke, 2018). This means that an understanding of the development of meaning in a computer science context is critical to understanding how meaning is transposed into the data extracted from individuals, in order to recognize how governments are utilizing that data to predict, manage, and *produce* security risks. It is also important therefore to understand the functioning and problems with the particular type of artificial intelligence that has been deployed to great success in the last ten or so years; that is, neural networks.

After understanding the history of the development of AI, and the cultural and societal significance of that development (Roberge & Castelle, 2021), we can move on to unpacking the applied literature on Neural Networks in their current iteration. Foundational literature on the structure of neural networks (LeCun, Bengio, & Hinton, 2015) provide a view into the nature of their success and flexibility, while also laying the groundwork for their problematic nature in relation to application in the political world. Some scholarship foregrounds the limits of machine learning models (Waldrop, 2019) and the role that adversarial examples play in the development and breakdown of different kinds of Deep Neural Networks (DNNs) (Goodfellow, McDaniel, & Papernot, 2018). There is also a robust literature on the application of machine learning and DNNs in a more headline worthy technology than surveillance, that of 'killer robots' or Autonomous weapons systems (Anderson & Waxman, 2017).

However, international institutions and governments are already engaging with the problems of employing DNNs in weaponry (United Nations Institute for

Disarmament Research, 2018), while that concern has not been extended with the same urgency to its use in other security tools. Perhaps it is the optics of 'killer robots' that animates the focus in security on the functioning of machine learning models in this context while the problems that persist in autonomous weapons are also present in surveillance technologies used for more subliminal, though no less dangerous, social and political management. As I will cite following this section, there has been important work done on policing and AI**.** However, that focus hasn't quite gained the same prominence as autonomous weapons in considerations by those who make regulations and international norms, and as such, is less present in international security scholarship. There is also a body of security scholarship on artificial intelligence and its effect on weapons of mass destruction (Boulanin et al., 2020) and disarmament. These more institutional power-focused **t**opics of war, strategy, and 'high' politics are important of course, but relatively less complicated, and probably a more comfortable topic for scholars and thinkers concerned with relations between states, and less with the ambiguity of security as a concept and its relation to communities/society.

The problems that need serious consideration in autonomous weaponry may have even more far-reaching impacts when deployed on a mass scale against one's own population, as can be seen in news reports and scholarship that filter out of Xinjiang Uyghur Autonomous region in China. In my later chapter on EU discourse on AI and Security, China is an important focus of one of the reports for China's rapid advancement of the technology and the global competition engendered by US- China tensions. China is also the leading non-"western" state (and perhaps in general leading the world) in terms of AI development, so to consider AI without China would be a miss. In Xinjiang , China, we can see some of the most glaring and extensive reach of the "problems" or lack of fairness screening and robustness in DNNs can be used in service of mass repression in the guise of security. Despite China's expulsion

of foreign scholars of the region (Thorpe, 2021) and crackdown on news-media and reporting, there is reputable reporting on of the types of technology used to carry out the large scale 'risk management' of the population via technology. Zeng (2022) further traces the recent development of artificial intelligence in China according to 'Chinese characteristics', and what that means in a global AI technology race. He also notes how China's approach to the development of AI shapes it as a scientific and social tool, all of which are important to consider when looking at the security uses of AI in that particular setting. The idea that there can be different kinds of AI depending on which country develops it is one that the EU will attempt to promote as well.

When it comes to the place and development of artificial intelligence in the EU, less scholarship is devoted to the link between its internal security and technological competition between states, as tends to focus on the border politics of the EU. There is a wealth of literature focusing on technology, surveillance, and risk management of the European Border and Coast Guard Agency (otherwise known as Frontex). Risk analysis and management is a key securitizing tool (or array of tools) within the EU arsenal and discourse. The post-modernist school of securitization theory arguably stems from scholarship on risk management of migration at the EU external border, so a focus on this particular exchange of ideas is particularly relevant to my exploration of EU discourse on AI. Within scholarship on risk is also a focus on how technology supports and forms a sort of discursive pathway for management. Biometric collection and datafication and exchange are foundational to the way the EU conducts its external security (Aradau, 2018).

Here is where securitization scholars and big data scholars once again enter the conversation on technology's relation to security. Many critical securitization scholars, including Didier Bigo, Balzacq, and Aradau, in fact locate the EU border as a main site of securitization and the development of risk regulation

regimes. Though, few take the same approach that Zheng does in tracking how national strategies of technology development influence what kind of technology is deployed and the historical development of that technology in the context of a global security and technology arena. This analysis would be useful in the literature, as many states make up the EU, and though there is not one single artificial intelligence doctrine, the overarching views of the EU as an institution are clustered around the major defence spenders and the states at significant migration points. It would be helpful in outlining the development of these risk management systems to understand the values and history of technology that underlies them.

Feminist Security Studies

Feminist security studies often parallels more mainstream currents of the field and has a shorter history compared with other traditions. Scholars who have laid the foundations for a feminist approach to security must contend with questions of legitimacy in their focus and may 'mainstream' their ideas in order to be included in more institutions (Youngs, 2008). Policies such as 'gender mainstreaming' in the EU are a testament to the nominal effect of feminist security concerns on broader policy and ideas about *who* security is for. However, there is a long tradition of deeply political, interdisciplinary, and critical feminist security studies, perhaps latent in its focus on those marginalised by security apparatuses. Therefore, feminist security scholars have conducted deeply insightful work that speaks to the intersections of marginalised populations concerns.

Some feminist scholars have grappled with the gendered effects of emerging technologies in security. Wilcox (2017) offers a compelling analysis of drones through a posthuman feminist perspective, and also discusses their autonomous

technology, enabled by various machine learning models, and their gendered dimensions on the battlefield (Wilcox, 2017). The bio/necropolitical implications of autonomous technology in conflict zones, and how human perceptions of gender meld with computation perceptions to graft an entirely new topography of gender have powerful implications for other tools that utilize machine learning models. Feminist scholars who identify with STS are an important bridge to computer scientists who grapple with the political and cultural implications of machine learning and computer science including those scholars in *The Cultural Life*. Feminist writing has a strong tradition of breaking boundaries between disciplines and introducing a critical approach to an otherwise enshrined mode of study, therefore whenever there are feminist forays into science, the output bear fruit ripe with interest. While there is a strong tradition now of feminist security studies, I find there is much room for security studies on a broader scale to embrace feminist analysis, beyond fairly middle of the road institutional attempts at gender mainstreaming or gender consideration. Sublimating a feminist approach to security within the wider framework of Human Security is also a rather lacking perspective, as the "problem" of security itself can affect and be affected differently based on gender. When gender is not considered on its own and becomes just one of many marginalised identities considered to be affected by security policy, then the true breadth of various problems cannot be fully communicated or studied.

What are the implications when the innovations of surveillance technology are now mostly progressing in the private/corporate sector? From a feminist perspective, we see the reproduction of racist and sexist power hierarchies into the "scientific" domain of computer science and corporate risk analysis (Stachowitsch & Sachseder, 2019). Without more rigorous, though still flawed, checks and regulations meant to combat the violation of civil and human rights power of scientific discourse, hierarchies will only become further cemented. This ability to reproduce, and in turn strengthen, existing power dynamics

requires an increased attention toward the role of technology and in turn visual media, on security policy creation and implementation. As such, I believe it is worthwhile to now expand the literature from which I will draw to understand the shift away from more traditional forms of surveillance toward the overwhelming application of models of AI.

Out of Security Studies

In order to make sense of these various disciplines, I propose tracing their common theoretical thread, post-modernism, and grounding my analysis in a seminal work of postmodernist thinking; Jean Baudrillard's Simulacra and Simulation. Surveillance technologies are a tool grounded in the generation of images as signs, which Baudrillard centres in his own analysis of the image making technologies of the late 20th century. Feminist security discourse engages with the structuralist underpinnings of gender as class and the constitution of security through discourse, which is explored by Lene Hansen's emphasis on the post-structuralist construction of securitization theory through an analysis of the Muhammad cartoon crisis' (Hansen, 2011).

The Simulacra is, one could argue, an increasingly relevant device for engaging in an understanding of modern security production and processes. It describes the incongruity between what is experienced by most individuals as their socio/political/cultural existence, and the policies of governments enacted onto them. Surveillance tools, which are needed to enact control and governance, outfitted with sensors and networks, analyse data and make 'decisions' based on that data (AI), which increasingly do not align with the 'real' world. That digital copy, then presides over the real social and political context. But that simulacrum is produced from the combination of power and process which governs other forms of securitization. The visual element of surveillance in

"computer vision" machine learning models in particular collapses the realm of visual media, science, and state security and politics in a way that necessitates moving beyond the distinction between those units of analysis, and toward a more inclusive schema of what *is* surveillance technology.

This is perhaps where the literature moves out of strict security analysis and into STS, sociology, and media studies, so I will not linger too long here. However, it is important to note the important work of surveillance studies scholars such as Gary Marx, David Murakami Wood, and Shoshana Zuboff, who respectively, deal with the groundwork of surveillance's relation to society (Marx, 2017), the effect of surveillance on physical and political space (Wood, 2009), and the importance of 'surveillance capitalism' on the landscape of technology (Zuboff, 2019). Exploring the greater effects of surveillance on the social landscape is key to understanding how groups and individuals act when they are being surveilled and how a society that relies on all kinds of surveillance, as in most information societies (Bunz & Meikle, 2018), is organized. I would be remiss to not at least mention the significant scholarship on surveillance and domestic policing, of which Marx contributes, as well as the important studies done on the recent integrations of machine learning with predictive policing and algorithmic law enforcement, especially in the US, such as the COMPAS recidivism study (Larson et al., 2016). This literature bridges then, sociology and security, where it is necessary in international security, to understand how security norms built in the communal and domestic level make their way into international discourses and norms.

Literature Conclusion

As we can see, the problems of surveillance technology and the emerging patterns of doing security weigh on the minds of scholars across disciplines.

Among securitization scholars, questions of data in governance, particularly at the borders of states, occupy an increasing amount of literature as the importance of datafication for systems of risk and control become ever more apparent. This dovetails with literature coming out of feminist security studies, prominent focus on gender and race as important units of analysis lend an even more critical dimension to the scrutinization of the implementation of AI as a tool of enforcement of existing power hierarchies.

Both security schools rely on the important work that makes the understanding of artificial intelligence models understandable and workable for non-computer science scholars. Computer scientists who write about the robustness problems of neural networks, make the analysis of the political implications of the technology possible. Computer scientists and sociologists involved in STS do critical work that often overlap to an extent with other critical disciplines, while injecting a deep knowledge of the science into their work. They explore the social implications of AI, and even contend with the boundaries of the concept itself. Here, STS owes much to the social philosophy of surveillance studies, and the postmodernist milieu it emerges from. From this point, surveillance studies begin to contend not only with the social implications of surveillance, but the political, with a direct interest in interrogating policing, and by extension, the now ubiquitous technologies that enable mass policing and incarceration. At this point, the literature circles back to security, and the concerns that underly the critical thread of its scholarship.

