International Institute of Social Studies

Erasmus

FROM 'KILLER ROBOTS' to AUTONOMOUS WEAPONS SYSTEMS (AWS)

A sociotechnical analysis of the role of actors and practices in relation to development of AWS

A Research Paper presented by:

Ankita Surabhi

India

In partial fulfilment of the requirements for obtaining the degree of

MASTER OF ARTS IN DEVELOPMENT STUDIES

Major:

Human Rights, Gender and Conflict Studies: Social Justice Perspectives

SJP

Specialization: **Conflict and Peace Studies**

Members of the Examining Committee:

Shyamika Jayasundara Smits

Jeff Handmaker

The Hague, The Netherlands

December, 2019

Disclaimer:

This document represents part of the author's study programme while at the International Institute of Social Studies. The views stated therein are those of the author and not necessarily those of the Institute.

Inquiries:

International Institute of Social Studies
P.O. Box 29776
2502 LT The Hague
The Netherlands

t: +31 70 426 0460
e: info@iss.nl
w: www.iss.nl
fb: http://www.facebook.com/iss.nl
twitter: @issnl

Location:

Kortenaerkade 12
2518 AX The Hague
The Netherlands

Contents

List of Tables

List of Appendices

List of Acronyms

AI	Artificial Intelligence
AMR	Autonomous Military Robots
ANN	Artificial Neural Network
AS	Autonomous Systems
CCW	Convention on Conventional Weapons
CIA	Central Intelligence Agency
CIWS	Close-In Weapon System
CSKR	Campaign to stop Killer Robots
DARPA	Defense Advanced Research Projects Agency
DL	Deep Learning
DLANN	Deep Learning Artificial Neural Network
DMZ	Demilitarized Zone
DoD	Department of Defense
EC	Epistemic Community
FLI	Future of Life Institute
GGE	Group of Governmental Experts
GPS	Global Positioning System
HRW	Human Rights Watch
ICRAC	International Committee for Robot Arms Control
ICRC	International Committee for Red Cross
IDF	Israel Defense Forces
IHL	International Humanitarian Law
IHRL	International Human Rights Law
IR	International Relations
ISLMUN	International School of London Mock United Nations

ISR	Intelligence, Surveillance and Reconnaissance
ISS	Institute of Social Studies
JAIC	Joint Artificial Intelligence Center
JEDI	Joint Enterprise Defence Infrastructure
MIC	Military Industrial Complex
MIT	Massachusetts Institute of Technology
NATO	North Atlantic Treaty Organization
NLP	Natural Language Processing
PC	Private Companies
RL	Reinforcement Learning
RnD	Research and Development
SCOT	Sociology of Technology
ST	Securitization Theory
TNO	Netherlands Organisation for Applied Scientific Research
UCAS	Unmanned Combat Air System
UK	United Kingdom
UN	United Nations
UNDIR	United Nations Institute for Disarmament Research
USA/US	United States of America

Acknowledgement

There are a number of people I would like to acknowledge who have contributed in the successful completion of this research.

I extend my deepest gratitude to my supervisor, Dr. Shyamika Jayasundara-Smits who chose to undertake this research with me, which was borne out of pure fascination with technology. She has been a guiding force in keeping this paper tethered to academic standards, which I only hope I have successfully delivered.

My Reader, Jeff Handmaker, who was patient and encouraging during our few brief encounters and for the excitement he expressed towards this research.

I am indebted to the candour of my Respondents who patiently engaged with me and gave me a crash course on the Markov Decision Process. I shall never forget.

Most importantly, my friends here at ISS, have been a rock and a shelter and pulled me through some rough patches, every time I tended to fell astray. For that, I am eternally grateful.

Last, but never the least, I thank my family who have never faltered in their belief in me. I hope to make you proud.

Abstract

Using Sociology of Technology, this paper analyzes Autonomous Weapons Systems as a constructed artefact by enumerating the military, private companies and, developers and researchers in Artificial Intelligence, as the relevant social actors, whose roles and practices are indispensable to the imagination, designing, acceptance, distribution and use of AWS, because of the growth of AI. In this layering, military has the power to use the weapon, AI community has the expertise in the form of AI and the public companies are mediators between the two. Empirical data was collected from a weapons exhibition and from interviews with AI developers and researchers, to deconstruct the nature of relationships between them and independent of each other. To further its agenda military plays the role of an epistemic community and security actor, to enable private companies to become security enactors and knowledge brokers in a symbiotic relation. AI community independently develops AI relevant to the military. As social and security actors, their imperative to make knowledge objective is flawed because the human element of technology can never be removed, and because of their dispersed specialization this community can become appropriated just like AI.

The threat of AWS and bad AI is causing emergence of an epistemic community of the bulwarks of AI industry driven to shape society in a futurist sense by making technology safe for humanity. AWS have a flexible character unlike a nuclear weapon, which keeps the options for their use wide open. Knowing that AI is only a tool actors are working to stabilize it by redefining it, polishing it and enabling the continuity of its use, which is making it feasible for use by the military. The narrative around AWS is creating a technological paradigm based on the potential of its use by companies and countries. Lastly, the Military Industrial Complex has grown to acknowledge and accommodate AI community which is transforming it from all directions, and diversifying it, which means a nascent version of AI or AWS has already entered the business of war.

Relevance to Development Studies

Technology is inextricably linked to development and AI is a multi-stable technology with applications spread across the digital and the physical realm (Bughin and Manyika, 2018; McKendrick, 2018). The growth of AI has been lauded as one of the development drivers and several countries have launched official AI-development strategies in a veritable race to become world leaders. As of 2018, 24 countries had national plans to integrate "AI policy with scientific research, talent development, skills and education, public and private sector adoption, ethics and inclusion, standards and regulations, and data and digital infrastructure" (Dutton, 2018), in which security ranks high on the policy agenda.

Technological innovation has always brought advantages, provisioning radical superiority for the *party in its possession* (Perlinski, 2017; 7). From nuclear weapons as 'state of the art' in weaponizable technology during the Cold War, the 21st century is powered by AI. To this, Vladimir Putin, prophetically pronounced that "whoever becomes the leader in this sphere (AI) will become the ruler of the world", triggering speculations regarding a global AI arms race which according to some is already underway, looking at the massive spike in defence budgets of nations, the unambiguous agreement over "autonomous weapons, crucial to military strategy" and the subsequent scaling of resources for development of weapons (Bartlett, 2019).

In recent times, security concerns have increasingly become related to development, by redefining root causes of disruption/conflict as 'conditions ideal for causing breakdown' to intervene in poverty reduction, institutional rearrangement and economic reforms. (Chandler, 2007; Stern and Ojendal, 2010). In this formulation, lack of development can be defined on any scale in any field and can become an "exercise of rhetoric in the pursuit of power" to "mediate experimental governance beyond national boundaries" (Reid-Henry, 2011; 100). AWS belong to the category of weapons which are unhindered by geography, while their development is both, justified and driven by security. The weapons industry is also a significant indicator of the state of an economy, even though direct correlations or causal mechanisms cannot be established on account of paucity of data (Broude et. al, 2013), but that does not diminish the research value in pursuing linkages and exposing them. This is because *"defense expenditures are more like public investment likely to affect private-sector productivity for private investment*" (Barro, 1991, p. 430). In bringing support from the private sector, who operate across borders, "boundaries between us and them (civil/uncivil, mor-

al/amoral, etc.)" are fluid and deployed under the security-development nexus formulation (Buur et. al., 2007; 14).

The development of AWS has global significance because of their cause-effect relationship with society, technology and in the formation of our immediate future. "As the study of security and insecurity becomes mainstream, diffuse and pervades development, issues that formerly were part of development are taken into the realm of security concerns and IR research, such as ontological security and cyber-security" (Hintjens, 2019). They are becoming part of critical security and development studies, due to their impacts analyzed by Wilcox, in the feminist framework with "drone assemblages which incorporate modes of embodiment from algorithmic, visual, and affective technologies that enable the individualization of gendered, racialized targets" (2017; 24). The global mood today is one of anxiety and fear pushing largely problematic and potentially dangerous practices to the fore, forcing an inexplicable turn in international norms that need methodological analysis instead of essentialist assumptions (Hellman et. al, 2014). The rampant and now-infamous use of drones by CIA during the Obama administration are riddled with questions, yet controversial targeted killings continue to be carried out (Sterio, 2012). The method of these operations ignited a turn towards a socio-political climate caught up in the throes of a post-human warfare articulated by the use of AI, where strategic decision making is encased in uncertainty and outcomes are unpredictable (Mitzen, 2006; 272).

Development strategies today, account for interdisciplinary approaches undertaken to assimilate broad emerging practices and perspectives functional at multiple levels. Technology in many ways is an actor on its own, mediating professional, social, regional and global relationships. As they change the nature and pace of development their commonplace occurrence becomes subsumed in our evolving cultures, sparking debates on all fronts, legal, ethical, social. AWS take these debates to another level, beginning with the use of drone technology, described by Chamayou as the 'eye of god', in his book 'Drone Theory', a rigorous polemic on changing global affairs and military discipline (2015). AWS raise peculiar dilemmas highlighted by various national and international organizations that have called it a game-changer, and part of their concerted efforts led to the formation of the GGE at UN CCW. Most pertinent issues are related to the relationship between society and technology, including individual action that can have far-reaching consequences in the globalized, interconnected world where power and technology is highly decentralized.

Then this research is relevant "to explore the overarching mechanisms of control emerging even from civilian spaces" (Surabhi, 2019; 2), to highlight the "uncertainty, unpredictability and the gradual erosion of the modern belief that we could indeed simply move on, assisted by science and technology, towards a condition where instrumental rationality would become the linchpin of government and human interaction irrespective of difference" (Jabri, 2006; 47).

Keywords

Autonomous weapons systems (AWS), Artificial Intelligence, sociology of technology (SCOT), security, epistemic communities, knowledge

1 Introduction

As long as humans have waged war, they have improved their methods of violent engagement. "The history of modern weaponry involves the construction of the technological capacity to produce lethal results while posing the operator to the least amount of risk of death or injury" (Ohlin, 2017; 15). Our weapons have changed from primitive tools which required on-the-spot thinking and acting to intelligence and data gathering which makes combatants out of soldiers, even before they reach the battlefield. This is the realm of Artificial Intelligence (AI) and their revolutionary power in making weapons smarter, faster, cheaper and more efficient. Although conventional weapons remain, that requires a human being to push a button or pull the trigger, emerging discussions today, pertain to the development, use and threat of "killer robots". These are non-biological entities to be used as weapons in war, albeit instead of a human being, they fulfil most of the task previously delegated to human beings, such as targeting, killing, maiming, destroying or attacking. Thus, the emphasis moves beyond physical aspects to what they represent, an interactive operative with sensors instead of five senses. Such a robot has yet to take its first steps in the battlefield. But, Autonomous Weapons Systems or weaponized systems with varying levels of autonomy may already be here. Conceptually, they are "weapons that, once activated, can select and engage targets without further intervention by a human operator" (DoD, 2016). This definition is similar to that used by the Geneva Academy and HRW, with minor variations using "human override" and "deliverance of force without human input or interaction", respectively (Henderson et al, 2017; 339). Simply, "Autonomous Weapons are weapon systems equipped with AI" (Verdiesen, 2013; 13). AWS are poised to become the new frontier in warfare, in being able to determine *which target will be selected* and the *actual attack function that results in the use of force*" (Ekelhof, 2017; 313). While questions regarding dangers of technology on the battlefield aren't new, the "endless quest to defeat adversaries more effectively has accelerated innovation and given rise to a new era of remote warfare" (Henderson et al, 2017; 335). AI's human-like cognitive capabilities have captured the imagination and aspirations of a range of actors, in paradigm-producing ways that are willing to invest in the potential of AI. This is the entry point for this research; it requires an understanding of AI.

AI is a type of technology which exhibits or demonstrates human characteristics, in an intelligent manner. Intelligence here means, the ability to perform certain sets of tasks, simple and complex, reason and react with the environment and learn from past interactions. Also known as machine intelligence, it is theory and development of computer systems able

to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.[1] The primary objective of development of AI is to make life better for humans (Google) which leads to its classification as "*practical AI,* associated with technical progress; and *fundamental AI* which is social, economic, psychological, philosophical and political implications of AI use" (Burton and Soare, 2019). More recently, definitions have begun to shift in accordance with the goals trying to be achieved, namely "systems that think exactly like humans do ("strong AI"), weak AI: without human reasoning", and "human reasoning as a model but not necessarily the end goal" which is the emulative character of AI and the blueprint for its growth (Marr, 2019). Button distinguishes it from frozen software which requires updates. AI uses deep learning through "Artificial Neural Networks (ANNs), which is software loosely modelled after the neuronal structure of the mammalian cerebral cortex" (2017). At present, *fundamental AI* or *Artificial General Intelligence* (AGI) is currently absent. So, while AI completes human tasks, awareness or consciousness of the meaning and implication of such actions is absent. On this, Henry Kissinger said "we are in the presence of a potentially dominating technology in search of a guiding philosophy" (2018). AI has become synonymous with technological culture to the point where questions about its expanding capabilities are reopening discussions on human values and emotions, which are uniquely manifested in the use of weapons in the battlefield.

1.1. Context

Commercial AI is the hotbed for revolutionary leaps, like image/face and voice recognition to amplify user-experience. Increased technology has also impacted skills, behaviour and habits, having expanded the limits of human-machine interaction by introducing quickly modifiable and replaceable interfaces. The algorithm used in spam filters, YouTube recommendations; speech and handwriting translation and search engines employ advanced AI and ML.[2] Japan is the ideal example of AI's versatility; being used in physiotherapy, household chores, assisted elderly living and managing transportation.[3]

AI is a game-changer in inaccessible regions, like disaster relief operations[4] by using predictive mapping and environmental conservation (PwC, 2018), whereas AI in sentiment

[1] https://www.information-age.com/what-is-artificial-intelligence-123475331/
[2] https://becominghuman.ai/10-powerful-examples-of-ai-applications-553f7f062d9f
[3] https://medium.com/next-level-german-engineering/of-values-robots-and-trains-five-souvenirs-from-japan-b238d7514735
[4] https://singularityhub.com/2019/04/12/ai-and-robotics-are-transforming-disaster-relief/

analysis, object detection/classification, DL on structured data and tracking, provides cost-effective solutions in the vein of social justice (Chui et al, 2018). Hackers and developers in cybersecurity have made profound impacts because automation has increased remote control over physical systems, with magnificent and daring implications in security. Critical infrastructures that have faced cyber-attacks, like nuclear power plants, guarantee attention because they expose the rustic structures of security, which are faltering in the presence of AI's audacious nature, as bundles of data can disappear without a trace[5], and centrifuges can be brought to a standstill without resorting to espionage.[6] In return, AI-based systems have also been exposed and their algorithms hacked to steal information from territorially-unbound online datasets or by "analysing satellite imagery to allow highly sophisticated attacks to be carried out" (Greenberg, 2017). The dual-use capabilities of AI are well-documented and problematized in their application post-9/11 in security and surveillance architecture (Ceyhan, 2008; Malik, 2012), through 'technologization' where technology 'does' something having been constructed, thus lacking neutrality. The use of algorithms for predictive policing or machine justice, denotes how (in) security is manifested in the dispositions of actors, like the military and police, who rely on 'Big Data' and algorithms to generate contexts. The multi-polarity of narratives on AWS incorporates these problems, some of which are addressed in this paper. On the one hand, AI has ushered a geopolitical revolution but at the top of "new technologies that promise significant strategic advantages" it has introduced mechanisms to "upset balances of power or disrupt previously stable global governance arrangements" (Maas, 2019; 285). In the institutional setup of global industrialization, weapons, their manufacture and sale are one of the surest indicators not only of nations' economic strengths, but also their domestic and foreign policies; which greases global value chains, competing interests and their proclivity to extract the best from everywhere, and make it profitably marketable.

The road to development of any weapons systems is lengthy involving a continuous tenuous process of assessment, evaluation and redirection at the development stage to achieve technological superiority. Typically, AWS are discussed on their effects as solitary entities and as non-conventional weapons with risks and rewards because of the 'human-out-of-the-loop' (Brown, 2016; Schmitt and Thurnher, 2013; Petman, 2017). Hence, the

[5] https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

[6] https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/

projection is, AWS are superior to conventional weapons on account of AI, and more complex because its autonomous function would be a product of several interacting networks, at micro and macro levels, which are heterogeneous, yet, seamless in operation. In conceptualizing AWS as artefacts, the creation of new macro-systems that lead to grand entrepreneurship, due to interaction between cultures of technology and society at large, entail a reconciliation of structural dynamics to pave the way for research (Constant II, 2012; 234).

