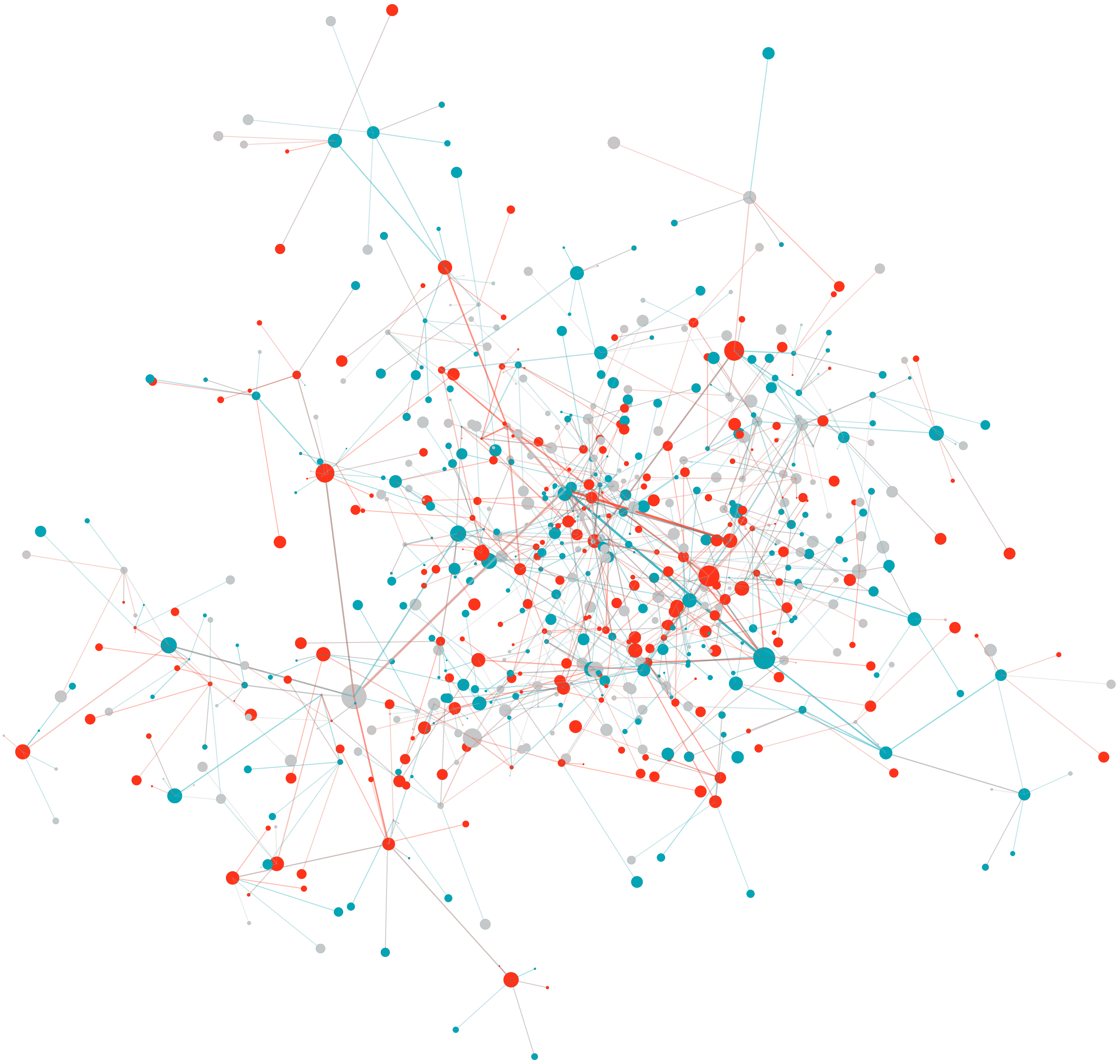
STUDIEN

ROSA LUXEMBURG STIFTUNG

LUCAS MAASER AND
STEPHANIE VERLAAN

BIG TECH GOES TO WAR

UNCOVERING THE GROWING ROLE OF US AND EUROPEAN TECHNOLOGY FIRMS IN THE MILITARY–INDUSTRIAL COMPLEX



LUCAS MAASER AND STEPHANIE VERLAAN

BIG TECH GOES TO WAR

UNCOVERING THE GROWING ROLE OF US AND EUROPEAN TECHNOLOGY FIRMS IN THE MILITARY–INDUSTRIAL COMPLEX

Study commissioned by the Rosa-Luxemburg-Stiftung

LUCAS MAASER is a programme officer at the NGO Corruption Tracker. After completing his studies in Intercultural Conflict Management, he worked as a coordinator at the International Peace Bureau (IPB). His research focuses on corruption, postcolonial perspectives on foreign policy, and the military-industrial complex.

STEPHANIE VERLAAN most recently worked as a coordinator at the International Peace Bureau (IPB). She has completed a Master's in Intercultural Conflict Management and is currently working on a degree in International Human Rights and Humanitarian Law. Verlaan is a mentee in the Young Women in Non-Proliferation and Disarmament Mentorship Programme of the European Consortium for Non-Proliferation and Disarmament, and her research focuses on weapons of mass destruction, deterrence, and "common security".

IMPRINT
STUDIEN 5/2022
is published by the Rosa-Luxemburg-Stiftung
Responsible: Loren Balhorn
Straße der Pariser Kommune 8A · 10243 Berlin, Germany · www.rosalux.de
ISSN 2194-2242 · Editorial deadline: November 2022
Illustration front page: Frank Ramspott/iStockphoto
Proofreading: Loren Balhorn
Setting/Production: MediaService GmbH Druck und Kommunikation
Printed on Circleoffset Premium White, 100 % recycled paper

Produced with the financial support of the German Federal Foreign Office. This publication is the sole responsibility of the publisher. The positions expressed herein do not reflect the views of the funding agency. The publication is distributed free of charge and may not be used for electoral campaigning purposes.

ABSTRACT

This study investigated several contractual relationships between the global defence sector and the world's most powerful private technology companies and the implications of these on the evolving military–industrial complex. A majority of the case studies centred on the US defence sector, given that it holds the world's largest defence budget, with the ensuing discussion expanding outwards to include these relationship trends within a European context. Contracts included Project Maven (Google LLC), JEDI (Microsoft, AWS), JWCC (Microsoft, AWS, Oracle, Google Cloud) and GAIA-X (a consortium of over 300 European and international companies). The investigation was formulated using four interviews and a review of current relevant literature and articles. Two interviews were with activist researchers representing civil society organizations that specialize in this area and two were with former Google employees. The discussion explores the implications of these defence-tech collaborations, and spans the War on Terror, dual-use technologies, digital bias, and the evidence suggesting similar trends are being transposed in Europe as Silicon Valley expands outside of the US. The study's aim was to kick-start a conversation within a European context and bring this issue to the attention of European civil society, drawing on the lessons from the US activist space on the ethical implications of allowing this technology to proliferate without sufficient monitoring and accountability infrastructures.

CONTENT

1 Introduction 7

2 Theoretical Framework 9
2.1 Technology, War, and the State: From the Early Modern Period to the Military–Industrial Complex 9
2.2 The Advent of Dual-Use Technology 9
2.3 New Frontiers of Warfare: Maintaining the MIC after the Cold War 10

3 The Private–Public Innovation Nexus in the US: A Case Study Analysis 12
3.2 JEDI, the Revolving Door, and its Implications for Domestic Civilian Control 14
3.2.1 The Joint Enterprise Defence Infrastructure (JEDI) 14
3.2.2 The Revolving Door as a Catalyst of "Counterterrorism" Policy 14
3.2.3 Facial Recognition, Bias, and the State 16
3.3 Apple and Facebook: Minor Players in the Military Innovation Market 18

4 Innovation Analogues and Divergences in Europe and Germany 19
4.1 GAIA-X 19
4.2 Beyond GAIA-X: The Future of Germany's Military Innovation Space 21

5 The Way Forward 23
5.1 Organizing the Opposition: Challenges and Opportunities of Becoming a Whistleblower 23
5.2 Finding Answers in Unexpected Places 23
5.3 Building Structures for a Sustainable Counter-Movement 23

6 Conclusion 25

Bibliography 27

Technical Term Glossary 31

1 INTRODUCTION

Imagine being ordered by your employer to build a product that will be used to wage war, even end the life of another. Imagine its purpose was only revealed to you after you contributed to its creation. Had you known, would you still have agreed to be involved? What would you do if you were asked not to speak about the situation with anyone outside the company? Would you, an ordinary civilian, still want to work for a company that helps facilitate war, the suffering of others, and death? This has been the situation hundreds of employees of Silicon Valley tech corporations have found themselves in.

The US military is well-known as a world leader in developing advanced technologies. Indeed, it is widely credited with developing the Advanced Research Projects Agency Network or ARPANET, commonly thought of as the prototype of the internet. Other technologies initially developed for and by the US military, such as GPS or satellite imagery, have revolutionized how the average person goes about their daily life. However, over the last 30 years, the US military has been toppled from its pedestal of technological innovation by the private tech industry's major players.[1] In order to remain on an equal footing with its adversaries, the Pentagon had little alternative but to formulate a relationship with Silicon Valley of its own.

To maintain this relationship, government agencies have ample financial resources to provide. In 2020, the budget nations across the globe spent on their military activities reached 1,981 billion US dollars. With a 2.6 percent increase over the previous year, this development not only continues a long-standing trend of growing military budgets worldwide in the face of an ongoing pandemic, but also further solidifies the US's position as the unequalled front-runner on the list, with an estimated 778 billion dollars and 39 percent of global military spending.

Endeavours like Project Maven[2] and the Joint Enterprise Defense Infrastructure (JEDI)[3] illustrate both the US military's increased focus on artificial intelligence (AI) in the development of new, decision-centric military strategy, as well as the affinity of major tech companies to contribute to this effort. To do so, self-imposed ethical obligations like Google's "Don't Be Evil" are cleverly circumvented for a share of the lucrative government contracts[4] while promoting an altruistic image in the public and attracting talent from a more conscious liberal workforce. Between 2004 and 2021, the US government's Department of Homeland Security (DHS) and the Department of Defense (DOD) alone invested more than 44 billion US dollars in the services of Google, Amazon, Facebook, Microsoft, and Twitter.[5] Silicon Valley's ambitions to build close relations with government contractors are not limited by state borders, however, as their contribution to the European cloud computing initiative GAIA-X spearheaded by France and Germany demonstrates.

While public discourse around the public-private military innovation space appears to have matured and developed a noteworthy civic opposition in the US, resources investigating these ties seem to be largely undeveloped in Europe and Germany. With this study, we aim to start building these resources, highlighting strategies to both investigate opaque collaboration practices and building meaningful civic alliances to observe them. Our work addresses academics and activists, politicians and private individuals engaged in issues of the private-public military innovation nexus alike.

The steep escalation of violence in Ukraine resulting from Russia's recent invasion of Ukraine, beginning on 24 February 2022 and which remained ongoing at the time of writing, catalysed a significant shift in traditionally hard-line government policies on military spending by the German government. Whether or not the planned upgrades to Germany's military equipment will be extended to AI innovation in the form of an increased number of contracts with private tech companies remains to be seen with heavy weaponry such as tanks, jets, and ammunition having been primarily earmarked for allocations.[6]

In our work, we first embed these recent developments within the wider history of technological innovation in the name of defence and security, to then illustrate how some of the most lucrative contracts between Big Tech firms and the US military contribute to the building of war machinery. To do so, we have identified case studies revolving around the so-called "Big Five" — Google, Apple, Facebook, Amazon and Microsoft — as major representatives of the consumer-driven technology innovation space and highlight the vast strata of other, seemingly more insignificant private actors involved in key contracts of recent years. In an analysis of the European and German market, we further give reasons why we should care about

[1] Chin, Warren (2019): "Technology, war and the state: past, present and future", in: International Affairs – Re-visioning war and the state in the twenty-first century, pp. 770–772; in URL: https://academic.oup.com/ia/article/95/4/765/5513164, last accessed on March 10, 2022. [2] Peitz, Dirk (June 8, 2018): "Google wird einfach ersetzt", ed. "Die Zeit"; in URL: www.zeit.de/digital/internet/2018-06/maven-militaerprojekt-google-ausstieg-ruestungsexperte-paul-scharre, last accessed on December 13, 2021. [3] Surpassed by the Joint Warfighter Cloud Capability (JWCC)- and Indefinite Delivery-Indefinite Quantity (IDIQ)-programmes. Comp. e.g. US Department of Defense (July 6, 2021): "Future of the Joint Enterprise Defense Infrastructure Cloud Contract"; in URL: www.defense.gov/Newsroom/Releases/Release/Article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/, last accessed on December 13, 2021. [4] Comp. e.g. Brewster, Thomas (December 22, 2020): "Google Promised Not To Use Its AI In Weapons, So Why Is It Investing In Startups Straight Out Of 'Star Wars'?, ed. Forbes Magazine; in URL: www.forbes.com/sites/thomasbrewster/2020/12/22/google-promised-not-to-use-its-ai-in-weapons-so-why-is-alphabet-investing-in-ai-satellite-startups-with-military-contracts/?sh=30ba15537595, last accessed on December 13, 2021. [5] Comp. data published through the campaign "Big Tech Sells War"; in URL: https://bigtechsellswar.com/, last accessed on December 13, 2021. [6] Rauwald, Christoph, Wilkes, William & Patel, Tara (February 28, 2022): "Europe is Re-arming, and Its Defence Firms Stand To Profit", via Bloomberg Quint; in URL: www.bloombergquint.com/business/europe-is-rearming-and-its-defense-firms-stand-to-profit, last accessed on March 10, 2022.

US innovation systems in our region and how civilians have organized in the past to build an opposition and make their voices heard.

In our research process, we were guided by the following four questions:

- *What forms of cooperation exist between the European and US defence sector and the "Big Five"?*
- *What are the (potential) negative consequences of these collaborations?*
- *What strategies can the peace and other social movements use to effectively counter this work?*
- *Which alliances and networks can be developed for future projects and actions?*

The limitation to the five major US players examined is first and foremost a decision in reflection of this study's scope. Other major players like IBM and HP Inc. — while no less significant — were therefore not considered. While we also acknowledge the multi-layered structure of the information technology sector, ranging from producers of semiconductors over providers of telecommunications equipment to network- as well as access- and service providers, the contracts examined on the basis of procurement stream analysis and publicly available data did not produce sufficient ties to these aspects and hence could not be considered in the scope of this study. As our work is meant to serve as a starting point to further investigation of issues inherent in this field, we explicitly invite researchers to complement our work with these aspects in mind.