All these disciplines contend with a few main points of interest. Specifically, how do systems of power use technology to reinforce and reproduce that power, how does the technology function both practically and discursively to build networks of management and control, and how are the subjects of that system affected by the way that power is reproduced. There are many more scholars and works which cover other facets of the consideration of AI, surveillance, and

security that are highly interesting and explore the range of the effects of technology on the social and political sphere.

In this dissertation I hope to bring the interdisciplinary underpinning of the study of surveillance and AI to bear on an analysis of the impact of AI discourse on policy against Muslim women's veiling practices in the EU. Without acknowledging the breadth of literature on the topic, I would not be able to approach this niche with the same open mind and attention to subtleties. And, I hope to contribute by own reading, through the prism of extant scholarship, on the issue.

Ch 2: Methodology: Discourse Analysis and Connecting Theory

My approach to analysing the impacts of machine learning on the securitization of women's veiling practices in the EU will be threefold. First, I will build my own theoretical argument supporting my idea of how the securitizing tool of surveillance technology imbued with artificial intelligence, contributes to a specific kind of securitization, using the breadth of secondary sources outlined in my review of the literature. Then, I will zero in on EU policy documents regarding AI, where I will analyse the discourse surrounding both domestic and international implementation and official reports. I hope to highlight the instances, especially since the beginning of the last AI Summer, or period of rapid advancement and boom in development, in which the ubiquity of AI in security has altered the nature of *how* AI fits into the security landscape. I will identify and track the specific language used to usher in this turn. Finally, I will connect the discourse of AI in official documents to the ongoing effort of member states and the broader EU to engage Muslim women's veiling as a political and security issue.

Methodology

The documents I will be using are the EU Commission's White Paper on Artificial Intelligence and the European Parliament's special committee on artificial intelligence in a digital age's commissioned study 'Artificial Intelligence Diplomacy'. I have chosen the EU as a body because despite being an organization of many states with their own internal security issues, militaries, and ideologies, the EU is an important norm building body both for European states and for the rest of the world. While the AI diplomacy document is a study written by one individual, Ulrike Franke, a senior policy fellow at the European

Council on Foreign relations, the fact the document was written for application purposes and was officially published by the European Parliament allows me to situate it within the context of official EU Discourse. The EU is also on the cutting edge of digital regulation, at the same time as it has a rich history of scholars who analyse its securitizing force and how technology plays a role in securitizing discourses. In the findings chapter, I will compare the discourse of the EU on AI to European Court rulings on member states' laws on veiling. The specific Court cases I have chosen will highlight in particular the envisioned security dimension of laws that are covertly intended, when couched in language of "neutrality", to prevent Muslim women from wearing religious garments. I have chosen one case from France, which has some of the most high-profile controversy around veiling, and Belgium, which until recently, was the only other European Union member state to have a national law that made the wearing of a full-face veil illegal. Both of these cases also contend with very similar laws, so analysing a prevailing discourse at the court level will be more relevant. I have also chosen cases heard by only one court, the European Court of Human Rights, for that same reason. It would be my preference to have analysed rulings from multiple courts, and laws from multiple states, but unfortunately there is not space within the limits of a dissertation.

Because my main theoretical ground is securitization, which initially stems from a 'speech act' rooted in the construction of particular discourses, I feel that this is the most appropriate approach. Securitization theorists have since hypothesized other mechanisms an actor may use to securitize an issue. I hope to demonstrate how the discourse surrounding AI and the policy on veiling respectively, can be shown to be part of an emerging pattern surrounding AI and surveillance. The specificities of European securitization will also be explored while I outline and parcel out the discursive building blocks of each document.

I will use post-structuralist discourse analysis to frame my own approach to the AI discourse of the EU. Thomas Jacobs's (2018) overview of post-structural discourse theory will inform my analysis. Post-structural discourse analysis theory meshes well with my analysis because securitization theory, as discussed by Lene Hansen is fertile field for considering post-structuralist questions such as

> "Through which discursive structures are cases and phenomena represented and incorporated into a larger discursive field? What is the epistemic terrain through which phenomena are known? And, what are the substantial modalities that define what kind of an issue a security problem is" (2011, pp. 357)

This means that discourse analysis and securitization can work together to interrogate the problem of how AI, integrated into surveillance systems and security networks, is being used by governments to construct an existential threat in the larger security landscape. Also, for my specific aim, post-structural analysis specifically questions "science" as a truth, and instead locates it as a type of discourse that exerts more power than others. Post-structuralist discourse is, by default, included in larger political discourses and has a disproportional effect on security policy due to the enmeshment of technological advancement with security industries. It also is used extensively by feminist theorists of multiple disciplines, who often have the aim of demonstrating gender's situation as malleable according to social discourse. By levelling ideas of security, technology, and gender as discourse, I hope to avoid elevating security and science above broader social issues, in the usual sense of those discussing 'high' politics, and relate how these matters are all connected and affected. Unfortunately, I will not inject as much theory from a feminist perspective, as the scope of this dissertation is to consider the institutional perspective.

Beyond the Copenhagen school's securitization theory, Foucauldian securitization scholars (including the Paris school and critical scholars) implicitly engage with a post-structuralist approach to the construction of security through discourse. I believe that post-structuralism is an engaging point of view to access the literature of the field I have chosen, which comes generally from critical scholarship of various stripes. Despite this, I will not be using critical discourse analysis due to its own lack of precision, and I hope to elucidate ideas in specific documents from governments with unique histories. As both discursive documents and securitization tools in the vein of Balzac's theorizing (2008), these documents serve a dual purpose in my analysis. They build norms of discourse while also putting those norms into practice.

I will locate certain vocabulary and phrases that pervade the documents, leading to the strengthening of certain ideas about security and AI. I will also analyse how the purpose of each document leads to certain kinds of norms and linguistic turns becoming emphatic of particular modes of thought. EU documents often focus on regulations and the AI white paper tracks alongside that trend. The AI diplomacy document is focused on presenting a distinctly "geopolitical" outlook and positions the EU as an international actor instead of an internal regulator. This means that the strategies for presenting AI will be different. While I am focusing on a security issue, it is one of internal security, so it is likely that the white paper will present more opportunities for me to understand how AI is presented as a component of internal security. However, the outward facing, globally minded diplomacy document will be important for understanding how geopolitical implications impact internal ideas of the EU and its inhabitants.

A relevant angle for discourse analysis in this case is that the building blocks of AI are also, in a way, a type of post-structural discourse. Coding languages underpin the functions and the rules of the digital world. As such, the way AI

comes to interact with our 'real' world, as opposed to the digital world, is through the discourse of the digital which in turn, enforces its own rules and limitations on otherwise far more flexible and open contexts. The basis of Machine Learning models, and all other computer operations, is the algorithm. In simple dictionary terms a "set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem" (Cambridge Dictionary). Algorithms are written in code, which can be formulated along various patterns or languages. Algorithms order the digital world, and the digital world is inherently constrained by the language of codes. When algorithms are allowed to reach out of the digital world, into the real world, they become the constraining discourse of social order along with spoken and written language more familiar to us. Algorithms have taken on enhanced focus in the cultural discourse (Burrell, 2016) for this reason. Suddenly, we have woken up to the idea, even the *reality,* that digital codes order the world. It is not a great leap to think they are now a discourse that orders other kinds of discourse, including security discourse.

My intent with this methodology and connection to theory is not to say corelation equals direct causation because the underlying reasons for even such as specific policy issue as veiling policy is varied and complex. Instead, it is to point to the way that discourses and tools can be part of national or supranational strategies in justifying securitization. I hope to build a discursive and theoretical bridge between two points that might not otherwise be immediately obvious, but which are both underpinned by a common thread. That connection comes not only from post-structuralist analysis of official discourse, but also of the application of theory to the context of the technologies discussed in the discourse and implemented further.

Theoretical Discussion

In the rest of this chapter, I will make a case for my theoretical approach to the assertion that the design of AI in surveillance systems has an impact on how an issue, in my later case; women's veiling practices in the European Union, are carried out and their outcomes in terms of policy application. I draw the basis of my argument from the literature presented in the previous chapter, and from literature outside the scope of this dissertation such as art scholarship, architectural and urban studies, and fiction, all of which are important to understanding the cultural impact of technology and surveillance. To begin to do this, I would ask a question that plagues security studies and International Relations; security for whom, by whom? That is, who can *be* secure and who *does* security. It is a question that implicitly examines the power relations of security, while also raising ontological and epistemological considerations. What is security, and how does one know that it is? It is a political, or as envisioned by securitization theorists an *extra*political, category therefore its construction takes place between political bodies with power to mobilize securitizing forces as well as produce security discourse (Buzan & Waever, 1998). In this framework, the securitizing actor is the one who *does* security, and dovetails with my primary question in this case which is that who/what *does* security, is also who/what has the ability to decide what security *is.*

Securitization theory views security as a process and the outcome of a process, not an innate state of being that a political issue possesses. For instance, issues like immigration or climate change only *become* security issues once they have passed through the process of securitization and have been determined to be a security threat to the state and thus an existential, rather than a political, crisis.The existence of this process-centred theory, which lacks the distinction between a 'real' or 'made-up' security issue, necessarily leads to questions regarding the nature and validity of whether such designations pose even the

slightest threat to the state or polity. More simply, if any issue can be treated as existential threat, due to the nature of political processes, are any threats themselves 'real' at all?

Securitization theory scholars, while highlighting that security is a process, in its use do tacitly acknowledge that there *are* such things as actual threats to a state, by sometimes asking *should* this issue be securitized. They ask, should the utility of the label of "security" issue be applied to a threat in order to elevate it and prioritize it in focus and funding? More institutionally deployed security theory, such as neorealism or emancipation theory, do not interrogate that ontological understand of security, and do not open the door for the same question that securitization does, which is, do threats to nation/state exist at all? Perhaps they did at one point, but now can any issue, besides a war of conquest, be truly categorized as an existential one. So, what is a process if not a construction, and then how can the end of that process be said to truly represent the original issue/activity/object?

Once we identify the air pockets between this securitization process and true or imagined 'reality,' I would like to return to the idea of the simulacra of security as a lens through which to view the effect of AI on policy. Complicating that matter is the possibility that in fact, the process is reversed. That the securitization may exist *before* an issue/activity/object becomes of any consequence to or a consideration of the political realm. That a model of a security threat exists *prior* to the existence of any actual problem.