Today nations are aggressively and diligently pursuing AWS development, such as US's 2014 Offset Strategy "which seeks to outmanoeuvre advantages made by top adversaries through technology, to exploit all advances in AI and autonomy and insert them into DoD's battle networks to achieve a step increase in performance that the department believes will strengthen conventional deterrence" (DoD 2016). In its 2019 Report, "State of AI", PAX concluded that the trend of states implementing national policies for developing military application of AI already resembles an arms race, including research programmes for simulating cooperation with tech companies and universities, for investing in military applications of AI with the overarching rhetoric to not fall behind adversaries" (34). Unambiguously supporting collaboration with the private industry, all states display a prerogative for RnD; like China's "institutionalized military-civilian integration" (PAX, 2019a) and Russia's Technopolis (Alaff, 2018) while Israel and South Korea already have AI departments within their ministries. The Chinese technopolitical age has expanded AI research, and officially designated companies like Baidu, Alibaba, Tencent, iFlytek, and SenseTime as the country's 'AI Champions' successfully integrated into the military (Allen, 2019; 21). This must be taken with a pinch of salt, because "Article 7 of China's National Intelligence Law gives the government legal authority to compel private assistance" under "Military-Civil Integration; one of the cornerstones of its national AI strategy", which while forcing oversight exempted them from "competition from state-owned enterprises" (*ibid.* 22). In the US, Google and Pentagon, entered into a contract, Project Maven for cloud computing, that fel through. PAX, followed up its previous Report with a survey of tech companies (2019b), with actual or potential connections with the military as a "development partner and/or as a supplier of specific products" demarcating those which show best practice to those which cause concern. Optimistically, it concluded that companies will not jeopardize their public image by being associated with practices that harm humanity and are trying to devise set of ethics and rules, but AI/dual-use technology nevertheless will attract investment/attention because it enables defences (spam filtering, malware detection). Notwithstanding this optimistic stance, companies like Amazon and Microsoft have garnered, public ire and concern,

vying for a 10 billion 'war cloud' contract as part of US DoD's Joint Enterprise Defence Infrastructure (JEDI) plan (Cuthbertson, 2019)[7], while other US companies emerged in the report as "working on technologies relevant to increasingly autonomous weapons" (47). This happened despite protest by Microsoft employees requesting withdrawal from the bid.[8]

1.2. Literature reflection

AWS are undefined, and according to NATO "*machines cannot be autonomous*"[9] (52) because autonomy is a measure of "*critical functions of concern and the interactions of different variables*" (UNIDIR, 2014; 5). Drones/robots are synonymous with autonomy like the RQ-1 Predator; developed for surveillance and subsequently be equipped with hellfire missiles, but the combination was swept along with the original approval for its non-lethal function (Canning et. al, 2004). These uncertainties are opportunities for states wishing to develop AWS using the legal and conceptual vacuum (X01) as "a pretext to limit further progress in discussions" and "take advantage of unclarified terms to prolong adapting IHL or further resolutions to the deployment and use of these weapons" for a morally acceptable deployment to "reduce civilian casualties and mass property damage in a foreign country" (ISLMUN, 2019; 2). For the purpose of clarity, a summarized version of backstage and frontstage discussions is produced, that can help shed light on the gravity of the problem in this paper.

[7] On 28 October 2019, Microsoft won the JEDI bid.

[8] https://www.theinquirer.net/inquirer/news/3064518/microsoft-employees-protest-firms-bid-for-us-govs-unethical-jedi-project

[9] https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf

Table 1: Different positions on AWS

Opposition (Calling for ban on AWS)	**Neutral/positive stance**
Complex algorithmic systems pose a 'black box' (Sparrow, 2009; Klincewicz, 2015; Cummings, 2017) instead causing "disproportionate harm" (Sparrow, 2009; 172)	'No new change' because systems are vulnerable everywhere (Klincewicz, 2015; 172) but instead provide an alternative to deviant and erroneous human judgement (McFarland, 2015; 1323). "ethical governor can restrict lethal action consistent with LoW and RoE" (Arkin et al, 2009; Galliott and Scholz, 2018).
Technological 'other' (HRW 2012, Johnson and Axinn, 2013; Jones, 2018)	Improving warfare (Scharre, 2014a) by reducing "risk to soldiers" (Scharre, 2014b; 6) and removing the 'inhuman element' (Schmitt, 2013, Klincewicz, 2015; Arkin, 2010; Noone and Noone, 2015; 132) to minimize the "psychological baggage" caused by taxing working conditions (Sukman, 2015; 51) and reduce friendly casualties (Heyns, 2016; Arkin 2018).
Global and regional security concerns, (ICRAC, 2014; Anderson and Waxman, 2013; Altmann and Sauer, 2017; Gerdes, 2018; Asaro, 2012; Sharkey 2012)	Define "meaningful human control" and "critical function" (Welsh, 2017)
Impact conducting of strategy to disrupt existing power balances" (Ayoub and Payne, 2016; 793)	Strategically make "war less brutal at least or render inter-state war obsolete at best" (Solovyeva and Nik, 2018; 190)
Proliferation (Meier, 2017; Altmann and Sauer; 2017)	"Enemy forces developing LAWS" hence countries actively investing in AI technology and AWS (PAX Report, 2019a; 6-30)
Loss of human control (Ekelhof, 2017; 313) and "'strategic robot problem' if AI can decide independently on strategic, operational and tactical levels" (Korac, 2018; 57 and Roff, 2014).	Contextual use to be judged case-by-case (Schmitt, 2013; 8)
Technology in politics inhibits reflection imposing radicalism over grounded thoughtfulness (Kissinger, 2018) Militarily dishonorable (Wagner 2014, Lin et. al 2008, Korac 2018)	"LAWS will end up in conflict regardless of the outcome of debates" (Singer, 2009)
Violation of human dignity: (Goose, 2017; Docherty, 2014; Heyns, 2017) due to ethical implications of AI (Lichocki et. al, 2011)	Human dignity is not an absolute concept (Birnbacher, 2016; Sharkey, 2019)

1.3. Research Problem

The implication of AI is that it's a general-purpose technology capable of performing tasks (Brundage et al. 2018, 9; Scherer 2016, 262) combining intelligence with computing properties to improve productivity across all industries by accelerating innovation (Brundage and Bryson, 2017) placing AI and society in relationships of radical transformation (Susskind and Susskind, 2015). As such, AI has strong sociotechnical nature. Linguistic and political barriers have caused emergence of "a range of terms like 'killer robots', 'robotic soldiers', 'lethal autonomous robotics', 'autonomous military robotics', and 'lethal behaviour in autonomous robots' to infuse the literature with confusion that detract from core concerns introduced by these systems, and may even skew opinion by their superficial connotations" (Liu; 2015; 1). The AI sector is largely unrepresented and under-researched although questions have begun to be asked on the role and responsibility of engineers and designers regarding the ethical consequences in causal chains by use of their technologies (Marino and Tamburrini, 2006; Surber, 2018). Because AWS do not exist yet, the conjectures on their impacts indicate an impasse', even amongst experts who are entrusted with the social guidance of society. This shows that they are both, shaped and shape AI, which by extension comes from "prevailing social relations", demonstrating its political nature, which is not "directly translated by economic imperatives" into tangible machines and operations; rather, various groups are involved in the processes of technological innovation (MacKay and Gillespie, 1992; 690). Even though forms of AWS are already in use and an arms race may already be underway (Geist, 2016), lack of a clear, formal definition, is used to excuse lack of consensus amongst countries, while the boundary parameters to classify AWS keep expanding (X01, DE01). Moreover, the contextualization of issues must be understood in the power and capacity of these actors who employ technological strategizing in social and politically charged contexts (Orlikowski, 2000; Amoore, 2011).

The problem then arises in situating the practices of power, knowledge and expertise that provide empirical instances where they are enacted. This is in line with the fact that technology does not develop linearly but is "extrapolated from the existing corpus of achievements" (Woolgar, 2012; 304). The current discussions on AWS are strong and implicate many actors, especially nations, but the commercial and military domain continue to be analysed separately, rather than as reinforcing forces which offer immense benefits to each other. The defence sector has enormous financial capital while profit-driven public companies possess incomparable expertise, seeking investors and partnerships, both for innovation and opportunity to grow, not just as business, but in the realm of advancing AI.

This combination of reasons makes PCs receptive to multiple, creative partnerships at micro and macro levels and in turn develops and deploys technologies in specific ways to cater to narrow requirements of defence actors. Then, in calling for a ban, AWS become trapped in a decentralized, complicated public debate powered by "axioms and hypotheses, which scrutinizes the consequences and benefits", but "fundamental questions about the relationship between society and technology" remain unaddressed (Perlinski, 2017; 12, Solovyeva and Nik, 2018; Noone and Noone, 2015). Yet, political nature of AI built through the knowledge and practice of society, remains largely unrepresented, while the sociotechnical nature of AWS is unexplored. Moreover, due to the decentralized development of AI, designers/developers cannot predict how, where and who will use them, signalling an important moment to study the social choices that will be made when the dynamism of AI becomes interlocked with questions of security and society.

1.4. Objective

The objective of this research is to illuminate the sociotechnical nature of choices made by different actors, leading to the social construction of AWS, such that they are not standalone entities.

1.5. Research Question

How do different actors and their practices socially construct AWS, towards its development?

Sub – Questions

a. **How do the military and PCs relate to each other in a localized setting, contextualizing the circumstances for development of AI-related technologies?**
b. **How can the practices of AI community be factored into AWS development?**
c. **What factors emerge as signifiers in driving AWS' development?**

1.6. Paper Outline

This paper is divided into 7 chapters. Chapter 1 describes AI and its applications, moving to a synthesized review of literature on AWS to contextualize the research problem resulting from the socio-technical and political manoeuvring occurring within society, to formulate the research question. Chapter 2 describes and justifies the methodological frame while describing research methods and the ways that field data was collected and interpreted. Chapter 3 elucidates the theoretical frame. Chapter 4 engages with the first sub-question to critically analyse the role of military and PCs in a given time and space. Chapter 5 branches into the role of AI community referring to findings from the previous chapter, and Chapter 6 consists of the main findings and observations to illuminate effects of the tessellated practices analysed in Chapter 4 and 5. Chapter 7 recapitulates this paper's contents and concludes it.

1.7. Researcher's Position

As an outsider, I have assumed the role of a knowledge-producer and interpreter to contextualize the incubating circumstances which seem far removed, yet play critical roles in substantiating AWS, away from the public eye. As an Indian citizen, this undertaking served an important function to reflect critically on geopolitical dynamics, the issues that create pockets of security and how different actors align themselves and justify their actions in using AI or more simply technology, a factor still considered under development and of a mystical nature in the global South.

1.8. Limitations

This research is limited in scope because of the small sample of Respondents whose views and practices are not representative of the AI community. The empirical data is only representative of Western culture situated in the Global North. Audio recordings at EXPO were not allowed to be shared publicly, so names have not been mentioned although content and excerpts have been analysed and paraphrased, respectively. As a personal dilemma: discovering the duality of technology, especially data mining, also entailed contributing to the corpus of data being hoarded by websites, in order to access internet content as a crucial source of research. In the process, my internet history is very well tracked by the very network that is under critical analysis in the paper, over which there is little control of the researcher.

2 Methodology

This section outlines the process of research. By analyzing AWS as a 'constructed artefact', the social, political and controversial driving forces or components become clear in the process of its development. The way any technology gets its identity is based on rigorous negotiations regarding its constructed formulation, to establish its nature and use.

2.1. Sociology of Technology (SCOT)

SCOT analyzes technology by opening the so-called 'black-box', to allow patterns embedded in its *content* and the *processes of innovation* to be exposed and understood (MacKenzie and Wajcman, 1985; Bijker and Law, 1992; Winner, 1993). This refutes the deterministic portrayal of technology as linear accumulations, to focus on its social construction (Woolgar, 2012) meaning that it does not have its own intrinsic logic, but even at the level of a singular machine, is socially shaped, "patterned by the conditions of its creation and use", such that "generation and implementation of new technologies" is affected by social and technical considerations "influencing their content, application and social implications" (Williams and Edge, 1996; 866). The three levels of analyzing technology are: *technological systems* naturalized as "problem-solving components which are socially constructed and society shaping" (Hughes, 2012; 45); *sociotechnical ensembles,* in which engineer-sociologists decide and explain the conditions of an artefact's conception in technical and social terms, like a seamless web, such that "heterogeneity and complexity" in case of radical innovations "are not progressively introduced along the way, rather they are present from the beginning" (Callon, 2012; 78); and, *technological culture* in language, behaviour and interaction which shapes and changes lives, like robots in a car factory, nanotechnology in medical surgeries, voice assistants in phones and homes or even the grammar correcting feature of a Windows Operating System. It changes how we define work, health, luxury, comfort, our interaction, dependence and definition of things (E01). Labour is no longer drudgery in the locomotive industry. Lastly, SCOT shows that there is no 'pure' technology, instead is shaped by heterogeneous factors, such as procedures, which lead to the occurrence of certain types of technologies (Bijker and Law, 1992). In the heuristic tradition of SCOT, some key concepts for analysis are:

- ***Relevant social group and interpretive flexibility***

The methodological dictum of SCOT is to suspend hierarchy in favour of negotiations between groups, to define an artefact, which may be a vast constitution of users, organizations and institutions, through their context of use, by a "process of 'invention through diffusion' which affect the outcomes of the implementation of innovation as well as the very technologies around which negotiations are located" (Harty, 2005; 516). The homogeneity in heterogeneous groups arising from conflicting interpretations on social, moral, judicial grounds creates versions of an object, but is not an isolated event, rather a long process, to give it *interpretive flexibility* related to the design of the artefact, possible to be done in multiple ways and can be demonstrated, one way through interviews with people who are engaged in a "contemporary technological controversy" (Pinch and Bijker, 1984; 421).

- ***Stabilization and Closure***

The context in which agreement over an artefact is reached is essential to determine its characteristics and make it stable enough for reliable usage, which leads to a closure. This closure is not the 'disappearance' of controversy or solving of problems; rather it may be rhetorically done or repackaged by "redefinition of the problem" (Pinch and Bijker, 1984; 427). There is a technological impact on society, such that interaction between groups can become unlimited and membership continues to change as technology evolves. Then, closure is the "meaning attributed by different relevant social groups to an artefact" and stabilization is "development of the artefact itself within one relevant social group, in terms of the modalities used in its descriptions" (Bijker, 1995; 87 in Humphreys, 2005; 241).

2.2. Research Methods

The methodological approach is of sense-making to acquire an orientation, fundamental for a perception on AWS. The methods of research were chosen to secure proximity to the stereotypical arenas, much like a laboratory where actors have been known to flock by virtue of their practices. In this research, the military, PCs and AI developers are identified as main actors in different sites and situations, owing to their professional and personal dispositions. Because of their absolute independence, AWS embody multiple knowledges, practices of communities and institutional features which may or may not be visible or evident, but this discovery of interactions was found to strengthen each sector through direct and discursive patterns of communication, in creating the material and non-material conditions for the

genesis of AWS. The tacit and practical knowledge of actors became apparent to ensure successful collaboration, especially between institutions to eradicate doubts, establish optimal epistemic certainty, reduce knowledge gaps and maintain autonomy in decision-making. Each actor's contribution directly and indirectly is analysed in terms of closing gaps based on their site-specific performance and interactions.

2.2.1. Site selection

In practice perspectives, engaging with relations demands attention towards sites where relations play out, are included, excluded or omitted by social agents especially with a technological imperative, when guaranteed success by devices towards actors' circumstances is a matter of fact (Davidshofer et. al, 2016; 212). The framework of analysis is important to tease out the underlying "dispositions and contexts of action" to consider "elements such as resources and patterns of domination and resistance, by insisting on both, situated places of politics and power, and on their specific and often unpredictable trajectories" (*ibid.)*. Some of the most advanced autonomous weapons in use today, like the US Phalanx Close-In Weapon System (CIWS), Aegis System[10], X-47 B[11], Israel's Harpy[12], UK's Taranis[13], Brimstone missile[14] and South Africa's Rheinmetall Skyshield Defence system[15] are manufactured by Lockheed Martin, Northrup Grumman, BAE Systems, Ryatheon, Rafale, Boeing, General Dynamics and United Technologies, in no particular order. These companies were some of the main participants at a weapons exhibition (EXPO) in Stockholm, Sweden in May, 2019.

The EXPO was chosen as a site of study because of the opportunities it would generate to observe processes by which 'business' is conducted in a market-like setting, like a trade fair, wherein people's interactions, opinions, ideas are constructed and played out. For the purpose of research, the EXPO is a part/product of the Military Industrial Complex (MIC) which is firmly established as the nexus between private interests and national defence and one of the most profitable undertakings (Wirls, 2019; Foster, 2019) and therefore selected as the 'focus site'. The researcher's knowledge or its lack thereof, is evident, because the mere intonation of weapons immediately, conjured up the image of the military,

[10] Equipped with guns and fully autonomous capabilities (Del Monte, 2018; 163)
[11] Unmanned Combat Air System (UCAS), an aircraft carrier that can take off, attack and return on its own (Anderson, et.al; 2016)
[12] A fire-and-forget autonomous weapon
[13] ISR drone with attack capabilities developed by BAE systems, although its details are classified
[14] MBDA Systems, 2019
[15] Gun-radar-pairing

which is hard to access. Hence the EXPO was an opportune moment, both in time and space.

The events required an online registration, through a mobile application and upon payment of a nominal fee. The events at the EXPO which form the beginning of this research are 'Underwater Defence Technologies' (UDT), 'Electronic Warfare Europe' (EW) and 'International Training Technology Exhibition & Conference' (ITEC). It is a yearly event where the scope and expanse of the MIC becomes pronounced. hardware and software manufacturers in the weapons industry building security, surveillance, radar, radio, training, simulation and other systems, participate as a rule to exhibit their 'products', for acquisition by buyers, of which national governments' are the prime target. Each year the event increases in scale of potential buyers, concept weapons are introduced and unveiled, emerging technologies gain more publicity, and the EXPO itself becomes an arena, to forge unique mosaic of relations patterned on objectives, potential and behaviour. Other events were instrumental in bridging knowledge-gaps and jargon-barriers for illuminating assumptions, positions and biases that would be encountered during interviews (Annexure 2).

2.2.2. Participant-Observation (PO)

PO is useful for unearthing "aspects of audience behaviour when on-site surveying techniques are inappropriate" (Mackellar, 2013; 57), and reasonable access is acquired in an "appropriate setting where the phenomenon of study is sufficiently limited in scope, size, and location to be examined" otherwise (Jorgensen, 2015; 6). Every research has certain "epistemological, normative and methodological biases" (Bloodgood, 2008; 6). AWS in popular culture usually mean 'The Terminator' or 'Apollo 11's HAL'; conscious machines defying and destroying humanity. While fictional, they create a false bias, against which the "fieldwork focused on meaning-making, for discovery of concepts, theory, and abstractions" (Merriam, 1998; 19-20). As a registered participant/student/visitor, access was free for central halls and stalls (main EXPO), all opening ceremonies, selected panel events and presentations by private companies, even though seminars and conferences were inaccessible. Jorgensen also states that PO is most helpful when accompanied by other sources of information such as interviews, documents and related materials (2015; 8). The choice of sessions was made, based on their description, focusing on keywords: AI, technology, future, warfare, security, safety, inter-operation, design, value," etc. because "human meanings are intersubjective and when expressed, their meanings are shared with other members of

the linguistic community" which resolves objection to purely subjectivist approaches (Jorgensen, 2015; 6). In the passive state of observation, 12 sessions conducted by defence personnel, private companies and industry experts in the form of presentations, panel discussions, ground-reports and Q n A sessions were attended and analysed using existing literature and *subsequent interactions with exhibitors*.