2 THEORETICAL FRAMEWORK

2.1 TECHNOLOGY, WAR, AND THE STATE: FROM THE EARLY MODERN PERIOD TO THE MILITARY–INDUSTRIAL COMPLEX

The relationship between private innovation and military application did not emerge in the twenty-first century. In order to understand the structures established by the intersections between the two sectors, we will contextualize the phenomena we see today in their shared history with a focus on dual-use technology.

In his examination of the relationship between technology, war, and the state throughout history, Warren Chin attests a "synergistic relationship"[7] between acts of war and the prosperity of the state, causing both to evolve exponentially from the early modern period to the mid-twentieth century. This mutually beneficial relationship may have superficially declined after World War II and given space for "new political and economic priorities to emerge"[8] which significantly impacted the role of the state. With the emerging framework of international institutions built on the legacy of the horrors of war, Chin argues, this development rather signifies a shift towards a more subtle form of war, however, characterized by its aversion of interstate confrontation and enhanced complexity.[9]

Along with the advancements in nuclear warfare, the significance of technology increased significantly with the shift towards nuclear deterrence policies. Chin finds that "technological development reduced the opportunities for war, but the arms race it generated also brought into being new technologies, and these facilitated new forms of conflict".[10]

In this environment, the US state took on a key role in sponsoring defence technology research. This was not an entirely new development at the time, as the evolution of military needs had caused persistently rising interests of states in technological solutions since the late nineteenth century.[11] While government-sparked innovation was largely bound to the need of quantity over quality on the battlefield and "required the mobilization of society and the economy via the state"[12] until 1945 — including an education and health care system providing the resources needed for an open confrontation[13] — the focus shifted towards a more diversified perspective on war in the post-modern era, redefining and deconstructing the margins within which peace and conflict operate "to employ war as a political tool in a nuclear world".[14] The emergence of the Cold War amplified the need for an enhanced non-military toolset, widening the scope of defence to the psychological, political, social, and economic spheres.[15]

With nuclear deterrence becoming the key driver of global power dynamics, Chin argues, "the rituals of war in terms of organizing, preparing and demonstrating an ability to fight nuclear war in the hope of deterring potential opponents and thereby preventing the possibility of war became substitutes for organized violence".[16] In the Cold War narrative, security thus became synonymous with the available nuclear arsenal and nuclear defence resources, increasing the need for the state to invest in technological advancements in both sectors.

Against the backdrop of a supposedly ever-present nuclear threat, continuously rising budgets for defence research were easily justifiable by the state. The provision of state-financed resources to looming technological innovations hence accelerated their development considerably, establishing sound ties between private corporations and the state through complex research and development (R&D) programmes.[17] In 1961, then-US President Dwight D. Eisenhower coined the term "military–industrial complex" (MIC) to highlight the potential collusion stemming from common interests within this environment between stakeholders from politics, the defence industry, and the military to further expand military expenditure.[18]

2.2 THE ADVENT OF DUAL-USE TECHNOLOGY

The bond between the military and private sector further had implications for the common space research outcomes shared, impacting the "mechanisms of technological transfer from civilian to defence (spin-in), and defence to civilian (spin-off)"[19] realms. In his examination of the "Technological Military/Civilian Duality", François-Xavier Meunier identifies a tipping point in this dynamic between 1970 and 1980.

With the prolonged nuclear threat and a growing international peace movement opposing defence policy strategies by major opposing state parties, the ever-growing amount of military expenditure with the military as a key driver in innovation was increasingly hard to justify. It was this environment in which the term "dual use" was first introduced in the US as a means to maintain "civilian R&D expenditure on defence budgets, and thus circumvent the rules of the [World Trade Organization]",[20] Meunier finds. By constructing this supposedly mutually beneficial intersection between the civilian and military market, dual use technology thus further contributed to the normalization of the close relationship between the two spheres.

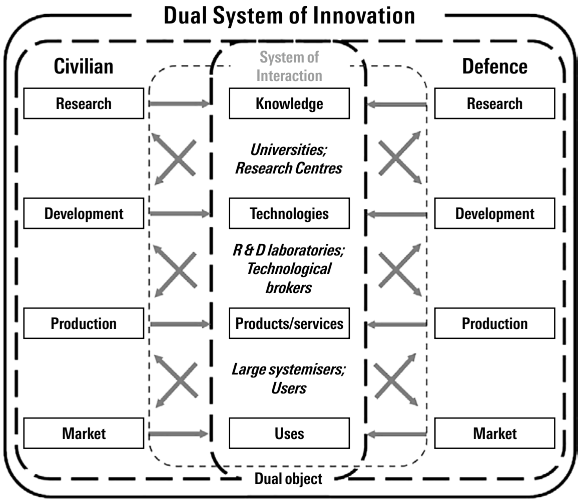
Since the 1980s, the concept of duality "has gradually liberated itself from the simple strategy of circumventing the rules of international trade"[21] and has since evolved into, as Guichard and Heisbourg describe it,

[7] Chin (2019): p. 765. [8] Ibid. [9] Comp. ibid. [10] Ibid. [11] Comp. ibid. [12] Ibid., p. 768. [13] Comp. ibid. [14] Ibid. [15] Comp. ibid. [16] Ibid., p. 769. [17] Comp. ibid. [18] Comp. Eisenhower, Dwight D. (1961): "Military-Industrial Complex Speech"; in URL: https://avalon.law.yale.edu/20th_century/eisenhower001.asp, last accessed on March 10, 2022. [19] Meunier, François-Xavier (2019): "Construction of an Operational Concept of Technological Military/Civilian Duality", in: Journal of innovation Economics & Management, 2019/2 n° 29, pp. 159–182, p. 162; in URL: https://doi.org/10.3917/jie.029.0159, last accessed on March 10, 2022. [20] Ibid., p. 160. [21] Ibid., p. 161.

"a method of managing research, innovation, and the production of systems of defence which seek to produce economies of scale, variety, and externalities with the civilian sector".[22]

Meunier differentiates between what can be described as "dual use" and "dual innovation". In the case of dual use, an array of technology may have both civilian and military use cases for which "the objective of duality is to facilitate transfers from one sphere to the other, taking into account the problems of technological adaptation that this operation can produce".[23] Conversely, in a "dual innovation" process, Meunier describes, "the challenge of duality is to facilitate technological co-production between the civilian and the military sphere. Transfer is no longer an issue because the defence and civilian specificities are taken into account during the innovation process."[24] In both cases, "managing duality … implies a mode of governance that connects public authorities, private firms, and research centers",[25] relying on public policy to regulate the boundaries within which knowledge and technology is disseminated while taking advantage of resources from increasingly global markets.

Figure 1: Dual System Innovation



Source: Meunier (2019), p. 172.

2.3 NEW FRONTIERS OF WARFARE: MAINTAINING THE MIC AFTER THE COLD WAR

With the conclusion of the Cold War in 1992, the sudden dissolution of an ever-present military threat resulted in a vast decline in both the defence budget and the involvement of the state in R&D programmes, allowing private corporations to become more prominent in the defence industry. This also meant a significant change in policy. While the state had been the key driver of innovation behind technological accomplishments like the internet and satellite surveillance during the Cold War, this responsibility now fell to major players on the private tech market.

"The subsequent exploitation of [military] technologies by the private sector", Chin finds, "reflected a conscious policy choice by most western governments, which was to promote technology spinoffs from defence research into the wider economy as a way of generating wealth creation." This led to a wave of "dual use" innovation and Cold War technology spin-off products on the civilian market. The demand for these products generated the capital for the private sector to shape technological innovation itself, allowing it to take on an increasingly central role in the information revolution.[26]

In this environment, Chin reflects, "military power relied increasingly on the existing pool of technological knowledge within the broader economy".[27] Along with the increasing demand for quality over mass on the battlefield and the resulting rising demand for complex systems in military operations, private companies became indispensable for the defence innovation sector, leading "western states [to] increasingly subcontract … the provision of internal and external security to the private sector".[28]

New technological advances and their impact on strategies of war allowed the state to continue military operations even if there was no domestic consensus concerning direct involvement in armed activities, upholding the interest of the state in perpetuating the MIC as a viable means to support defence policy between the end of the Cold War and the beginning of the "War on Terror"[29] (WoT). The WoT then ushered in a new evolutionary step in how war was conceived, relying on less risk-, but more capital-intensive resources like satellites and drones.[30] Along with these technological advances' enhanced capabilities, their application shifted further towards the domestic sphere, amplifying the state's ability to exercise power over its citizens through technology. While technological progress and domestic policy may have shaped an environment in which overt surveillance and control could be justified with a counterterrorism narrative, the state further explored opportunities to assert control over individuals via technology intended for civilian services more actively.[31]

The environment in which this evolution occurred can be conceived as what is called the Fourth Industrial Revolution, first put forward by Klaus Schwab in 2017.[32] The idea postulates that digital technologies that incorporate computer hardware, software, and networks and the extreme intricacy in which they interact with each other are reinventing our societies and global economic networks. What makes this significant is the capacity of these technologies to be trans-

[22] Guichard, Renelle, Heisbourg, François (2004): "Recherche militaire: vers un nouveau modèle de gestion?", Paris, Economica, p. 97. [23] Meunier (2019): pp. 163–164. [24] Ibid., p. 164. [25] Ibid., p. 166. [26] Chin (2019): p. 770. [27] Ibid. [28] ibid. [29] An ongoing international military campaign headed by the US government following the terrorist attacks on September 11, 2001. [30] After ibid., p. 772. [31] After Graham, Stephen (2011): "Cities under siege", chapter 3: 'The military urbanism', section: 'Tracking: citizen–consumer–soldier'. [32] Klaus Schwab (2017): "The fourth Industrial Revolution", London: Penguin Random House.

posed across digital, physical, and biological spaces, interconnecting what had previously been relatively separate technological dimensions, thereby opening up an entirely new realm of possibilities. These new abilities are expanding into multiple areas with multiple types of technologies now possible, including "a much more ubiquitous and mobile internet, … smaller and more powerful sensors that have become cheaper, and … powerful artificial intelligence (AI) and machine learning".[33] It is the fusion of these areas which signifies entrance to a new era of innovation.

This framework highlights pathways to the central means needed for the Pentagon's Third Offset Strategy (TOS). Introduced in 2014, it proposes US defence innovation priorities in response to potential threats from opposing powers like Russia and China. The TOS aims to ensure both the defence sector's access to knowledge generated by commercial and civilian R&D internationally as well as explore feasible opportunities to exploit this knowledge for maintaining US military superiority. This also means taking advantage of more recent civilian technological innovation trends like AI and machine learning.[34] The establishment of the Silicon-Valley based "Defence Innovation Unit" in 2015 may be seen as a symptom of this endeavour.

Meanwhile, this strategic development has been accompanied by attempts by private Silicon Valley stakeholders to push for the re-establishment of a Cold War-like working relationship between the civilian sector and the state, reinvigorating Eisenhower's concerns over a MIC. The Silicon Valley Defense Group, which major players of civilian market-oriented services like Microsoft, Amazon Web Services (AWS), and Google actively contribute to, mourning the "eroded trust" caused by the ever-growing gap between industry and the state and advocating for higher investments and more liberal regulation policies is just one of many examples of this dynamic.[35]

[33] Ibid., p. 7. "Machine learning" signifies a process by which a digital machine learns and improves its abilities using algorithms and experience. [34] After Meunier (2019): p. 773. [35] Silicon Valley Defense Group (2020): "Fall 2020 Roundtable Series Insight Paper – Unlocking New Sources of Techno-Security Advantage", p. 6.

3 THE PRIVATE–PUBLIC INNOVATION NEXUS IN THE US: A CASE STUDY ANALYSIS

The following chapters investigate some of the key tendencies of this relationship. Through the analysis of prominent contract case studies, we highlight a multitude of dimensions of concern, touching upon ethics in project goals, the procurement of government projects, meddling, and technological bias. The selection of examined private technology corporations was first and foremost driven by their degree of consumer market capitalization and civil consumer awareness in both the US and Europe. Despite the award of contracts with considerable volumes, corporations like IBM and HP have therefore not been considered. We would like to actively encourage the analysis of related cases, however, like IBM's contributions to the US military IT modernization endeavour ITES-2S, for which its awards cumulated to an estimated 1 billion US dollars between the initiative's inception in 2005 and May 2020,[36] or HP's 3-billion-dollar contract for the provision of IT support for the US Navy in 2017.[37]

3.1 PROJECT MAVEN

"Project Maven" is one of the most prominent examples of a major civilian player cooperating with the US military in recent years. The endeavour was conceived with the aim to autonomously identify "objects of interest" through the automated analysis of massive picture and video data pools.[38] Valued at an estimated 250 million dollars per year,[39] the project gained notoriety in 2018 when Google employees organized a walk-out to protest its employer's support of the initiative, claiming a breach of Google's ethical commitment to omit any active contribution to technology with the potential of war application.[40]

In April 2017, then-Deputy Defense Secretary Bob Work started assembling an Algorithmic Warfare[41] Cross-Functional Team. Its self-declared goal was to integrate artificial intelligence and machine learning technologies into existing DoD resources more efficiently with the intent to "maintain [its] advantages over increasingly capable adversaries and competitors"[42] at the time. This endeavour could only be realized "with commercial partners alongside us",[43] said Drew Cukor, Marine Corps Col. and chief of the newly founded team at a 2017 presentation.