My main assertion theoretically then, is that artificial intelligence, integrated into surveillance systems, reverses the process of securitization, in a way, producing a securitized issue *prior to* its political incarnation and prior to the existence of a political issue at all. And it does this as a product of the architecture and design of the most prevalent models of AI in

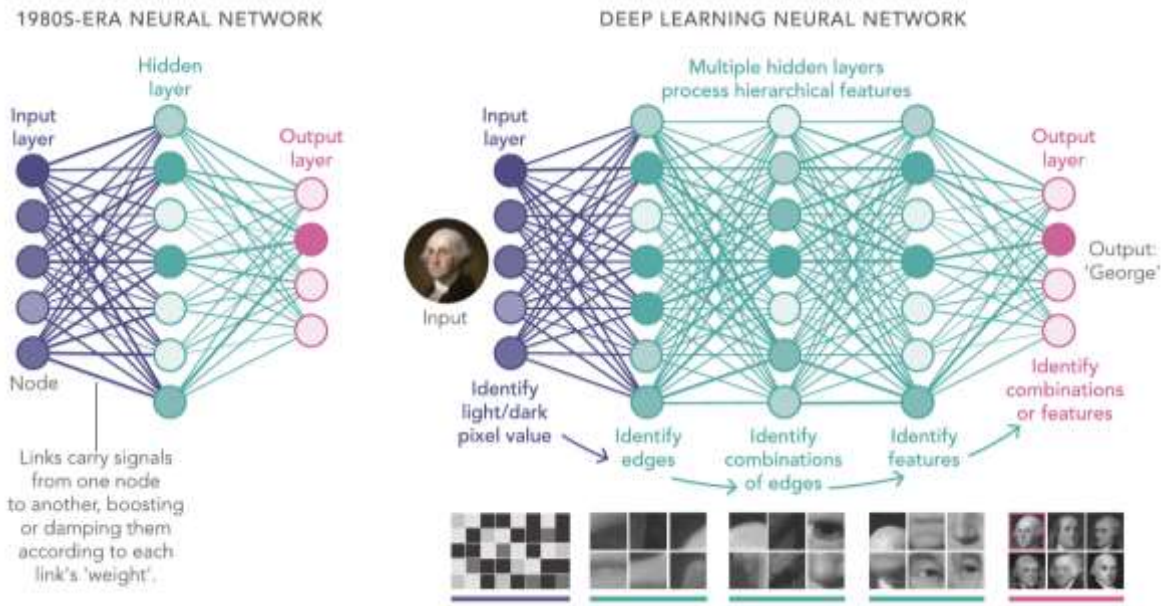
security/surveillance systems, deep neural networks. That is, the security produced through use of AI imbued surveillance is a simulacrum of security, in that it precedes its model.

Other forms of post-structuralist analysis make the case that there is no 'reality' to return to, that whatever the issue, it is merely constructed out of discourse. But my reading of Baudrillard moves through and beyond this for the effect of AI on an issue. Instead of constituting reality, I would say that AI *annihilates* the existence of any 'reality' in its preceding articulation of that issue. This does not imply that there are not real women walking around, interacting with their cultural environment and making their own decisions, but that the *reaction* is not to these women, but to their reconstructed simulacra.

Most processes in an information society are processed through this AI mechanism, to say nothing of its ubiquity in security, so can there be a return to the real? And who does this departure from "real" security and real threat benefit? If AI reproduces power structures, as they have been found to do consistently, (Gebru, 2020) then it would stand to reason that the further we go from a 'real' security space, the more those with power serve to gain, and the more malleable a concept security itself becomes. Computers to not only replicate human biases within their own neural networks, they enforce them in the world outside as tools of scientific authority, through the presumed 'truth' that science, uncritically accepted, holds in discourse.

Fundamental to the way security is produced preceding the threat, is the design of deep neural networks, as briefly touched upon in my literature review. In order for machines to learn they must first be trained on massive amounts of data selected or at least first produced by humans. The images must be cleaned, labelled, and categorized so that the neural networks and their algorithms can learn to recognizes objects in supervised learning. In unsupervised learning, the

images (or other bits of discreet data) are not categorized, though they still need to be cleaned and labelled. The labelling and cleaning of data or images infuses a semiotic and discursive element into AI that cannot be ignored. For humans, the act of categorizing is a social one. The idea that computers could then generate an 'objective' or truly accurate outcome must be problematized in the face of the social and political work we now find computers to be doing.



Above is a useful visualisation of the way that deep neural networks learn (Waldrop, (2019) Image credit: Lucy Reading-Ikkanda (artist)). One can observe visually how an image, video, or piece of language is disassembled, and reassembled within a neural network. While this structure is likened to the human brain, it's clear that this is not analogous to the way humans reason or identify, despite the naming conventions used to denote this kind of system. Furthermore, with unsupervised learning, developers may not actually know how the neural network arrives at conclusions, in what is known as the black box problem. A neural network building connections independent of human supervision, is necessarily, not making human connections. Whatever the neural network spits out *becomes* the 'truth' of the situation, and it can never be fully

assessed by humans. The opacity of AI 'decision making' further removes the outcome from any 'reality', even beyond the question of accountability.

This manifests in the dislocation of the policy and focus of discourse from any otherwise observable 'reality' of existential threat. Why does unveiling policy focus so heavily on the niqab and burqa, when their use is relatively minuscule? Because they, both symbolically and technically, obstruct most completely the use of AI as a security tool, and as a whole-of-society tool in the elevation of the EU as a global technology player. I will, in my final chapter, interrogate the direct impact of EU discourses on the way policy is implemented and at what levels, but I'd like to think of this line of reasoning as applicable to more than one policy issue, in that as the use of AI increases in security, problems that obstruct the ability of AI to simulate security issues will become more numerous.

Ch 3: Discourse Analysis of AI in the EU

In this section I will analyse the political and discursive processes of cementing artificial intelligence as a securitizing tool in EU official policy and documentation. I will begin my analysis with the EU White Paper on Artificial Intelligence**.** The EU is not a body where security is the main organizing factor, such as NATO, so one might wonder why EU documents are particularly relevant to analysing the security developments of the region. Despite not commanding the same decisive military capacity as NATO or an individual state's standing force, the EU is an important body for setting international norms around security and is the organizing force of what is arguably one of the most influential agencies in building European concepts of what constitutes a security issue, the European border and coast guard agency, Frontex. The EU, through Frontex, Maybe determines and projects a unique way of articulating and building security that is present in other EU documents and circulates among member states. This rhetoric also influences what kind of securitizing tools are privileged and become ubiquitous, and I would argue, goes hand in hand in the adoption of deep learning AI as a standard.

I will identify patterns of language in the documents and contextualize them within the larger security and geopolitical contexts of their authors. Alongside this, and in line with post-structuralist theory, I will look at the vocabulary and phrasing as constitutive not only of the messaging and intent of the EU, but also of the construction of the security practices of the institution.

Analysis of the EU White Paper on Artificial Intelligence

The White Paper (European Commission, 2020), like other norm building policy documents, rests on a variety of assumptions. The vocabulary of the

document emphasizes continuities in EU law, regulation, and economic discourse and European political and cultural identity. This document focuses on the internal use of AI and is weighted in concern on the economic and social implications of AI, with internal security as a latent consideration that flows through not only the particular sections dealing with security, but also those otherwise 'unrelated' subjects.

The definition of artificial intelligence employed by the EU in this paper is a simple yet flexible one refined by the commissions High Level Expert Group. It states that:

> "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions." (High level expert group, pp. 8)

To start off with, it is noteworthy that even the definition in a rather dry policy document uses anthropomorphic language, in a way that is relatively standard when discussing AI used in political/social situations. Words like perceiving, reasoning, and behaviour are words not generally attributed to non-sentient objects, even if they perform functions that are meant to replace human action, such as a Roomba or automated manufacturing machines. This is meant to emphasise and legitimize the validity and relevance of AI in the political and social process. It would be odd to find this type of language when discussing AI optimized for advertising or medical sequencing, despite the fact that the systems operate using the same technology and manner, and particularly in the

case of advertising, to an overwhelming degree. Targeted ads are rarely described as perceiving the users' buying habits and adapt their behaviour to sell more. That would probably be too reminiscent of *Blade Runner* for Amazon or Google's tastes. In situations where they are used to influence more political or social processes, AI is portrayed as a social actor, akin to a human decisionmaker. This overarching theme, of AI as both possessing human qualities while retaining the powerful discourse of truth imbued by science, intersects with other patterns in the discourse, as discussed below.

Almost all EU documents that deal with ideas of collective defence and threats mainly articulate security in the language of *risk* and *risk management and* are a constant motif in the AI White Paper. In EU discourse, AI is a key tool for managing securitized *risk* such as migration (European Commission, 2020, pp. 17) and climate change (*Ibid, pp*. 2) (in the White Paper climate change is frequently mentioned as a key issue that AI will help mitigate or manage to some capacity) but also AI itself presents security and social risks, which in turn must be managed (by regulation also laid out in the White Paper). AI is assessed on a scale from *low to high risk (Ibid,*pp. 17). The risks of AI can be managed as long as certain EU norms regulate its use, and as long as those laws and regulations are abided by. The word "*risk*" appears 95 times in the White Paper. Scholars such as Bigo, Stachowitsch, and Balzacq all highlight risk management as a key securitizing tool for the EU, but it is interesting that it appears so frequently in a context that is not explicitly security focused. This feature underlies the subtilty by which securitization can operate even on otherwise ostensibly fully economic or culturally focused discourse. Securitization can take place through multiple tools, even ones that do not seem to primarily focus on international security, the military, or geopolitics.

In the White Paper, the EU places *fundamental human rights* at the centre of its discourse and *equates* them with *European values. Europeanness,* therefore,

becomes something which must be secured, both against AI and by AI. *Europeanness* is integral to understanding the envisioning of AI regulation as well as how the EU defines what human rights are.

This is in line of discourse that also emphasises unity in policy regarding AI and security, and in continuity with legal statutes across member states. Establishing normative and legal *Europeanness* is a core EU feature. It posits the existence of a united Europe as necessary to ensuring security. The EU platforms speedy adoption as a necessary good and an inevitability, and *trustworthiness*, as the avenue throughout which to ensure that adoption proceeds at a competitive level with the rest of the world. Key features of trustworthiness are transparency and accountability to a clear legal framework. The discourse surrounding trustworthiness is positioned as the path to not only speedy adoption and expanded research, but also to what is called *ethical AI. Ethical (Ibid,* pp. 6). AI is another core tenant of the EU's vision of a European AI, and what EU discourses imagine as a unique European offering to the commercial AI sector. *Ethical AI* reappears as a concept throughout each push by the EU towards development.

The EU White Paper also emphasises that the AI arena is a *globally competitive (Ibid,* pp. 6) space of security and economics. This gamifies the development of AI, and implicitly introduces the ability for there to be winners and losers in such a game. Once again, the White Paper is not explicitly a security document, but it still employs discourses of security. This emphasises the central role AI plays in the EU's concepts of collective security alongside the organizing principle of the common economic area and market. Because the EU is foremost an economic union, regulation and management is principally about standardizing trade and private sector regulation, so to see the language of security slip in should alert readers to the encompassing nature of AI in the future of EU discourse and policy. If the EU is competing on a global level, with potential rivals and allies alike, then the urgency of investment in AI

increases. This particular part of the discourse comes to look distinctly like a securitizing move, in that it is attempting to move the development of AI out of the normal political-economic sector, into one of global, and thus *existential* significance.