In explaining one's intent the active component of participant-observation has two advantages, namely insiders' willingness to talk to "attentive strangers" and brief encounters preventing chances to go native or get subsumed in the process of discovery (Pearsall, 1970). The switch between passive and active roles, while causing discontinuity in the observation process led to continuity in the analytical and cognitive process, as each encounter led to clearer comprehension of the succeeding session, to remain involved, without committing to the values and goals of the event (Adler and Adler, 1994; 380). Moreover, this ensured a balance was maintained in both the academic and personal position, as an outsider, to interpret findings at a gradual pace allowing space for reflexivity and adjustment of expectations while observing the interactions between participants. These encounters confirmed assumptions and made revelations; predominantly, increasing numbers of military personnel in civilian positions with private-sector defence organizations (Tinoco and Arnaud, 2013; Grassiani, 2018; Lieberson, 1971), exponential increase in Research and Development combining private and government interests for security (Bellais, 2013; PAX, 2019; Gronlund, 2019) and the threat of other nations and non-state actors developing lethal AI (PVCO/DP/IE/NRD/A04/DE01/X01).

In PO 'socialization' is the way in which knowledge is transmitted (Collins, 1984) which "does not interrupt the event experience for participants" and the researcher can "uncover, explore, and describe new behaviours" to provide a "deeper understanding of participants' subculture through analysis of their phrases and semantics, leading to discovery of the reasons situations are occurring" (Mackellar, 2013; 58-59). In understanding the application of such a method, Getz states that opportunities also exist to look at the behaviour of participants, media, and host communities and its greatest potential lies in examining social dynamics of audiences" (2010; 10). For instance, officials took great care to clarify differences between modes of operations, to dispense confusion, while exercising liberty in socio-political positions, in highlighting matters of military urgency and security. This is also a way for event managers "to record the experiences of audiences and analyse them for future event development" (Mackeller, 2013; 61).

2.2.3. Interviews

Preceding the interviews, the action-relations of respondents were observed in locations where the focus of interaction was the exchange and elaboration of knowledge on AI (Annexure 2).

The interviews were conducted more than a month after the respective events. Unstructured and semi-structured questions helped to engage with the participants with vibrant "professional, educational and personal histories" while allowing "exploration and probing for clarification in the answers" (While and Bariball, 1994; 330). "With parsimonious yet phenomenological aims, the epistemological privilege was of the participant, as 'knower'" (McIntosh and Morse, 2015; 4) because their subjective knowledge critically expanded the scope of AWS, while revealing, in-depth, their personal standpoints in engaging with the topic in course of their professional ambitions. Leaning against and towards dominant discourses regarding security, AI, surveillance and state-sponsored control, differences and similarities were discerned in perspectives on AWS, to fertilize the research with social depth. Because AI applies widely and no, one company will manufacture AWS (A04), Respondents represent the diversity of AI-related practices, formal and informal, that are now being considered as socially relevant phenomena, instead of standalone, standard professions.

2.3. Data Analysis

Prioritizing site-specific phenomenon and correlating it with individual practices through constructivist inquiry allowed for isolation of meta, macro, meso and micro narratives and reflection upon 'symbolic interactionism' against purely technicist or objectivist thinking (Charmaz, 2008). An 'insider's view' was created by contextualizing the motivations of private companies, military and AI developers as overlapping groups driven by economic gains, security considerations and research, respectively, assembled as part of a bigger whole in terms of their socio-temporal-technical-political relevance and situation (Charmaz, 2006). Subjective experiences in the field, revealed or rather confirmed how structure was enacted with the correct social conditions, proffered and successfully executed for educationally immersive, awareness generation and business affiliation purposes among the concerned milieu. Instead of a dogmatic adherence to existing literature, categorization and clustering of data was oriented to 'discovery' and 'sense-making' reflective of the researcher's position/apprehension, as an outsider. In dealing with military, business and technological jargon, extracting meanings from contextual language and behaviour, difficul-

ties in interpretation were resolved through interpellation tactics used in interviews. This helped to understand meaning of texts, like notes from PO, writings or transcriptions of interviews, which is turn allowed expansion of analytical approaches and conclusions.

The theoretical analysis is done on the content of literature reviewed, academic documents and Reports from meetings, conferences and seminars, and briefing papers. The empirical thread relates to transcribed audio recordings from the event and interviews with 7 experts in; AI research as freelancers and private companies namely, TNO, Salesforce and Rabobank; Post-Doctoral researcher from academia; Dutch Lt. Colonel and part-time PhD student researching in engineering of value-by-design for autonomous drones and Project Officer on LAWS at PAX, NGO, Utrecht. The PO was carried out between May and July, 2019 in Stockholm and The Netherlands, and the interviews were conducted in August and September, 2019, in The Hague.

Recordings from the event were analysed via interpretation while information from presentations was corroborated and in included as quotes from the online profile of each company. Opinions shared during informal interactions were not recorded, rather are used in the process of analysis, while information pamphlets, books, magazines and brochures from the EXPO of selected/relevant companies were used in conjugation with personal observations, contextualized against company's public position. Data was selected on account of its proximity to the broad theme of actors' perspectives and patterns of individual and group behaviour to identify patterns in the discourse on AWS, its driving forces and influences. To avoid micro-scoping of issues, meta-analyses have been done using multiple theoretical approaches, also due to the interdisciplinary nature of the problem.

3 Theoretical Frames

The theories of 'Epistemic Communities' and 'Securitization' have been selected, on the basis of their success; as knowledge-based communities instrumental in influencing international order/practice due to their professional expertise (Adler, 1992; Haas, 1992; Cross 2013); and securitization practices which move critical decision making into undemocratic, executive spheres on account of power and ability of actors in framing security issues (Buzan et. al, 1997; Waever et. al, 1993; Waever, 1995).

3.1. Epistemic communities (EC)

Ruggie defined '"epistemic communities' as 'a dominant way of looking at social reality, a set of shared symbols and references, mutual expectations and a mutual predictability of intention" (1975; 570).[16] It was developed by Haas(1992; 2) as "a network of individuals or groups with an authoritative claim to policy-relevant knowledge within their domain of expertise, adhering to, shared consummatory values and principled beliefs; causal beliefs or professional judgment; and, common notions of validity based on intersubjective, internally defined criteria for validating knowledge". In cases of ambiguity, lack of evidence and fragmented opinions, consensual knowledge is achieved out of analytical interpretations, based on interrelations of social and physical processes (*ibid.)* such that "professionalism, becomes the glue that holds epistemic communities together, facilitates consensus, and enables persuasion" (Cross, 2013; 155). ECs "engage with state and non-state actors with claims to expertise" (Graz and Nolke, 2012; 2) which cross-links "different ways of accounting for collectives" to shed *a priori* existence in favor of how they emerge, become materialized and organized that explores the drivers of such formations, like "practices, metaphors, instruments, and discourses" (Meyer and Molyneux-Hodgson, 2010; 3).

Smirnova and Yachin, explain that "expert communities exhibit a new phenomenon of self-organization promoting a decision based on a shared vision, making them epistemic by their shared values, making the community *a process, a state of mind which is enabled by a number of factors including human factor*". Elaborating further, they outline salient features to estimate behaviour and operation in an epistemic mode, namely "political influence, high level of interdisciplinarity and focus on global problems which affect human development, well-being, security indicated by activities like foresight or scenarios of possible future variants" (2014; 654-655).

[16] *Epistemes*: borrowed from Michel Foucault (1970)

3.2. Securitization theory (ST)

Security is the outcome of specific intersubjective social processes, unobstructed by objectivity, in which issues exist and are managed with a discursive and political force, to make exemplary decisions as counter-measures (Balzacq and Guzzini, 2015; 99). ST provides a framework for "articulating security characters of new transnational/global issues, for deciphering the social commitments and practices of accountability in the designation of some phenomena as threats," (Balzacq et al., 2016; 521) policy making in response to addressing threats and consequences of agreeing to something as threats (*ibid*; 496). In ST, a 'securitizing actor' convinces and sometimes mobilizes an appropriate 'audience', towards 'threats', and on the exacerbating implications of its continuation for undertaking exceptional or innovative 'measures' to respond to them. For example, when analysing cyber-threats and national security, the "conceptualization of values which shape technical design and public policy related to security, motivate its attraction and public support" (Nissenbaum, 2005; 73). Notions of security include the technical, where political debates increasingly refer to "a complex constellation of public-private responsibility and governmental authority" encompassing hyper-securitization, everyday security practices and technification (Hansen and Nissenbaum, 2009; 1162). 'Fields of practice' in securitization constitutes the content of power relations among those with capital to frame security (Bigo, 2013) leading to regimes of practices including members from various fields like academia, researchers, experts, not uncommon in the field of insecurity who confer scientific legitimacy to the knowledge produced, which is again a field of contestation for domination of opinions (Balzacq et al, 2016; 506) to transform existing systems. In this paper securitization is understood as a "dynamic, interactive process involving an assemblage of actors" who transform social reality by labelling threats in certain settings (Oberdick, 2018; 22). Functional differentiation is the way in which current society operates, using logics of interaction to think about itself and is thus open to change and interpretation (Albert and Buzan, 2011; 422).

Relevant to this research, is to comprehend the underlying processes shaping and influencing AWS development, and how they can be understood in terms of change or reimagination, furthered by the conjunction of knowledge and power, in which the role of actors in different time and space becomes pronounced in furtherance of specific agendas. This is the crux of EC and ST.

4 Relationship between the Military and Private Companies

This chapter answers the first sub-question elucidating how epistemic strength was exercised in a localized setting for a specific audience. In the ensuing process, it is shown how a temporary security architecture was imagined as a concept, with potential benefits that would accrue to both actors. This is because the act of doing security is a process which changes the "boundary between one identity, against that given to the 'referent object'" that in itself "would not determine emergency action, but would condition the range of measures actors could undertake legitimately" (Wilhelmsen, 2016; 169).

4.1. Military

> "Enemies like it when you are lazy, apathetic, incompetent and passive. We can't afford that, so we need aggressiveness, and developments in hardware AI and Software AI, are urgent" (DP)

Epistemic community: Similarity and overlapping career experiences of high-ranking officials, like generals, lieutenants and officials from administrative wings of cyber and intelligence, identified problems of future security, much like an 'imaginary', based on their transnational interactions having professional norms and expertise for collective policy goals. Their authoritative knowledge was taken for granted, because of past alliances and professional convergences. Actors had had the experience of each other's strategies, like joint operations of Swedish, Finnish, Norwegian, Dutch, British, Australian and US forces (PD01/02/03, DP), rooted in shared classical notions on security for strengthening Western powers against rapid geopolitical influences. In a simultaneous process of giving credit and enrichment via acknowledgement of difficult mission achievements, uniformed military officials were bound in solidarity, appearing as one, irrespective of their nationality. Using military jargon enhanced the depth of issues which affected the audience who were made privy to ground realities of soldiers, tasked with national security, which demanded attention. In effect, this setup resembled "society which confers authority, to expertise in military doctrine, force orientation, war strategies and logistics" like in Europe, wherein "shared military expertise, culture, and tradition evolved towards transnational cohesion" (Cross, 2013; 155). Officials used persuasive language for conjoining understanding of aims in a worldview, such that knowledge about emerging realities in on/off field operations was produced in a cohesive manner making their authority and expertise, legitimate. Their dy-

namics as a community was based on shared professional judgment on governmental policies, weighed in their validity in use, through common set of practices based on principled beliefs, such as, mission success, welfare of soldiers, collaboration-by-design and integrity of binding norms, in an arena relatively 'free from political interference' (Haas, 2004). By exercising their collective agency in a setting which encouraged not only formal interactions but brainstorming sessions in workshops and interactive forums, the military became the catalyzing force for bringing in other groups of experts/personalities based on what they 'say' (Drake and Nicholaidis, 1992; 39), *i.e.* in a professional frame, articulated in causal beliefs, appearing as scientifically objective. This objectivity is achieved because officials became epistemically responsible for 'rationally grounded trust' (Scheman, 2001) within and outside of their community.

Security actor: The military's engagement with private sector became relevant behaviour, similar to security practice, with respect to real and perceived threats (Floyd, 2010: 52–4). In the fundamentally risk-averse/avoidant geo-political climate, decisions and strategies are devised on a healthy amount of information, trust, reliance, knowledge, intelligence and the like which is threatened by uncertainties. In a rigid trust frame, this can lead to an imminent need to secure, oftentimes by "projecting negative aspects of the Self onto an Other or otherwise essentializing Self and Other, such as through stereotyping, relying on enemy images, resurrecting national myths, etc" (Mitzen, 2006; 274). The power configurations created by speakers and listeners (Balzacq et. al, 2016; 502) were based on existing discourse on 'Western competence and superiority' to achieve audience support by usage of perlocutionary language that appealed to their needs, desires and emotions. References to Chinese incursion due to its expansive AI program, Russian interference in the 2016 US elections, conflicts in the South China Sea (DP, DE01, PVCO), uncertainty over China and Russia's compliance with existing international norms and unpredictability in violent engagement in the absence of a regulatory frame for AWS, became the threats over which action for deliberation and vice versa was established. Armed with epistemic and hierarchical superiority, the military instituted a coupling of, threats with alternatives to address them, and in the process exercised interpellation, in its positionality because the problem was largely understood, whereas the solutions were not, to maintain continuity with parallel discourses of security and technology. The audience was discursively constituted because the rhetoric on security was meant to mobilize those who *should* be involved in doing security to convince them for reinventing the current security landscape through novel solutions. In this way, an

entrepreneurial approach was evident because solutions were sought, for both micro and macro, political and technological issues, in an advantageous institutional setup to describe complex decision-making which can be influenced by external and internal factors, in changing organizational setups (Oberdick, 2018; 25) The opportunity was well used, since in an act of micro-securitization, the military, also showed its tendency to exhibit multiple roles in a favourable assemblage, both as an actor and the audience (*ibid.*).

4.2. Private companies

> "The role of tech is to reduce the scale of war and with more information, prevent nations from going to war or having conflict on unclear issues which make them susceptible to launching and receiving attacks" (WEX)

Knowledge actor/enactor/broker: Possessing both, practical and epistemic advantage over the commercial use of technologies like speech analytics, psychological AI, Natural Language Processing (NLP), large data processing through DLANN, private sector espoused breakneck innovation relying on its ability to deliver results in record time, in sharp contrast to the slow, methodical style of the military. As public businesses, they operated as knowledge brokers to demystify and deconstruct apprehensions regarding safety of AI which would go into providing technical solutions to manual problems, resulting from excess data and inevitable increased use of AI. The Pentagon's Project Maven debacle was interpreted as the lack of contextual communication with Google that would have fomented much needed understanding and agreement over which private companies can engage with security issues in a positive manner, while being true to their company policies (Moss, 2019). By producing solutions that first and foremost reduce and efficiently replace human labour to buy time, their engineering prowess was enmeshed in delivering relatively cheap and reproducible technology. Knowing that commercial AI thrives on proliferation, companies shared their values and goals in keeping up with the times, as it depends on short cycles of innovation. These short-term consequences project and protect their relevance, at a time of hyper technological progress. Even though companies presented their products and their uses in a sales pitch, the metanarrative accompanying the shift from hardware to software, implied that large institutions can no longer be managed and improved as a behemoth without the aid of AI, which begins with small changes such as data processing using ML, photo and voice recognition, common in China, and with the right power structure, can be scaled up to any number of things. The companies were thus instrumental in reducing epistemic uncertainty. This is one way for tacit and acquired

knowledge to create perceptions on what is, what can be and what ought to be; hence a common ground. Here, intellectual and academic rigor played a crucial role as many AI giants have emerged out of university projects (Facebook, Google), much like the participants: Phonexia (Brno University, Prague), 100 Worte (Heidelberg University, Germany) or market leaders (Deloitte Analytics Berlin, ATOS IT solutions, SONARTECH Australia).

'Audience' for enacting security: Security never happens in isolation, and in technological systems depends on deep networking and delegation of authority in chosen locales aimed at selected audiences. Balzacq called it backstage securitizing moves with public effects (in Salter, 2008) encompassing "a scene in which actors and things are brought into a relation to enact the unexpected, unknown, unpredictable" (Isin, 2008: 27) signifying "a break in instituted normality, making it political" (Huysmans, 2011; 373). The act of making security became performative as actors, exchanged places to produce socio-political consequences, not necessarily with public assent, rather in a network of micro-sociologies, following an "internal social grammar invoked by metaphors, tropes, expectations within the universe of the audience imagination, in a knowledge-authority game" (Salter, 2008; 328-330). Taking a cue from the EC framework, this euphemistically characterized the role of PCs in enabling the securitization process.

The power-knowledge exercised by the military incentivized the inclusion of private companies to aggregate their prowess for human welfare proven in use by the military, whose epistemic hierarchy validated the former's participation to insinuate itself, both as an audience and the actor, to provide the input for creating a sphere of influence and embedding layers of emphasis. Replacing total truth with local truth, concerns like 'low security by design' (PVCO, DP) causing high kinetic damage paved the way for validating AI solutions, even as sales pitch for calculative economic gains, were conveyed to convince the military elite, which in turn would convince the political elite and thereafter the general population (Salter, 2008; 330). Besides pivoting products, defence actors elucidated growing need for smart solutions, and this knowledge from the field created positive encounters with potential partners, contractors, dynamically interlocked in a reflexive relationship to conform and correspond to the 'audience'.