One of these commercial partners was Google, supporting the initiative by providing the Pentagon with their open-source AI software TensorFlow. "The US military does not use [TensorFlow] in weapons systems, and certainly not in supposedly autonomous ones. But the mere fact that Google is working with the US military has led to employee protests and ultimately to the company not renewing its existing contract with the Department of Defense", said US security expert and senior fellow at the Center for a New American Security Paul Scharre in 2018.[44] As an attempt at controlling some of the damage caused by the affair both internally and externally, Google CEO Sundar Pichai committed to "not design or deploy AI" in the area of "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people" in a 2018 blog post titled "AI at Google: our principles".[45]

These self-imposed obligations allowed Google to frame its ethics independently, allowing substantial carve-outs for surveillance and other AI-driven technology related to the defence sector. It is arguable that even Project Maven would qualify as a legitimate project under Google's new AI principle umbrella, Laura Nolan, former Google employee and founding member of the Campaign to Stop Killer Robots — a major global initiative calling for a ban on lethal autonomous weapon — suggests.

> Nobody was saying that Maven was a weapon. Maven is an information system that you use to select your target. The weapon is a relatively trivial part — the tip of the spear. So Google was actually saying: "We'll build the spear and the DoD will provide the tips." Google's omission to address surveillance was also extremely disappointing because that's fundamentally what Maven was.
>
> It's a surveillance project, not a weapon. But this individualized warfare paradigm very much depends on the sort of mass surveillance, which is damaging in and of itself. We have people living under surveillance for years, working communities apart. People won't gather in groups, people won't send their kids to school, people won't go to each other's funerals. What does that do to a community over a decade?[46]

The degree to which ethics merely signified a strategic means to avert further damage amid the crisis triggered by Google's involvement with Project Maven is evidenced in the reliance on patriotic narratives to

[36] Moss, Sebastian (May 1, 2020): IBM gets $18.8m contract modification for ongoing US Army IT modernization award, ITES-2S, ed. Data Center Dynamics; in URL: www.datacenterdynamics.com/en/news/ibm-gets-188m-contract-modification-ongoing-us-army-it-modernization-award-ites-2s/.

[37] Bylund, Anders (April 6, 2017): Meet Hewlett-Packard, the Defense Contractor, ed. The Motley Fool; in URL: www.fool.com/investing/value/2010/07/09/meet-hewlett-packard-the-defense-contractor.aspx.

[38] Pellerin, Cheryl (July 21, 2017): "Project Maven to Deploy Computer Algorithms to War Zone by Year's End", ed. US Department of Defense; in URL: www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/, last accessed on December 13, 2021.

[39] Brewster (December 22, 2020).

[40] Comp. Wakabayashi, Daisuke; Shane, Scott (June 1 2018): "Google Will Not Renew Pentagon Contract That Upset Employees", ed. The New York Times; in URL: www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html, last accessed on December 13, 2021.

[41] The combined employment of systems and resources relying on algorithms in their use. These include autonomous weapons, AI and the analysis of big data.

[42] Pellerin (July 21 2017).

[43] Ibid.

[44] Peitz, Dirk (June 8, 2018): „Google wird einfach ersetzt", ed. "Die Zeit"; in URL: www.zeit.de/digital/internet/2018-06/maven-militaerprojekt-google-ausstieg-ruestungsexperte-paul-scharre, last accessed on December 13 2021.

[45] Pichai, Sundar (June 7, 2018): "AI at Google: our principles"; in URL: www.blog.google/technology/ai/ai-principles/, last accessed on December 13 2021.

[46] Transcript of Interview with Laura Nolan (Campaign to Stop Killer Robots), led by the authors on February 18, 2022, in URL: https://docs.google.com/document/d/1uado2xvqcdTs5yIDljbxD7N6QBmmc5bu/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true.

address internal concerns around the contract prior to the publication of Pichai's blog post. In the course of internal town hall meetings organized by Google's leadership in March 2018 to address employees' concerns over the project, decision makers heavily relied on a "support our troops"-argument to justify the continuation of Google's contributions to this endeavour, Nolan finds.

> I should say that a minority of people thought it was a good thing to "support our troops". Google is a very international organization and for most Googlers, they were by no means our troops. But that was how the US-based leadership always phrased it.

By signalling the disposition to consider and adhere to demands for enhanced ethical guidelines, the image of a consumer service-driven player with altruistic maxims can be maintained — not only towards the public, but especially towards the workforce.

> Google has for years been attracting a fairly liberal, fairly left set of employees — and a very international set of employees as well. Even if you go to the US offices, particularly the engineering offices, very many people are not US in origin. Google has always hired very heavily across the globe. So there's a lot of non-Americans working for Google and a lot of Americans who would have anti-war sympathy.[47]

With the self-imposed and supposedly enhanced ethical guidelines in place, pressure moreover decreased for lawmakers to further regulate the space in which private technology corporations could cooperate with the military. With a highly evolved and well-functioning lobby for private-military R&D endeavours in the US, obstacles are often insurmountable for a stronger regulatory legislative framework to develop.

As reactions to Google cutting ties with Project Maven while continuing to work on "Project Dragonfly", a search engine in line with the Chinese government's domestic policies, PayPal co-founder and Trump-donor Peter Thiel deemed Google's behaviour "seemingly treasonous",[48] a critique mirrored by Chairman of the Joint Chiefs of Staff Marine Corps Gen. Joseph Dunford.[49]

A recent analysis by Forbes associate editor Thomas Brewster revealed that AWS and Microsoft filled the gap left by Google in 2019, securing a combined 50 million US dollars in Pentagon contracts since.[50] He further found that despite his enhanced ethical commitment, Pichai becoming Google parent Alphabet Inc.'s CEO in late 2019 did not impact its thriving investments in start-ups like Orbital, Planet, and ClarifAI, offering satellite image data and analysis services to the military through Alphabet's venture capital wing GV.[51] Not only is their field of expertise reminiscent of Google's Project Maven contribution, but Orbital evidently even won a contract under the Maven umbrella, scoring a total of 1.8 million dollars for the development of "high-altitude still imagery multispectral models".[52]

With Rebellion Defense, Orbital is joined by another start-up working on Maven with direct links to the Mountain View-based tech giant. Founded by Google's former CEO Eric Schmidt,[53] Rebellion Defense commits to "design AI products purpose-built for defence in the era in which software superiority will determine national security advantage".[54] Schmidt has built a reputation in bridging the gap between Silicon Valley and the defence sector, raising concerns over conflicts of interests through his membership in two DoD advisory boards for the enhancement of its AI technologies while retaining his role as a technical advisor at Alphabet and holding 5.3 billion dollars in shares of the Google parent.[55]

Rebellion Defense CEO and co-founder Chris Lynch also holds a role as founding director at Defense Digital Service (DDS), a Pentagon "rapid response team"[56] which initiated JEDI, an initiative best-known for the legal stalemate it created between Google and AWS over the 10-billion-dollar project and focus of this study's following chapter.[57] Lynch's founding partners Nicole Camarillo and Oliver Lewis both share his extensive background in the security sector.[58]

This dynamic not only feeds into a history of Google actively following the money to Pentagon contracts while working hard to maintain their image as a "Don't Be Evil" consumer tech innovator — it is also indicative of the much-evolved revolving-door hiring practices between the US defence sector and Silicon Valley,[59] a dynamic highlighted more prominently in the following chapter.

[47] Ibid. [48] Chafkin, Max (July 14 2019): "Peter Thiel Urges U.S. Probe of Google's 'Seemingly Treasonous' Acts" , ed. Bloomberg; in URL: www.bloomberg.com/news/articles/2019-07-15/thiel-urges-u-s-probe-of-google-s-seemingly-treasonous-acts, last accessed on December 13 2021. [49] Magnuson, Stew (November 18, 2018): "Dunford Slams Google for Working with China, But Not U.S. Military", ed. National Defense; in URL: www.nationaldefensemagazine.org/articles/2018/11/18/dunford-slams-google-for-working-with-china-but-not-us-military, last accessed on December 13 2021. [50] Brewster, Thomas (September 8, 2021): "Project Maven: Amazon And Microsoft Scored $50 Million In Pentagon Surveillance Contracts After Google Quit", ed. Forbes; in URL: www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after-google/?sh=52af312f6f1e, last accessed on December 13, 2021. [51] Brewster (December 22, 2020). [52] Brewster (September 8, 2021). [53] Rebellion Defense was not co-founded by Schmidt personally, but through his company Innovation Endeavors. [54] Comp. self-description of Rebellion Defense's products, accessible in URL: https://rebelliondefence.com/rebellion-products, last accessed on December 13, 2021. [55] Conger, Kate; Metz, Cade (May 2, 2020): "'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive", ed. The New York Times; in URL: www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html, last accessed on December 13, 2021. [56] Comp. self-description of the DDS, accessible in URL: www.dds.mil/, last accessed on December 13, 2021. [57] Conger, Kate; Sanger, David E. (July 6, 2021): "Pentagon Cancels a Disputed $10 Billion Technology Contract", ed. The New York Times; in URL: www.nytimes.com/2021/07/06/technology/JEDI-contract-cancelled.html, last accessed on December 13, 2021. [58] Brewster (September 8, 2021. [59] For a more in-depth analysis, comp. the campaign "Big Tech Sells War" (https://bigtechsellswar.com/), along with its project "Big Tech Sells War: A Revolving Door" (https://littlesis.org/oligrapher/7155/share/a8e846a75c90f5a6d14e).

3.2 JEDI, THE REVOLVING DOOR, AND ITS IMPLICATIONS FOR DOMESTIC CIVILIAN CONTROL

3.2.1 The Joint Enterprise Defence Infrastructure (JEDI)

Even before attracting attention over its legal dispute between competing contractors, the Joint Enterprise Defence Infrastructure (JEDI) signalled another major area of development for which the DoD sought assistance from the US civilian tech market. JEDI was a multi-cloud computing project which aimed to support enhanced communication between the Pentagon and soldiers in the field as well as between the different defence agencies. The contract, for which AWS had been the anticipated awardee, was ultimately assigned to Microsoft over alleged conflicts of interest related to AWS employee Deap Ubhi.

Following prior concerns, JEDI co-competitor Oracle had filed a lawsuit with the US Court of Federal Claims, alleging that AWS had significantly influenced the procurement process through Ubhi's employment with the Pentagon.[60] Ubhi left AWS in 2016 to join the DDS where he also contributed to the JEDI contract. In this new role, he continuously referred to himself as an "Amazonian" while taking positions favouring the previously criticized single-contract award. In 2017, he then withdrew from his role in the JEDI procurement process while running a tech start-up that aimed to provide restaurants with additional resources to do business online, which drew the attention of AWS. Ubhi then recused himself from his work on JEDI entirely, citing potential conflicts of interest due to partnership negotiations with his former employer. While the outcomes of these discussions remain unclear, Ubhi left the Pentagon to re-join AWS shortly after.[61]

The Defense Department was tasked with further investigating Ubhi's role in the contract, suspending its procurement for the duration of the investigation. The Department found that Ubhi's "participation in the procurement did not and could not negatively affect the integrity of the procurement going forward"[62] and his role in the JEDI contract had been permitted "because his employment with Amazon ended more than one year before the procurement began".[63] Oracle criticized the investigation for its superficial examination of the case, disregarding the DoD's lack of oversight over the contract and ignoring Ubhi's employment at AWS after leaving the Pentagon in its considerations.[64] AWS later contested the decision to award the contract to Microsoft in court.

In July 2021, the DoD then announced it was dissolving the 10-billion-dollar JEDI contract, reasoning that it no longer met the Department's needs. In addition to the controversy's potential impact on the contract's realizability, this decision may also be a reflection of the rapid pace at which the military innovation market operates. Further, the legal battle between the vendors had pushed the deliverable timeline beyond an acceptable limit. Immediately after dissolving JEDI, the DoD announced the Joint Warfighting Cloud Capability (JWCC) project as its replacement. The JWCC differs from JEDI in that, rather than developing a single cloud entity via a single vendor, the contract would be awarded to multiple Cloud Service Providers that the DoD deemed capable of meeting its requirements. Each vendor would be tasked with developing a cloud entity with a specific purpose. This approach intended for each cloud to be better protected and make containing security breaches easier. Awarded contracts would take the form of "indefinite delivery indefinite quantity" (IDIQ), stipulating an indefinite amount of services within a specific timeframe. The DoD announced in November 2021 that it expects to award IDIQ contracts to both Microsoft and AWS. It also put out a request for proposals to Google Cloud and Oracle to join the initiative.

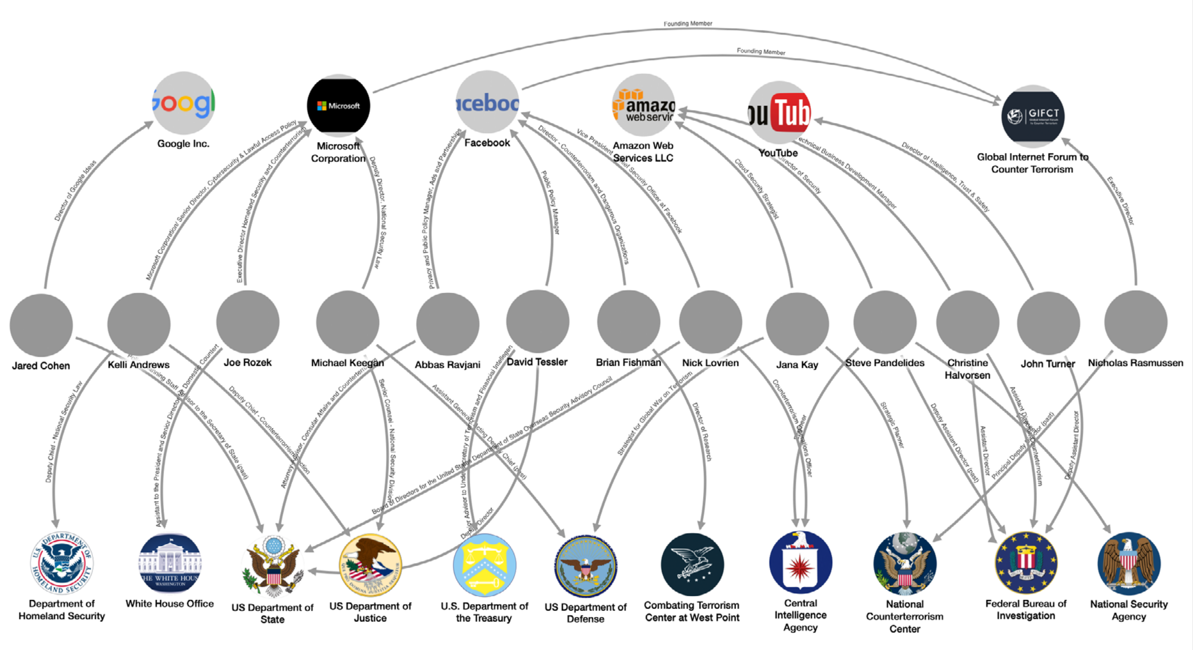
The walk-out staged by Google employees over its involvement with Project Maven set the precedent for the company's decision not to bid on the JEDI contract. Google Cloud CEO Thomas Kurian explained in a blog post dated 12 November 2021 that, although its decision to recuse itself from JEDI was due to a lack of assurance its work would not violate its AI ethics principles, he believed joining the JWCC would not violate this code. He did acknowledge, however, that it was understood not all employees would agree with this reasoning.[65] Kurian attempted to justify this by differentiating between JEDI and JWCC and highlighting other defence-related projects it had successfully collaborated with the DoD on without violating its ethics code. Kurian's blog post was a response to questions raised in a company-wide all-staff meeting during which over 1,000 employees questioned Google's involvement in JWCC.[66] AWS had not, at the time of writing, reported any internal controversy or ethical concerns surrounding its involvement with either JEDI or JWCC.