The White Paper outlines some of the technical features of AI, of which the most used now are Machine Learning and its subfield of Deep Neural Networks, that increase the risk of their misuse towards ends which threaten the *European values* of *fundamental human rights*. The EU highlights *discrimination* as a *flaw* in the *use or training of* AI (pp.19), not as a function of its being designed in order to categorize. This connects to much of the applied deep learning research, where adversarial examples are often treated as opportunities for improving a model, as opposed to an instance of failure in the premise of using a technology that categorizes patterns to react to and reflect reality (Waldrop, 2019). There is a longer technical description in the AI Diplomacy document, where these "bugs" in Machine Learning techniques are also deemphasised, despite their opposition to the goal of developing AI according to *European Values* and *Ethical AI*. However, the various regulations for *trustworthiness* of a European developed AI are zeroed in on the way to ensure rapid adoption, and to lead globally on norms that centre fundamental human rights. It seems like a purposeful choice to gloss over the very real problems that exist inherently with ensuring robustness and fairness that pervade deep learning models.

In the brief discussion of technical features, the White Paper discusses some *limitations* of machine learning and deep neural network model techniques. which are critical to our understanding of the EU's focus and the assessment of AI as a tool that produces *risk* as well as manages it. The White Paper specifically highlights the *opacity* of these models (European Commission, 2020, pp. 19) and their reliance on human categorized training data (*Ibid,* pp. 18). It highlights how people are at risk of discrimination from AI, due to the

bias of the humans who build them (*Ibid,* pp. 11). However, through the insistence that AI is developed widescale and quickly, the White Paper obfuscates that fact that ML and DNN's can only "make choices" (to use the humanizing language of the paper) by being imbued with categories which are by nature simplifications of the world around us. Regardless of whether or not the humans training the AI attempt to eliminate the bias they input into the model, it can only draw conclusions from a limited set of data, which is still a simplified or datafied version of human existence. This cannot fully capture the context in any situation, as ML and DNN's, despite their name, do not actually function anything like human decision-making. They are still purely statistical models, though highly complex and reflective ones. This is something that the White Paper does not contend with, and likely will not, as this could impede *trust* in the very concept of AI, and thus increased investment, development, and adoption.

One of the most important passages for determining the institutional discourse surrounding the most sensitive application of AI is on pages 21-22, which discuss the necessary effect of the input of human oversight on systems by noting that the "objective of trustworthy, ethical, and human centric AI can only be achieved by ensuring an appropriate involvement by human beings in relation to high-risk AI applications" (European Commission, 2020, pp. 21) and goes on to outline the degrees of human intervention in *high-risk* AI scenarios. Social security benefits, credit card approval, and driverless cars are mentioned as *high-risk* scenarios, but this once again takes it as unquestionable that AI should be used for these situations, and that their use in some way improves the outcome. But why, if they are so *risky*, would there be a reason to inject AI into them? It is likely in pursuit of the *efficiency* and associated productivity, that would make the EU competitive globally, that these questions aren't being asked by legislators and bureaucrats? What is the actual value of having an AI decide if someone should be given a loan, or if they can be trusted to serve the

conditions of their parole? What is truly the normative and social value of efficiency, and does it outweigh quality or reliability?

The section then goes on to outline the most dangerously *high-risk* application of AI according to the EU, the collection and deployment of biometric data for identification. This is the area of use that is most relevant to security concerns and *risk*, and the area most likely to lead to a degree of abuse. It is also there that this dissertation will become most interested in the findings chapter. The document makes reference to facial recognition for remote identification purposes and distinguishes between use for identification versus use for verification or authentication (*Ibid,* pp. 21). At this point in the document, an interesting language shift occurs. Suddenly, *natural person (Ibid,* pp. 22) is used to describe individuals whose biometrics are being collected and identified. This term isn't used to refer to a person anywhere else in the document and isn't mentioned in AI diplomacy. Words like *user* and *consumer* are common obfuscations of "human" or "person" when referring to the subject of AI surveillance and data collection, but this term stands out, and deserves further analysis.

What or who is a natural person? A natural person, by legal classification, "is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (European Parliament, 2018) This is a definition tied to the creation of personal data collection, and naturally distinguishes a "living, real, physical, human person" from an "artificial person" or "juristic person". While this is not an unusual legal term, it is worth asking why it is being utilized now, at the end of a long document that deals continuously with personal data and AI? The sudden reference to the General Data Protection Regulation (GDPR) and natural

personhood feels like a distinct retreat into legalese in order to construct a distinction between the companies, people, citizens, actors, and humans in the rest of the document. It is also a step away from more humanizing language for, well, humans. It is perhaps an attempt to bring AI decision-making and the people who will have their lives moulded by it, onto a more similar level of "human". This term does not appear in the AI Diplomacy document, nor in either of the court cases dealing with veiling laws I will analyse in my findings chapter, despite the fact they are legal documents. This signals that the White Paper may be attempting to shift the larger discourse about what makes a person or a human, out of the realm of AI.

Alongside the focus of developing AI tools according to *European values*, and part of the implicit crux of the push towards speedy adoption, is the insistence that AI has the technical capacity to, if used according to EU normative and legal values, accurately reflect and replicate the world that it acts upon. This underlying assumption is not problematized by the authors of the White Paper. Instead, the question of whether AI can truly do what it is advertised to do by its mostly private and profit driven developers is never assessed from a critical standpoint. There is nothing quoted in the White Paper from scholars across Europe who study questions like this, and it represents a serious, and likely wilful, blindness to an alternative way of imagining the future of the EU economy and security.

Overall, the aim of the White Paper is to attempt to build norms that relate a specific definition of *Europeanness* to AI, and connect it with the main discourse which directs European security*; risk management*. A distinctly European AI would be one that both helps regimes manage risk and function according to *European values* embodied in *ethical AI*, while simultaneously being a risk that itself is in constant need of management.

Analysis of Artificial Intelligence Diplomacy

The Second EU document, Artificial Intelligence Diplomacy **(**Franke, U., 2021**),** published by the European Parliament. is more firmly focused on the effect of AI on external relations, politics, and security. It emphasises the geopolitical implications, not just for the EU but for other great power relations and calls explicitly for security-focused initiatives in AI development. Artificial Intelligence Diplomacy is more focused on constructing a narrative view of the state of international relations to AI than using the institutions and tools of the EU to build consensus between states and agencies surrounding regulations. However, it is no less a powerful discursive tool for constructing bonds around the understanding and view of AI and a security based on common *Europeanness*. It positions *European security* as a singular unit, just as the White Paper does, and so therefore is also helpful in analysing discourse between member states and EU institutions around security as well as external security. The AI diplomacy document contains more tension between the norms and policies the EU is trying to construct, likely because here an attempt is being made to balance the importance of external security and relations with internal norms and development values. Throughout the document, tension exists between ideas, the political landscape, and the imagination of the future are at work in this discursive document. Despite the lack of focus on internal norms of *Europeanness,* external projections of *Europeanness* are privileged.

EU norms of *ethics, trustworthiness, and human rights* are subliminally called into question in the document, though not explicitly thrust aside, as other types of AI development are explored as legitimate. For instance, in the section on the U.S.-China competition, it is noted that the unwavering compliance of Chinese companies and citizens' inability to dissent from data collection is part of what makes China such a strong competitor (*Ibid,* pp. 14), as all kinds of mass data

can be collected more easily. This juxtaposes how AI can help power authoritarian goals (*Ibid,* pp. 15), while AI can itself be empowered by authoritarianism. The document implies that authoritarian regimes can make AI advancement, a main strategic goal of the EU, more achievable (*Ibid,* pp.18). The document does not detail what makes the way European AI collects its data different from how the Chinese government does it, as though the extent of intrusion is different, but it is also through surveillance and compulsory datafication. There are important privacy laws and regulations on the books in the EU, but functionally, AI needs the same kinds of data to develop. The document notes that "democracy and the rule of law are primary EU values" (*Ibid, pp*.18) and that AI development without those European values is a risk if the EU does not step up to the plate on developing its own AI. However, there is a clear tension between *European values* and the road to the competitive AI development the EU envisions on the global stage with China and the US.

This document is also far more illustrative than the almost strictly regulation focused White Paper. It calls up events, such as the defeat of South Korean player Lee Sedol by AlphaGO (*Ibid,*pp.13) and the resulting shift in Chinese AI strategy it caused, the protests of American tech workers against developing AI for project Maven, and the differences between Chinese and American data, to illustrate the competition between the two main AI superpowers (*Ibid,* pp. 13). The attempt to draw on narrative here positions the EU as a protagonist in an unfolding story, with the development of the technology being the driving element, with other actors, mainly China and the US, occupying antagonistic and supporting roles. This constructs a world in which certain kinds of AI adoption are to be feared and distrusted, while others align with the *European values* of the main actor, and are thus to be championed. This tracks with the positioning of the EU in a global narrative, or to invoke a more often used metaphor in security, a global "game" of AI. As mentioned in the analysis of

the White Paper, this positioning is evidence of a speech act, moving AI out of the normal political realm into the existential.

AI Diplomacy evokes the theme of global competition around AI frequently, yet unlike the White Paper, specifies who the global competitors are, and explicitly brings up the possibility of being a "loser" in the AI competition. It is clear from the document that the US and China are the main players of this global game. It is not explicitly stated what will happen if the EU officially "loses" (nor how that is even a quantifiable state) to the US or China. It is interesting that other technologically advanced states such as Japan, India, or South Korea are not mentioned as other players the EU could potentially "lose" to. There are dire consequences for losing the AI competition outlined in the document, which include complete economic dependence on either the US or China (*Ibid,* pp.16). This sets up a situation where someone arguing against putting mass resources, devoting private and public funding to AI, or even wary of rapid adoption for whatever reason, could be accused of wanting the EU to become less sovereign, a vassal AI state. As outlined in the document, the more numerous and diverse the data gathered from AI, and thus the more diversified situations it is engaged in, results in an increase of training data and thus, the more training data the better the AI becomes.

An interesting feature of the AI diplomacy document is its portrayal and acknowledgement of AI as an enabler or a tool with multiple applications (*Ibid,* pp. 9), but specified individually toward the perfection of one task or problem, coupled with apparent anxiety about the lack of utilization by member states. If the companies of a state find no use for ML-enabled AI, it follows they won't invest or use it. The diplomacy paper then appears implicitly to endorse the idea that AI can and, more importantly, should, be used to do almost everything. This likely aligns with the White Paper's equivocation of efficiency with normative good, and therefore suited for use in all situations. Then, the White

Paper's anxiety surrounding the private sector's dominance of AI a paradoxical one, as it is the private sector which develops AI for most sectors' applications, and the private sector is even outsourced to by states for national security purposes (Ragazzi, Et al., 2021). There is clear anxiety about the effect of sovereignty due to "the rise in digital technology [which has led to] a significant rise in power of the private sector, *rivalling* the power of states" (*Ibid,* pp. 19-20). It is mainly the thrust of the private sector that is making AI ubiquitous across applications and industry, yet technology firms can be fickle and uncooperative as highlighted by Apple's refusal to provide a back door to the FBI (*Ibid,* pp. 20). The document also notes the problematic nature of many features of private firms such as surveillance capitalism (*Ibid,* pp. 20), without acknowledging that surveillance capitalism is the mechanism that improves AI, through the constant collection of data (Zuboff, 2019). This is a running theme in the AI diplomacy document, to acknowledge the symptoms of a problem or risk but not the cause. The cause is inconvenient for the goal of the paper, which is to spearhead AI as a geopolitical necessity and to convince that AI is a boon to all sectors of European society.