4.3. Threat/issue framing using uncertainty

> "Machine will only be able to make decisions when told to do so. Humans love power and they will not give it up, so AWS brings us into the more dangerous domains….that is not being discussed at all" (PVC/PVCO)

In the absence of any prior experience, as with a nuclear war scenario and in the case of AWS strategic thinking was derived from global and human behaviour "arrived mainly on the basis of conjectures, assumptions, and non-scientific expectations" that created an imaginary in order to explain how weapons would be used in a hypothetical scenario. (Adler, 1992; 107) Along with the long history of arms control, fears about strategic instability (Altmann and Sauer, 2017), robotic malfunctions (Roff, 2014) as well as recent developments like the US's announcement to withdraw from the 1987 Intermediate-Range Nuclear Forces Treaty[17]; tensions over the renewal of Russia-US New Start Treaty before 2021[18] create fear. This fear was manifest in clear intonations regarding global value chains, since each component comes from different sources, raising risk, more serious in armament, because expensive conventional weapons when mounted on one platform, having accumulated data through long distances, digitally, can become vulnerable to hacking. Moreover, improved data collection does not equal usefulness, rather adds to the complexity generating a paradoxical situation of information without utility (EXDP, DP, PVCO). Use of AI in weapons is not new (Scharre, 2018), but anxiety-inducing AWS, implicates the military in its fray, known for its stringent adherence to rules within a bureaucratic system, possessing multiple levels of accountability; to the nation, government and to itself, hence needing vetting, authentication and familiarization. Improving EW depends on coherence of the multiplicity of its platforms (radars, sensors, surveillance drones, radio signals and transmissions) which can be "fraught with uncertainties" (Borraz, 2011; 970) on account of their decentralized nature, needing conversion tactics to eliminate them. These uncertainties arise due to the risks associated with them in unsupervised learning scenarios (EXDP, DP), since military operations are highly sensitive and require assurance that a system will not fail or risk soldiers or mission objectives. These issues formed the bedrock of discussions over which solutions were forwarded. The interface of technology and security, intertwined when ex-

[17] https://www.france24.com/en/20190802-usa-russia-withdrawal-intermediate-range-nuclear-forces-treaty-mikhail-gorbachev-ronald-rea

[18] https://www.reuters.com/article/us-usa-russia-arms/future-of-last-nuclear-pact-between-russia-and-u-s-uncertain-u-s-envoy-idUSKCN1V41R0

pected outcomes were co-opted by PCs, with the express intent to join the defence sector. This episteme, constructed the reality in which technocratic training and bureaucratic position came together (Cross, 2013; 141) in a context of security discourse which empowered new actors (Balzacq, et. al, 2016; 504).

4.3.1. New concerns

These interactions led to a filtering down of problems. In highlighting operational challenges in the Baltic Sea, limited technological resources for tactical responses in minesweeping in shallow waters (PD01) posed high risk for soldiers and exposed them to live mines; an operation that can improve with disposable technology. The success of cyber-operations was indirectly proportional to the number of humans involved who had proven to cause irregularities and intelligence became better with ML, as it reduced reaction time (PVCO, DP, IE). Rapid integration of AI would generate concerns about the accumulated arsenal of conventional weapons which always require a human being to operate them. In trying to keep up with changes, at the same pace as commercial AI, the military would have to encounter governmental policies and political structures, which at the helm of and govern any military activity. The extreme networking through the use of internet exposes one to hacking, and technology like this, may increase the risk. Lastly, unregulated AI lacks clarity on their legality so if analysed speech recognition was used to distinguish and target an enemy, how would this evidence be justified as admissible in court (IE).

4.4. Addressing uncertainty

In order to maintain compliance with their own rules, militaries bridge knowledge gaps and even if "selective forms of utilization can obstruct engagement with strategically available research, practitioners learn and develop context sensitive decision-making processes" (Phillips, 2018; 296). Capability assessment of aggressors, mainly China and Russia with AI power, acted as the reference points against which actors legitimized their interventions (Floyd, 2011; 431) using a combination of past experiences, field information like 'simulation training which can monitor soldier's performances while keeping them engaged in creative ways of training' (DP, PVCO) and projected futures such as Vikings program[19]. The military's imperative is not just security of territory, but also identity *as an actor,* an ontological security which is a "cognitive affective source of resistance to identity change in world politics" (Mitzen, 2006; 272). States do this when they perceive outcomes, or relations whose trajec-

[19] https://www.forsvarsmakten.se/en/activities/exercises/viking-18/

tory they cannot predict, or based on past behaviour can help formulate ideas about their intentions and future scenarios. In the realm of strategic stability, interdependence is unavoidable in the 21st century and the hoarding of nuclear weapons is testament of that, which in the second nuclear age is consistently deteriorating (Garcia, 2017).

4.4.1. Success stories as roadmaps

> "AI in autonomous systems, provides tools to improve the intelligence cycle to go from a few large, heavy, expensive sensors to smaller, precision-based sensitive sensors, better at collecting and processing data within the sensors themselves" (PVCO).

The switch to autonomy, in intelligence has led to "synchronization and real time processing by intelligent platforms with the ability to take everything from everyone and create a multidimensional picture using signal intelligence (SIGINT) and other sensors" (PVCO). The system then provides the ability to say with high probability *about what happened in a form interpretable by human operators to simultaneously categorize between enemy and friendly forces.* From the time that sensors were used, their technological impact improved decision-making processes, through which their required values were set to form a framework in which future, detailed design decisions are made (MacKenzie, 2012; 196). These decisions reflect organizational temperaments, and the health of the intelligence system which affects whole branches of defence services, as well as the multiplicity of users' which use them in different contexts, like secret service, private companies, cable manufacturers for combat-ready aircraft carriers (WEX). The continued use and success of smart sensors, is dominated by the contribution of operators/users, who seek optimization to derive information about future requirements in their usage. Based on their interests and need fulfilment, their projections have influential power over those seeking clarity in AI adoption in other domains whereas smart sensors in radars has the effect of locking in the technology to the point of closure, described as an "irreversible process" (Bijker, 1993; 119). At this point, the cultural, technical and institutional practices have converged structurally in the sense that AI is synonymous with intelligence, although, their stabilization is dependent on their "constant potential for change and reinvention" (Humphreys, 2005; 247). Without the drive to collaborate and upgrade, any institution falls to disrepair, and the military is well-aware of it. US DoD has already rolled out a detailed program to integrate with cloud-service providers against the tedium of rapid

hardware and software rollouts.[20] Moreover, identification and targeting through surveillance and other monitoring mechanisms, are crucial to the security architecture in the 'technological production of identity' and safety, and to distinguish one from another, or 'us versus them' (Den Ploeg 1999; Salter 2006, 2007; Ceyhan, 2008). Using this construction in the machinized sub-structure, military AI plays a critical role in maintaining the systems of control relied upon by countries to exhibit/project power, stability and as norm-abiding, liberal, human-rights protective and representative entities which design and decide the security narratives. For instance, while 9/11 marks a pivotal moment in history, the geopolitical climate has propelled into mulches of uncertainty where decision making must be swift, causing a surge in techno-politics of the state at the national and domestic level (Malik, 2012).

The arrangement of this chapter is indicative of the researcher's assumption, having taken AWS as objective 'things' due to which the EXPO was selected. The power of the military is unquestioned because civilians cannot fathom battle realities for which extraordinary decisions have to be made, especially in security for society's benefit. With the veneer of jargon and expertise, this analysis shows how PCs can also become excluded and unproblematized, limiting questioning. This can be researched further in the context of AWS. This co-constitutive emboldening of both actors is effected by the use of security by channelling their respective epistemic strengths, where the EC and ST framework provides profound insights. I have argued that conventional boundaries between institutions can be successfully perforated to capitalize on opportune moments which are both within and outside of the public eye, much like the nature of AI.

[20]https://www.datacenterdynamics.com/analysis/dod-outlines-cloud-strategy-focuses-jedi-and-military-ai/

5 AI Community

Answering the second sub-question, this chapter shows the location of the AI community, its practices and perceptions to highlight how they become relevant to the construction of AWS. While technologically essential, this chapter also analyzes the elements which place them in the path to AWS development, to be successfully harnessed, as and when the time arises.

5.1. Knowledge engineering

AI has moved on from data to knowledge engineering. For AWS the expectations sustaining technological trajectory (Belt and Rip, 2012; 151) of AI are very specific, seeking stable platforms, suited for challenging environments. Independently, the bottom-up approach of AI is to impregnate machines with knowledge extracted from different domains often through formal and informal channels. to improve its value. Military training which uses simulation techniques draws inspiration from the commercial sector that is algorithm rich but context poor. AI developers are situated in between experts and end-users, which are usually the same, to create a loop in which PCs play a mediating role. For instance, simulated training software is developed using field data and experiences of soldiers to re-enact/re-create battlefield situations, to eventually train for enhancing situational awareness (DP/IE). Practices like these enable the military to desensitize, monitor and aid recruits when exposed to real-world situations. This kind of knowledge-encoding "facilitates common understanding and interpretation" shaping not only the explicit knowledge, that has analytical and empirical boundaries, but it is also made portable and available for transfer, thus claiming an expertly-shaped-and-acquired system, to have universal or locally unbound applications (Evers, Kaiser and Muller, 2009; 58). Succeeding sections shows how this is done.

5.2. Removing 'reverse salient'

In military terminology, 'reverse salient' are blockades that hold up the advance of an army in one spot while the rest moves forward. Within the AI community, these are new starting points. The uncertainties associated with AI discussed in the previous chapter, were related to contextualization of data amassed during military operations that creates a deluge of unusable information, limiting military capabilities. So the sensors which enable, can have an equally debilitating effect, requiring pooling of manual labour to sort and sift through information. Moreover, this work cannot be hastened, shared or put onto open network plat-

forms due to confidentiality concerns. The problem now, is not the lack of data (PVC, PVCO, EXDP, IE) rather how to contextualize it at a useful rate.

5.2.1. Data Science

> "In order to make AWS safe, our needs should be aligned to have explainability, and ability to figure out the engineering process behind it" (DE01)

Data science (DS) is the domain of AI to reduce complexities in data bundles through pattern recognition (A02). Developers selectively work in DS, which not only requires knowledge about statistics, but an interdisciplinary approach so that anomalies/patterns in different contexts can become apparent and recognizable by an algorithm. DS engineers function at this junction to liquidate the reverse salient. Their ability lies in patching up gaps, by devising complicated programs to make standalone models which are then trained on massive terabytes of data, to predict what a bundle of images-noises-voices means. Developers achieve success by refining their codes using multiple model training and swathes of data that is provided by the client. Some of the best examples today are, advanced image/speech recognition, targeted marketing, fraud and risk detection.[21]

One of the hurdles in AI adoption is normal faults within algorithms (Brehm, 2017), called bugs, which are unintelligible, rather undetectable (invisible) by the untrained eye. Private companies, like banks increasingly employ 'experts' or data scientists/engineers to reduce risks and eliminate vulnerability in their systems. In the cyber domain, these experts act as 'spotters' who detect irregularities visible in codes to craft robust clean-up solutions, which the system learns over time, and like infection-fighting anti-bodies in the human bloodstream, removes those irregularities at the very outset. Independently, these subsidiary problems decompose into opportunities for innovation, which in Silicon Valley talk, is rapid failure, adaption and stability; aggressive robotization and acquisition to quickly resolve any impediments and present them as upgrades keeping current systems relevant, till milestones are achieved and the technology changes drastically, becoming a new paradigm, as in the case of smartphones (E01/A03/A04). Data scientists are indispensable in the security architecture, where data is textualized by mining it from different sources, like surveillance networks to create files on people or groups being targeted or monitored which was revealed in the Snowden leaks (Vleet, 2017) and more recently, was used by US, ICE to conduct

[21] https://www.edureka.co/blog/data-science-applications/

raids on illegal immigrants[22]. So, even if it was Palantir, the company which sold the software, the "computer program was ignorant of social circumstances that were used to carry out the target-selection" (Petit, 2019; 23).

5.2.2. Reinforcement Learning (RL)

"We humans are neural nets. What we can do, machines can do"

Geoffrey Hinton

RL is a combination of ML and DS which can solve sequential decision-making problems in which, multiple iterations are used to teach/train an 'agent' which interacts with its environment 'over time' to perform actions in a punishment-reward formulation. In due time, this agent is expected to become aware of its surroundings because "agent and the environment interact continually; the agent selecting actions and the environment responding to these actions and presenting new situations to the agent" (Ashraf, 2018). As opposed to supervised learning, in RL, the ML algorithm develops itself, because the reward is a consequence of a sequence of actions. (Roessingh et al, 2017). Autonomous/self-driving cars are designed this way (A04, A02). By its very definition, the potential for RL can be imagined, to "help human users with tasks with unknown dynamics, user policies, and goal representations" (Reddy et al, 2018; 8), behaviour generating programs of autonomous agents in military simulation programs (Roessingh et. al, 2017) stabilization and structuration of multi-agent military systems like unmanned aircrafts in adversarial environments, by teaming human-machine intellect "because humans alone cannot sustain the volume, and machines alone cannot issue creative responses when new situations are introduced" (Nguyen, 2019; 19), in which RL is becoming more proficient and adding compatibility, especially in case of development of intelligent unmanned autonomous systems (Zhang et al., 2017).

5.3. Social role of AI developers

So far, the technical contribution of AI developers has been discussed which are relevant to the hard components of AI, meaning coding. In this section the social role and practices of AI community is investigated that allows a critical analysis. Continuing from the previous section, developers are publishing strong, detailed papers on open source plat-

[22]https://www.vice.com/en_us/article/9kegq8/activists-explain-how-palantirs-tech-is-used-in-ice-raids

forms like "arxiv"[23], run by Cornell University and "Open AI"[24] for disseminating and creating cumulative knowledge. Practical knowledge in this way is being tested rather than *gathering dust as annals of information which become privatized* (A03). Its democratic approach is geared towards objective knowledge creation (A04) as more participation in AI would make it a social project. This way AI encompasses "experiences of people who are traditionally excluded from scientific knowledge production" (Harding, 2011) through participation of multiplicity of sciences so that knowledge-flows do not get tangled up in duplicated efforts. This is a step towards hard objectivity, and is reflected in the practice of AI community to establish a global epistemic project unhindered by linguistic barriers and in effect install new paradigms. This is evident by the multiplicity of knowledge brought to AI like cell biology, quantum physics, literature, etc. (A01, A04, A03) The technocratic knowledge of developers was accompanied by myriad motives: 'data interpretation for improved application of AI in technological systems like autonomous cars and military equipment' (A04), 'pushing the boundaries of knowledge' (A03), 'increasing tech expertise for professional gains and market value' (A02) and 'augmented human-machine interaction' (A01). Causal beliefs apart, they are at the creation end, wherein their intersubjective objectivity is in a technological frame that can converge in expanding the limits of applicable AI, to make it safer, relevant and ethical in return for epistemic, intellectual and professional advantage. In so doing, they exercise subtle, yet compelling agency producing symbolic coherence when they define and re-define how, where, why and when AI evolves in different contexts. For instance, one Respondent's aim was to *transform all this academic knowledge and make it useful* for devising ethical design parameters, for AI in household devices, like Google Home or Alexa, which have a fast adoption rate, especially in Western countries (E01). This can be seen to make AI relatable, by imbibing it with human-like behaviour, while also researching and learning how human behaviour and values are changing, which creates feedback loop for engineering new knowledges. Due to its dispersed nature, AI possesses the capacity to project equality but access to knowledge fails in the face of systemic inequality which pervades the physical and the cognitive realm.

This dispersed nature of AI has given it a sociological dimension meaning technical innovation is culturally and socially produced (Bodewitz, et al, 2012; 251) and the interaction between different social actors happens on account of AI's sociotechnical aspects,

[23] https://arxiv.org/
[24] https://openai.com/

which in turn makes them acutely aware of AI's implications, for reconfiguring and expanding the technological frames of its identities. AI being open-source means that the realm of hierarchy is constantly challenged, because once the code is written, it's like a judicial precedent, except it's customizable. However, democratization does not equal objectivity, because knowledge production requires robust relations through and in-between actors, on similar grounds, which is both a boon and bane of this community.

In problematizing this issue, first the meaning of objectivity must be clarified because the AI community is driven by innovation. In casting obstacles as opportunities, such that philosophically nothing ever fails, rather objectively, success is measured negatively, as a mark of absence (Hacking, 2015) of anomaly or bug, which is no longer a concern. Knorr-Cetina's 'epistemic cultures' criticizes knowledge on the ground that because of its social production, it lacks objectivity (2001) Another way to look at it is, there are no courses on AI or rudimentary ML, as such, which means it is a process of learning-by-doing, in essence, towards creation and exploration, to see what can be made. Hence, as more AI becomes synonymous with monetary value and market skill, the more motivations may tilt towards certain aspirations which serve private ends, rather than contribute to the project where AI becomes moderate, still robust. This does not mean that many companies are eager to adopt AI, because the problem of *unexplainability* still remains (A01). Developers in generating information, are significantly detached from the effects of their work, making AI perverse with epistemic challenges that add to the complexity. This aspect has been noticed not just by society, but within the AI community too, which is discussed in the last section of this chapter.

This scattering of professionalization in AI also problematizes it. Ironically, and even cruelly, AI developers who exercise free reign in sharing knowledge for equality, fairness and mutual benefit, contribute to the growing corpus of technologies which create, exacerbate and sustain inequality. Increased openness exacerbates a 'race dynamic' and companies take higher risks to incorporate advanced tech, without proper vetting while political consequences could be even higher as AI proliferates on account of its known benefits, and unknown dangers (Bostrom, 2017). The safety of not only systems but companies and consumers thus get compromised by the very technology that is supposed to enable their growth. So, while unrestrained by corporations, independent development and consolidation of AI carries the risk of adding technologies to the mix which may contain bugs and biases; at times discovered too late (Dastin, 2018). This is not to say, that developers are unaware of the pitfalls of AI's philanthropy, as one Respondent put it "*An average Joe with*

enough computational power and skills, could bring down an entire nation, without leaving his seat" (A01). Exaggerated doom-saying apart, the threat perception is clear because "*too many things can and have gone wrong in the battlefield and sometimes no amount of preparation can counter, predict or mitigate it"* (DE01), so the technology should not be kept at a pedestal, rather needs to be made more efficient and in anthropomorphic speak, more ethical.

Moreover, AI is at the interstices of innovation, where it outpaces the ossified comprehension of regulators and thrusts the 'Uncertainty Paradox' to deal with, a two-edged sword, in which decisions are affected by concerns around the stifling of innovation versus its crystallization beyond intervention (Leenders, 2018). So, AI grows, like a neural network of the globe.

In their arguments, developers usually exclude themselves from accountability, regarding the application of their programs, mostly because the code itself is assumed to be unbiased and will function as it is applied. The overarching assumption is that because of the plethora of actors, codes usually do not retain their original character and can thus change over time. Rather it is the *unbalanced data* fed to it that makes it erratic (E01/A01/A02), along with the way that output from the data is analysed, which is considered problematic (A03/E01/A01) since that is an administrative and political process.