3.2.2 The Revolving Door as a Catalyst of "Counterterrorism" Policy

The controversy around Deap Ubhi is situated in an environment which is prone to a vivid exchange of personnel and expertise between the private tech and defence sectors, as Munira Lokhandwala, director of technology and training at the grassroots watchdog network LittleSis, attests. As part of the campaign Big

[60] Gregg, Aaron; Greene, Jay (October 30, 2019): "Fierce backlash against Amazon paved the way for Microsoft's stunning Pentagon cloud win"; in URL: www.washingtonpost.com/business/2019/10/30/fierce-backlash-against-amazon-paved-way-microsofts-stunning-pentagon-cloud-win/, last accessed on March 10, 2022. [61] Davenport, Christian; Gregg, Aaron (January 24, 2019): "Pentagon to review Amazon employee's influence over $10 billion government contract"; in URL: www.seattletimes.com/business/pentagon-to-review-amazon-employees-influence-over-10-billion-government-contract/, last accessed on March 10, 2022. [62] Gregg; Greene (October 30, 2019). [63] Ibid. [64] Davenport; Gregg (January 24, 2019). [65] Kurian, Thomas (November 12, 2021): "Update on Google Cloud's work with the U.S. Government", in URL: https://cloud.google.com/blog/topics/inside-google-cloud/update-on-google-clouds-work-with-the-us-government, last accessed on December 13, 2021. [66] Elias, Jennifer (November 15, 2021): Google's pursuit of military cloud deal was among top issues at last week's all-staff meeting", ed. CNBC; in URL: www.cnbc.com/2021/11/15/google-pursuit-of-jwcc-among-issues-of-top-concern-at-tgif-meeting-.html, last accessed on December 13, 2021.

Figure 2: Big Tech Sells War — A Revolving Door


Founding Member
Founding Member
Google Inc.
Microsoft Corporation
Facebook
Amazon Web Services LLC
YouTube
Global Internet Forum to Counter Terrorism
Director of Google Ideas
Microsoft Corporation/ Senior Director, Cybersecurity & Lawful Access Policy
Executive Director Homeland Security and Counterterrorism
Deputy Director, National Security Law
Privacy and Public Policy Manager, Ads and Partnerships
Public Policy Manager
Director - Counterterrorism and Dangerous Organizations
Vice President, Chief Security Officer at Facebook
Cloud Security Strategist
Director of Security
Technical Business Development Manager
Director of Intelligence, Trust & Safety
Executive Director
Jared Cohen
Kelli Andrews
Joe Rozek
Michael Keegan
Abbas Ravjani
David Tessler
Brian Fishman
Nick Lovrien
Jana Kay
Steve Pandelides
Christine Halvorsen
John Turner
Nicholas Rasmussen
Deputy Chief - National Security Law
Deputy Chief - Counterterrorism Section
Senior Counsel - National Security Division
Board of Directors for the United States Department of State Overseas Security Advisory Council
Strategist for Global War on Terrorism
Director of Research
Counterterrorism Operations Officer
Strategic Planner
Deputy Assistant Director (past)
Assistant Director
Principal Deputy Director (past)
Deputy Assistant Director
Department of Homeland Security
White House Office
US Department of State
US Department of Justice
U.S. Department of the Treasury
US Department of Defense
Combating Terrorism Center at West Point
Central Intelligence Agency
National Counterterrorism Center
Federal Bureau of Investigation
National Security Agency

Source: Lokhandwala, Munira (2021), created using LittleSis Oligrapher; in URL: https://littlesis.org/oligrapher/7155/share/a8e846a75c90f5a6d14e, last accessed on March 10, 2022

Tech Sells War (BTSW), a collaborative effort in cooperation with MPower Change and the Action Center on Race and Economy (ACRE), Lokhandwala analysed and mapped 13 cases in which individuals repeatedly changed positions between the private tech industry and the Pentagon:

> In 20 years of what we call the global war on terror, we've seen this massive inflation of the tech sector. We have these private companies that do business and make products. But then we have this massive industry around them that supports their agenda. With Big Tech Sells War, we wanted to see how these two entities are relating to one another on the level of lobbying. This is what we — in the context of the US — call the revolving door between the public and private sector.[67]

The War on Terror was a term coined by the George W. Bush Administration following the 9/11 terrorist attacks in 2001. It catalysed America's 20-year war in Afghanistan. One of the major aspects of BTSW is its contribution to the MIC discourse in highlighting the correlation between the rise of big tech with the beginning of the WoT. Further, the campaign was able to demonstrate direct causation and motives of Big Tech. BTSW launched a side campaign called "WhoseTube" which calls out the complicity of YouTube, owned by Google, in spreading anti-Muslim narratives by allowing Islamophobic content to be circulated on its platform, thereby fuelling public support for aggressive government stances toward Muslim populations and the development of weapons to engage in the WoT. By creating the conditions for Muslims to be feared and therefore seen as legitimate targets, its parent company Google inherently increases its ability to profit further by selling technology to the US government that will be deployed throughout its combat operations in the WoT.[68]

One of the key aspects in conceiving the project was to illustrate the multitude of dimensions the revolving door affects, Lokhandwala explains:

> We wanted to give examples that highlighted the range of ways that tech is influencing policy making and the range of actors within this "global war on terror". It's not just the Department of Defense. We have people who worked in the FBI for 20 years and people who worked in the CIA — these different arms of the US military surveillance state — then transitioning into very comfortable high-level jobs within the tech industry. We're also not just talking about tech companies. I think it's important to realize that when we're taking on [private corporations like] Google, we're not just talking about Google, we're talking about all the other entities that are profiting from Google's existence. We're talking about think tanks, trade organizations and all different arms of the tech sector as well.[69]

Combined with a mindset that promotes a very particular understanding of security through purported counterterrorism policies, Lokhandwala finds that this dynamic has very real consequences for civilians in the domestic sphere — especially for non-white US citizens:

[67] Transcript of Interview with Munira Lokhandwala (LittleSis), led by the authors on February 02, 2022, in URL: https://docs.google.com/document/d/1erwtg_LcvxU-cRK12vu2Kp-heYtV4YYgs/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. [68] Action Center on Race & the Economy (2021); in URL: https://acrecampaigns.org/wp-content/uploads/2021/12/Website-2022-21-ACREI-Overview.pdf, last accessed on March 10, 2022. [69] Ibid.

> The group of people that we zeroed in on in our research also represents a very particular ideology within the war on terror", which is one that is focused on this idea of counterterrorism. The counterterrorism industry as a sort of subsector of the "global war on terror" is massive and it has justified the profiling and surveillance of people of color in the US and abroad. It has created its own monster.[70]

3.2.3 Facial Recognition, Bias, and the State

One means to implement these domestic profiling and surveillance policies are facial recognition technologies (FRTs). Although not a new type of technology, FRTs are a massive influencing factor in the construction of a new MIC. Like many other technologies initially developed for military or highly exclusive purposes, FRTs have become commonplace in everyday life, e.g. as a built-in security feature of smartphones.

Prior to this expansion, their use and capabilities were predominantly relevant only to a limited group working in tech or funding its development. Today, the implications of their utilization are more widely discussed outside of technical contexts. Opinions differ widely between populations on the ethical applicability of FRTs and the importance of understanding how an algorithm is created, including its use in private versus public spaces or between the user and the FRT target. Whilst an iPhone user might not particularly care to understand the algorithm it uses to identify their face, a police officer should care to understand the algorithm used to identify persons suspected of lawbreaking given the consequences an inaccurate match could have. It is here that the ethical implications of built-in biases to FRT algorithms come into question and a conversation is needed.

AI technology simulates human decision-making processes by using a set of algorithms designed by a human programmer. As AI advances in capabilities, the range and complexity of tasks it is used for also increases. More and more, it is incorporated into the everyday functioning of society, capable of carrying out actions and processes traditionally only able to be completed by humans.

Such technologies are used to enhance human ability in some areas and completely eliminate the need for human involvement in others. In certain areas of application, the use of algorithm-based technology has been championed as a solution for eliminating subjective biases which were often seen as inhibitors to equitable access to resources and opportunities.

For example, algorithms can be used to determine a person's eligibility for a loan, a process which historically would have been done by an employee of a bank who may have personal and preconceived biases about certain groups of people such as persons with a criminal record, single parents, or people of colour. Under an algorithmic system, a person's loan application is processed via risk-analysis software, returning a set of calculated predictions on the person's financial risk and reliability potential. Financial institutions claim this process to be fairer as the decision-making process is removed from their employers. Despite this fact, however, studies have shown that trends in lending bias seen prior to algorithms being used continued, reflecting the replication of human biases in human-created algorithms. Investigation of lending trends in the US turned up evidence that black and brown loan applicants were 40–80 percent more likely to have their application denied than white applicants with the same financial profile.[71] The fact is, a person's risk score is calculated only in part by the algorithm, the other part is calculated by the industry professionals who created the technology.

The trend in financial risk analyses algorithms, although frustrating and disadvantageous to the individual, falls at the lower end of seriousness of consequences. Algorithmic AI is being increasingly employed across all sectors, especially the police and military, with built-in biases manifesting in different ways and on different scales. What was, and still is, proclaimed to be a solution for eliminating traditional trends in discrimination, pre-conceptions, and biases appear to simply replicate the same patterns with the same implications, the only difference being that there is no longer a person who can be held accountable for decisions — only a machine.

All inventions will inevitably inherit some biases from their human creators. This is even true for inventions designed using input from large sets of data, thereby claiming to be a "one-size-fits-all" model. The populations from which these data sets are collected tend to be rather narrow, however, constricting the range of users that they actually benefit. For example, much public infrastructure such as public bathrooms and transport are designed based on data collected from mostly male populations and therefore cater much better to male needs.[72]

The same trend is also true for algorithms. As the tech sector is largely composed of white males, logically this translates into AI algorithms functioning the best when applied to this population. In terms of FRT, this means that programmes are best at recognizing faces with lighter skin tones and male facial structures, its accuracy falling when applied to white women and black and brown men and women. Immediately, this poses some substantial questions to claims that the use of algorithmic software to replace humans in decision-making processes is fairer and more neutral.

The expanding use of FRTs by US law enforcement agencies has already begun to demonstrate the moral implications of its bias, progressing adversely along

[70] Ibid. [71] Martinez, Emmanuel; Kirchner, Lauren (August 25, 2021): "The Secret Bias Hidden in Mortgage-Approval Algorithms"; in URL: https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms, last accessed on March 10,2022. [72] Criado Perez, Caroline (2020): "Invisible Women. Exposing Data Bias in a World Designed for Men", Random House.

racial and gender lines.[73] Robert Williams, a black man living in the US city of Detroit, became the first person to be wrongly arrested in January 2020 after police falsely matched his photograph with that of a suspect using FRT. All charges were dropped when the matter came to court, citing a lack of evidence, but the traumatic impact this had on Williams and his family cannot be erased.[74]

The ease with which police assumed Williams was the culprit is but one link in a chain of thousands of AI-produced, potentially false matches, representing a new means by which to imprint historically established racial biases and associated traumas onto a new generation. Civil society and activist groups across the US have spoken out against the deployment of FRT by police, who are aware of its tendencies for gender and racial biases and yet continue deploying it.

That said, these efforts have not been in vain, such as in June 2020, when Amazon placed a one-year moratorium on law enforcement using its FRT technology following mounting evidence that they were producing biased results — a decision made at the height of protests against police brutality following the murder of George Floyd by a police officer in Minneapolis.[75] In May 2021, Amazon announced it was extending the ban indefinitely.[76] IBM, on the other hand, announced that it was exiting the FRT space altogether, reasoning that technology which enabled the violation of human rights was against company values. However, analysts who monitor IBM's activities also noted that its FRT was one of its least-profitable ventures, raising the question of whether the decision was more of a financial than moral nature.[77]

The digital replication of human biases has created a new dimension of surveillance in domestic policing as well as warfare, but is by no means a new development. Ramah Kudaimi of the Action Center on Race & the Economy (ACRE), a leading body in public awareness campaigns on the increasing role of tech within MIC, speaks clearly about the importance of extinguishing the claim that technology can be a way to wage war neutrally: "Tech is not neutral, humans are behind it."[78]

Conceiving technology through this lens, we also become complicit through our choices as consumers and voters. Organizations like ACRE are integral to social justice advocacy given the extreme secrecy surrounding the tech-military-government triad, and choose to conduct their work by "thinking about ethics … and the better world we are seeking to build",[79] which is very different from a legal approach. Kudaimi unambiguously pointed out that "a lot of time, the point of these partnerships for these big tech companies is to profit from war on Muslim and other communities across the globe".[80]

A final point to note is FRT's ability to collect masses of highly sensitive data, which is then in the possession of third-party contractors. The Internal Revenue Service (IRS), the US tax department, was recently forced into reversing its decision to contract with ID.me, a private software company, to provide FRT as part of the log-in process for taxpayers wanting to access certain features in their filing process. From the moment the IRS announced the planned partnership, a coalition of social rights activist groups led by the Algorithmic Justice League proactively coalesced around the issue and formulated a strong successful campaign opposing the contract. Among the concerns were that ID.me would be unable to keep secure the masses of sensitive and highly personalized data it collected and that taxpayers were forced into having their data collected if they wanted to access the online services. Following the IRS's announcement that they would not be renewing the ID.me contract, signalling the campaign had succeeded, Algorithmic Justice League founder Joy Buolamwini said, "We need to ask ourselves: what kind of society do we want to live in?"[81]

Biometric data is the broader category into which FRT fits. Biometric data covers a large range of data sources all pertaining to a person's physical, biological, and mental being including fingerprints, retina scanning, a person's gait, DNA, and even heartbeat. The US Department of Defense recently developed a new laser vibrometry tool that can detect a person's unique cardiac signature from up to 200 metres.[82] More and more, states are choosing to experiment with different types of biometric identification methods at their border entry ports. This also often comes in tandem with information-sharing agreements between the states deploying the technologies and the companies providing them. With large amounts of data being stored in international databases such as Interpol[83] or the Migration Information and Data Analysis System (MIDAS) developed by the International Organization for Migration,[84] or transferred between stakeholders, the risk

[73] Grentzel, Michael (June, 2021): "Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy", Philosophy & Technology; in URL: https://link.springer.com/content/pdf/10.1007/s13347-021-00478-z.pdf, last accessed March 2, 2022.