The tone of the document is less dispassionate than the White Paper and has a distinct feeling of anxiety. The feared speed of adoption by rivals and the use of AI to force the EU into a state of *dependence* and weakness clashes with the need to adopt the technology on a wide scale within the EU as quickly as possible. *Fear* and *concern* appear at least 40 times in the document. The section on AGI, or Artificial General Intelligence, injects a shock of existential fear and dread into a discourse that is otherwise focused on practical security and geopolitics, and serves to heighten a sense of anxiety around AI developed *irresponsibly* or *unethically.* A type of AI that would "make humans obsolete" (*Ibid,* pp.28), if created without regard to trust and ethics or a "value alignment" (*Ibid,* pp.29). Once again, we can see the document begin to approach what might be the fundamental problems with an EU wide focus and investment in

AI for all social problems, but it backs off after recognizing the symptoms. If AGI is such a *threat and risk*, why is the EU running full force in its direction?

In both EU discursive documents, *European values* are inherently tied to *fundamental human rights*, *trustworthiness*, and *ethics*. In order to maintain a sense of *Europeanness* the EU must maintain its face as a global norm setter in these areas. The document not only juxtaposes European AI against a more distinct one such as China, but also against the EU's most constant collaborator and ally, the US (*Ibid,* pp.35). Implying that the two most advanced AI states are not concerned with the ethics of their technology development is interesting from the standpoint of once again positioning the EU as a moral norm builder, while self-admittedly relying on the US for research and cooperation, especially in the security arena. If the EU, and member states, can become completely self-reliant in AI, *then* their AI will be *ethical* and *trustworthy*, (through regulation and concern for theses norms) because it is a *uniquely European (Ibid,* pp. 36*)* approach to technology. The document states that member states "have expressed scepticism about the extent to which Europe and the US are indeed aligned on ethical AI principles" (*Ibid,* pp. 36). However, was Europe to singularly advance toward *ethical* AI for commercial purposes, it is yet to be seen if those values and goals are compatible with the EU's other strategic goal of being a dominant force on the world stage in the advancement of AI. But, once again, this section on EU-US partnership serves to build a narrative with the EU as the central, norm building, protagonist.

Overall, in AI Diplomacy we can see several recurrent themes and patterns at play that align with those expressed in the AI White Paper. At the very centre of both documents is a focus on a distinctly *European type of AI*, which includes commitment to *ethical* regulation and implementation as well as the *trustworthy development* of the technology as a way toward their ultimate goal of speedy and widespread adoption. The documents use language of promise and

prosperity, but also notably of *fear and anxiety* about global competition and the consequences of being left behind by the US and China. When it comes to military applications, the EU is concerned about autonomous weapon systems (AWS), for ethical and legal reasons (*Ibid,* pp. 25) that are rooted in the technology, yet do not connect those concerns to other applications of the technology. The White Paper states that "Autonomous systems are problematic because they may lead to the delegation of decisions over life and death to machines and algorithms or create 'responsibility gaps' making it unclear who is responsible for mistakes' (*Ibid,* pp.25). This unclear delegation of responsibility is an issue with any application of AI in decision-making (the White Paper takes steps to recommend how to ensure responsibility is managed in some situations on page 19 (European Commission, 2020), but still does not link to more *high-risk* security concerns).

But the most troubling of these two concerns is the ethical quandary of allowing machines to make 'life and death' decisions. Of course, the battlefield is where literal life and death decisions may be made, but credit approval, movement regulation, job seeking, and other forms of social regulation can be equally life or death scenarios for individuals, they just have no consequence to states. The outcry from the EU as well as other international organizations such as the UN (United Nations Institute for Disarmament Research, 2018) show that institutions are aware of the 'risk' and problems that arise from use of AI in war, yet why does the same sense of urgency not manifest for other applications? Autonomous weapons may level the playing field in a way that causes more concern for states. That is, AI in other sensitive scenarios only uphold already oppressive forms of state control, and so do not evoke the same *fear* from governments and institutions (*Ibid*, 2018). This development of a dichotomy between *high risk* and *low risk* AI means that discursively it is difficult for those affected severely by lower risk applications to link their own experiences to this

more high-profile issue. Also, linking the two would slow the goal of a speedy adoption across Europe.

The themes and patterns present in both the AI White Paper and the AI Diplomacy study paint a picture of the type of world the EU is attempting to build mainly through the discursive power of official policy documents, and secondly through the discourse that AI as a set of technology creates. As AI itself is in a sense discursive and also serves, alongside the more conventional language of risk, to securitize. "All social structure is discursive in nature." (Jacobs, 2018, pp. 298) Therefore, practice and discourse are constitutive of each other. The development of risk analysis and management surrounding the use of AI in EU documents constitutes its practice in domestic and international security arenas. This could be strongly argued as the case for deep learning techniques used in AI, which mimic a simplified human brain structure. AI is composed of computer code, itself a type of language (or one of many coding languages), and that language structures the reality through which social decisions are derived by security practitioners. Through these two documents, we can see the EU attempt to merge the discourses of *risk* with those of technology and economy, to position AI as both an existential threat and as the EU's only saviour from that threat. I will now go on to analyse the further discursive implications of this move for areas of security policy which are becoming subsumed by applications of AI as the end all be all to solving or mitigating them. And while I chose to focus on one particular issue for analysis, it must be said that these factors are now playing in a variety of issues, and that discourse outlined above will only have increasing impact, as the goals of EU policy are realized.

Ch 4: Findings: The Impact on Policy Towards Women's Veiling Practices

It may seem like a long arc to take, from literature and theory into discourse, to then find a way to focus in on this issue. However, to have a complete consideration of one angle of the picture, I hope to demonstrate how the security issue is built upon multiple layers of decisions and technicalities. How technical, political, and theoretical factors come together to animate the reaction of the EU, and in a feedback loop the reaction of member states to Muslim women's veiling practices, is a complex task, utilizing the analysis of patterns in discourse, in artificial intelligence policy, and in law or rulings. The thread of findings stems not only from this more structured pattern finding and document analysis but also from an engagement with other disciplines' reactions to AI, as touched upon in the literature review. The wealth of literature from STS, sociology, and security, contribute to the underlying connections found between these findings. Furthermore, art and culture disciplines have much to say on similar topics, and unfortunately, they are beyond the scope of this dissertation but would be an interesting field for those who wish to seek out a wide scope of views.

Technology races have powered security policy and strategic competition between great powers before, and both EU documents explicitly frame AI development and deployment as an international competition. So it is worth looking at how other technology races compare to the current one in their effect on security. Once such game-changing yet controversial technology, the atomic bomb, has generated much discussion about the inherent *values* of the bomb, with one line of scholarship claiming that that they are *inherently* undemocratic due to their form and function (Pelopidas, 2019). Pelopidas quotes Daniel Deudney as writing "Nuclear explosives are intrinsically despotic for three related reasons: the *speed* of nuclear use decisions, the *concentration* of the

nuclear use decision in the hands of one individual, and the *lack of accountability* stemming from the inability of affected groups to have their interests represented at the moment of nuclear use" (*Ibid*, pp. 3). Similar arguments about AI application in security could be made. For AI, problems are; the *ubiquity* of AI use decisions (in that they are being applied to all security problems), the *concentration* of AI application in the hands of profit-seeking corporations or loosely regulated and isolated agencies (such as FRONTEX or the US Department of Homeland Security), and *the lack of accountability* of affected groups to have their interests represented in the training data and design of AI used *on and through them*. The undemocratic nature of AI is alluded to in the EU's notice of the particular efficiency and success of Chinese AI development (Franke, 2021, pp. 14). The attempt to have AI developed alongside espoused *European values* therefore, could be seen as paradox in this context as well. There will ultimately likely need to be some kind of compromise reached by EU institutions and member states on the extent to which they are prepared to become embroiled in a global AI race, if the trade-offs are European values (which include respect for democracy and human rights) and the needs of advancing the technology.

What kinds of current or future policy can we expect to see as an effect of the discursive power that securitizing tools have on policies in the EU? For a simple example, drawn from the AI Diplomacy document itself- a policy output that may emerge from the securitization of AI that the paper makes is a sincere recommendation for increasing the salary of AI engineers. If AI and the computer industry are considered "strategic assets" retaining the talent of already well-paid individuals in the face of even more exorbitant salaries in the US becomes a security concern. This means not only do both AI papers recommend funding increases for AI R&D, but they also view individual *talent* as key to "winning" the AI race technologically and geopolitically. This is an explicit recommendation of the EU, what I will do next is looks at how the

implicit ideas built in these documents around AI contribute to the securitization of another type of individual, positioned as almost a diametric opposite of the *strategically valuable, European*, AI *talent.*

To zero in on the focus of this policy section, I will look at the interaction between AI (and its associated surveillance dimension) and the host of anti-veiling policies that have sprung up around Europe and in EU countries. The policies are mostly geared towards preventing Muslim women from adhering to certain religiously prescribed forms of modesty which include different types of veils.

The way this issue is securitized is *related* to the use of AI in the EU not *because* of it. The cause is comprised of multiple factors, and direct movements in the politics in individual countries. Still, there is something that unites the individual member state policies, and that is the umbrella of the EU and its socio-political unity. The cultural and discursive image of the -veiled Muslim woman- looms large in policies that are allegedly aimed at ensuring public safety or preventing the appearance of any religious affiliation in business places or government institutions. There is a clear disconnect in appeals to neutrality born out by the fact that in many European states that claim religious neutrality, businesses and government institutions are still closed on Sundays, and workers are given time off on Easter and Christmas, so it isn't difficult to see why the actual intention of these policies are questioned, when their burdens fall predominantly on non-Christian individuals.

Conversations around banning full face veils or hijabs have come up in almost every EU country at some point or another. France has explicit policy against wearing full face veils in public (even after mask mandates were enforced), and restrictions of the hijab in establishments in Austria, Belgium, and Denmark also prohibit religious face coverings in all public spaces. Meanwhile the

Netherlands, Norway (though Norway is not in the EU), and Kosovo and Bosnia (on the docket for accession into the EU) have certain locations where they are banned. At a regional level, Italy, Switzerland, Germany, and Spain have okayed bans on the hijab as well as other garments that cover the face (BBC, 2018). The Court of Justice of the European Union (2021) has ruled that private employers are allowed to prohibit employees from wearing headscarves as long as they employ the prohibition of the display of religious belief across the board. It is worth interrogating the fact that this policy necessitates that employers know what all religious displays may look like, a reality which often rests on ignorance or stereotypes about non-Christian cultures. For example, how many employers would know what tzitzit(Jewish knotted ritual tassels) or tzinius (a principle guiding modest dress) looks like, and thus prohibit it? Contrast this with the fact that there is a large-scale knowledge (based on ignorance and stereotyping) about what a 'typical Muslim woman' looks like. Despite the fact that all these ways of dressing signify a high level of devotion to a religion, only one of these is securitized.