> "Beyond the hype and noise, we see AI which has immense power and can transform society for good, through its complete lack of biasness" (A03)

There are two main objections to this subjective stance taken by developers. It is of relevance to note that all the Respondents interviewed are in Europe, giving them a geographical advantage. The Silicon Valley culture mentioned in this paper is with regard to the non-conformity of the AI community to a bureaucratic or rule-based structure. It is instead supportive and even encouraging of 'failures', and despite the economic implications of AI, the notion of an 'end product' is discarded (A01/X01) favouring innovation and creation in the purest scientific sense. Even with "meta-competencies, as a new type of knowledge" on the larger scale of development the centrality of knowledge is based in the West, over which it retains control (Evers et al, 2009; 61) because the economy supports RnD that can pivot the emergence of technologies, while incentivizing and incubating, new and old developers (A01/02). This retains the exclusivity of the "epistemic community of development" that is closed to all others whereas the "constitutive form of global knowledge is deeply rooted in a self-referential organizational system" (*ibid.*). It is this liberty of pace and cultural freedom, which accelerates AI, untrammelled by social considerations or implications, whereas a similar culture is absent, and in some way exactly the opposite in non-Western nations

(A03). This is not to say that AI is restricted, rather its genetics are manufactured, and mutations are introduced only in certain parts of the world. This is evident by the fact that the only nations joining the ban on AWS, belong to Asia, Latin America and Africa[25] whereas US and Russia have refrained from joining the call.

Secondly, AI developers are social actors and products of the sociotechnical regime which sustains them, and their "identities and interests" cannot be "conceived as natural, given and definite", because their shared knowledge, resources and practices have evolved through dynamic structuration processes (Antoniades, 2003; 23). They do not exist in isolation, or independent of the political economy they inhabit, hence they have biases coded into their consciousness, as a natural rule. Any reference to impartiality or 'clean-coding' should thus be problematized and highlighted fully. Criticisms have been levelled against technocrats who operate under the "epistemology that any problem can be solved through big data, algorithms, automation, and 'smart' technologies" whereas, "choices about type of data and algorithmic processing, weightage and treatment of certain variables, presentation, interpretation and operationalization, of finished products are still routinely discussed as objective when they are not".[26] Sedowski and Selinger reject the objectivity of algorithms "embedded with their creators' biases, values, and politics, but are often difficult to discern, and their mathematical form provides a sense of rational ordering" (2014; 164). This was also evident in the Respondents' perspectives, armed with "engineering prestige" who demonstrated a tendency to "create rhetorical appeals to optimization and objectivity, that depicted their favoured approaches to social control as pragmatic alternatives to grossly inefficient political mechanisms" as responses to social frailties which have security implications (*ibid,* 162). Then, these knowledge-producing machineries are less effective in "producing instrumental knowledge that can be used to put information into social" (Evers et al, 2009; 56) but instead the transparency of AI is revealed to have multiple layers of meanings because of the subjectivities of its developers. The macro level effect is that while AI gains more followers, it gathers momentum, in which its objectivity is superficial and can be easily constructed or deconstructed based on the organizational power of those who wish to yield it.

[25] https://www.stopkillerrobots.org/action-and-achievements/
[26] https://newrepublic.com/article/91916/google-schmidt-obama-gates-technocrats

5.4. AI community within the security architecture

The democratization of knowledge by the AI community has been contextualised for "giving primacy to the social recognition of knowledge authority" that can allow its "integration as epistemic communities" using the "social context" (Antoniades, 2003; 26). One of the impacts is that knowledge has become unbound by regime or politics, and instead is pursuing its own course. On the level of AI, it has raised the possibility of AWS and Superintelligence, but at the organic level, this has opened opportunities for developers to work anywhere, for anyone. Using Hansen and Nissenbaum's problematique of 'technification', conventional security actors are baffled at the pace of threats and attacks which grants "legitimacy to experts and epistemic authority to information scientists" (2009; 1166) who become involved in hypothetical securitizations to "create a particular space for technical, expert discourse" (*ibid.*) However, this expertise is dispersed when it comes to the AI community because the same logic which makes it diverse, also creates a lack of coherence, preventing the emergence of an *episteme,* making it suitable for repurposing. As opposed to an EC, AI community beyond circulating a form of knowledge-by-practice is also volatile and bears no allegiance to any one party, and lacks professionalism, such that the knowledge whether good or bad, is left to the device of users, and much like their epistemic artefact, AI, they can be molded by a social management of their trust. Looking at how the literature of AWS is spread out, added to the lack of an internal character, even disagreement on forms of security, can allow the hooded practices of the military to be tuned into advantages, such that exaggerated estimations of damage (Hansen and Nissenbaum, 2009; 1167) become starting points for innovation. This follows the logic of problem-solving, which AI is mastering faster than humans, projecting the idea that more research needs to be undertaken for capitalizing on AI's benefits without writing it off from certain sectors. Private Companies are suitably located at this juncture, because they bear the hallmark of AI community's entrepreneurial pursuits that have resulted in its expansion. So, as companies seek business opportunities with clients like the military, they can easily leverage developers' fungibility fixating on areas, people, institutions which fit well into the security mould. This management is essential because instead of heavy handedness, there is no dearth of the talent pool which can be groomed to serve the needs of security. Remarkably, the workload that security creates can perpetuate a cycle of innovation pushing for more strengthening of AI, in essence shaping it as well.

5.5. A nascent epistemic community

> Just as most chemists and biologists have no interest in building chemical or biological weapons, most AI researchers have no interest in building AI weapons
>
> - Open Letter from AI & Robotics Researchers, 2015[27]

For some years now, a cross-disciplinary labyrinth of academics, AI experts and non-profits has materialized, through transient collaborations for raising concerns about long-term entanglements with, and character of, AI. This new assemblage is an act of mobilization with a coherent imperative to heighten communication, knowledge and awareness regarding AI. Through periods of intense interaction, members who subscribe to a doomed future narrative, to those who hold relatively agnostic views about AI's orbits, have coalesced in a shared vision, extensively informed by their loci and foci of practice. This configuration bears a strong resemblance to an EC, in a compelling, symbolic way. One way to identify it is by locating the narratives of its members (Lorenz-Meyer, 2010), like the Future of Life Institute (FLI), founded with the objective of safeguarding life and developing positive ways for humanity to steer its course of development. Its quorum consists of authors who contribute heavily to this research and industry experts like Elon Musk, Nick Bostrom, Stuart Russell, Jean Tallinn, and the late Stephen Hawking.[28] FLI's Asilomar Principles signed by 1521 AI/Robotics researchers and 3298 others, is a pledge to harness opportunities and empower people[29]. NGOs like Article 36[30] from the UK and PAX[31], have made the issue of Autonomous Weapons part of their human rights endeavours by global engagement, "*because people need to be made aware of the trajectory of their current sociotechnical practices"* (X01). In 2009, ICRAC was formed by a group of "experts concerned about the dangers of military robots in peace, international security and civilians in war"[32]. ICRC has focused on state consensus for arriving at a shared understanding of MHC and acceptable levels of autonomy[33] while working with the UN GGE on CCW to expand arms control discussions on the level of threat from nuclear weapons (2014). Following Google's fallout with the Pentagon, the company released a "set of AI principles against developing technologies" which "cause

[27] https://futureoflife.org/open-letter-autonomous-weapons/
[28] https://futureoflife.org/team/
[29] https://futureoflife.org/ai-principles/
[30] http://www.article36.org/issue/weapons/autonomous-weapons/
[31] https://www.paxforpeace.nl/our-work/programmes/killer-robots
[32] https://www.icrac.net/about-icrac/
[33] https://www.icrc.org/en/document/autonomous-weapons-states-must-agree-what-human-control-means-practice

or directly facilitate injury to people"[34]. MIRI[35], Open AI and MIT Design lab[36], are conducting multidisciplinary research through context-based innovation for clean design and analysis of AI systems using values of ethics and social justice. More pertinently, The **Campaign to Stop Killer Robots (CSKR)** is a global coalition formed in 2012, supported by almost all the tech-sector, at least temporally with normative commitments, pressurizing states to pre-emptively ban AWS. The members of CSKR are legitimized by their authoritative knowledge recognized by society, mainly on account of their political defiance that gives them integrity, wherein lies their influence (Antoniades, 2003; Haas, 2004). Apart from their knowledge-oriented work, their cultural standards have adopted a social project, which interpenetrates their epistemic criteria for producing universally applicable norms (Tiller et al, 2012). Weaving multiple approaches, this new constellation of actors has inserted itself in formal and informal structures operating in an epistemic mode, possessing all the necessary features of self-organization; scientific truth as 'shared value' and adherence to it, 'personal responsibility', political influence, interdisciplinarity, and lastly "focus on global problems which affect human development, well-being and security" (Smirnova and Yachin, 2015; 649). Moreover, they are not an invisible force, rather they have "transcended their specific scientific locations to speak to the broader public" through social media channels, podcasts and TV interviews about security issues, in which, how their "socially constituted subject positions differ, subject to historical change" can help shed light on "how securitizations are legitimated or challenged" (Hansen and Nissenbaum, 2009; 1168).

While "bottom-up norm institutionalization can be slow" this setup of experts, institutions and think tanks, mirror the phenomenon of a "research community in US and Soviet Union" that were instrumental in highlighting the perils of emergent nuclear technology, especially vertical proliferation, that led to the "bilateral arms control agreement", in the shape of the 1972 Anti-Ballistic Missile (ABM) Treaty (SALT-I)" (Maas, 2019; 296, Adler, 1992). Paraphrasing Adler, his framework is based on 5 variables that trace the journey undertaken by collaborative efforts of scientists, and civilian strategists who framed an arms control approach for "intellectual, ideological and political reasons" against another epistemic community which preferred "counterforce strategies" believing US's technological advantage to reduce the likelihood of a nuclear war (1992; 110). In the absence of an actual war, intellectual expertise was pooled together and technical exper-

[34] https://www.blog.google/technology/ai/ai-principles/
[35] https://intelligence.org/about/
[36] https://design.mit.edu/about

tise was used to create abstract models, whereas "practical ideas turned into political expectations" (Foradori et al 2018; 332) that further diffused into Soviet leadership through the efforts of their own epistemic community, that included military institutions. Cooperation was gained amongst opposing communities that further convinced the government and vested interests opening new vistas for research and development. Lastly, general awareness regarding arms control led to public support, realizing a favourable climate, albeit with a strategic stability. This new EC is not threatened by an external force, but driven by an internal motive to prevent AI from unravelling at the hands of its creators and prevent it from becoming a Frankenstein's monster.

The chapter can be understood in three levels. The first level picks up to show how AI developers are perfectly in sync with fulfilling the requirements highlighted in the previous chapter for successful embedding of AI in more systems. The second level shows what developers are doing in the normal course of business to turn AI into a creative and intellectual project that encompasses multiple disciplines within it. Then, from being a component in things, AI has become the 'thing' in which all components reside. Purposefully, developments in AI are happening as personal endeavours at the atomic level of developers devoted to adding and disseminating/democratizing knowledge that is amplified by machines, both, digital and physical. Subtly, it declares their power and agency, because at the level of AI, no one can restrict them. Because the AI community is scattered lack of an organizational character is a clear innovation for change. This by itself is not problematic rather it goes on to show how AWS will come closer to reality because the expertise for it can be acquired with relative ease. This is because of the cognitive bias entrenched within actors. Lastly, the organizational problem is shown to be resolving itself, because of the debates on AWS as one of the primary reasons, that is aligning he AI community as a political force, guarding its ideology of keeping AI safe.

6 Analysing the significance of findings

Capitalizing on the analyses of roles and practices, this chapter answers the last sub-question, to highlight certain factors that can be considered as signifiers in driving AWS' development. This can help us to imagine and perceive the aggregated set of *conditions* optimal for AWS development.

6.1. Flexible interpretation of AWS

> "No need to create weapons with autonomy because things that can be weaponized for harm, manipulation, targeting is already present" (A02).

None of the social actors defined AWS as replacements, rather extrapolated circumstances, where a machine would yield better results, in lethal and non-lethal ways. There was no skirting around the issue, but acknowledging the winds of change, which are sweeping in the future, faster than we can adapt to the vagaries of the present. Using AWS also means changing rules, norms, doctrines and even organizational aspects (DE01), which projects an overhaul of current practice that is difficult to achieve. But due to the expansion of military objectives and addition of hardware, their upkeep, maintenance and use requires more personnel, in which non-lethal AS can add complementarity, like logistics support, take-off and landing of aircrafts, etc. (DP, IE, WEX). AWS are subject to flexibility of language, use and structure, because AI is largely open, or in the language of SCOT, it can be appropriated. For the military, a superordinate characterization through security entailed merely an improvement/upgrade in the normal course of things, in which mission completion and risk removal are paramount. The localized security action was facilitative and skilfully maneuvered, so that new devices would function as filtration systems to segregate/simplify mounds of data already collected during missions. Like drone technology is a huge improvement over carpet bombing, ML in surveillance systems falls under the rubric of changing regimes of practice, now commonplace in remote warfare, fundamental to making interoperability of forces reliable, as a sure-sign of regional cooperation. Most significantly soldier's safety and performance, in extreme environments like under water, rescue-missions, bomb-diffusion and urban warfare entail high casualty/injury rates, because of enemy non-compliance, natural factors and surprise attacks which is more a matter of lack of self-preparedness, than the opposition's superiority, which in technological terms is in-

conceivable on account of military superiority of the West. Like a phone which is a medium to the world, an AS would be a self-sustaining medium to tackle rising irregularities in the battlefield. All indications towards increase in autonomy were done keeping the details on the technology itself, muddy and abstract yet attributing its applicability subject to actors' efforts and choices. PCs improved the marketability of AI, by disguising security problems as technical issues, using verbal flexibility. As one DARPA official put it "human is becoming the weakest link in defence systems" (Singer, 2010; 64) and machines are already doing half the jobs, previously allocated to soldiers. While most Respondents agreed on ethical dilemmas, a technological bias was evident on the neutrality of AWS, which wouldn't be driven by revenge or bloodlust, and with the proper design wouldn't adversely target humans, specifically the unarmed and powerless. Using the analogy of nuclear energy, one Respondent opined that political forces have deep biases that are exposed in their pursuit and hoarding of power to pander to public emotions, like the continued use of fossil fuels, even though 'nuclear is cleaner in the long run'. But, lack of political will and short-term power cycles, infect foresight much like AWS use, which entails responsibility that countries and governments refuse to take, even on matters where it matters (A01/02). By postponing political responsibility in defining AWS, the narrowing passage of time is creating a cascading effect and the advancement of AI is once again highlighting the inequality of humanity (A04). These disparities keep the nature of AWS wide open, hence vulnerable to reformulation and acclimatization.

6.2. AI stabilization

> "With tech, values become more apparent and that's when we can read them, analyse them and have a philosophical discussion about them" (E01)

In SCOT, "stabilization is a process through which one artifact becomes the prototypical design for a particular technology" (Humphreys, 2005: 242), *i.e.* AI for AWS, for which negotiations are underway at multiple sites, for its features to be made stable. Taking SCOT's diachronic view, the technological frames of AWS, on account of AI's absorptive capacity is contextualized by different actors and conceptualized as interpretive flexibility. Resultantly, converging and diverging views have emanated independent of, and due to the threats posed by AWS. Among the most pertinent, is overlapping of consensus regarding AI's *explainability* for purposes of installing controls, that can begin with "algorithm regulation" (A03) upon deciding what can and cannot be coded into programs bearing in mind, a

consideration for human values (A04). The emergence of an EC around AI is indicative of collective consciousness and engendered responsibility for building robust AI, which is no longer the domain of hackers and hooded programmers, rather "*it can be a tool that can transform realities"* (E01/DE01). This EC is not because of AWS, but because developers themselves have been outsmarted by the technology they built, on account of its abuse. As one Respondent put, "*tech gives us power and if only developers realized how much power they held, they could actually disrupt and expose the misaligned intent of nations who are really powerless…we can take the power back…Google did a bad thing and its developers corrected it"* (A03). The lack of clarity of AI is addressed by redefining problems into degrees of stabilized AI, which makes its innovation and adoption a gradual process.

Increasingly, initiatives are launched by companies and stakeholders called 'standardization or good governance of AI'; to improve their products. The result is, certain ethical issues cannot be resolved because human values and laws are deeply contextual, so that laws that punish us, also protect us. This makes AI products a gamble, and in essence re-defines the limits of acceptability and morality, in ways that technology can now begin to develop alongside society, in a dynamic way. Amazon Web Services (WMA) offered by Amazon, is a cloud-computing and data storage facility that hosts millions of servers and incalculable data, even of companies which are its direct/indirect competitors, because beyond business, every AI milestone is a step forward for the whole community and society.

Preceding chapters established how actors generated interactions on AI's multiple attributes, in which developers have *considerable* control over AI's design with a high degree of freedom to rectify errors and ensure perfectibility, to replace older, obsolete systems by exerting its superiority on other systems, groups and individuals in society (Hughes, 2012; 46-48). Having learnt that AI can become volatile any moment, actors are confronted with concerns about becoming party to unmitigated harm and to the acts of war. Can a private company and its products be held responsible for crimes committed on the battlefield? There is no clarity on this because of the strict ways in which military or security related actions are carried out, due to which AI in the commercial realm is being fine-tuned to reflect society's most cherished principles, for which researchers are calling for more scientification and diversification, so that people both realize, how they make technology, and how technology makes them, so they can make conscious decisions, without the excuse of ignorance. This echoes, Winner's criticism of SCOT's social constructivist approach, to move on from "interpreting interpretations of interpretations" to "offer coherent arguments about which ends, principles, and conditions deserve not only our attention but also our commitment,

and for better or worse, take a stand on choices to develop or limit the technologies available to humankind" (1993; 374).

Lastly, AI has an obduracy to it, much like the internet, that cannot be dispensed with, because we dependent on it. Then its 'closure' is rhetorical, by redefinition of problems, like extent of safety, keeping it in a state of flux, with the potential to be improved, allowing the long term processes of change to become dynamic during which AI will be fine-tuned. This is to account for the host of conditions needed for AI to work in which causes of failure may not be self-evident and that the working of a technology "does not automatically confirm every decision taken in its design" (MacKenzie, 2012; 207).