[74] Allyn, Bobby (June 24, 2020): "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest Of Black Man"; in URL: www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig?t=1646734852841, last accessed on March 5, 2022.

[75] Allyn, Bobby (June 10, 2020): "Amazon Halts Police Use Of Its Facial Recognition Technology"; in URL: www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology, last accessed on March 5, 2022.

[76] Dastin, Jeffery (May 18, 2021): "Amazon extends moratorium on police use of facial recognition software"; in URL:www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/, last accessed on March 5, 2022.

[77] Allyn, Bobby (June 9, 2020): "IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance"; in URL: www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance, last accessed on March 5, 2022.

[78] Transcript of interview with Ramah Kudaimi and Jessica Quiason (Big Tech Sells War) lead by the authors on December 14, 2021 in URL: https://docs.google.com/document/d/1pVXPnqhNroZgF1IM7CaJ9ckEp7PkWZ5a/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true.

[79] Ibid.

[80] Ibid.

[81] Metz, Rachel (March 7, 2022): "Activists pushed the IRS to drop facial recognition. They won, but they're not done yet"; in URL: https://edition.cnn.com/2022/03/07/tech/facial-recognition-activists-irs/index.html, last access on March 10, 2022.

[82] Hambling, David (June 27, 2019). The Pentagon has a laser that can identify people from a distance – by their heartbeat"; in URL: www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/.

[83] Interpol; in URL: www.interpol.int/en/How-we-work/Databases/Our-19-databases, last accessed on April 1, 2022.

[84] International Organization for Migration; in URL: www.iom.int/sites/g/files/tmzbdl486/files/documents/midas-brochure18-v7-en_digitall.pdf, last accessed on April 2, 2022.

of misuse, leaks, or data falling into the wrong hands (accidental or otherwise) also increases .

This collection and sharing of mass data of this nature accelerated following the 9/11 attacks, and has been one of the major means by which the US and its allies have been able to wage the WoT. The UN Security Council's adoption of Resolution 1373[85] provided the legal justification, and although it did not specify by which means states were to abide by its mandates, many have chosen to follow the US's lead and interpret it to mean heavy investment in personnel identification tools, such as biometrics. In 2017, the Security Council adopted Resolution 2396, which for the first time obliged states to "develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law".[86]

Like the General Data Protection Regulation (GDPR) in Europe, data protection management systems are also in place for these systems. That said, they come more in the form of guidelines, open to interpretation, opaque, and with few or weak mechanisms of enforcement. A 2020 report by the Human Rights Center at the University of Minnesota rang the alarm bell on this development, noting the lack of a human rights focus in Resolution 2396.[87]

UN Security Council Resolution 2396 and its predecessors (including Res/1373) stipulate that states must carry out implementation in accordance with international and domestic laws, and that is it is to be done in a way that is both proportional to the perceived threat and necessary for mitigation of the alleged threat. However, the resolution's binding nature could quite likely cause due diligence to the principles of proportionality and necessity to be downplayed or overlooked. This gives rise to concerns that the binding nature and concerns mentioned could give states license to target any person whose profile characteristics align with those conventionally tied to terrorism, and act without regard for human rights principles and without fear of repercussions. Historically, this has translated into the disproportionate targeting of people of colour, people who are or appear to be similar to Muslims or hold citizenship of a predominately Muslim country, and/or a country out of which terrorists have previously emerged.

These concerns are central to the work of civil society organizations and activists like those interviewed for this study. Researchers, activists, human rights advocates, and politicians are active in this space are aligned in their concerns. They are sounding the alarm now as an early warning for states to take action to preserve and protect the rights of persons who have already been subject to unjust persecution from being harmed further.

3.3 APPLE AND FACEBOOK: MINOR PLAYERS IN THE MILITARY INNOVATION MARKET

Of the major tech companies the DoD is seeking to collaborate with, Apple appears to be a relatively small player. In 2015, it became a member of a consortium of 162 companies called the FlexTech Alliance that was commissioned to develop various hardware technologies for defence purposes. The 75-million-dollar project aimed to develop flexible electronic systems that could be embedded in materials such as silicon and were lightweight enough to be worn by soldiers, yet resilient enough to be moulded onto the outside of aircrafts.[88]

While Apple had not partnered with the military prior to joining the Alliance, its senior management was concerned that the company's profit growth margin would begin to stagnate if it did not explore new and alternative markets to expand into. Traditionally, the sale of its iPhone represented the vast majority of its profits. With the market increasingly crowded as its competitors rose to meet its bar, however, it needed to break out into alternative product markets in order to continue its upward trend in profit margins.[89] In a similar vein, with a total of 365,000 dollars in DHS and 170,000 dollars in minor DoD contracts, Meta Platforms Inc. – previously known as Facebook, Inc. – appears to have joined Apple as a relatively small player in the military contracting business.[90]

[85] S/RES/1373 (2001). adopted on 28 September 2001; in URL: www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf, last accessed on April 1, 2022. [86] S/RES/2396 (2017) pg. 8, adopted on 21 December, 2017; in URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/25/PDF/N1746025.pdf?OpenElement, last accessed on April 5, 2022. [87] Huszti-Orbán, Krisztina & Ni Aolàin, Fionnuala (2020). Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?, Human Rights Center, University of Minnesota. [88] Itnews Staff (August 31, 2015): "Apple, Boeing partner with US Defence for wearables", ed. Itnews; in URL: www.itnews.com.au/news/apple-boeing-partner-with-us-defence-for-wearables-408632, last accessed on December 13, 2021. [89] Green, Adam (October 9, 2020): "Apple Inc. (AAPL) Is About to Become a Military Contractor", ed. LearnBonds; in URL: https://learnbonds.com/news/apple-inc-aapl-is-about-to-become-a-military-contractor/, last accessed on December 13, 2021. [90] Comp. data published through the campaign "Big Tech Sells War"; in URL: https://bigtechsellswar.com/, last accessed on December 13, 2021.

4 INNOVATION ANALOGUES AND DIVERGENCES IN EUROPE AND GERMANY

Shifting our focus from the US to Europe in general and Germany in particular, there appears to be little conscientiousness in German leadership to overtly establish an innovation framework along a narrative comparative with the Pentagon's TOS. In 2018, Christian Mölling, research director at the German Council on Foreign Relations (DGAP), evaluated that

> there are many governmental and civil actors who recognize the importance of investing in defence-related innovation within Germany, but only in general terms. In Berlin, there is recognition that a competitive defence industry and capable military requires investing in civilian companies that develop dual-use technologies. But there are not yet any official statements or analyses that propose a way forward. … It is necessary to preserve the country's own technological sovereignty by preserving key technologies and securing military capabilities and supply.[91]

With the establishment of bodies like the Bundeswehr's Cyber Innovation Hub (CIH.Bw)[92] as early as 2017 and the Centre for Digitalization and Technology Research (DTEC.Bw)[93] in 2020, however, it is evident that a military innovation structure based on key propositions of the TOS has taken priority in German defence policy. The Bundeswehr's status quo evaluation of its innovation space contextualizing the CIH.Bw's work in fact closely mirrors Chin and Meunier's notion of a transforming technological innovation environment driven by the civilian private sector, proclaiming that "whereas in recent centuries it was mostly the state – above all the military – that was the decisive driver of technological progress, today disruptive innovations are primarily driven by civilian actors. These are becoming less and less dependent on critical mass – making it increasingly easy for companies to bring disruptive technologies to market."[94] Meanwhile, the DTEC.Bw, building on the cooperation between military universities, private German stakeholders from both the established corporate and growing start-up scene and the Ministry of Defence, is particularly reminiscent of the cooperation models set forth by the DoD.

With regard to the preservation of Germany's technological sovereignty, projects like the massive cloud computing endeavour GAIA-X exemplify the degree to which this goal is pursued in recent years. It is equally apparent, however, that the German (and European) leadership heavily relies on outside resources exceeding leading European technology corporations' capacities, as the collaboration with a vast body of international hyperscalers exemplifies. In the next chapter, we further investigate how the project was originally conceived, how it developed over time, and how it undermines its self-determined goal of autonomy from international tech service providers while attracting support from questionable partners.

4.1 GAIA-X

Initiated in 2019 "with the goal of developing a trustworthy and sovereign digital infrastructure based on European rules",[95] GAIA-X is the German-French attempt to build an open-source European alternative to the cloud computing technologies of leading American and Asian technology corporations dominating the market.

To realize the endeavour, 22 partners from the tech, economic, and science sector initially founded the Belgian non-profit organization GAIA-X European Association for Data and Cloud AISBL in September 2020, bringing together major German players like BMW, Bosch, Deutsche Telekom, the Fraunhofer Gesellschaft, SAP, and Siemens.[96] While military applications are not communicated as a major purpose of the project, the German Bundeswehr's IT provider, BWI, describes GAIA-X as a capable resource for armed forces to maintain "the necessary control and action options in the cyber and information space in order to be able to fulfil their constitutional mission – self-determined and free from unwanted third-party influence".[97]

Since its inception, the number of parties to the initiative rapidly grew to over 300, attracting criticism for including Chinese partners like Huawei or Alibaba as well as major US firms. "While there is a lot of talk about cloud sovereignty, current plans by governments in Europe as part of GAIA-X still rely on US technologies by AWS, Google and Microsoft which are subject to foreign surveillance",[98] comments the European Cloud Industrial Alliance (EUCLIDIA), which was founded in 2020 by 23 companies monitoring the development.[99]

Jack Poulson, former Google data scientist and founder of Tech Inquiry,[100] highlights the crucial function of cloud computing contracts to de-politicize contributions of private technology corporations to government contracts, rendering them irrelevant for

[91] Mölling, Christian (March 23, 2018): "Defense Innovation and the Future of Transatlantic Strategic Superiority: A German Perspective", in URL: www.gmfus.org/news/defense-innovation-and-future-transatlantic-strategic-superiority-german-perspective#_ftnref2, last accessed on March 10, 2022.

[92] Comp. www.cyberinnovationhub.de/.

[93] Comp. https://dtecbw.de/home.

[94] BDI (May 15, 2019): "Digitale Innovationen für die Bundeswehr"; in URL: https://bdi.eu/artikel/news/digitale-innovationen-fuer-die-bundeswehr/, last accessed on March 10, 2022.

[95] Knoll, Andreas (February 9, 2021): "European Association for Data and Cloud – GAIA-X AISBL is officially founded", ed. Elektroniknet.de; in URL: www.elektroniknet.de/international/gaia-x-aisbl-is-officially-founded.183417.html, last accessed on December 13, 2021.

[96] For a full list of founding members, comp. ibid.

[97] BWI Staff (September 24, 2020): "Digitale Souveränität für Deutschland und Europa: Der Weg zwischen Autarkie und Abhängigkeit", in URL: www.bwi.de/news-blog/blog/artikel/digitale-souveraenitaet-fuer-deutschland-und-europa-der-weg-zwischen-autarkie-und-abhaengigkeit, last accessed on December 13, 2021.

[98] Comp. EUCLIDIA (undated): "Background: European tech innovation"; in URL: www.euclidia.eu/background/, last accessed on December 13, 2021.

[99] Comp. Steins, Teresa; Kerkmann, Christof (November 18, 2021): „Gaia-X-Gipfel in Mailand: Das Cloud-Projekt wird zum Problemfall", ed. Handelsblatt; in URL: www.handelsblatt.com/politik/deutschland/datensouveraenitaet-gaia-x-gipfel-in-mailand-das-cloud-projekt-wird-zum-problemfall/27809120.html?ticket=ST-56859-kZqD5Q9O2MZjdewebntt-cas01.example.org, last accessed on December 13, 2021.

[100] Tech inquiry is a nonprofit focusing on the analysis of contract procurement streams to render ties between private tech corporations and the US government more transparent.

military and domestic policy applications. With this perspective in mind, he further elaborates on potential consequences and the need for action of civil society actors:

> If these tech companies frame cloud computing as morally neutral, which is what we saw post-Maven, then how do we actually show what they're actively contributing? What levers for accountability really exist at that phase besides, say, employees leaking internal communications? I think the more we can show what these so-called black box cloud contracts actually result in, the more we can push back on the narrative that this material support for militaries and intelligence agencies around the world is not just the equivalent of selling them a pile of steel, that there's an actual direct contribution to their activities.[101]

While GAIA-X pursues the generally uncontested goal of a more independent and secure digital infrastructure in a GDPR-regulated space, it is thus apparent that close examination of its capabilities will be vital to prevent applications limiting individual freedoms of Europe's citizens and/or endangering the basic democratic order of its countries.