There are a myriad of cultural, historical, and political reasons for each state's engagement with this kind of restrictive legislation and general rhetoric. The post 9/11 global war on terror, the European migration crisis, cultural and historical discrimination towards non- Christians, individual member-state policy toward religion, and colonial mindsets are all contributing factors (Open Society Justice Initiative, 2022). My attempt here is not to simplify or show the "real" reason these measures are passed, but to consider how the simultaneous development of AI, as a particular securitizing tool, leads to a unique kind of securitization taking place. My own view, informed by the literature on the topic, as well as my own analysis of the securitization tools of the EU official documents, will be used to identify correlations.

To briefly show the connection, this has to a specifically gendered discourse. Feminist scholars of multiple disciplines use post-structural analysis to critique gender as a system of discourse and therefore practice (Lazar, 2005**), j**ust as science is in discourse analysis, and as I have done in the previous chapter. The engagement with science as "truth" instead of "discourse" plays an important role in how AI is talked about, as well as applied in security. The needs of AI as a technology, decree its policy objectives as objective security instead of a kind of politics and policy designed to specifically accommodate the expansion and privileging of a certain kind of discursive alignment. Now that we have seen how AI is used and presented in discourse as a critical tool for building and enhancing security discourses now enacted across the EU, we can see through the language and phrases used, despite how they differ, that the powerful visual and data technology at the fingertips of legislators and security professionals allow issues to become envisioned as solvable by AI. That is simply, security professionals and governors have acquired a very powerful hammer, but reality isn't a nail to be hammered down. Women are often the objects of security policy, and their agency largely goes unconsidered which makes them the perfect subjects of AI control.

The subject of AI enabled surveillance is not *strategically valuable,* is often not identified as European, and is transformed into a body in the sense she is decoupled from her humanity and her cultural and social context. Unlike the AI technology, which is humanized through the emphasis on its *choices, decisions, and behaviours*, the subject of surveillance is not afforded that humanity, and in fact the humanization of the AI is what triggers the dehumanization of the subject. Policy against shades of veiling for Muslim women have in the last 20 or so years become ubiquitous and a constant topic of politicking (Open Society Justice Initiative, 2022**)**. Sometimes couched in language about separation of church and state, or in fact a desire to protect women from oppression, nonetheless little input is sought from the target of these campaigns and policies.

Member states pursue bans on veils and are in turn supported by larger EU institutions such as the European Union Court of Justice, The European Commission, and the European Court of Human Rights.

Let us zero in specific instances of these of these laws and the EU institutional response to them. First, the French ban on face coverings in public spaces coupled with the ban on religious garments in government aligned institutions. *LOI interdisant la* dissimulation *du* visage *dans l'*espace public (Assemblée Nationale, 2010) or The Act prohibiting concealment of the face in public space and *LOI n° 2004-228 du 15 mars 2004 encadrant, en application du principe de laïcité, le port de signes ou de tenues manifestant une appartenance religieuse dans les écoles, collèges et lycées publics* (Assemblée Nationale,2003) otherwise known as Law #2004-228 of 15 March 2004, concerning, is an application of the principle of the separation of church and state, the wearing of symbols or garb which show religious affiliation in public primary and secondary schools. Both correspond with the French policy of *laïcité*, or secularism, and discussions about what *kind* of society France is to be. This is an internal and complex debate within France, and part of a discourse unto its own. However, we can see the voice of the EU in member state laws that relate to women's veiling practices by observing challenges to these laws at the EU level. Legal discourse is different from security discourse, in that it is contained within its own language or jargon, yet it is also a norm building discourse within the EU.

The EU courts have not always upheld member state laws that passively discriminate against Muslim women for wearing the veil (Open Society Justice Initiative, 2022), either full face covering or hair covering, yet it is illuminating to discuss how these laws, which some argue actively undermine *fundamental human rights,* are handled. Some cases brought by applicants affected by these laws have been dismissed by the European Court of Justice, and the European

Court of Human Rights have further upheld the laws as permissible. The language of the courts reflect the language in the AI discourse. I will highlight one particular case, *Case Of S.A.S. V. France* (2014), where the applicants appealed to the court through references to *European values* (*Ibid,* pp.19) by aligning them with tolerance and *multiculturalism.* The French government response to such a plea would likely be that *Republic (French) values* expressed in '"liberty, equality, fraternity" do not include *this kind of tolerance (Ibid, pp. 5).* The European Court of Human Rights approaches this case cautiously, and carefully considers the arguments presented yet still "sacrifices concrete individual rights guaranteed by the Convention to abstract principles." (*Ibid,* pp. 61).

The court makes its position clear on the alleged violations of rights, and within the argument are several interesting approaches to the positions of the French Law. In the case of this particular dissertation the point below offers an interesting insight into how European ideas surrounding the public visual space feature as central to security.

> "139. As regards the question of necessity in relation to public safety, within the meaning of Articles 8 and 9 (see paragraph 115 above), the Court understands that a State may find it essential to be able to identify individuals in order to prevent danger for the safety of persons and property and to combat identity fraud. It has thus found no violation of Article 9 of the Convention in cases concerning the obligation to remove clothing with a religious connotation in the context of security checks and the obligation to appear bareheaded on identity photos for use on official documents (see paragraph 133 above). However, in view of its impact on the rights of women who wish to wear the full-face veil for religious reasons, a blanket ban on the wearing in public places of clothing designed to conceal the face can be regarded as proportionate only in a context where there is a general threat to public safety. The

> Government have not shown that the ban introduced by the Law of 11 October 2010 falls into such a context." (*Ibid,* pp. 54-55)

This section of the ruling reflects both the position of the French government, that coverings of one's face in public constitutes a security risk, and the EU's answer, which is that the French government has not demonstrated *how* wearing a burqa or niqab in a general public space is the same as a specific security situation where someone is *asked* or notified of their identity being affirmed. Yet, the Court still finds claims of facial concealment in all public places a legitimate security concern, enough that even this *un-proportional* response can be left standing. I would argue this is due to the double-edged sword of the securitization of the expression of Islam in Europe as related to radicalism, and the suspicion of the unidentifiable face to the state security/technology apparatus. The European Court legitimizes the claim that obscuring identifiable features, even when going about in any random space, is a potential security *risk*. Without the unobscured face, surveillance technology, and thus AI technology, cannot do its job of mitigating risk. Both of these occurrences serve to further securitize the body of the Muslim woman in the EU context. It would serve readers of the case to understand *why* the court and the French government have come to the conclusion that an obscured face in public poses that risk from a technological perspective, as this is an assumption the Court of Human Rights does not make clear ontological support for in either majority or the dissenting opinions.

In a similar situation, the European Court of Human Rights ruled in favor of the Belgian government, that their own "veil ban" did not violate the European Convention on Human Rights (Library of Congress, 2017). The Loi du 1er juin 2011 visant à interdire le port de tout vêtement cachant totalement ou de manière principale le visage, or in English, the Law of 1 June 2011 to Prohibit the Wearing of Any Clothing That Hides the Face Completely or to a Significant Extent, is quite similar to the French Law. The ruling thus had similar

justifications for ruling against the aggrieved applicants, In *Dakir v. Beligium* (2017):

The European Court of Human Rights held, unanimously, that there had been:

> "no violation of Articles 8 (right to respect for private and family life) and 9 (right to freedom of thought, conscience and religion) of the European Convention on Human Rights, no violation of Article 14 (prohibition of discrimination), taken together with Articles 8 and 9 of the Convention, and a violation of Article 6 § 1 (right of access to a court)." (European Union Agency for Fundamental Human Rights, 2017)

This ruling also echoes a point made in *S.A.S v. France,* in making the argument that in some cases a state can be justified by the aim of promoting *living together* (*Dakir v. Beligium*, 2017). What is it that these member states see as incompatible with "living together" and that the Court agrees with? The Belgian Government outlines the opposing natures of covering the face and of "living together", which the European Court of Human Rights upholds and legitimizes.

> "The individuality of every subject of law (sujet de droit) in a democratic society is inconceivable without his or her face, a fundamental element thereof, being visible. Taking into account the essential values that the legislature sought to defend, it was entitled to take the view that the creation of human relationships, being necessary for living together in society, was rendered impossible by the presence in the public sphere, which quintessentially concerned the community, of persons who concealed this fundamental element of their individuality. Whilst pluralism and democracy entail the freedom to display one's beliefs, in particular by the wearing of religious symbols, the State must pay attention to the conditions in which such symbols are worn and to the potential consequences of wearing such symbols. To the extent that the concealment of the face has the consequence of depriving the subject of law, a member of society, of any possibility of individualisation by

> facial appearance, whereas such individualisation constitutes a fundamental condition related to its very essence, the ban on the wearing of such clothing in a public place, even though it may be the expression of a religious belief, meets a pressing social need in a democratic society." (*Ibid,* 2017)

This law and the subsequent EU institutional opinion is, therefore; that covering one's face is fundamentally at odds with *Europeanness itself.* The fact that an individual's face is necessary to democracy and society is an assumption that is not interrogated by the law epistemologically and has no real grounding It is not addressed. The Court backs up Belgium's case for this argument, that the covering of one's face does inhibit a vague *living together.* In hindsight, after the Covid-19 pandemic, when masking the lower face in public became mandatory, there does not seem to have been a complete crumbling of democratic societies. This strengthens the point that Muslim women's veils have undergone a unique type of securitization.

Discourse of community and *risk* are a thread through policy and rulings on policy, and feature in encompassing European Community, the precursor to the European Union. An *existential risk* to community is thus envisioned as an existential threat. How could the discourse of AI be seen to show similarities with the rulings of the Court? Furthermore, how would the EU support the claim that covering one's face, in any public space where individuals must *live together*, inhibits *security?* Theoretically, this can be approached by outlining the technological basis for security in public as contingent on AI analysis, and that in public is where individuals must *live together*, thereby drawing these two discourses together.

As discussed in the chapter using discourse analysis, while the EU in its AI documents does make cursory attempts to describe the structures and basis of AI, using machine learning models (such as DNN's), they fail to outline how

the technical limitations actually work when utilized in biometric and computer vision surveillance tools, to perform social functions. Abstractly, they discuss world changing effect of the technology, without outlining how AI actually improves social, economic, and security mechanisms, or why it is vital that that improvement is done the way it is. Rhetorically, it would be difficult to square the critical needs of the development of AI with aims of *ethical application and trustworthiness,* if they also had to carefully outline how much data was necessary and the viable avenues of collecting that data. The dehumanization of the surveilled and datafied subject is an intrinsic part of the use of AI, without it, and with the recognition of the subject as a full and complete individual, capable of making her own decisions including what to wear and when not to be seen, the development and implementation of AI would slow down or grind to a halt completely, both for practical and for discursive reasons.