6.3. Construction of Social reality

> "The question is not about China's internal policy, rather their efficiency in conducting global affairs and exerting control on such a large scale" (PD01)

The EXPO was a platform to represent and redefine problems for feasible solutions (Evers et. al, 2009; 57) by approving and accrediting the knowledge disseminated by actors. Each sector provided its own notion of reality and validity as a version of the 'truth'. By entrusting each other with the knowledge that could be made actionable, they engaged in a communicable experience, to be observed symbolically while remaining independent of each other. On this scale, military's cognitive authority on politically relevant policy matters, created "intersubjective understandings imposing particular discourses and worldviews" (Antoniades, 2003; 29) conveying best practices and options for compromising solutions that have diplomatic and operational benefits on collective concerns (PD01/02/03). A security-development nexus was built as a framework to address the "acutely needed progressive solutions" especially in light of the economic resources available in service of both technological progress and security for the "attendant revamping of national institutions, as things must "fundamentally change to better reflect the empirical reality of a globalized world in which distinctions blur" (Stern and Ojendal, 2010; 20). The multiple discourses on security, policy and society, shaped the language of interaction, which in technocratic substantiation pulled the strands of issues that would normally belong to the public sphere. The tendency to do so is not extraordinary, because the acknowledgement of AWS in countering threats is a discursive move in such encounters to constructively isolate problem areas and install problem-solving features. One of the arguments in this paper is on the decentralized nature of knowledge, such that there are no elites rather there are varieties with different normative

approaches and social imaginaries creating a field of contestation. This is the realm of overt and covert struggles to structure social meanings of things, processes and networks. In such a pocket of actions and exchange, responding to radical innovation for future use, against dystopian or utopian strands was measured by the plurality of viewpoints, in a deliberative democratic fashion (Boyd and Holton, 2018; 343). AI expertise became the focal point through which current problems or roadblocks to technological transformation or adoption were addressed using the 'success of dual-use technologies', to validate solutions in improving the security architecture. So, the chain of information conveyance moved to convince the military elite, which in turn would convince the political elite and thereafter the general population (Salter, 2008; 330).

6.4. Co-production of knowledge

In the spatio-temporal tessellation of security issues at the EXPO, sectors engaged with each other to reconstruct and reinterpret their normative commitment based on mutually reinforcing causal ideas, adding weight and salience, to the information shared by both. Heavyweights in their respective sectors, participants did not represent the whole of either, rather proposed the ways in which the 'what and how' of current technological and military knowledge can become materially embodied as a product of constitutive practices (PVCO, PVC, DP). The localized milieu was exposed to the ground realities of security actions which carry immense transformative power, much like AI, that shapes society in radical ways. Playing off each other's strengths and requirements, the result was a sensitization towards subjectively held stances especially through identity adjustment, institutional rearrangement and discourse development to accompany the new representation. Co-production allowed the participants to consider the importance of such encounters which formed the bedrock for reformulation of "conceptual, material, and social orders, thereby helping to explicate pervasive shifts in consciousness" (Jasanoff, 2010; Jasanoff and Martello, 2004), like AI triggering a transformational take-off wherein machines will become a general-purpose platform (Boyd and Holton, 2018; 333). The internal and external realities pertinent to both sectors and the issues under consideration were juxtaposed at the EXPO to reinforce the socio-technical imaginary in which security practices and solutions were validated against internal and external threats, such that the knowledge produced became subservient to the EXPO's cultural imagination (Jasanoff, 2015; 28).

6.5. Technological paradigm

The combination of capital, investments and people surrounding AWS is helping it acquire an identity of its own, gathering direction and speed. Nowhere is this more apparent than in the case of state investment in military technology, especially but not limited to weapons, in ways that help "overcome what might otherwise have been insuperable economic barriers to its development and adoption" to suit military-security concerns to "coerce or force technological change", against anticipated punishment of falling behind (MacKenzie and Wajcman, 1999; 26). Competition is routine for PCs. In a selection environment comprised of the military and government, and market competitors like Google's Deep Mind and Amazon's AWS, companies innovate and invest in RnD to secure their future. The occurrence of a paradigm here is because of shared understanding of the exemplary nature of AI, such that "*turning back seems like turning your back to development or going back to the stone ages of war*" (DP, WEX, EXDP). However, as shown in this paper, it was not just the portrayal of AI, but the combination of perceptions, rationale and expectations around it, clustered in heuristics that became "embedded in the subculture of technical practitioners" (Belt and Rip, 1987; 140) to create a matrix of articulations towards a technological trajectory (*ibid.)* Using phrases like *"avoid getting caught like a frog in boiling water"* (PD01) influence was exerted on a niche environment through the use of successful heuristics to protect the AI trajectory against myopic selection/interpretation. The contrary is also true, because security narratives can be purely illusory, and there was no threat per se, rather the 'actor' and 'audience' composed of a "speculative market for early promises" (Belt and Rip, 1987; 136). The trajectory here denoted the incorporation of AI into "capital equipment, complex institution of defence or towards organization-and-equipment-embodied technology" (Dosi, 1984; 193).

6.6. Diversification of the MIC

> "If the military is so capable, why didn't it develop AI. After all, it claims to have everything" (A02)

The intersecting points between AI and security are such that "countries may put aside safety concerns" to attract and support the AI industry (Dafoe, A. in Brundage et al. 2018, 10) whereas perception of risk has led the military's coveted tasks to be delegated to actors with wider knowledge, skills and expertise. While big public companies like Amazon, Microsoft

and Palantir have sparked debates about the ethical implication of joining the business of war, the issue of militarization of AI remains at peak because it is unhindered by sector and liberated by domain. The militarization of AI is evident like Israel's IAI ELTA Systems, which specializes in 'development of advanced defence and intelligence electronics, sensors, radars, electronic warfare and communication systems' (PVCO). ELTA's close relationship with the IDF enables it to 'extract crucial data from feedback from IDF's operations and integrate it into products' which is then deployed to 'customers' benefiting from the expertise of technicians, engineers, scientists, specialists and intellectuals who devise systems for customizable use (ELTA). With lines blurring between the military and industry, military capital is built upon security as a driving force "in which security skills become increasingly important" (Grassiani, 2018; 92). While big companies are vying for big contracts, smaller companies are liberally expanding to fulfil small, yet crucial roles paving the way for greater autonomy beyond conventional weapons, but rather for systems or apparatuses which can be contextually weaponized. The US DoD forges partnerships as part of its JAIC[37] program, but the act of making security becomes multilateral, and once private companies, convinced of security threats, start contributing to the response mechanisms, they also embody the role of security actors and potential light bearers for other companies. Their inclusion should also be considered since each company (EXPO) was in some tangential way involved in monitoring, surveillance or investigative work, and was working on legal aspects of deploying technology (PVC). The epistemic merger, although temporary, was significant because it represented interests and apprehensions on an equal footing, in evaluating future technology under the banner of 'AI in warfare'. In this scenario, the existing MIC was not only enriched but also acted as a meso-level EC, in which security issues became technological problems and technological issues became security concerns, mainly competitive disadvantage against other nations and failure to sustain global superiority to benefit, both commerce and human rights.

Recapitulating everything, this chapter shows how interactions are built on account of the promise of a technology which consolidates power, position and expertise to provide positive epistemic and economic encounters between new actors, who are also in a state of flux, negotiating their relation to the narratives surrounding AWS, beginning with AI.

[37] https://www.datacenterdynamics.com/analysis/dod-outlines-cloud-strategy-focuses-jedi-and-military-ai/

7 Conclusions

This paper begins by establishing that AWS, with offensive capabilities are not in use today, but global competition and motivating factors of ontological security underline countries' imperatives to construct the incubatory temperaments, propitious to their development. Because AI is so successful commercially, the private sector has run up against the MIC, buoyed by the impetus provided by national governments for collaboration, economic profits and patriotic duty. This variety of actors inserts a multiplicity of features into the design and use of AWS, which is problematized to justify the research objective, translated as the need to conduct a sociotechnical inquiry. This inquiry is undertaken, because of AI's social nature in shaping perceptions, opinions and worldviews mediated by political and bureaucratic devices. Technologically, AI has granted kinetic control in strenuous areas unimpeded by biological limitations, exploited in its dual-use, well-captured by the impeccable record of drones.

This leads us to the research question to investigate AWS as a constructed consolidation of contextualized needs and narratives, propagated and practiced by actors. The hierarchical order of sub-questions is to communicate the flow of discoveries as they unravelled from AWS as only militarily relevant, to AWS as derivations of the knowledge of AI community, which harnesses dispersed data generated by sociotechnical practices of society. The methodological approach of SCOT is chosen specifically to untangle objective truths from constructed truths that emerge as a result of interactions between different actors, by virtue of their relevance to AWS, concentrated in a specific time and space. Not only does SCOT prove that AWS are socially constructed much like any other artefact, but any technology's core features can be teased out, like components in a technological system to be studied, challenged and altered. Using SCOT's heuristics, the relevant actors for AWS are identified, namely military, private companies/sector and AI developers/researchers.

The theoretical approach of Epistemic Communities and Securitization, is modelled upon the performance and portrayal of power-bearing actors, who exercise knowledge and authority, by default or through delegation to make impacts in strictly contextual realms; meaning thereby that their authority has transience, subject to legitimation. Because there is no pre-determined security actor, epistemic unity with regard to uncertainty regarding use of new technologies was achieved by forging symbolic novel associations at the EXPO.

The operative function of the EXPO was to provide impetus for discussion and deliberation regarding the choices that will eventually be made as more AI becomes inevitably synonymous with weapons. This was a dramatic shift, from being, hardware oriented for *physical weapons* containing smart technological apparatuses, towards an acknowledgement regarding immense potential of AI as weaponizable technology in the correct hands, and to play host and mediator for building actionable relationships between military and private interests. The paper shows, how military officials drew upon similar experiences on and off the battlefield, to create a blueprint for imagining the extraneous circumstances, in which the affirmation of the 'other' was actualized. Moving to the role of AI community, this paper connects the technological gaps identified by the military to highlight how developers are independently committed to eradicating the 'reverse salient'. In this process, their motivations are scrutinized, because even without a direct correlation, those gaps act as provocations for enterprising advancements that bolster AI. Then, the position of developers is problematized in their cognitive bias, which ignores the role of power in how AI can and will be used by security actors who can coopt AI to any end. Foregrounding AWS's sensationalist descriptions as 'killer robots', an argument is made regarding the emergence of a new futurist epistemic community, committed to lifting the veil over design and use of technology, to make it beneficial and safe.

Lack of a definition on AWS does not hinder their development, rather expands the boundaries to envision possibilities where their applicability would be an improvement over conventional methods, including the use of humans. The technological bias is clear, shrouding AWS in flexible interpretations. AI is the fuel of AWS, but equally relevant to be safe within the civilian sphere, for which definite measures are being taken, that in effect stabilize AI to the degree, which can be used, till future problems arise. Again, there is no direct application but that does not forestall AI's venture into the military which possesses all the qualities of an ideal customer/client. The success of interactions at the EXPO was based on the construction of a social reality that suited both actors, leading them to collaborate in producing local knowledge in a perfect fit with the larger political project of assembling affiliations for smarter technologies. Lastly, the potential benefits accruing from technologization of military operations is creating the buzz around which private companies are huddling, to develop AI, thereby diversifying the constellation of manufacturers who have traditionally been associated with the weapons industry.

In conclusion, this paper shows how AWS will be made, with varying features because all the phenomena analysed in this research were independent, yet harmoniously communi-

cating with each other much like an ANN in an active, naturally intelligent way, such that a version of AI, a nascent AWS has already joined the business of war.

Appendices

Appendix 1: Participant Observation at EXPO

No.	Topic and participants/ respondents	Description of the event / Position/	Date	Code
1.Panel Discussion	UDT EW ITEC	Challenges in the Baltic region Security measures and solutions in Europe Interoperability by design	13/05/2019 14/05/2019 15/05/2019	PD01
2. Presentation by private companies	AI software "for use and adoption" – sales pitch	Phonexia, 100 Worte, IAIELTA, Sonartech ATLAS, Deloitte Analytics	13/05/2019 14/05/2019 15/05/2019	PVC
	In use, status report and successful encounters	Deloitte Analytics, Sonartech ATLAS, ATOS Information, IAIELTA	14/05/2019 15/05/2019	PVCO
3. Presentation	Defence personnel	Cybersecurity and Electronic Warfare	13/05/2019 14/05/2019 15/05/2019	DP
	Industry experts	Closed Q n A on SIGINT and AI in warfare	13/05/2019 14/05/2019 15/05/2019	IE
4. Interaction	Exhibitors (UDT, EW Europe, ITEC)	NG, Raytheon, Rafale, BAE Systems, Boeing, etc.	13/05/2019 14/05/2019 15/05/2019	WEX
	Private Consultant	From Finland	14/05/2019	PCo
	Ex-defence	With the Association of	13/05/2019	EXDP

	personnel	Crows	14/05/2019	
	NATO RnD dept. rep.	EW	15/05/2019	NRD
	Embassy Representative	From Germany	14/05/2019	ER

Appendix 2: PO preceding interviews

a. Panel discussion at movie screening of "Do you trust this computer?" (COMP)
b. Panel discussion on 'state responsibility on the use of AWS' (TMC)
c. 2 closed study meetings on RL, AI and ML conducted by AI researchers. (SMA)

Appendix 3: List and details of interviews

No.	**Position and Organization**	**Field of work and expertise**	**Date of interview**	**Code**
1	Freelance Researcher	Machine Learning, Teaching AI	24/08/2019	A01
2	Senior Software Developer: Rabobank, NL	Machine Learning, Data Science, Teaching AI	27/08/2019	A02
3	AI Consultant with Salesforce, NL	-Philosophy of language - Work in helping companies restructure their usage, understating and infrastructure - Working with KONE (Finnish company making elevators)	08/09/2019	A03
4	Post-Doctoral Researcher at	-Ethics of technology -Technological mediation	09/09/2019	E01

	TU Delft	-Value dynamism due to technology in personal and social sphere, especially in the household -Working with designers		
5	Project Officer on AWS at PAX, NGO	- Background in IHL and IHRL. - Advocacy against AWS and awareness generation as part of the NGO (member of campaign – proponent of ban)	09/09/2019	X01
6	Engineer, Lieutenant Colonel with Dutch defence forces and part time PhD at TU Delft	- Work on how to have value by design in autonomous drones to account for the responsibility gap - working at the innovation center of defence forces to assess and identify new developments in startups, think tanks, universities, collaboration hubs - Teaching and conducting seminars with/for defence personnel	13/09/2019	DE01
7	AI researcher at TNO.	- Quantum Physics - Information Processing and innovating to integrate values, psychology, sociology, neuroscience and ethics into machine learning, design and operation of systems so that they can be made efficient and justifiable for use using all these parameters. - Ways to introduce more scientific design into understanding machines	03/10/2019	A04

References

A, Chang (2018) 'The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram' Vox. Accessed 8 November, 2019 <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>

A, Cuthbertson (2019) 'War Cloud: Why Is The Us Military Building A Vast Ai System And How Will It Change The Battlefield Of The Future?' *Independent* Accessed on 11 October 2019 https://www.independent.co.uk/life-style/gadgets-and-tech/news/war-cloud-what-is-explained-amazon-microsoft-ai-military-jedi-a8999551.html.

Adler, P.A. and Adler, P (1994) 'Observational techniques', In Denzin, N. K. and Y. S. Lincoln (eds.), *Handbook of qualitative research* pp. 377–392. Thousand Oaks, CA: Sage Publications.

AlaffCreator (2018), 'Era Technopolis: Russian Mod's Military Innovation Complex Of The Future' Accessed on 11 October 2019 https://alaff84.wordpress.com/2018/06/27/era-technopolis-russian-mods-military-innovation-complex-of-the-future/

Albert, M and B. Buzan (2011) 'Securitization, sectors and functional differentiation', *Security Dialogue* 42(4-5): pp. 413-425.

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

Altmann, J. and Sauer, F (2017) 'Autonomous weapon systems and strategic stability', *Survival* 59(5): pp.117-142. Doi: https://doi.org/10.1080/00396338.2017.1375263

Amoore, L (2011) 'Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times', *Theory, Culture & Society*, 28(6), pp. 24–43. doi: 10.1177/0263276411417430.

Anderson, K. and M.C. Waxman (2013) 'Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and how the Laws of War can'. USA: Stanford University, The Hoover Institution (Jean Perkins Task Force on National Security and Law Essay Series).

Antoniades, A (2003) 'Epistemic Communities, Epistemes and the Construction of (World) Politics', *Global Society* 17(1): pp. 21-38. https://doi.org/10.1080/0953732032000053980

Arkin, R (2010) 'The Case for Ethical Autonomy in Unmanned Systems', *Journal of Military Ethics* 9(4): pp. 332-341. https://doi.org/10.1080/15027570.2010.536402

Arkin, R. (2018) 'Lethal Autonomous Systems and the Plight of the Non-combatant' In Kiggins R. (ed.) *The Political Economy of Robots. International Political Economy Series*. Pp. 317-326 Palgrave Macmillan: Cham

Arkin, R.C., P. Ulam and P. Duncan (2009) 'An Ethical Governor for Constraining Lethal Action in an Autonomous System '. Atlanta Mobile Lab.: Georgia Institute of Technology.

Asaro, P. (2012) 'On banning autonomous lethal systems: Human rights, automation and the dehumanizing of lethal decision-making', special issue on new technologies and warfare *International Review of the Red Cross* 94(886): pp. 687–709.

Asaro, P. (2012) 'On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making' *International Review of the Red Cross* 94(886): pp. 687-709 doi:10.1017/S1816383112000768

Ayoub, K. and Payne, K. (2016) 'Strategy in the Age of Artificial Intelligence', *Journal of Strategic Studies* 39(5/6): pp.793-819.

Balzacq, T. and Guzzini, S. (2015) 'Introduction - What kind of theory – if any – is securitization?', *International Relations*, 29(1): pp. 96 – 102 https://doi.org/10.1177/0047117814526606

Balzacq, T., S, Leonard and J. Ruzicka (2016) 'Securitization' revisited: theory and cases', *International Relations* 30(4): pp. 494-531.