Even bigger concerns raised the involvement of big data integration corporation and US spy agency contractor Palantir, announcing to have joined "GAIA-X as a proud Day 1 Member" in December 2020,[102] a move observers prompted "should at least raise an eyebrow for people in Europe".[103] Considering the stark voices of protest from both political and corporate opposition, one could say that it did — one of them being Anne Roth, network policy consultant of the German party Die Linke, who commented on Twitter: "And there goes the trust in European sovereignty."[104]

Co-founded by Peter Thiel, Palantir has built a reputation developing AI tools to aid both autocratic and liberal democratic governments in the surveillance of their citizens and borders.[105] Christopher Soghoian, a technician at the US civil rights organization the American Civil Liberties Union, dubbed it "a key force in the surveillance-industrial complex".[106] GAIA-X is not the surveillance corporation's first major contract in Europe. Since 2016, Europol has used their anti-terror tool "Gotham" for their investigations.[107] Since 2017, German federal state of Hesse has also used their software under the name "Hessendata".[108]

Even before Palantir's GAIA-X announcement, Sophie in 't Veld, Dutch Member of the European Parliament and contributor to the Renew Europe Group, stated in October 2020: "A company with Palantir's track record should not be considered as a partner for any EU-wide project, and the European Commission knows it. This secretive corporation is at odds with the European values many EU citizens hold dear, such as privacy, civil liberties, and transparency of government — not to mention the strategic implications of cooperating with an American intelligence contractor."[109] Besides data sovereignty concerns, recent reports show the project to be suffering from over-bureaucratization, a lack of focus, and confusion over conflicting interests, resulting in French cloud provider Scaleway not renewing its contract with the project in November 2021.[110]

Despite Germany's close cross-Atlantic ties, the contract further illustrates the inherently anti-proportional relationship between the degree of collaboration with US partners from Silicon Valley and the ability of European governments to further develop their strategic autonomy. As European leadership attempts to build technological infrastructure following the example of the US and China, it actively cements the ties it so desperately attempts to cut by expanding collaboration between international private technology innovators and European governments.

It is evident that this space not only possesses high potential for a misguided sense of autonomy and security – it further offers ample opportunity to deepen relationships with and widen access avenues towards the European civil and government R&D sectors for the advancements of national Third Offset Strategy goals. Jack Poulson describes to what degree this already represents the reality in the European private-public innovation space: "There is a colonial element to US tech giants infiltrating a European consortium whose entire purpose was countering US tech giant power", Poulson finds. "Obviously there are human rights issues everywhere – whether that's Palantir coming in and wanting to sell technology to amplify border surveillance or deportations. It's certain these companies have close relationships with the intelligence communities across Europe."[111]

Concerning the investment of US tech firms in enhancing these relationships, Poulson elaborates: "I don't really see why it would develop fundamentally differently than in the US, even if one might expect that Europe is going to try and create its own analogues of these companies."[112]

[101] Ibid.

[102] Palantir Editorial Staff (December 18, 2020): "Palantir and GAIA-X", in URL: https://blog.palantir.com/palantir-and-gaia-x-85ab9845144d, last accessed on December 13, 2021.

[103] Comp. Transcript of Interview with Jack Poulson (Tech Inquiry), led by the authors on November 22, 2021, in URL: https://docs.google.com/document/d/1uado2xvqcdTs5yIDljbxD7N6QBmmc5bu/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true.

[104] Comp. Anne Roth's Twitter-reply to Palantir and then-German Federal Minister for Economic Affairs Peter Altmaier (CDU), in URL: https://twitter.com/annalist/status/1340035887619592195, last accessed on December 13, 2021.

[105] Malik, Kenan (September 22, 2019): "Think only authoritarian regimes spy on their citizens?", ed The Guardian; in URL: www.theguardian.com/commentisfree/2019/sep/22/think-only-authoritarian-regimes-spy-on-their-citizens, last accessed on December 13, 2021.

[106] Hardy, Quentin (May 31, 2014): "Unlocking Secrets, if Not Its Own Value", ed. The New York Times; in URL: www.nytimes.com/2014/06/01/business/unlocking-secrets-if-not-its-own-value.html, last accessed on December 13, 2021.

[107] in't Veld, Sophie(October 20, 2020): "Palantir is not our friend", ed. about:intel – European Voices on Surveillance; in URL: https://aboutintel.eu/palantir-eu-independence/, last accessed on December 13, 2021.

[108] von Bebenburg, Pitt (May 10, 2021): "Polizei in Hessen: Datenschützer prüft Palantir-Einsatz", ed. Frankfurter Rundschau; in URL: www.fr.de/rhein-main/landespolitik/polizei-in-hessen-datenschuetzer-prueft-palantir-einsatz-90530135.html, last accessed on December 13, 2021.

[109] in't Veld, (October 20, 2020).

[110] Mahn, Jan (November 18, 2021): "Gaia-X: Cloudprovider Scaleway zieht die Reißleine und tritt aus", ed. heise online; in URL: www.heise.de/news/Gaia-X-Cloudprovider-Scaleway-zieht-die-Reissleine-und-tritt-aus-6271342.html, last accessed on December 13, 2021.

[111] Comp. Transcript of Interview with Jack Poulson (Tech Inquiry), led by the authors on November 22, 2021, in URL: https://docs.google.com/document/d/1uado2xvqcdTs5yIDljbxD7N6QBmmc5bu/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true.

[112] Ibid.

4.2 BEYOND GAIA-X: THE FUTURE OF GERMANY'S MILITARY INNOVATION SPACE

While the expansion of resources particularly focused on improving the German military's innovation infrastructure currently does not rely on the support of major civilian service providers like Google, it does closely resemble R&D investment structures established in the US. This strategy builds on the common understanding of the directions in which future strategies on the battlefield will evolve. In their comparative examination of collaborative potentials between Germany and the United Kingdom on military innovation, Becker, Mölling, and Schütz identify three key metatrends defining Germany's military innovation strategy:

- The "reconnaissance-fire-complex, meaning that the network is becoming more important than the individual asset",[113]
- The "battlefield to become truly transparent through the further proliferation of sensors and command and control capabilities able to process the plethora of information from those",[114] and
- The "human role in this kind of warfare", especially building on the notion that the "use of inhabited systems and human operators becomes riskier — to their life as well as to military efficiency."[115]

The authors stress, however, that "humans will have to retain their function as decision-makers"[116] – not only due to ethical concerns, but also to avoid challenges in communicating entirely autonomous systems in public discourse, risking controversies with a potentially negative impact on the policy and therefore funding level. In order to tackle challenges generated by these anticipated developments effectively, initiatives like the CIH.Bw and the DTEC.Bw seek to foster ties to the private sector and generate spaces for civilian collaboration from multiple, mutually supportive angles.

While the CIH.Bw is intended to "identify innovative technologies in the start-up world, develop them further with users and make them usable in everyday life as quickly as possible",[117] the DTEC.Bw seeks to develop a university-driven innovation environment spearheaded by the two German military universities in Munich and Hamburg. One example is the latter's collaboration with the private corporation Hensoldt AG in efforts to develop an advanced AI decision-making tool for military use. The initiative is part of the DTEC.Bw-funded project "Ghostplay",[118] directly linking advancements in automated weapon systems to the German private sector.

With the expansion from European-only to international partnerships within the scope of GAIA-X, it is plausible that the current limitation of these research ambitions to German civilian private partners might be abandoned for US and other international actors for richer outcomes in the future. The initiative for larger-scale projects of this nature may actually be driven by Silicon Valley. Based on her observations within the US tech innovation market, Munira Lokhandwala infers that "there's going to be a point of saturation in the US where there's not as much money to extract [from US government contracts] in order to continue to grow and profit. They will be looking for contracts outside the US. And I think monitoring those, which many organizations around the world have been doing, is going to be really important because the tools that they want to build in other parts of the world are just as dangerous and just as concerning as the ones that they're building here in the US."[119]

One key difference between the US and Europe lies in the regulatory framework, which defines the nexus within which military and civilian technological innovation can occur more rigidly. In place since 2018, the GDPR lays out a gold-standard set of rules for when and how data is permitted to be used within Europe and applies to all its member-states. Its jurisdiction is comprehensive and considered to offer the best protection for personal data in the world.[120] It includes important protections such as the "Right to be forgotten" (Article 17),[121] which specifies that a person has the right to request their data be erased if the original purpose for its collection is no longer valid. Particularly relevant to algorithm bias is Article 22,[122] "Automated decision-making", including profiling through which the person has the right to not be subject to any decision that is based solely on an algorithmic process and which could have legal implications for them.

The GDPR also has additional built-in safeguards such as the requirement that all systems falling under the GDPR's jurisdiction have "Privacy by Default" (PbD) built into its processes, meaning that an individual's data is automatically protected without additional steps. Furthermore, the GDPR specifies that every government, public entity, or private corporation gathering personal data implement "Data Protection Impact Assessments" (DPIA), a process that identifies risks associated with the collection and storage of an individual's data. This component is particularly applicable to areas such as FRT use by law enforcement, its purpose being to ensure oversight of the process and that data collection is justified.[123] The DPIA is particularly integral in that it forces organizations to analyse and understand the algorithms they use in order to justify data collection.

[113] Becker, Mölling, Schütz (2020): "Learning together: UK-Germany cooperation on military innovation and the future of warfare", Hanns Seidel Foundation (CSU), The Policy Institute, King's College London (ed.), p. 2; in URL: https://dgap.org/sites/default/files/article_pdfs/uk-germany_military_innovation_.pdf, last accessed on March 10, 2022. [114] Ibid. [115] Ibid. [116] Ibid. [117] BDI (May 15, 2019). [118] Comp. DTEC.Bw (undated): "GhostPlay – Simulation für KI-basierte Entscheidungsverfahren"; in URL: https://dtecbw.de/home/forschung/hsu/projekt-ghostplay, last accessed on March 10, 2022. [119] Transcript of Interview with Munira Lokhandwala (LittleSis), led by the authors on February 02, 2022, in URL: https://docs.google.com/document/d/1erwtg_LcvxUcRK12vu2Kp-heYtV4YYgs/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. [120] Almeida et al (2021): "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks, AI & Ethics", in URL: https://link.springer.com/article/10.1007/s43681-021-00077-w, last accessed on March 10, 2022. [121] Article 17, GDPR; in URL: https://gdpr-info.eu/art-17-gdpr/, last accessed on March 10, 2022. [122] Article 22, GDPR; in URL: https://gdpr-info.eu/art-22-gdpr/, last accessed on March 10,2022. [123] Almeida et al (2021).

An extra component of the DPIA is the mandated requirement that every public entity whose core function depends on large-scale and systematic personal data collection, especially when related to criminal matters, also employ a “Data Protection Officer” (DPO), a kind of built-in whistle blower. The DPO’s role is be to monitor the organization’s compliance with the GDPR and report any violations to the national ombudsman. What is more, the GDPR’s ability to enforce data regulation extends beyond Europe, as any organization that wishes operate within or have contracts with EU entities, even if based outside of the EU, must also comply with the GDPR.[124]

[124] Ibid.

5 THE WAY FORWARD

5.1 ORGANIZING THE OPPOSITION: CHALLENGES AND OPPORTUNITIES OF BECOMING A WHISTLEBLOWER

The mountain of evidence indicating a strong connection between major US tech firms and military projects both nationally and globally raises the question of how to sustainably address its consequences. While there may be a wide variety of potential paths to do so, following the journey of one former tech employee aiding the analysis and publication of potentially harmful contracts might best highlight the struggles and pitfalls connected to such an endeavour and resources needed to work past them.

Virtually all available investigative reports on the subject matter are based on information provided by Poulson's non-profit, Tech Inquiry. After his 2018 resignation over Google's later cancelled censored search engine project "Dragonfly" in China, the transition to the non-profit sector was not immediate, he recalls. "For about the first year and a half, we were about as luddite as you could be. Our entire focus laid on speaking with journalists, raising awareness over issues that folks in the non-profit sector had been familiar with."[125]

The approach to monitor both conditions and connections between contractors developed out of an observation in the industry. "When I met with some of the more senior officials, I found that human rights issues were not much of a concern of theirs. It was much more about maintaining a close military relationship with the US tech companies", he recalls.[126] "As part of that, I started to become more aware of just how much bureaucracy there was surrounding those relationships, whether it's the Defense Innovation Board, the Defense Innovation Unit, the National Security Commission on AI, In-Q-Tel, etc. I began to do Freedom of Information requests into some of those relationships and came to the conclusion that there are a lot of relationships between these companies that are just not very well documented."[127]

Tech Inquiry emerged out of this practice, harbouring other former employees from the tech industry both as board members and contributors to the non-profit's research. While their work does not explicitly focus on disarmament, some members bridge the gap to pacifist movements through their engagement in anti-militarist campaigns. One prominent example is the previously mentioned Campaign to Stop Killer Robots. "Several of the members and board members of Tech Inquiry have played a major role in it. For example, Liz O'Sullivan had left ClarifAI over their work on drone surveillance and Laura Nolan had left Google for the same reason over their work on Project Maven."[128]

5.2 FINDING ANSWERS IN UNEXPECTED PLACES

Limiting connections between major US tech companies and the US government to their impact on military actions, however, is not particularly helpful to grasp the reality of how tech companies conduct their business, Poulson suggests. "I tend to find that if you're looking from the perspective of tech companies, they're really just trying to sell their technologies everywhere. There's another lens where one can view a lot of military technology as being upstream from technology that will end up in the hands of the Department of Homeland Security through drone surveillance, autonomous border surveillance, facial recognition, etc. And then it works its way into more municipal usage."[129]

Widening the scope of analysis to a broader range of contracts may reveal issues in areas that might otherwise be left unconsidered, Poulson finds. "I think if you do a lot closer monitoring of procurement and have a deeper understanding of the bureaucracy of the US government, you understand that the intelligence community works very closely with a lot of agencies people don't tend to think of."[130]

This practice further helps re-contextualize the purported ethical neutrality of contracts within a public discourse. One area this may have a particular impact on is cloud computing, Poulson suggests. "One of our big wins was showing that Google Cloud was being sold to a company called Thundercat Technology, which is a fairly prolific contractor with US Customs and Border Protection. We found evidence that Thundercat planned to use Google Cloud's AI to process thermal imagery from Anduril Industries' autonomous border surveillance, which pretty well contradicts the way Google has positioned itself in terms of what it would and would not do at the US border. This raises an interesting question considering the role cloud computing plays financially and technologically. It's both a huge component of defence sales and a driving source of revenue for major tech companies."