Intrinsic to the functioning of AI, as we can see from both the EU's AI documents and from the scholarly literature, is the process of breaking down a piece of data into its segments that algorithms can analyse. They might be keywords, or edges, or colours, or pixels. The image or information contained within is dissembled. Components become the whole, which must be completely reconstructed on the other side of the neural network. This is not how a human analyses a situation and it is not a functional engagement with the *real* world. This is another world entirely that is being created wholesale on screens that security practitioners view and use to make further decisions. This returns us again to the rhetorical and mental device of the simulacrum. In this case, the simulacrum generated through AI surveillance leads to the annihilation of the *real* world for security practitioners, and then on through political actors attempting to make reality match this simulated version of the world they actually inhabit. For this reason, the dehumanized subject can be singled out and targeted as a *security threat herself*. Women who wear veils, in a way, stand

in the way of a complete simulation of security and the complete optimization of AI enabled risk discourse as a means of constructing security.

Notions of security and society are bound up in the visual field, in the need to be fully technologically visible. Concealment of any kind is *risky*, Women who are concealed are risky, both under possible threat (from the amorphous oppressive Muslim man enforcing the veil on her) and a threat to the European community by her suspicious refusal to unveil *herself.* The evasion of cameras and visual analysis is risky, as everywhere, everyone should be analysable by the *powerful and world-changing technology of AI. This manifests itself in the target of securitization.* The most actively targeted garment is the full-face veil, either a burka or a niqab, however very few women in Europe, relative to the size of the Muslim population, actually wear such coverings. So why do they loom so large in policy and discourse around veiling?

The technology of risk management, artificially intelligent surveillance systems, need visible faces to function and to advance. Not only is it very difficult for facial recognition systems to identify people in burqa and niqab especially with low quality visual sensors, but databases of training data also lack significant collections of women in various kinds of cultural Muslim veils (Alashbi & Sunar, 2020)**.** The act of covering one's face is, practically and symbolically, in direct opposition to EU goals to deploy AI in all areas of life rapidly. The burqa and niqab represent both the dangerous and risky "other" as well as the opposition to assimilation into *Europeanness* and allegedly stand in direct contrast to *European values.* What is interesting is the emphasis on the EU leading the way to an *ethical AI* through *trust* and its equation with transparency in relation to the EU stance on women who prefer to be literally opaque.

There is an equation with openness and *Europeanness* which obscures an inconvenient concept of privacy. Even in the EU policy documents, privacy is

prioritised not as the right not to have data collected, but as the right to know how your data is being used or to have its use controlled. The right to personal opacity does not exist in regard to AI, because doing so would make it obsolete. In order to reach the strategic position of AI dominance, values of privacy, modesty, seclusion, and separation from the public sphere must be made a risk, or a way of life incompatible with Europeanness. Ultimately the application of AI enabled technology heightens the impact of securitization of veiling in the European Union, leading, along with an array of complex factors, to the further marginalisation of Muslim women.

The European Union has a unique way of constructing and identifying security issues, and the specific language and terms used in official documents show ideological consistency and clear discursive development. This allows for an analysis, and to draw connections between the securitizing tools employed (both technical and policy oriented) and how they affect policies deployed by and throughout the Union.

Many scholars have done work on critiquing the place of technology in security situations, envisioning where to go with AI as a part of our politics and culture, and discussing the ethical implications of deployment of AI in commercial settings. Yet, critical approaches to AI cannot be seen in the official discourse of the EU. Critical approaches do not serve power, no matter how allegedly dedicated to *fundamental human rights* or *ethics* that power is. Approaches to security that elevate institutional power and already dominant power paradigms are still the main drivers of policy surrounding AI. Despite the opportunity for reimagining the future and security arena that emerging technologies such as AI present, and some recognition of that novelty (in the form of marginal policies protecting privacy from private companies), there is still a underwhelming tendency in discourse to envision AI alongside more conventional and entrenched security paradigms. The EU is, somewhat paradoxically, attempting

to build a discourse where it is a *trustworthy* norm builder and *ethical* regulator, while using technology and policy which have the effect of deploying securitizing tools that mainly impact the already marginalised.

When combining the findings of relevant literature with the discourse of the EU we can see how the language of risk, in concert with the very nature of the functioning of AI, serves to magnify the existential *risk* of certain behaviours or practices, due to their relation to those securitizing tools. We can also see how the *humanization* of AI in discourse, even beginning from the use of *intelligence* to describe how statistical models lead to outcomes, serves in the *dehumanizing* of subjects that are surveilled and rendered as data. When in official terminology, AI can *perceive*, *interpret*, *reason*, and *decide (*European Commission, 2018), that framing filters into national strategies, commercial documents, and common discussion, the distinction between human processes and machine processes are blurred, thus allowing the myth of scientific objectivity and truth that science imbues to assume power *over* human reasoning and objections (which are assumed to be subjective, and perhaps stemming from flawed culture or feeling).

Cultural and religious decisions do not operate according to the discourses of modern science and generate their own systems of meaning and values. One of the aspects of the issue that demonstrates the discursive power of AI to securitize, is the related policy focus on relatively infrequent practices which most symbolically and unflinchingly stand in the way of the societal values that AI need to function. AI can only progress through mass surveillance, and the complete covering of the human body, the retreat from modernism and secularism, and a refusal to become one with the masses mean that this practice and the practices that approximate its totality, such as wearing only a hair covering, are a repudiation of its core needs, and are treated as an existential threat to it and the new state built on that technology. AI drafts a simulacrum of

the world which has no relation to reality, and transposes that into the discourses and minds of security practitioners, one where going unseen is a risk and ultimately, a threat.

Undermining the goals of the EU to develop and deploy *ethical* and *trustworthy* AI, but supporting the aversion to risks of all kinds, is the technical reality of the way AI functions using machine learning techniques. These techniques have no relation to ethics, democracy, or human rights, they are statistical computer processes without values. Patterns can only be gleaned from mass amounts of data, collected with the incomplete knowledge or total ignorance of individuals, which is then bounced through neural layers trained on an unverified collection of data. The outcomes of which are then enforced into the social world.

Fundamentally, AI is a statistical technology which can only reinforce and replicate the outcomes of past events and knowledge, it contains no possibility for the future or for imagination. By reinforcing the past onto the future, unknowable risks may certainly be mitigated, but by confining human politics and society to the biases and hierarchies of the past, the *reality* of the world AI claims to interpret and act upon is destroyed before it comes to exist. “The crisis consists precisely in the fact that the old is dying and the new cannot be born; in this interregnum a great variety of morbid symptoms appear.”. This quote, attributed to Italian communist Antonio Gramsci (1971, pp. 276.), is used to describe the rise of fascism and breakdown of social order in the interregnum between the capitalist order and a realized (or indefinitely unrealized) communist future, and can be interpreted as pertaining to the breakdown of liberal order (Milan, 2020). However here I think it serves to help highlight a building crisis forged by AI’s application in security. A security space where old *risks* can rapidly become outdated or where focuses are constantly evolving, the pattern seeking and replicating nature of AI can reject them as outliers, or simply not recognize them for the same significance as human reasoning would,

thereby reenforcing an old security paradigm that is inescapable due to overreliance on technology.

Having AI subsume not only our security, but our way of doing politics and society, means we will forever be trapped by the limitations of this one kind of technology, as is becoming clear in the EU's articulation of policy outcomes of the last decade or so. The future becomes trapped in the coded enforcement of algorithms, leading to a breakdown between the world projected by AI and the real world. "Morbid symptoms" such as the weakening of institutions, social cohesion, and political strife are a part of the current European milieu, and AI plays a part in that milieu. Adversarial examples, opacity, and other limits point to a real problem in deep learning techniques, especially when it comes to the implications they have for social and political applications. While many researchers are attempting to remedy these limits through various new approaches (Waldrop, 2019), perhaps in an attempt to reach something closer to a general intelligence, no matter how advanced AI systems become, replacing or even supplementing human reasoning in security decision making, is a precarious road to walk

It is also worth asking what the actual value of inserting AI into security situations is and who benefits from it? Once again, the question of *security from what and security for whom?* If the EU is claiming that AI will increase security for *states* and place member states in a better strategic position, then that may be true. But if the EU is truly focused on *ethical and trustworthy* AI security and claims that AI provides better security for *Europeans*, then that claim requires further interrogation, and to a larger extent, the assertion that AI in all areas of life will actually make European citizens lives *better* not just more *efficient or convenient*. The trade-offs must be considered as privacy in public and in one's own body continue to erode, despite the claims of values of *ethics* and *trust.*

When it comes to condemning the complicity of private technology companies, the AI White Paper identifies this as a distinctive European angle for companies that want to position themselves as in opposition to authoritarianism or out of control surveillance capitalism, but functionally, what will be the difference for individuals? Can the EU compete with China and the US to a degree where these norms are powerful enough and pervasive enough to affect the vast majority of AI companies that operate out of these two allegedly less ethically minded states? Furthermore, if the reason that companies from the US and China are able to generate more cutting-edge technology is that they operate under more lax values, it may be that *European values* undergo an accommodation that allows for the EU to compete with these two tech giants. The private sector plays an outsized role in the development and implementation of AI enabled technology in the public sector, and the ability of the EU to enforce norms of ethics and respect for human rights will hinge on the trade-off between what is profitable for companies and what respects the rights and humanity of European citizens.

Some limitations of this dissertation are that I can draw no concrete cause and effect between AI discourse and Veiling Policy, not that I intend that to be result of the dissertation, but I can't point to a political saying "this policy is x because of y". Furthermore I can only read information printed in English, so documents written in another EU language or which uses language differently cannot be taken into account. As my methodology rest on the construction of language, the entire method is limited by my only speaking English fluently, and my own training and ability to analyse the language. I have a limited ability to analyse the computer science of Machine Learning and AI models, as I have no training in building or working with the technology. I can only analyse it from a situation within the perspective of the social sciences. Despite this, there is ample scholarship from social scientists who do meaningful and accurate work on the

topic of technology without being able to code or build computer programs themselves. However, I have done my own research on deep learning models in various areas, such as generative adversarial networks (GAN's, which are a very interesting area if the reader happens to be interested in art), in order to gain a broader understanding of the field outside of security applications. Assumptions that underpin my work are as follows; the European Union is a coherent discourse and norm generator, despite the nature of its various member composition; AI is employed in security mostly on a population that does not fully understand the implications; AI technology serves those in power, yet it contains the potential for alternative applications; and most importantly, AI is a value neutral tool, but its mechanisms and inner workings do lead to certain kinds of behaviours on the part of developers and implementors.

Further questions raised by this research are; does AI affect the discourse of other international bodies and individual states. It would be interesting to see if other branches of the EU talk about AI in differing ways. Securitization is easily applied in a European context, as that is where the theory originates, but it would be interesting to see the various securitizations on other contexts, such as the U.S. or China. It would also be interesting to explore the impact on other gendered, politicized, or securitized issues that are distinct to other states.