Barriball, K.L. and While, A. (1994) 'Collecting data using a semi-structured interview: a discussion paper', *Journal of Advanced Nursing*, 19: pp. 328-335.

Barro, R. J. (1991) 'Economic growth in a cross section of countries', *Quarterly Journal of Economics* 106: pp. 407-444.

Bartlett, S. (2019) 'The AI Arms Race In 2019', *Towards Data Science,* 28 January 2019. Available at: https://towardsdatascience.com/the-ai-arms-race-in-2019-fdca07a086a7 (Accessed: 5 November 2019).

Bellais, R. (2013) 'Technology and the defense industry: real threats, bad habits, or new (market) opportunities?', *Journal of Innovation Economics & Management*, 12(2): 59-78. doi:10.3917/jie.012.0059.

Belt, H. and Rip, A. (2012) 'The Nelson-Winter-Dosi Model and Synthetic Dye Chemistry' In Bijker, W.E., Hughes, T.P. and T. Pinch (eds.) *The Social Construction of Technological Systems* pp. 129-154 USA: Massachusetts Institute of Technology

Bigo, D. (2013) 'Analyzing transnational professionals of (in) security in Europe' In Rebecca Adler-

Bijker, Wiebe E. (1993) 'Do not dispair: There is life after constructivism', *Science, Technology, and Human Values* 18 (1): pp. 113–38.

Birnbacher, D (2016) 'Are autonomous weapon systems a threat to human dignity?' In Bhuta, N, S. Beck, R. Geiβ, H. Liu, and C. Kreβ (eds.) *Autonomous weapons systems: Law, ethics, policy,* pp. 105–121. Cambridge: Cambridge University Press.

Bloodgood, E. (2008) 'Epistemic Communities, Norms, and Knowledge', 26-29 March, 2008. Annual meeting of the International Studies Association Conference pp. 1-28.

Bodewitz, Henk.J.H.W., H. Buurma and H. de Vries, Gerard (2012) 'Regulatory Science and the Social Management of Trust in Medicine' In Bijker, W.E., Hughes, T.P. and T. Pinch (eds.) *The Social Construction of Technological Systems* pp. 243-260 USA: Massachusetts Institute of Technology.

Bostrom, N (2017) 'Strategic Implications of Openness in AI Development', *Global Policy* 8(2): pp. 135-148. Accessed on 12 November 2019 < https://onlinelibrary.wiley.com/doi/epdf/10.1111/1758-5899.12403>

Boyd, R and R.J. Holton (2018) 'Technology, innovation, employment and power: Does robotics and artificial intelligence really mean social transformation?' *Journal of Sociology* 54(3): pp. 331–345.

Brehm, M. (2017) Defending the Boundary: Constraints and Requirements on the Use of Autonomous Weapon Systems Under International Humanitarian and Human Rights Law, *Geneva Academy of International Humanitarian Law and Human Rights*, pp. 1-72

Broude, M., S, Deger. and Sen, S. (2013) 'Defence, innovation and development: the case of Israel. *Journal of Innovation Economics & Management*, 12(2): pp. 37-57. doi:10.3917/jie.012.0037. https://www.cairn.info/revue-journal-of-innovation-economics-2013-2-page-37.htm?contenu=article

Brown, G. (2016) 'Out of the loop' *Temple International Comparative Law Journal* 30(1): pp. 43-52.

Brundage, M, and Bryson, J (2017) *Smart Policies for Artificial Intelligence*. Available at: https://arxiv.org/pdf/1608.08196.pdf

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Allan Dafoe, et al. 2018. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Burton, J. and S.R. Soare (2019) 'Understanding the Strategic Implications of the Weaponization of Artificial Intelligence' 11th International Conference on Cyber Conflict (CyCon): IEEE.

Button, R.W. (2017), Artificial Intelligence and the Military, *The Rand Blog,* Available at https://www.rand.org/blog/2017/09/artificial-intelligence-and-the-military.html Accessed on 17 October, 2019.

Buur, J., Jensen, S. and Stepputat, F. (eds.) (2007) 'The Security–Development Nexus' In *The Security–Development Nexus: Expressions of Sovereignty and Securitization in Southern Africa*. pp. 9–33. Cape Town: HSRC Press.

Buzan, B., O, Waever and De Wilde, J. (1997) *Security: A new framework for analysis*. Boulder CO: Lynne Rienner.

Callon, M. (2012) 'Society in the Making: The Study of Technology as a Tool for Sociological Analysis' In Bijker, W.E., Hughes, T.P. and T. Pinch (eds.) *The Social Construction of Technological Systems* pp. 77-98 USA: Massachusetts Institute of Technology

Canning, J., G, Riggs., O, Holland and C, Blakelock (2004) 'A concept for the operation of armed autonomous systems on the battlefield' In *Association for Unmanned Vehicle Systems, International Annual Symposium and Exhibition*, Anaheim, CA.

Ceyhan, A. (2008) 'Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics', *Surveillance & Society* 5(2): pp. 102-123

Chamayou, G (2015) *Drone Theory* UK: Penguin

Chandler, D (2007) 'The security–development nexus and the rise of 'anti-foreign policy', *Journal of International relations and Development* 10(4): pp. 362-386.

Charmaz, K. (2006) *Constructing grounded theory: A practical guide through qualitative analysis*. SAGE Accessed on 11 November, 2019 < https://books.google.nl/books?id=2ThdBAAAQBAJ&dq=charmaz+2006+constructing+grounded+theory&lr=&source=gbs_navlinks_s>

Charmaz, K. (2008) 'A future for symbolic interactionism', In Denzin, N., Salvo, J. and Washington, M. (eds.) *Studies in Symbolic Interaction* 32: pp. 51-59 Emerald Group Publishing Limited: Bingley https://doi.org/10.1016/S0163-2396(08)32005-5

Chui, M., Harrysson, M., Manyika, J., Roberts, R., Chung, R., Nel, P. and Heteren, A., (2018) Applying artificial intelligence for social good *Discussion Paper,* McKinsey

and Company, Available at https://www.mckinsey.com/featured-insights/artificial-intelligence/applying-artificial-intelligence-for-social-good Accessed on: 5 November, 2019

Collins, H.M. (1984) 'Concepts and Practices of Participatory Fieldwork', In Bell, C. and H. Roberts, (eds.) *Social Researching: Politics, Problems and Practice* pp. 54-64. London: Routledge and Kegan Paul.

Constant II, E.W. (2012) 'The Social Locus of Technological Practice: Community, System, or Organization?' In Bijker, W.E., Hughes, T.P. and T. Pinch (eds.) *The Social Construction of Technological Systems* pp. 217-236. USA: Massachusetts Institute of Technology

Cross, MAI'A K.D (2013) 'Rethinking epistemic communities twenty years later', *Review of international studies*, 39(1): pp.137-160.

Cummings, M.L. (2017) 'Artificial Intelligence and the Future of Warfare', International Security Department and US and the Americas Programme, pp. 1-18Chatham House for the Royal Institute of International Affairs.

Daase, C and O, Kessler (2007) 'Knowns and Unknowns in the "War on Terror": Uncertainty and the Political Construction of Danger' *Security Dialogue* 38(4): pp. 411–434. doi:10.1177/0967010607084994.

Davidshofer, S., Jeandesboz, J and F, Ragazzi (2016) 'Technology and Security practices: situating the technological imperative', In Basaran, T., Bigo, D., Guittet, E and R.B.J. Walker (eds.) *International Political Sociology: Tranversal lines* pp. 205-227. Routledge Accessed on 11 November, 2019 <https://www.researchgate.net/publication/305751594_Technology_and_security_practices_Situating_the_technological_imperative>

Docherty, B.L (2012) 'Shaking the foundations: The human rights implications of killer robots' Accessed on 12 November 2019 <https://www.hrw.org/report/2014/05/12/shaking-foundations/human-rights-implications-killer-robots>

Dosi, G (1984) *Technical change and industrial transformation* London: Macmillan

Drake,W and K. Nicolaïdis. (1992) 'Ideas, interests, and institutionalization: "trade in services" and the Uruguay Round', *International Organization* 46(1): pp. 37-100.

Dutton, T. (2018) 'An Overview of National AI Strategies' *Wired* Available at: https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd (Accessed: 5 November 2019).

Ekelhof, M.A.C. (2017) 'Complications of a Common Language: Why it is so Hard to Talk about Autonomous Weapons', *Journal of Conflict & Security Law* 22(2): pp. 311-331. Accessed on 12 November 2019 <https://research.vu.nl/ws/portalfiles/portal/42807463/krw029.pdf>

Evers, H., C. Muller and M. Kaiser (2010) 'Knowledge in Development: Epistemic Machineries in a Global Context', *International Social Science Journal* 60(195): pp. 55-68.

Evers, H-D., M, Kaiser. and C, Muller. (2009) 'Knowledge in development: epistemic machineries in a global context' *International Social Science Journal* 60(195): pp. 55-68.

Fallaha, P.Y. (2019) 'Addressing the use of autonomous weapons', 29-30 March. Model United Nations pp. 1-12.

Floyd, R (2011) 'Can securitization theory be used in normative analysis? Towards a just securitization theory' *Security Dialogue* 42(4-5): pp. 427–439

Floyd, R. (2010) "A revised securitisation theory," in *Security and the Environment: Securitisation Theory and US Environmental Security Policy*. pp. 43–60. Cambridge: Cambridge University Press. doi: 10.1017/CBO9780511730146.003.

Foradori, P., G, Giacomello and A, Pascolini. (2018) *Arms Control and Disarmament: 50 Years of Experience in Nuclear Education*, Palgrave Macmillan, Cham.

G. D. Foster (2019) 'Beware Anew the Military-Industrial Complex: Revisiting Eisenhower's Warning' History News Network. Accessed 9 October 2019 <https://historynewsnetwork.org/article/171840>

G. Leenders (2018) 'The Regulation of Artificial Intelligence — A Case Study of the Partnership on AI' Medium. Accessed 12 November 2019 <https://becominghuman.ai/the-regulation-of-artificial-intelligence-a-case-study-of-the-partnership-on-ai-c1c22526c19f>.

Galliott, J. and J. Scholz (2018) 'Ai in Weapons: The Moral Imperative for Minimally-just Autonomy'*, Journal of Indo-Pacific Affairs* 1(2): pp. 57-67.

Garcia, Z. (2017) Strategic stability in the twenty-first century: The challenge of the second nuclear age and the logic of stability interdependence, Comparative Strategy, 36:4, 354-365, DOI: 10.1080/01495933.2017.1361207

Geist, E.M. (2016) 'It's already too late to stop the AI arms race—We must manage it instead', *Bulletin of the Atomic Scientists*, 72(5): pp. 318-321 DOI: 10.1080/00963402.2016.1216672

Getz, D. (2010) 'The nature and scope of festival studies', *International Journal of Event Management Research*, 5(1): pp. 1-47.

Goose, S (2017) 'The growing international movement against killer robots' *Harvard International Review*. Accessed on 12 November 2019 <https://www.hrw.org/news/2017/01/05/growing-international-movement-against-killer-robots>

Grassiani, E. (2018) 'Between security and military identities: The case of Israeli security experts', *Security Dialogue*, 49(1–2): pp. 83–95. doi: 10.1177/0967010617747202.

Graz, J and A, Nölke (eds.) (2008) *Transnational Private Governance and Its Limits*. New York: Routledge.

Greenberg, A. (2016), "The Jeep Hackers are Back to Prove Car Hacking Can Get Much Worse," *Wired*, Available at https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/ Accessed on: 5 November, 2019

H.A, Kissinger (2018) How the Enlightenment Ends *The Atlantic,* Available at https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/ Accessed on 17 October 2019.

Haas, P (2004) 'When does power listen to truth? A constructivist approach to the policy process', *Journal of European Public Policy* 11(4): pp. 575-576.

Haas, P. (1992) 'Introduction: Epistemic communities and international policy coordination', *International Organization,* 46(1): pp. 1-35. doi: 10.1017/S0020818300001442

Hacking, I (2015) 'Let's not talk about objectivity' In Padovani, F., A. Richardson, & J. Y. Tsou (Eds.), *Objectivity in science: New perspectives from science and technology studies* pp. 19–33. Dordrecht: Springer.

Hansen, L. and H. Nissenbaum. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly* 53(4): pp. 1155–1175, https://doi.org/10.1111/j.1468-2478.2009.00572.x

Harding, S (2011) 'Other cultures' sciences' In S. Harding (Ed.) *The postcolonial science and technology studies reader* pp. 151–158. Durham: Duke University Press.

Harty, C (2005) 'Innovation in construction: a sociology of technology approach', *Building Research & Information* 33(6): pp. 512-522, doi: 10.1080/09613210500288605

Hellmann, G., Herborth, B., Schlag, G. and Weber, C. (2017) 'The West: a securitising community?', *Journal of International Relations and Development* 20(2): pp. 301 -330. https://doi.org/10.1057/jird.2013.9

Henderson, I.S., Keane, P. and Liddy, J. (2017) 'Remote and autonomous warfare systems: precautions in attacks and individual accountability' in Ohlin, J.D. (ed.) *Research Handbook on Remote Warfare* pp. 335-370 UK: Edward Elgar Publishing Limited.

Heyns, C (2017) 'Autonomous weapons in armed conflict and the right to a dignified life: An African perspective', *South African Journal on Human Rights* 33(1): pp. 46–71.

Heyns, C. (2016), 'Autonomous Weapons Systems: Living a Dignified Life and Dying a Dignified Death', In Bhuta, N., S. Beck, R. Geiβ, H. Liu, and C. Kreβ (eds.) *Autonomous Weapons Systems: Law, Ethics, Policy,* pp. 122-142. Cambridge: Cambridge University Press. doi:10.1017/CBO9781316597873.006

Hintjens, H. (2019) 'Learning Outcomes in Introduction to emerging issues in global security and development' for Session 5 of Securitization of Development (4227).

Hughes, T.P (1986) 'The Seamless Web: Technology, Science, Etcetera, Etcetera' *Social Studies of Science*', 16(2): pp. 281-292. Retrieved from http://www.jstor.org/stable/285206

Hughes, T.P (2012) 'The Evolution of Large Technological Systems' In Bijker, W.E., Hughes, T.P. and T. Pinch (eds.) *The Social Construction of Technological Systems* pp. 45-76 USA: Massachusetts Institute of Technology

Human Rights Watch (2012) 'Losing Humanity: The Case Against Killer Robots'. USA: Human Rights Watch.

Humphreys, L (2005) 'Reframing Social Groups, Closure, and Stabilization in the Social Construction of Technology', *Social Epistemology* 19(2-3):pp. 231-253, DOI: 10.1080/02691720500145449

Huysmans, J (2011) 'What's in an act? On security speech acts and little security nothings', *Security Dialogue* 42(4-5): pp. 371-383.

International Committee of the Red Cross (2014), 'Autonomous Weapons Systems: Technical, Military, Legal, and Humanitarian Aspects' (Expert Meeting), Switzerland: Geneva. Accessed on 11 November, 2019 < https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014>

Isin, E.F (2008) 'Theorizing acts of citizenship' In Isin E.F. and Nielsen G.M. (eds.) *Acts of Citizenship* pp. 15–43. London: Zed

J. Dastin (2018) 'Amazon Scraps Secret AI Recruiting Tool that showed Bias Against Women' Reuters. Accessed 12 November 2019 <https://www.reuters.com/article/us-amazon-com-jobs-automation-

insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>.

J. McKendrick (2018) 'How Fast is Artificial Intelligence Growing? Look at the Key Bellwethers' Forbes. Accessed 11 November 2019 <https://www.forbes.com/sites/joemckendrick/2018/12/19/how-fast-is-artificial-intelligence-growing-look-at-the-key-bellwethers/#1605f652474a>.

Jabri, V (2006) 'War, Security and the Liberal State', *Security Dialogue* 37(1): pp. 47–64 https://doi.org/10.1177/0967010606064136

Jasanoff, S (2010) 'A New Climate for Society', *Theory, Culture and Society* 27(2-3): pp. 233-253.

Jasanoff, S (2015) 'Future Imperfect: Science, Technology, and the Imaginations of Modernity' In Jasanoff, S. and Kim, S (eds.) *Dreamscapes of modernity: sociotechnical imaginaries and the fabrication of power*, pp. 1-49. Chicago: University of Chicago. doi: 10.7208/chicago/9780226276663.001.0001

Jasanoff, S and Martello, M.L. (eds.) (2004) *Earthly Politics: Local and Global in Environmental Governance*. Cambridge, MA: MIT Press.

Johnson, A.M. and Sidney, A (2013) 'THE MORALITY OF AUTONOMOUS ROBOTS' *Journal of Military Ethics* 12(2): pp. 129-141. Accessed on 12 November 2019 <https://doi.org/10.1080/15027570.2013.818399

Jones, E (2018) 'A Posthuman-Xenofeminist Analysis of the Discourse on Autonomous Weapons Systems and Other Killing Machines' *Australian Feminist Law Journal* 44(1): pp. 93-118. Accessed on 12 November 2019 <https://www.tandfonline.com/doi/abs/10.1080/13200968.2018.1465333>

Jorgensen, D. (1989), *Participant Observation: A Methodology for Human Studies*, Sage Publications: Newbury Park, CA.

Klincewicz, M (2015) 'Autonomous Weapons Systems, the Frame Problem and Computer Security' *Journal of Military Ethics* 14(2): pp. 162-176, DOI: 10.1080/15027570.2015.1069013 Accessed 6 October 2019 <https://www.researchgate.net/publication/281285922_Autonomous_Weapons_Systems_the_Frame_Problem_and_Computer_Security>

Knorr-Cetina, K (2001) 'Objectual practice' In Schatzki, T.R., K, Knorr-Cetina and E, von Savigny (Eds.) pp. 175-188 *The Practice Turn in Contemporary Theory* London: Routledge.