5.3 BUILDING STRUCTURES FOR A SUSTAINABLE COUNTER-MOVEMENT

As an employee, the decision to object to practices perceived as unethical often creates a field of tension between doing what's right and pursuing a long-term career — a conflict that Tech Inquiry attempts to alleviate through the protection of whistleblowers' identities. Even without this layer of security, there are opportunities for tech workers to speak out, however.

[125] Comp. Transcript of Interview with Jack Poulson (Tech Inquiry), led by the authors on November 22, 2021, in URL: https://docs.google.com/document/d/1uado2xvqcdTs5yIDljbxD7N6QBmmc5bu/edit?usp=sharing&ouid=113280576371631986367&rtpof=true&sd=true. [126] Ibid. [127] Ibid. [128] Ibid. [129] Ibid. [130] Ibid.

"If nothing else, you don't have to put your name on something. If you want to share something with the press, you can do so anonymously",[131] Poulson explains.

Even with additional resources provided by the non-profit sector, the pressure emerging from this individual conflict may prompt employees to opt for a less confrontational approach towards addressing issues they see — a practice which is often used as an opportunity for executives to stay inactive, Poulson finds. "This also gets to the heart of a debate over organizing versus speaking out in protest. I think organizing is obviously one of the more sustainable paths. It also, in a sense, builds power. I think it should come up more in circles relating to whistleblowing. And it's something I've pushed a lot for.

I think one of the pitfalls I experienced is that a lot of the senior people I knew weren't doing anything close to what we would traditionally think of as organizing. The 'change from the inside' narrative is often used as an excuse for why it is okay for them to do nothing. I feel like that side of the conversation isn't talked about much. One question might be how to prevent people from getting away with the bad faith application of a 'change from the inside-narrative'"[132] — a process in which unionizing can play a crucial role.

According to Poulson, however, unions can only serve as one contributor to a much more holistic approach towards addressing these issues. "The complication is that unions often represent the interests of the workers, which can dramatically differ from the interests of the public. So I think it's always worth emphasizing that beside unions, we also call for coalitions, including independent civil society organizations."[133] This also means a better organization of collaborative efforts between non-profits in the area, he suggests. "That doesn't mean not ever criticizing. But I think when non-profits can come together and work on projects that combine their strengths instead of just competing with each other it tends to lead to incredible impact."[134]

To do so sustainably, however, support from the wider public is needed.

> I think one of the major problems in the non-profit space is that most of the money comes from the very tech billionaires that you're trying to critique. If we genuinely want to tackle tech billionaire influence, we really need to be able to be self-sustaining.
>
> Even at the most respected organizations, you constantly see even high-level figures moving into tech companies because there's so much power and honestly, non-profits just can't usually pay very well. So I think there's no real substitute for just making civil society a place in which people can actually have a career, and that's going to ultimately come from taxes and before that from grassroots donations.[135]

131 Ibid. **132** Ibid. **133** Ibid. **134** Ibid. **135** Ibid. **136** Cuthbertson, Anthony (2018): "Google quietly removes 'don't be evil' preface from code of conduct", in URL: www.independent.co.uk/tech/google-dont-be-evil-code-conduct-removed-alphabet-a8361276.html, last accessed on July 18, 2022.

6 CONCLUSION

The rapid and massive advance of technology within the context of the military–industrial complex and the implications thereof for the future conceptualization of war and policing tactics is exemplified in the US. With advances occurring so rapidly and in the face of increasing adversaries, the Pentagon and its agencies were forced to outsource research and development in this sphere to private companies with human capital and expertise already mobilized in order to remain ahead of the game.

The implications that this has for areas that have long been sites of chronic human rights and ethics concerns are expanding into a new and relatively uncharted digital dimension. There is good reason to be concerned that similar patterns of human rights and code of ethics violations, as are currently playing out in the US, will be transposed to Europe as long as projects like Gaia-X continue to be rolled out and involve the same companies.

Initiatives like Project Maven highlight the degree to which civilian companies stand to gain from cooperating with state defence agencies. However, the response of Google employees to its involvement in Maven exemplifies the discord between the company's leadership and its staff. The leadership, emboldened by its shareholders and charged with the mandate of ensuring continual growth in profit margins, appear to be prepared to deliver this at any cost, even if this means straying from its "Don't Be Evil" principles or even abandoning them altogether. In fact, this process was already set in motion by Google in 2018. In the wake of the Maven protests, the phrase — along with most of the original preface — was removed from its code of conduct and replaced with the more generic terms "ethical business conduct" and "Google's values".[136] The commitment does remain in the document, however, with its last line stating: "And remember… don't be evil, and if you see something that you think isn't right — speak up!"[137]

The incentives by way of profit and influence offered to tech companies and defence agencies to collude with one another is a major concern of civil society. The rewards that come from collaboration far outweigh the consequences, or at least it does for those who stand to benefit directly from the projects coming to fruition. The revolving door between the two sectors and through which DoD officials and tech CEOs are constantly passing showcases the degree to which collusion occurs. These alliances, highlighted by the LittleSis project, and their implications, laid out by Big Tech Sells War, explain the liberal and steep increases in defence budgets.

Regarding Germany's tech space, while there are some promising local companies emerging, these are small players in comparison to Silicon Valley, and they still rely on basic framework technologies designed by the major US-based tech players. This same trend is true for European governments, who must also rely heavily on outside resources, exemplified by the inclusion of AWS, Google, and Microsoft as well as Chinese companies including Huawei and Alibaba in Gaia-X. This is an early signal that preserving Europe's and Germany's tech space sovereignty is going to be extremely tricky if it is to continue evolving at the pace it has set for itself.

The facet of human biases transferred into an automated digital realm is one of the major areas of concern for civil society and human rights activists investigating this development space. Whether technologies are deployed in domestic policing operations or on foreign battlefields, biases against certain population groups in any form are never a desirable trend.

What is most concerning is that this is known. It is known that digital biases exist and continue to proliferate within new technologies. The consequences are evident, and yet it has hardly garnered the attention it warrants. Despite the best efforts of individuals and organizations like those interviewed by the authors to bring about discussion, awareness, and change, those holding the purse strings and calling the shots have barely acknowledged the problem, let alone taken steps to rectify it.

On the other hand, the GDPR is arguably one major step in the right direction by European governments to implement at least some safeguards — that said, it should be viewed as a starting point to be built on, and quickly.

Key Findings

- Some of the most prominent private tech players are Google LLC, Amazon Web Services, Oracle, and Microsoft. Facebook and Apple are proportionately small players in the field. Ventures of other major players like IBM and HP were not included the current analysis due to their relatively tight focus on private consumer-driven services and the study's limited scope.
- The majority of government contracts make up a small percentage of these companies' revenue. These contracts provide a steady stream of income and the potential to adapt outcomes of defence innovation processes to the private market, while the main source of revenue remains their civilian consumer products.
- Procurement of contracts often goes through an opaque network of private actors. This blurs connections between major private tech innovators and the Pentagon enabling major companies to be a step removed from the possible implications and claim unliability.

[137] Alphabet Inc. (2022): "Google Code of Conduct", in URL: https://abc.xyz/investor/other/google-code-of-conduct/, last accessed on July 18, 2022.

- Technology developed through the military-private innovation nexus is usually not directly describable as (automated) weaponry or technology directly linked to killing individuals. Instead, technologies developed through these contracts are indirectly contributing to new forms of warfare, e.g. through automated data processing for targeted reconnaissance and cloud computing resources. While no evidence of this type of technology being directly linked to automated killing was found, it was found that the targeted outcomes of investigated contracts were:
  - equally important for the use in military operations as well as domestic policing
  - generally capable of being applied to a more prominent role in automatic decision-making and automated weapon systems.
- The German/European innovation market is evolving in a direction reminiscent of the US context. First and foremost, this means growing ties between the German/European defence and private technology market as well as strengthening cooperative efforts, as exemplified in the example of Gaia-X.
- The General Data Protection Regulation (GDPR) in Europe is currently considered the most comprehensive set of regulations able to provide protection of an individual's data in the world. It serves as a legislative foundation inscribed with basic human rights principles on which future legislation can build and be modelled.
- The pressure on tech employees to voice their ethical concerns against contributing to military-related contracts is heightened by concerns doing so would jeopardize their careers. Their conviction to speak out is often contained by "change from the inside" narratives and assurances from colleagues and superiors. This pressure is usually not matched with incentives in the non-profit environment to provide information anonymously or pursue a career within the non-profit framework.

Prospects for Challenging These Developments

- Besides work from trade unions, there needs to be a wider support structure supported by civil society for making this work more attractive and effective. Most of the work done by the non-profit sector consists of working through procurement stream analysis, Freedom of Information requests, and publicly available data. This is a very inefficient way of working, and would be greatly assisted by more whistleblowers coming forward.
- There needs to be a greater focus on discrimination throughout R&D processes.
  - Historical forms of discrimination, such as along racial, gender, or religious lines, are replicated in the digital sphere.
  - European non-profit research must place greater focus on this discrimination as well as emphasise building intersectional coalitions between actors to bring attention to this aspect.

Yet, to acquire these means and forge meaningful alliances to build a sustainable and organized civil society corrective to the tech sector's business of war in Germany and Europe, we first need to create spaces of discourse and exchange. These spaces define war both interdisciplinarily and intersectionally, allowing for the consideration of perspectives of those affected most by the technology of war — from communities in active war zones to refugees dying at the European borders or groups who are particularly marginalized and policed domestically.

It is only from this discourse that a movement can emerge to hold tech companies accountable for their actions on the basis of human rights, not self-imposed ethical obligations. This is a movement that does not limit itself to targeting Google for circumventing its ethical guidelines, but raises the question of why more companies are not formulating them in the first place.

Technology is a human invention. Its purpose and usage are controlled by us. With this in mind, there is no basis to claim that it is neutral. Technology has always been political and will continue to be. In a world where every person using consumer-targeted services of Silicon Valley corporations adds to their data pool and revenue, there is no excuse to remain inactive – in the US, in Europe and around the world.

BIBLIOGRAPHY

A

Action Center on Race & the Economy (2021): in URL: https://acrecampaigns.org/wp-content/uploads/2021/12/Website-2022-21-ACREI-Overview.pdf, last accessed on March 10, 2022.

Allyn, Bobby (June 10, 2020): "Amazon Halts Police Use Of Its Facial Recognition Technology"; in URL: www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology, last accessed on March 5, 2022.

Allyn, Bobby (June 24, 2020): "'The Computer Got It Wrong': How Facial Recognition Led To False Arrest Of Black Man"; in URL: www.npr.org/2020/06/24/882683463/the-computer-got-it-wrong-how-facial-recognition-led-to-a-false-arrest-in-michig?t=1646734852841, last accessed on March 5, 2022.

Allyn, Bobby (June 9, 2020): "IBM Abandons Facial Recognition Products, Condemns Racially Biased Surveillance"; in URL: www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance, last accessed on March 5, 2022.

Almeida et al (2021): "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks, AI & Ethics", in URL: https://link.springer.com/article/10.1007/s43681-021-00077-w, last accessed on March 10, 2022.

Alphabet Inc. (2022): "Google Code of Conduct", in URL: https://abc.xyz/investor/other/google-code-of-conduct/, last accessed on July 18, 2022.

Article 17, GDPR: in URL: https://gdpr-info.eu/art-17-gdpr/, last accessed on March 10, 2022.

Article 22, GDPR: in URL: https://gdpr-info.eu/art-22-gdpr/, last accessed on March 10, 2022.

B

BDI (May 15, 2019): "Digitale Innovationen für die Bundeswehr"; in URL: https://bdi.eu/artikel/news/digitale-innovationen-fuer-die-bundeswehr/, last accessed on March 10, 2022.

Becker et al (2020): "Learning together: UK-Germany cooperation on military innovation and the future of warfare", Hanns Seidel Foundation (CSU), The Policy Institute, King's College London (ed.), p. 2; in URL: https://dgap.org/sites/default/files/article_pdfs/uk-germany_military_innovation_.pdf, last accessed on March 10, 2022.

Brewster, Thomas (December 22 2020): „Google Promised Not To Use Its AI In Weapons, So Why Is It Investing In Startups Straight Out Of 'Star Wars'?, ed. Forbes Magazine; in URL: www.forbes.com/sites/thomasbrewster/2020/12/22/google-promised-not-to-use-its-ai-in-weapons-so-why-is-alphabet-investing-in-ai-satellite-startups-with-military-contracts/?sh=30ba15537595, last accessed on December 13, 2021.

Brewster, Thomas (September 8, 2021): "Project Maven: Amazon And Microsoft Scored $50 Million In Pentagon Surveillance Contracts After Google Quit", ed. Forbes; in URL: www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after-google/?sh=52af312f6f1e, last accessed on December 13, 2021.

Brewster, Thomas (September 8, 2021): "Project Maven: Startups Backed By Google, Peter Thiel, Eric Schmidt And James Murdoch Are Building AI And Facial Recognition Surveillance Tools For The Pentagon", ed. Forbes; in URL: www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-startups-backed-by-google-peter-thiel-eric-schmidt-and-james-murdoch-build-ai-and-facial-recognition-surveillance-for-the-defence-department/?sh=f56cfbd6ef26, last accessed on December 13, 2021.

BWI Staff (September 24, 2020): "Digitale Souveränität für Deutschland und Europa: Der Weg zwischen Autarkie und Abhängigkeit", in URL: www.bwi.de/news-blog/blog/artikel/digitale-souveraenitaet-fuer-deutschland-und-europa-der-weg-zwischen-autarkie-und-abhaengigkeit, last accessed on December 13, 2021.

Bylund, Anders (April 6, 2017): Meet Hewlett-Packard, the Defense Contractor, ed. The Motley Fool; in URL: www.fool.com/investing/value/2010/07/09/meet-hewlett-packard-the-defence-contractor.aspx, last accessed on September 4, 2022.

C

Chafkin, Max (July 14 2019): "Peter Thiel Urges U.S. Probe of Google's 'Seemingly Treasonous' Acts", ed. Bloomberg; in URL: www.bloomberg.com/news/articles/2019-07-15/thiel-urges-u-s-probe-of-google-s-seemingly-treasonous-acts, last accessed on December 13, 2021.