As Europe comes to operate completely using AI as stated in official documents as an intended outcome, practices that repudiate those values and discourses become an *existential threat* to Europe. While I chose to focus on Europe in this dissertation, I hope that the mechanisms of similar processes can be identified in any state where AI becomes a central focus of security and economy. Because this securitization is thrust from AI technologies, a trend of securitization for the sake of AI optimization will likely become apparent going forward in most technologically advanced states. This should not be taken as a kind of anti-tech stance on my part. It is only an observation about the discourses being built

around it, and a caution against making it central to security and social processes without understanding how technology/science privileges the power of already extant hierarchies and reinforces marginalities and is not in any way an objective arbiter of "truth". The unique type of securitization carried out as a result of AI's utilisation in surveillance as security is evident from the various angles of analysis. It will be interesting to see how Europe's thrust towards AI manifests, and if its alleged values will remain a key point going forward.

Bibliography

1. Alashbi A.A.S., & Sunar M.S. (2020) “Occluded Face Detection, Face in Niqab Dataset”. In: Saeed F., Mohammed F., Gazem N. (eds) *Emerging Trends in Intelligent Computing and Informatics*. IRICT 2019. *Advances in Intelligent Systems and Computing,* vol 1073. Springer, Cham. https://doi.org/10.1007/978-3-030-33582-3_20
2. Anderson, K. and Waxman, M. (2017) “Debating Autonomous Weapon Systems, Their Ethics, and Their Debating Autonomous Weapon Systems, Their Ethics, and Their Regulation Under International Law Regulation Under International Law”, in Brownsword, R., Scotford, E., and Yeung, K. (ed.) *The Oxford Handbook of Law, Regulation and Technology*. Washington D.C.: Oxford University Press, pp. 1097-1117.
3. Aradau, C and Blanke, T (2017), “Politics of prediction: security and the time/space of governmentality in the age of big data”, *European Journal of Social Theory*, 20(3), pp. 373-391, doi:10.1177/1368431016667622.
4. Aradau, C. & Blanke, T. (2018) "Governing others: Anomaly and the algorithmic subject of security", *European journal of international security,* 3(1), pp. 1-21.
5. Aradau, C. & Bunz, M (2022) “Dismantling the apparatus of domination?: Left critiques of AI”, *Radical Philosophy* 212: pp. 10–18. Available at : https://www.radicalphilosophy.com/article/dismantling-the-apparatus-of-domination#fnref7
6. Assemblée Nationale (2010) *LOI interdisant la dissimulation du visage dans l’espace* public available at: https://www.assemblee-nationale.fr/13/ta/ta0524.asp
7. Balzacq, T. (2008) "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies", *Journal of common market studies,* 46(1) pp. 75-100.
8. Balzacq, T. et al. (2015) “What kind of theory – if any – is securitization?”, *International Relations*, 29(1), pp. 96–96. doi: 10.1177/0047117814526606.
9. BBC News (2018) The Islamic veil across Europe. *BBC News Europe*. Available at: https://www.bbc.co.uk/news/world-europe-13038095

10. Bigo, D. (2014) "The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts", *Security Dialogue*, 45(3), pp. 209–225. doi: 10.1177/0967010614530459.
11. Boulanin,V., Saalman, l.,Topychkanov,P., Su, F., and Peldán Carlsson, M. (2020) 'Artificial Intelligence, Strategic Stability and Nuclear Risk'. *SIPRI*. Sweden
12. Bunz, M. & Meikle, G. 2018, *The internet of things,* Polity Press, Cambridge.
13. Burrell, J. (2016) "How the machine 'thinks': Understanding opacity in machine learning algorithms". *Big Data & Society*. Available at: http://journals.sagepub.com/doi/10.1177/2053951715622512.
14. Buzan, B., Wæver, O., & Wilde, J.d. (1998) *Security: a new framework for analysis*, Lynne Rienner Publishers, Inc, Boulder, Colorado.
15. Cambridge Dictionary. *Algorithm.* Available at: https://dictionary.cambridge.org/dictionary/english/algorithm
16. *CASE OF S.A.S. v. FRANCE* (2014) European Court of Human Rights
17. Court of Justice of the European Union (2021) *PRESS RELEASE No 128/21* Luxembourg,
18. *DAKIR v. BELGIUM* (2017) European Court of Human Rights. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175660%22]}
19. Dick, P.K. (2007) *Do androids dream of electric sheep?* Gollancz, London.
20. European Commission (2020) WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust. Brussels
21. European Parliament (2018) General Data Protection Regulation (GDPR), Official Journal of the European Union Available at: https://gdpr.eu/article-4-definitions/
22. European Union Agency for Fundamental Human Rights (2017) Belgium / ECtHR / Application no. 4619/12 / Dakir v. Belgium. Available at: https://fra.europa.eu/en/databases/anti-muslim-hatred/node/6823
23. Franke, U., (2021) Artificial Intelligence diplomacy | Artificial Intelligence governance as a new European Union external policy tool, Study for the special committee on Artificial Intelligence in a Digital

Age (AIDA), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.
24. Gebru, T. (2020) “Race & Gender” In: Dubber, M.D., Pasquale, F. & Das, S. (eds)*, The Oxford handbook of ethics of AI* Oxford University Press, New York.
25. Gee, J.P. 2(014) *How to do discourse analysis: a toolkit,* Second edn, Routledge, Abingdon, Oxon.
26. Goodfellow, I., McDaniel, P. & Papernot, N. (2018) “Making machine learning robust against adversarial inputs”, *Communications of the ACM,* [Online], vol. 61(7), pp. 56-66.
27. Gramsci, A., Hoare, Q. & Nowell-Smith, G. (1971) *Selections from the prison notebooks of Antonio Gramsci,* Lawrence & Wishart, London.p. 276.
28. Green, B., Hu, L. (2018) “The Myth in the Methodology: Towards a Recontextualization of Fairness in Machine Learning.” *Machine Learning: The Debates workshop at the 35th International Conference on Machine Learning* (ICML).
29. Hansen, L. 2011, "The politics of securitization and the Muhammad cartoon crisis: A post-structuralist perspective", *Security dialogue*, 42 (4/5), pp. 357-369.
30. High-Level Expert Group on Artificial Intelligence (2019) A Definition Of Ai: Main Capabilities And Disciplines. European Commission: Brussels
31. Human Rights Watch, (2019) “How Mass Surveillance Works in Xinjiang, China”, May 2, Available at:https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang (Accessed July 20)
32. Jacobs, T. 2018, "The Dislocated Universe of Laclau and Mouffe: An Introduction to Post-Structuralist Discourse Theory", *Critical review, New York, N.Y.,* v30(3-4) pp. 294-315.
33. Jinghan Zeng, (2021) “Securitization of Artificial Intelligence in China”, *The Chinese Journal of International Politics*, 14(3), pp. 417-445, https://doi.org/10.1093/cjip/poab005
34. Kam, S. Clarke, M. (2021) Securitization, surveillance and ‘de-extremization’ in Xinjiang, International Affairs, 97(3), pp. 625–642, https://doi.org/10.1093/ia/iiab038
35. Larson,J, Mattu,S, Kirchner,L, and Angwin, J (2016)How We Analyzed the COMPAS Recidivism Algorithm, *ProPublica* Available

at: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm
36. Lazar, M.M. 2005, *Feminist critical discourse analysis: gender, power and ideology in discourse,* Palgrave Macmillan, Basingstoke, Hampshire.
37. LeCun, Y., Bengio, Y. & Hinton, G. (2015). Deep learning. *Nature* 52**1,** 436–444 https://doi.org/10.1038/nature14539
38. Library of Congress *(2017) Belgium/European Court of Human Rights: Ban on Full-Face Veil in Public Does Not Violate European Convention on Human Rights*. Web Page. Available at: www.loc.gov/item/global-legal-monitor/2017-08-30/belgiumeuropean-court-of-human-rights-ban-on-full-face-veil-in-public-does-not-violate-european-convention-on-human-rights/
39. Marx, G.T. 2017, *Windows into the soul: surveillance and society in an age of high technology,* The University of Chicago Press, Chicago.
40. Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think.* London: John Murray.
41. McCarthy, J. (2007) 'What is Artificial Intelligence?' Stanford University
42. Milan, B. (2020) Let's talk about the interregnum: Gramsci and the crisis of the liberal world order, *International Affairs*, 96(3), Pp. 767–786, https://doi.org/10.1093/ia/iiz254
43. Mozur, P. , Xiao, M., & Liu, J. (2022) An Invisible Cage': How China Is Policing the Future, *The New York Times*. June 25. Available at: https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html (Accessed July 20)
44. Murgia, M. (2019) How London became a Test Case for Using Facial recognition in Democracies, *Financial Times,* August 11. Available At: https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959 (Accessed July 20)
45. Open Society Justice Initiative (2022) Restrictions on Muslim Women's Dress in the 27 EU Member States and the United Kingdom. Open Society Foundation: New York
46. Pelopidas, B. (2021) **'**The birth of nuclear eternity*',* in *Futures* Edited by S. Kemp and J. Andersson. Oxford, Oxford University Press
47. Ragazzi, F. Et al., (2021) Biometric and Behavioural Mass Surveillance in EU Member States: Report for the Greens/EFA in the

European Parliament. Available at: https://www.greens-efa.eu/biometricsurveillance/#
48. Roberge, J. & Castelle, M. 2021, *The cultural life of machine learning: an incursion into critical AI studies,* Palgrave Macmillan, Cham, Switzerland.
49. Stachowitsch, S. & Sachseder, J. (2019) "The gendered and racialized politics of risk analysis. The case of Frontex", *Critical studies on security,* 7(2), pp. 107-123.
50. Thorpe, J. (2021) Understanding China Is Getting Harder Every Month", *Foreign Policy*. Available at: https://foreignpolicy.com/2021/05/27/china-expels-foreign-journalists-crackdown-transparency/
51. United Nations Institute for Disarmament Research, (2018) Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies. United Nations, Geneva, Switzerland
52. United States Department of Defense (2018) Summary Of The 2018 Department Of Defense Artificial Intelligence Strategy, Washington D.C.
53. Waldrop, M., M. (2019). 'What are the limits of deep learning?' *Proceedings of the National Academy of Sciences of the United States of America 116*(4).
54. Wilcox, L. (2017) 'Drones, Swarms and Becoming-Insect: Feminist Utopias and Posthuman Politics', *Feminist Review*, 116(1), pp. 25–45. doi: 10.1057/s41305-017-0071-x.
55. Wilcox, L. (2017) "Embodying algorithmic war: Gender, race, and the posthuman in drone warfare", Security Dialogue, 48(1), pp. 11–28. doi: 10.1177/0967010616657947.
56. Wood, D.M. (2009) "The `Surveillance Society: Questions of History, Place and Culture", *European journal of criminology,* 6(2), pp. 179-194.
57. Youngs, G. 2008, "From Practice to Theory: Feminist International Relations and 'Gender Mainstreaming'", *International politics (Hague, Netherlands),* vol. 45, no. 6, pp. 688-702.
58. Zeng, J. 2(022) *Artificial intelligence with Chinese characteristics: national strategy, security and authoritarian governance,* Palgrave Macmillan, Singapore.
59. Zuboff, S. (2019) *The age of surveillance capitalism: the fight for the future at the new frontier of power,* Profile Books, London