Korać, S.T (2018) 'Depersonalisation of Killing: Towards A 21st Century Use Of Force Beyond Good And Evil?' *Philosophy and Society* 29(1): pp.49-64. Accessed 11 November, 2019 < http://www.doiserbia.nb.rs/img/doi/0353-5738/2018/0353-57381801049K.pdf>

Lichocki, P, P. Kahn Jr, and A. Billard (2011) 'The Ethical Landscape of Robotics', *IEEE Robotics and Automation Magazine* 18(1): pp. 39-50. Accessed on 12 November 2019 < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.226.4568&rep=rep1&type=pdf>

Lieberson, S. (1971) 'An empirical study of military-industrial linkages', *American Journal of Sociology* 76(4): pp. 562- 584.

Lin, P., G, Bekey., and K, Abney. (2008) *Autonomous military robotics: Risk, ethics, and design*. California Polytechnic State University: San Luis Obispo. Accessed 11 November 2019 < https://apps.dtic.mil/dtic/tr/fulltext/u2/a534697.pdf>

Liu, H. (2015) 'Weapons Systems: Autonomy in', in M. Dubnick and D. Bear field (eds.) *Encyclopaedia of Public Administration and Public Policy (EPAP),* (Third edn). pp. 1-6. Taylor and Francis.

Lorenz-Meyer, D. (2010) 'Possibilities of Enacting and Researching Epistemic Communities' *Sociological Research Online*, 15(2): pp. 1–13. https://doi.org/10.5153/sro.2151

M. Ashraf (2018) 'Reinforcement Learning Demystified: Markov Decision Processes (Part 1)' Towards Data Science. Accessed 7 November 2019 <https://towardsdatascience.com/reinforcement-learning-demystified-markov-decision-processes-part-1-bf00dda41690>.

Maas, M.M (2019) 'How viable is international arms control for military artificial intelligence? Three lessons from nuclear weapons', *Contemporary Security Policy* 40(9): pp. 285-311. https://doi.org/10.1080/13523260.2019.1576464

Mackay, H. and G. Gillespie (1992) 'Extending the social shaping of technology approach: ideology and appropriation', *Social Studies of Science* 22(4): pp. 685-716.

MacKenzie, D. (2012) 'Missile Accuracy: A Case Study in the Social Processes of Technological Change' In Bijker, W.E., Hughes, T.P. and T. Pinch (eds.) *The Social Construction of Technological Systems* pp. 189-216 USA: Massachusetts Institute of Technology

MacKenzie, D. and Wajcman, J. (eds.) (1985) *The Social Shaping of Technology* Milton Keynes and Philadelphia: Open University Press.

Mair, J., Whitford, M. and Mackellar, J. (2013) 'Participant observation at events: theory, practice and potential', *International Journal of Event and Festival Management* 4(1): pp. 56-65 https://doi.org/10.1108/17582951311307511

Malik, M. (2012) 'Technopolitics: How Technology Shapes Relations Among Nations', Plenary Session in *The Interface of Science, Technology & Security* 12: pp. 21-29. http://apcss.org/wp-content/uploads/2012/12/Mohan-Malik.pdf

Manyika, J. and Bughin, J. (2018) 'The promise and challenge of the age of artificial intelligence', *McKinsey and Company,* . Available at: https://www.mckinsey.com/featured-insights/artificial-intelligence/the-promise-and-challenge-of-the-age-of-artificial-intelligence (Accessed: 5 November 2019).

Marr, B., (2018) The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance, *Forbes* Available at https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#5b55b39a4f5d Accessed on 17 October 2019.

McFarland, T. (2015) 'Factors Shaping the Legal Implications of Increasingly Autonomous Military Systems,' *International Review of the Red Cross* 97(900): pp. 1313–1339 Accessed 11 November 2019 < https://www.cambridge.org/core/journals/international-review-of-the-red-cross/article/factors-shaping-the-legal-implications-of-increasingly-autonomous-military-systems/9D5E20943ABC778DA20D33DCBB45BE4D/core-reader>

McIntosh, M. J and Morse, J. M (2015) 'Situating and constructing diversity in semi-structured interviews', *Global qualitative nursing research*: pp.1-12.

Meier, M.W (2017) 'The strategic implications of lethal autonomous weapons' In Ohlin, J.D. (ed.) *Research Handbook on Remote Warfare* pp. 443-478. UK: Edward Elgar Publishing Limited.

Merriam, S.B. (1988), *Case Study Research in Education: A Qualitative Approach*, San Francisco, CA: Jossey-Bass.

Mitzen, J. (2006) 'Anchoring Europe's civilizing identity: habits, capabilities and ontological security', *Journal of European Public Policy* 13(2): pp. 270-285.

Molyneux-Hodgson, S. and Meyer, M. (2009) "Tales of Emergence" Synthetic Biology as a Scientific Community in the Making', *BioSocieties* 4(2): pp. 129-145. doi: 10.1017/S1745855209990019.

Nguyen, T. T., N. D. Nguyen and S, Nahavandi (2018) Deep reinforcement learning for multi-agent systems: a review of challenges, solutions and applications. *arXiv preprint arXiv:1812.11794*.

Nissen (ed.) *Bourdieu in International Relations: Rethinking Key Concepts in IR* pp. 114-130 London: Routledge.

Nissenbaum, H. (2005) 'Where Computer Security Meets National Security', *Ethics and Information Technology* 7(2): pp. 61–73.

Noone, G.P and D.C. Noone (2015) 'The Debate Over Autonomous Weapons Systems', *Case Western Reserve Journal of International Law* 47(1): pp. 24-35. Accessed on 12 November 2019 < https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1005&context=jil>

Oberdick, M. R. (2018) 'Reconceptualizing the Actor-Audience Dichotomy in Securitization Theory *A Dynamic Actor-Oriented Framework for Understanding the Securitization of Migration and the Expansion of Immigration Detention in the United States'* Master's Thesis in Conflict and Human Rights, Utrecht University.

Ohlin, J.D. (ed.) (2017) 'Remoteness and reciprocal risk' In *Research Handbook on Remote Warfare* pp. 15-49. UK: Edward Elgar Publishing Limited.

Orlikowski, W.J. (2007) 'Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organization', *Organizational Science* 11(406): pp. 404-428 doi: https://doi.org/10.1287/orsc.11.4.404.14600

PAX (2019a) 'State of AI: Artificial intelligence, the military and increasingly autonomous weapons' Utrecht: PAX for Peace. Available at: < https://www.paxforpeace.nl/publications/all-publications/the-state-of-ai>

PAX (2019b) 'Don't be Evil? A Survey of the Tech sector's Stance on Lethal Autonomous Weapons'. Utrecht: PAX for Peace. Available at: < https://www.paxforpeace.nl/publications/all-publications/dont-be-evil>

Pearsall, M. (1970) 'Participant observation as role and method in behavioral research' in Filstead, W. J. (ed.) *Qualitative methodology: Firsthand involvement with the social world* pp. 340–352. Chicago: Markham.

Perlinski, W.A. (2018) 'Autonomous Weapons – the "Kalashnikovs" of Tomorrow? an Analysis of the Meetings of Experts on Lethal Autonomous Weapons Systems within the Framework of the United Nations' Convention on Certain Conventional Weapons', Master's Thesis. University of Gothenburg School of Global Studies.

Petit, P. (2019) 'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization. *Science as Culture*, pp.1-27. doi: 10.1080/09505431.2019.1586866

Petman, J. M (2017).*Autonomous Weapons Systems and International Humanitarian Law: 'Out of the Loop'?* (Research reports). Helsinki: Erik Castrén Institute of International Law and Human Rights.

Phillipps, J (2018) 'The role of epistemic communities: local think tanks, international practitioners and security sector reform in Kosovo', *Southeast European and Black Sea Studies* 18(2): pp. 281-299, DOI: 10.1080/14683857.2018.1474553

Pinch, T and W.E, Bijker (1984) 'The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other', *Social Studies of Science* 14: pp. 399-441.

PwC (2018) 'Fourth Industrial Revolution for the Earth: Harnessing Artificial Intelligence for the Earth', pp. 1-48 Accessed 11 November, 2019 <https://www.pwc.com/gx/en/sustainability/assets/ai-for-the-earth-jan-2018.pdf>

Reddy, S., A, Dragan and S, Levine (2018). Shared autonomy via deep reinforcement learning. Pp. 1-10. *arXiv preprint arXiv:1802.01744*.

Reid-Henry, S. (2011) 'Spaces of security and development: An alternative mapping of the security–development nexus', *Security Dialogue* 42(1): pp. 97-104. Retrieved from http://www.jstor.org/stable/26301787

Roessingh, J.J., J, van Oijen., G, Poppinga., O, Brouwer and A, Aliko (2017) 'Towards modeling the learning process of aviators using deep reinforcement learning', 5-8 October, 2017 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) pp. 3439-3444.

Roff, H.M. (2014) 'The Strategic Robot Problem: Lethal Autonomous Weapons in War', *Journal of Military Ethics* 13(3): pp. 211-227 DOI: 10.1080/15027570.2014.975010

Sadowski, J. and Selinger, E (2014) 'Creating a taxonomic tool for technocracy and applying it to Silicon Valley', *Technology in Society* 38: pp.161-168. https://doi.org/10.1016/j.techsoc.2014.05.001

Salter, M. B (2008) 'Securitization and desecuritization: a dramaturgical analysis of the Canadian Air Transport Security Authority' *Journal of International Relations and Development* 11(4): pp. 321-349.

Salter, M.B (2006) 'The Global Visa Regime and the Political Technologies of the International Self: Borders, Bodies, Biopolitics', *Alternatives: Global, Local, Political* 31(2): pp. 167-89.

Salter, M.B (2007) 'Governmentalities of an Airport: Heterotopia and Confession,' *International Political Sociology*, 1(1): pp. 49-66.

Salter, M.B. and Mutlu, C.E. (2013) *Research Methods in Critical Security Studies: An Introduction*. New York: Routledge.

Sauer, F. (2014) 'ICRAC Statement on Legal Issues to the 2014 UN CCW Expert Meeting'. Geneva: ICRAC.

Scharre, P. (2014) 'Robotics on the Battlefield - Part I: Range, Persistence and Daring' CNAS.

Scharre, P. (2014) 'Robotics on the Battlefield Part II: The Coming Swarm' CNAS.

Scharre. P. (2018) *Army of None: Autonomous Weapons and the Future of War*. New York/London: W. W. Norton & Company.

Scheman, N. (2001) 'Epistemology resuscitated: Objectivity and trustworthiness', In Tuana, N. and S. Morgen (eds.) *Engendering rationalities* pp. 23–52. Albany: State University of New York Press.

Scherer, M. U (2016) 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies', *Harvard Journal of Law & Technology* 29(2): pp 353–400.

Schmitt, M.N. (2013) 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics', *Harvard National Security Journal Feature*, pp. 1-37. Accessed 11 November, 2019 <https://harvardnsj.org/2013/02/autonomous-weapon-systems-and-international-humanitarian-law-a-reply-to-the-critics/>

Schmitt, M.N. and J. Thurnher (2013) "Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict', *Harvard National Security Journal* 4: pp. 231-281.

Shachtman, N (2007) 'Robot Canon Kills 9, Wounds 14' *Wired magazine* https://www.wired.com/2007/10/robot-cannon-ki/ Accessed on 11 October, 2019.

Sharkey, A (2019) 'Autonomous weapons systems, killer robots and human dignity' *Ethics and Information Technology* 21(2): pp. 75-87. Accessed on 12 November 2019 < https://link.springer.com/article/10.1007/s10676-018-9494-0>

Sharkey, N. (2017) 'Why Robots Should not be Delegated with the Decision to Kill', *Connection Science* 29(2): pp.177-186.

Singer, P.W. (2009) *Wired For War: The Robotics Revolutions and Conflict in the 21st Century* USA: Penguin

Smirnova, M.Y. and S.Y. Yachin (2015) 'Epistemic Communities and Epistemic Operating Mode', *International Journal of Social Science and Humanity* 5(7): pp. 646-650. doi: 10.7763/IJSSH.2015.V5.533

Soete, L. (1985) 'International diffusion of technology, industrial development and technological leapfrogging', *World Development* 13(3): pp. 409-422. Accessed 11 November, 2019 < https://doi.org/10.1016/0305-750X(85)90138-X>

Solovyeva, A. and Hynek, N. (2018) 'Going Beyond the "Killer Robots" Debate: Six Dilemmas Autonomous Weapon Systems Raise', *Central European Journal of International and Security Studies*, 12(3): pp. 166-208. http://www.cejiss.org/issue-detail/going-beyond-the-killer-robots-debate-six-dilemmas-autonomous-weapon-systems-raise-0

Sparrow, R. (2009) 'Building a Better WarBot: Ethical Issues in the Design of Unmanned Systems for Military Applications', *Science and Engineering Ethics* 15(2): pp.169-187.

Sterio, M. (2012) 'The United States' Use of Drones in the War on Terror: The (Il)legality of Targeted Killings under International Law', *Case Western Reserve Journal of International Law* 45(1): pp. 197-214 Available at: https://scholarlycommons.law.case.edu/jil/vol45/iss1/26

Stern, M. and Ojendal, J (2010) 'Mapping the Security–Development Nexus: Conflict, Complexity, Cacophony, Convergence?', *Security Dialogue* 41(1): pp. 5-30.

Sukman, D (2015) 'Lethal Autonomous Systems and the Future of Warfare', *Canadian Military Journal* 16(1): pp. 44-53. Accessed on 12 November 2019 < https://www.files.ethz.ch/isn/195724/CMJ161E.pdf>

Surabhi, A. (2019) 'Genius Weapons: Artificial Intelligence, Autonomous Weaponry and the Future of Warfare' *Book Review* Unpublished.

Surber, R. (2018) 'Artificial Intelligence: Autonomous Technology (AT), Lethal Autonomous Weapons Systems (LAWS) and Peace Time Threats '. Zurich: ICT4Peace Foundation.

Susskind, R. and D. Susskind (2015) *The Future of the Professions*. Oxford: Oxford University Press.

Tiller, R., T. Brekken and J. Bailey (2012) 'Norwegian aquaculture expansion and Integrated Coastal Zone Management (ICZM): Simmering Conflicts and competing claims' *Marine Policy* 36(5): pp. 1086-1095

Tinoco, J. K. and Arnaud, A. (2013) 'The Transfer of Military Culture to Private Sector Organizations: A Sense of Duty Emerges', *Journal of Organizational Culture, Communications and Conflict*, 17(2): pp. 36-62 Retrieved from https://commons.erau.edu/publication/81

Ulgen, O. (2016) 'Human dignity in an age of autonomous weapons: Are we in danger of losing an 'elementary consideration of humanity'?' *8*(9). In *ESIL conference paper series, 1–19. European Society of International Law (ESIL) 2016 annual conference (Riga).* Published on January 31, 2017, ESIL SSRN.

UNIDIR (2017) 'The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations'. Geneva: UNIDIR.

US Department of Defense (2012), *Autonomy in Weapon Systems*, Directive 3000.09, Glossary, Part II Definitions, p.13.

Van der Ploeg, I. (1999) 'The Illegal Body: "Eurodac" and the Politics of Biometric Identification', *Ethics and Information Technology*, 1: pp. 295-302.

Van Vleet, E (2017) 'Edward Snowden and the Privacy vs. National Security Debate', Thesis in Politics/Government, Pacific University. https://commons.pacificu.edu/cashu/27

Verdiesen, I. (2017) 'Agency Perception and Moral Values Related to Autonomous Weapons: An Empirical Study using the Value-Sensitive Design Approach', Master's Thesis. TU Delft Technology, Policy and Management.

W.E. Bijker, J. Law (eds.) (1992) 'Shaping technology/building society', In *Studies in sociotechnical change*, pp. 1-p14, Cambridge, Massachusetts: MIT Press.

Waever, O. (1995) 'Securitization and Desecuritization' In Lipschutz, R. (ed.) *On Security* pp. 46-86. New York: Columbia University Press.

Waever, O., Buzan, B., Kelstrup, M. and Lemaitre, P. (1993) *Identity, Migration and the New Security Agenda in Europe*. New York: St. Martin's Press.

Wagner, M. (2014) 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' *Vanderbilt Journal of Transnational Law* 47(5): pp.1371-1424. Accessed 11 November 2019 <https://www.law.upenn.edu/live/files/4003-20141120---wagner-markus-dehumanizationpdf>

Welsh, S (2017) 'Clarifying the Language of Lethal Autonomy in Military Robots' In Aldinhas Ferreira, M., J, Silva Sequeira, M, Tokhi, E. Kadar and G, Virk (eds.) *A World with Robots. Intelligent Systems, Control and Automation: Science and Engineering*, pp. 171-183 Springer, Cham. Accessed on 12 November 2019 < https://link.springer.com/chapter/10.1007/978-3-319-46667-5_13#citeas>

Wilcox, L. (2017) 'Embodying algorithmic war: Gender, race, and the posthuman in drone warfare', *Security Dialogue* 48(1): pp. 11–28. https://doi.org/10.1177/0967010616657947

Wilhelmsen, J (2016) *Russia's Securitization of Chechnya: How War became acceptable* Taylor and Francis.

Williams, R. and Edge, D (1996) 'The social shaping of technology', *Research policy*, 25(6): pp. 865-899.

Winner, L. (1993) 'Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology' *Science, Technology, & Human Values,* 18(3): pp. 362-378. Retrieved from http://www.jstor.org/stable/689726

Wirls, D. (2019) 'Eisenhower Called it the 'military-Industrial Complex.' It's Vastly Bigger Now.' The Washington Post. Accessed 9 November 2019 <https://www.washingtonpost.com/politics/2019/06/26/eisenhower-called-it-military-industrial-complex-its-vastly-bigger-now/>

Woolgar, S. (2012) 'Reconstructing Man and Machine: A Note on Sociological Critiques of Cognitivism' In Bijker, W.E., Hughes, T.P. and T. Pinch (eds.) *The Social Construction of Technological Systems* pp. 303-320. USA: Massachusetts Institute of Technology

Zhang, T., Li, Q., Zhang, C. S., Liang, H. W., Li, P., Wang, T. M., .and Wu, C (2017) Current trends in the development of intelligent unmanned autonomous systems. *Frontiers of information technology & electronic engineering*, 18(1): pp. 68-85. Available at: < https://link.springer.com/article/10.1631/FITEE.1601650>