Chin, Warren (2019): "Technology, war and the state: past, present and future", in: International Affairs — Re-visioning war and the state in the twenty-first century, pp. 770–772; in URL: https://academic.oup.com/ia/article/95/4/765/5513164, last accessed on March 10, 2022.

Clark, Bryan; Patt, Dan; and Walton, Timothy (March 3, 2021): Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage, Hudson Institute; in URL: www.hudson.org/research/16729-implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage, last accessed on September 4, 2022.

Conger, Kate; Metz, Cade (May 2, 2020): "'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive", ed. The New York Times; in URL: www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html, last accessed on December 13, 2021.

Conger, Kate; Sanger, David E. (July 6, 2021): "Pentagon Cancels a Disputed $10 Billion Technology Contract", ed. The New York Times; in URL: www.nytimes.com/2021/07/06/technology/JEDI-contract-cancelled.html, last accessed on December 13, 2021.

Conn, Ariel (November 30, 2016): The Problem of Defining Autonomous Weapons, ed. The Future of Life Institute; in URL: https://futureoflife.org/2016/11/30/problem-defining-autonomous-weapons/, last accessed on September 4, 2022.

Criado Perez, Caroline (2020): "Invisible Women. Exposing Data Bias in a World Designed for Men", Random House, Abrams Press, New York.

Cuthbertson, Anthony (2018): "Google quietly removes 'don't be evil' preface from code of conduct", in URL: www.independent.co.uk/tech/google-dont-be-evil-code-conduct-removed-alphabet-a8361276.html, last accessed on July 18, 2022.

D

Dastin, Jeffery (May 18, 2021): "Amazon extends moratorium on police use of facial recognition software"; in URL:www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/, last accessed on March 5, 2022.

Davenport, Christian; Gregg, Aaron (January 24, 2019): "Pentagon to review Amazon employee's influence over $10 billion government contract"; in URL: www.seattletimes.com/business/pentagon-to-review-amazon-employees-influence-over-10-billion-government-contract/, last accessed on March 10, 2022.

Department of Defense (November 21, 2012): Directive re Autonomy in Weapon Systems; in URL; www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf, p. 13, last accessed on September 4, 2022.

DTEC.Bw (undated): "GhostPlay — Simulation für KI-basierte Entscheidungsverfahren"; in URL: https://dtecbw.de/home/forschung/hsu/projekt-ghostplay, last accessed on March 10, 2022.

E

Eisenhower, Dwight D. (1961): "Military–Industrial Complex Speech"; in URL: https://avalon.law.yale.edu/20th_century/eisenhower001.asp, last accessed on March 10, 2022.

Elias, Jennifer (November 15, 2021): Google's pursuit of military cloud deal was among top issues at last week's all-staff meeting", ed. CNBC; in URL: www.cnbc.com/2021/11/15/google-pursuit-of-jwcc-among-issues-of-top-concern-at-tgif-meeting-.html, last accessed on December 13, 2021.

EUCLIDIA (undated): "Background: European tech innovation"; in URL: www.euclidia.eu/background/, last accessed on December 13, 2021.

G

Graham, Stephen (2011): "Cities under siege", chapter 3: 'The military urbanism', section: 'Tracking: citizen–consumer–soldier', Verso, London.

Green, Adam (October 9, 2020): "Apple Inc. (AAPL) Is About to Become a Military Contractor", ed. LearnBonds; in URL: https://learnbonds.com/news/apple-inc-aapl-is-about-to-become-a-military-contractor/, last accessed on December 13, 2021.

Gregg, Aaron; Greene, Jay (October 30, 2019): "Fierce backlash against Amazon paved the way for Microsoft's stunning Pentagon cloud win"; in URL: www.washingtonpost.com/business/2019/10/30/fierce-backlash-against-amazon-paved-way-microsofts-stunning-pentagon-cloud-win/, last accessed on March 10, 2022.

Grentzel, Michael (June, 2021): "Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy", Philosophy & Technology; in URL: https://link.springer.com/content/pdf/10.1007/s13347-021-00478-z.pdf, last accessed March 2, 2022.

Guichard, Renelle, Heisbourg, François (2004): "Recherche militaire: vers un nouveau modèle de gestion?", Paris, Economica, p. 97.

H

Hambling, David (27. Juni 2019): The Pentagon has a laser that can identify people from a distance - by their heartbeat; unter: www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/, last accessed on September 4, 2022.

Hardy, Quentin (May 31, 2014): "Unlocking Secrets, if Not Its Own Value ", ed. The New York Times; in URL: www.nytimes.com/2014/06/01/business/unlocking-secrets-if-not-its-own-value.html, last accessed on December 13, 2021.

Huszti-Orbán, Krisztina & Ni Aolàin, Fionnuala (2020): Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?, Human Rights Center, University of Minnesota.

I

in't Veld, Sophie(October 20, 2020): "Palantir is not our friend", ed. about:intel — European Voices on Surveillance; in URL: https://aboutintel.eu/palantir-eu-independence/, last accessed on December 13, 2021.

Itnews Staff (August 31, 2015): "Apple, Boeing partner with US Defence for wearables", ed. Itnews; in URL: www.itnews.com.au/news/apple-boeing-partner-with-us-defence-for-wearables-408632, last accessed on December 13, 2021.

K

Knoll, Andreas (February 9, 2021): "European Association for Data and Cloud — GAIA-X AISBL is officially founded", ed. Elektroniknet.de; in URL: www.elektroniknet.de/international/gaia-x-aisbl-is-officially-founded.183417.html, last accessed on December 13, 2021.

Kurian, Thomas (November 12, 2021): "Update on Google Cloud's work with the U.S. Government ", in URL: https://cloud.google.com/blog/topics/inside-google-cloud/update-on-google-clouds-work-with-the-us-government, last accessed on December 13, 2021.

L

Layton, Peter (2018): "Algorithmic Warfare — Applying Artificial Intelligence to Warfighting", Commonwealth of Australia, p. iii. in URL: https://airpower.airforce.gov.au/publications/algorithmic-warfare-applying-artificial-intelligence-warfighting, last accessed on September 4, 2022.

M

Magnuson, Stew (November 18, 2018): "Dunford Slams Google for Working with China, But Not U.S. Military", ed. National Defense; in URL: www.nationaldefensemagazine.org/articles/2018/11/18/dunford-slams-google-for-working-with-china-but-not-us-military, last accessed on December 13 2021.

Mahn, Jan (November 18, 2021): "Gaia-X: Cloudprovider Scaleway zieht die Reißleine und tritt aus", ed. heise online; in URL: www.heise.de/news/Gaia-X-Cloudprovider-Scaleway-zieht-die-Reissleine-und-tritt-aus-6271342.html, last accessed on December 13, 2021.

Malik, Kenan (September 22, 2019): "Think only authoritarian regimes spy on their citizens?", ed The Guardian; in URL: www.theguardian.com/commentisfree/2019/sep/22/think-only-authoritarian-regimes-spy-on-their-citizens, last accessed on December 13, 2021.

Martinez, Emmanuel; Kirchner, Lauren (August 25, 2021): "The Secret Bias Hidden in Mortgage-Approval Algorithms"; in URL: https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms, last accessed on March 10,2022.

Metz, Rachel (March 7, 2022): "Activists pushed the IRS to drop facial recognition. They won, but they're not done yet"; in URL: https://edition.cnn.com/2022/03/07/tech/facial-recognition-activists-irs/index.html, last access on March 10, 2022.

Meunier, François-Xavier (2019): "Construction of an Operational Concept of Technological Military/Civilian Duality", in: Journal of innovation Economics & Management, 2019/2 n° 29, pp. 159–182, p. 162; in URL: https://doi.org/10.3917/jie.029.0159, last accessed on March 10, 2022.

Mölling, Christian (March 23, 2018): "Defense Innovation and the Future of Transatlantic Strategic Superiority: A German Perspective", in URL: www.gmfus.org/news/defense-innovation-and-future-transatlantic-strategic-superiority-german-perspective#_ftnref2, last accessed on March 10, 2022.

Moss, Sebastian (May 1, 2020): IBM gets $18.8m contract modification for ongoing US Army IT modernization award, ITES-2S, ed. Data Center Dynamics; in URL: www.datacenterdynamics.com/en/news/ibm-gets-188m-contract-modification-ongoing-us-army-it-modernization-award-ites-2s/, last accessed on September 4, 2022.

P

Palantir Editorial Staff (December 18, 2020): "Palantir and GAIA-X", in URL: https://blog.palantir.com/palantir-and-gaia-x-85ab9845144d, last accessed on December 13, 2021.

Peitz, Dirk (June 8, 2018): „Google wird einfach ersetzt", ed. "Die Zeit"; in URL: www.zeit.de/digital/internet/2018-06/maven-militaerprojekt-google-ausstieg-ruestungsexperte-paul-scharre, last accessed on December 13 2021.

Pellerin, Cheryl (July 21 2017): "Project Maven to Deploy Computer Algorithms to War Zone by Year's End", ed. US Department of Defense; in URL: www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/, last accessed on December 13, 2021.

Pichai, Sundar (June 7, 2018): "AI at Google: our principles"; in URL: www.blog.google/technology/ai/ai-principles/, last accessed on December 13 2021.

R

Rauwald, Christoph, Wilkes, William & Patel, Tara (February 28, 2022): "Europe is Re-arming, and Its Defence Firms Stand To Profit", via Bloomberg Quint; in URL: www.bloombergquint.com/business/europe-is-rearming-and-its-defense-firms-stand-to-profit, last accessed on March 10, 2022.

S

Schwab, Klaus (2017): "The Fourth Industrial Revolution", Currency, New York.

Silicon Valley Defense Group (2020): "Fall 2020 Roundtable Series Insight Paper — Unlocking New Sources of Techno-Security Advantage", p. 6, in URL: https://static1.squarespace.com/static/5f82250a85dd3125aeba053d/t/600081281ec43d45da33b4cf/1610645802845/SVDG+Fall+2020+Roundtable+Insights+Jan+2021.pdf, last accessed on September 4, 2022.

SIPRI (2021): "World military spending rises to almost $2 trillion in 2020"; in URL: https://sipri.org/media/press-release/2021/world-military-spending-rises-almost-2-trillion-2020, last accessed on December 13 2021.

Steins, Teresa; Kerkmann, Christof (November 18, 2021): „Gaia-X-Gipfel in Mailand: Das Cloud-Projekt wird zum Problemfall", ed. Handelsblatt; in URL: www.handelsblatt.com/politik/deutschland/datensouveraenitaet-gaia-x-gipfel-in-mailand-das-cloud-projekt-wird-zum-problemfall/27809120.html?ticket=ST-56859-kZqD5Q9O2MZjdewebntt-cas01.example.org, last accessed on December 13, 2021.

V

von Bebenburg, Pitt (May 10, 2021): „Polizei in Hessen: Datenschützer prüft Palantir-Einsatz", ed. Frankfurter Rundschau; in URL: www.fr.de/rhein-main/landespolitik/polizei-in-hessen-datenschuetzer-prueft-palantir-einsatz-90530135.html, last accessed on December 13, 2021.

W

Wakabayashi, Daisuke; Shane, Scott (June 1 2018): "Google Will Not Renew Pentagon Contract That Upset Employees", ed. The New York Times; in URL: www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html, last accessed on December 13, 2021.

TECHNICAL TERM GLOSSARY

A

Advanced Research Projects Agency Network (ARPANET): A research project funded by the US Department of Defense in the 1960s that created the first computer network between terminals located at different universities.

Algorithmic Warfare: The combined employment of systems and resources relying on algorithms in their use. These include autonomous weapons, AI, and the analysis of big data.[138]

Artificial Intelligence (AI): A branch of computer science that develops machines able to perform tasks that typically require human intelligence.

Attrition-Centric Military Strategies: Military strategies building on the use of military personnel and equipment to gradually weaken enemy forces. Attrition-centric military strategies typically suggest the willingness to accept considerable losses of resources and lives of military forces. One example of attrition-centric warfare is the counter-action of Allied forces against Germany during World War II.

Autonomous Weapon System: The US Department of Defense defines an autonomous weapon system as "a weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation."[139] This definition is commonly criticized in academic discourse, however, raising concerns over what the "selection" of targets may entail and the lack of differentiation between "autonomous" and "automated" weapons.[140]

B

Big Tech: The collective term for the largest, most dominant and prestigious technology companies in the world. Most of these companies are US-based and commonly refer to five main companies in particular: Apple, Microsoft, Amazon, Google, and Facebook.

D

Decision-Centric Military Strategies: Decision-centric military strategies build on the military exploitation of artificial intelligence and autonomous (weapon) systems for the identification and prioritization of targets to weaken enemy forces. One current example of decision-centric military strategies is the Mosaic Warfare concept employed by the US Defense Advanced Research Projects Agency (DARPA).
It builds on the premise that the integration of autonomous and manned military equipment under AI-supported human decision-making has the ability to wage war more effectively while potentially endangering fewer human lives.[141]

F

Facial Recognition Technology: Originally, a technology created for the military, Facial Recognition Technology aims to identify individuals from video or photo materials based on discernible facial features.

M

Machine Learning: A process by which a digital machine learns and improves its abilities using algorithms and experience.

Military-Industrial-Complex (MIC): A term first coined by US President Dwight D. Eisenhower in 1961 to highlight the potential collusion stemming from common interests within this environment between stakeholders from politics, the defence industry and the military to further expand military expenditure.

W

War on Terror: An ongoing international military campaign headed by the US government following the terrorist attacks on 11 September 2001.

[138] Layton, Peter (2018): "Algorithmic Warfare – Applying Artificial Intelligence to Warfighting", Commonwealth of Australia, p. iii. in URL: https://airpower.airforce.gov.au/publications/algorithmic-warfare-applying-artificial-intelligence-warfighting

[139] Department of Defense (November 21, 2012), Directive re Autonomy in Weapon Systems; in URL: www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf, p. 13

[140] Conn, Ariel (November 30, 2016). The Problem of Defining Autonomous Weapons, ed. The Future of Life Institute; in URL: https://futureoflife.org/2016/11/30/problem-defining-autonomous-weapons/

[141] Clark, Bryan; Patt, Dan; and Walton, Timothy (March 3, 2021); Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage, Hudson Institute; in URL: www.hudson.org/research/16729-implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage