

This item is the archived peer-reviewed author-version of:

Contractors or robots? Future warfare between privatization and automation

Reference:

Calcara Antonio.- Contractors or robots? Future warfare between privatization and automation
Small wars and insurgencies - ISSN 0959-2318 - Abingdon, Routledge journals, taylor & francis ltd, 33:1-2(2022), p. 250-271
Full text (Publisher's DOI): <https://doi.org/10.1080/09592318.2021.1957534>
To cite this reference: <https://hdl.handle.net/10067/1805150151162165141>

Contractors or Robots? Future Warfare between Privatization and Automation

Antonio Calcara (University of Antwerp)

Forthcoming on Small Wars and Insurgencies

Abstract

Contemporary warfare is increasingly shaped by the complex relationship between the privatization of security and technologically driven automation. On the one hand, there is a growing tendency to employ private military and security companies for a range of military support tasks. On the other hand, the growing automation of security technologies is bound to make war less manpower intensive. Combat systems will have much more autonomy and humans will be working more closely with machines than they do today.

The article provides an original analysis on the interplay between the privatization of security tasks and technologically driven automation and investigates their impact on the defence industry and the armed forces. These two sets of actors are arguably among the most impacted by the multi-faceted relations between privatization and automation.

Technological progress creates the need for contractors to maintain and operate platforms that militaries do not have expertise to run. However, technologically driven automation - often developed in value chains far removed from the military-industrial pipeline - might also replace private contractors in non-core security tasks. The possibility to employ automated and autonomous systems will hence impact on the already delicate balance between private contractors and publicly-funded armed forces.

Keywords: Armed Forces; Automation; Contractors; Defence Industry; Privatization; Security.

Introduction

Contemporary warfare is increasingly shaped by the complex relationship between the privatization of security and technologically driven automation. On the one hand, there is a growing tendency to employ private military and security companies (PMSCs) for a range of diverse security tasks. On the other hand, the growing automation of security and defence technologies is bound to make war less and less manpower intensive. Combat systems will have much more autonomy and humans will

be working more closely with machines than they do today. Privatization and automation seem also to respond to a similar logic, namely the states' aim to externalize the burden of warfare to minimize their exposure to political financial, political, and diplomatic costs.

Given these considerations, the article's goal is twofold: first, it aims to describe privatization and automation in contemporary warfare and discuss the economic, political and strategic logics that drive these processes. Second, it investigates the impact of privatization and automation on the defence industry and the armed forces. These two actors are arguably among the most impacted by the multi-faceted relations between privatization and automation.¹ What is the relation between the privatization of security and technologically driven automation? What will be the impact of privatization and automation on the defence industry and armed forces? Will robots completely replace both soldiers and private military contractors? In this article, I seek to provide a first step towards answering these questions by arguing that technological progress creates the need for private contractors to maintain and operate platforms that militaries do not have expertise to run. However, technologically driven automation – often developed in value chains far removed from the traditional military-industrial pipeline – might also directly replace private contractors in non-core security tasks. The possibility to employ automated and autonomous systems will hence substantially impact on the already delicate balance between private contractors and publicly-funded armed forces.

The article is structured as follows: the first two sections describe the trend towards privatization of security tasks and technologically driven automation, highlighting their distinctive features and presenting the debates on their application to the military field. The following sections investigate the implications of privatization and automation for the defence industry and the armed forces. The conclusions summarize the study's findings and identify potentially fruitful avenues for future research.

1. Privatization

In the last thirty years, governments have systematically employed PMSCs to perform security tasks that were previously carried out by publicly funded armed forces.² The scholarly debate on PMSCs has experienced spectacular growth after the conflicts in Afghanistan and Iraq. The reliance on private contractors in these two military operations has been indeed unprecedented in size and scope. In the latest phase of Operation Herrick in Afghanistan the total force of the UK army was composed of more than 40% of private military contractors.³ In 2011, the US Commission on Wartime Contracting in Iraq and Afghanistan estimated that at least \$117 billion has been spent on private contractors since October 2001.⁴ In 2017, the US spent \$320 billion on private contractors – more than China and

Russia spent on their militaries combined in that year.⁵ In 2019, the Pentagon allocated \$370 billion on contracting, 164% higher than its spending on contractors in 2001.⁶ Yet, this growing trend towards the employment of PMSCs is not an exclusive feature of the UK or the US. Russia, for instance, is increasingly relying on contractors in the Libyan, Ukrainian and Syrian conflicts.⁷ Other examples include – among others - the Israeli privatization of checkpoint missions in the West Bank, Nigerian war against Boko Haram, Indonesian border security, and China's growing footprint in Africa.⁸ Similarly, international organizations and multinational corporations have also made extensive use of private contractors in their security-related operations.⁹

Much of the media attention has been so far devoted to the PMSCs that are directly employed on the battleground. Two events have catalysed public attention: in September 2007, military contractors employed by Blackwater Security Company murdered fourteen Iraqi civilians and wounded twenty more while escorting a US embassy convoy. Five years later, the guards employed by Blue Mountain Group abandoned their posts when Ansar al-Sharia militants attacked the US consulate in Benghazi, Libya. This attack, which resulted in the deaths of Ambassador Stevens, a State Department employee and two CIA private security contractors who were protecting the compound, directed public attention to PMSCs in conflict zones. As a consequence, the public and academic discussions on PMSCs have focused predominantly on ensuring public accountability of private force. In a seminal book on the topic, Avant¹⁰ observed that the privatization of security tasks has strengthened the executive power by eroding the power of the legislative to scrutinize foreign policy. Leander has focused on the ability of PMSCs to lobby and to influence Western states' security posture.¹¹ Overall, there is a negative perception of private contractors, often called mercenaries, and prone to self-serving and predatory behaviours.¹²

However, this picture fails to adequately examine the nuances of PMSCs' involvement in security-related tasks. There has been indeed a limited elaboration, both conceptually and empirically, of the distinctive features of this industry. Singer's *Corporate Warriors* is ground-breaking in its attempts to outline a new global military industry, distinguishing between military providers, military consultants and military supporters.¹³ This distinction is particularly helpful because - contrary to common assumptions and media representations - private military contractors are rarely used for combat missions and they are often unarmed. To make a striking example, in Iraq, most of the contractor personnel were employed for base support (65.3%) with only 12.2% used for security.¹⁴ In contrast, PMSCs are widely used in the service and logistics sectors.¹⁵ In 2015, 75% of all contractors employed by the US CENTCOM were providing logistical support.¹⁶

Experts and scholars have long debated on the ideational roots behind the increasing privatization of security tasks. Some have argued that privatization of security has gained momentum due to the

belief in the superiority of market solutions and the neoliberal commitment to reduce the size and functions of the public sector.¹⁷ The UK – inspired by public management reforms in public administration - has radically reformed its defence ecosystem in the 80s, systematically relying on private actors for defence procurement, services, and logistics.¹⁸ Recent studies have also linked the systematic use of PMSCs in logistics to a broader “post-Fordist” transformation of the armed forces: military tends towards greater centralization of management control and to the systemic outsourcing of non-core functions.¹⁹ These ideas may also explain cross-national differences in states’ reliance on PMSCs. While countries with a more liberal model of civil-military relations like the UK and the US have systematically relied on PMSCs, other states with a different civil-military culture (for instance France and Germany) have displayed a lower propensity to outsource military tasks.²⁰

The privatization of security and military support may also be related to functional reasons. After the Cold War, budgetary and manpower cuts in armed forces worldwide made a large number of trained military personnel available in an increasingly globalized security market.²¹ In addition, the rising demand for expeditionary out-of-area military operations puts a strain on lines of communication and logistics. In the era of “everywhere wars”, simultaneous deployments overseas to theatres where local facilities and logistical supply lines are limited have become more frequent.²² To overcome logistical shortfalls and fill sustainment requirements, armed forces are increasingly constrained to rely on external agencies and firms to support services ranging from transportation over base support.²³

There is a broad consensus that privatization of security tasks and increasing reliance on contractors is closely related to the growing political costs of warfare. Specifically, the resort to contractors has gained momentum as a response to the tightening constraints on the deployment of uniformed personnel in military operations.²⁴ Private contractors, whether armed or unarmed, allow Western states to fight wars remotely by minimizing the operational, financial, human, and political costs of war.²⁵ To be sure, non-liberal states such as Russia, Iran, and the United Arab Emirates (UAE) – among others – have all distinct motivations to externalize the burden of war. Political opportunity costs may incentivize states to rely on PMSCs to enjoy a shield of plausible deniability for the actions conducted by their commercial proxies. To make a striking example, scholarly works have documented how Russia has used remote warfare by contractors to not incur the political costs of violating international law in Ukraine.²⁶

Finally, privatization is also related to technological innovation and, specifically, with greater complexity and sophistication of security technologies. PMSCs are indeed systematically employed to provide technological support for information technology (IT), infrastructure, and complex high-tech weapon systems.²⁷ Armed forces no longer have in-house skills and know-how to maintain and update their sophisticated arsenal and they rely on private contractors to perform these important

roles.²⁸ This consideration urges a reflection on how privatization is related to the current wave of technological innovation driven by automation and autonomy.

2. Automation and Autonomy

The history of military innovation has been traditionally characterized by long phases of technological stagnation punctuated by occasional spikes of revolutionary change.²⁹ While most technologies alone have rarely caused the military balance to shift³⁰, there are also phases of technological innovation that have had a disruptive effect on the organization and practice of war. The classical example is the development of nuclear weapons and the so-called nuclear revolution in military affairs.³¹

Today, scholars and experts argue that we are living in a revolutionary technological phase. Drawing on the digital wave in the cyber domain from the 90s, we are now seeing multiple, overlapping, and converging technical revolutions in various domains, increasingly blurring the lines of the digital, physical and biological.³² The founder of the World Economic Forum, Klaus Schwab, labelled this new technological era as the “Fourth Industrial Revolution”.³³ Significant advancements in automated, autonomous and robotic systems, artificial intelligence (AI), remote sensing, cyber technology, hypersonic vehicles, additive manufacturing, stealth, precision guidance, and other areas have spread the idea that emerging technologies have the potential to be game-changers in military affairs.³⁴ Autonomy and AI are also central aspects of today’s military strategies. China’s National AI strategy suggests that leadership in AI will be critical to military power, and the US Department of Defence (DoD) considers autonomy as a crucial factor in preserving its military dominance.³⁵ Russia has targeted 30% of its entire military force structure to be robotic by 2025. Even the EU is currently pointing to invest in autonomy and AI to finally strengthen its defence posture.³⁶

This emerging technological wave is primarily characterized by automated and autonomous security technologies.³⁷ Notwithstanding they are often used interchangeably in the public debate, automated and autonomous systems possess distinct characteristics. Automated systems simply respond mechanically to well-defined input. In the military realm, a classical example of an automated system are the landmines. Other more sophisticated systems, such as Israel’s Iron Dome missile defence, can be also defined as automated as they are pre-programmed rule-based systems, which provide largely predictable outcomes.³⁸ In contrast, autonomous systems are far more complex, as they would be ideally able to reason probabilistically based on a set of inputs, compose different courses of actions, and then select and execute the best option without human intervention at any of these stages.³⁹ According to Scharre and Horowitz⁴⁰, to understand military-related autonomy is indeed important to specify the degree of human involvement in the execution of a machine’s tasks. Following this

argument, they identify “human-in-the-loop” systems as characterized by pervasive human control in the machine’s core tasks. In “Human-on-the-loop” systems, machines can operate autonomously, but humans can still review and intervene in these decisions. A system that can carry out its tasks completely independently is defined as a “human-out-of-the-loop” system.⁴¹ These considerations are also helpful to distinguish between narrow and general AI. Narrow AI focuses on a singular or limited function and specific tasks. An example of narrow AI is AlphaGo, the algorithm developed by DeepMind that defeated one of the world’s best Go players in 2016.⁴² On the contrary, general AI denotes the capability to perform a broad range of complex intellectual tasks.

Much of the discussion so far has been devoted to “Lethal Autonomous Weapon Systems”, that – once activated – are “intended to select and engage targets where a human has not decided those specific targets are to be engaged”.⁴³ These systems will be ideally able to attack various sets of targets, including vehicles, structures, and individuals, operate over an extended period after activation, and will potentially be able to learn and adapt their behaviour.⁴⁴ According to these studies, autonomous systems can essentially enable faster operations. New autonomous battle networks of sensors and shooters rapidly accelerate the process of detecting, targeting, and striking threats, the so-called “kill chain”.⁴⁵ For instance, an autonomous plane might be more adept at identifying and avoiding air defence threats or better at predicting and defeating adversaries in an air-to-air dogfight.⁴⁶ Moreover, autonomous systems could help humans to overcome some of their intrinsic cognitive and physical limits, especially in terms of fatigue, stress, confusion. An autonomous sniper would not get tired or hesitate after a certain number of hours, as any human would do.⁴⁷ To be sure, there is currently a debate on the stage of scientific research in military autonomy and AI. According to some experts, existing applications of AI are in any case still narrow in nature.⁴⁸ Others highlight that general AI, even if not mature, is emerging quickly.⁴⁹ A 2017 review by the Stockholm International Peace Research Institute identified 49 deployed weapon systems with autonomous targeting capabilities sufficient to engage targets without the involvement of a human operator.⁵⁰

Automated and autonomous systems give militaries the ability to reduce the risk to their soldiers while still projecting power in similar ways to how they used force previously.⁵¹ Operating autonomous systems would allow the military to operate in complex operations, with minimal human involvement at the tactical level. According to some scholars, fully autonomous aerial weapons would eventually not even necessarily need ground elements to analyse battlespace intelligence.⁵² The number of soldiers on the ground would dramatically decrease. Relatedly, studies are reflecting on if and how automated and autonomous systems will gradually decrease the need to mobilize political support before deploying military capabilities⁵³ and on countries’ ability to demonstrate resolve in military confrontations.⁵⁴

3. Privatization, Automation and the Defence Industry

The impact of privatization and automation on the defence industry is developing along two different and partially conflicting lines. First, the defence industry is clearly benefiting from the privatization of security tasks. Since the 80s, the combination of increasing weapons' costs (and technological complexity) and declining defence budgets have forced defence industries to embark on a process of privatization and concentration of the market.⁵⁵ The growing technological complexity of weapon systems has forced states to involve the industry in the whole lifecycle of defence equipment from the initial design to decommissioning.⁵⁶ Prime contractors or systems integrators have now a key role in the overall defense procurement process, as they translate military requirements into acquisition programs and combine diverse technological, technical and physical components into functioning systems.⁵⁷ The defence industry has also been able to successfully penetrate the security services market. Now defence contractors are active in cyberoperations, intelligence analysis, and advisory forces in failing states.⁵⁸ This trend was evident in the US when the Bush Jr. Administration created the Department of Homeland Security, mainly to procure systems in the same way (and with a huge budget) the Pentagon does.⁵⁹ In Europe, defence industries are also key players in the security market, especially for what concerns border security, facial recognition, and profiling.⁶⁰

Second – and partly in contradiction with the first trend – technologically driven automation resides in value chains far removed from the traditional military-industrial complex. New players and a rapidly evolving defence market may significantly threaten traditional defence contractors in the medium and long-term. To be sure, this is not entirely a new trend, since for more than thirty years now dual-use technologies opened-up the defence market to newcomers specializing in IT and related services⁶¹ However, technologically driven automation – because of its intrinsic characteristics – may represent a true paradigm shift in the defence market. As highlighted by Verbruggen, civilian advances in autonomous technologies will have greater dual-use utility than more military-oriented R&D.⁶² This is because automated and autonomous technologies are general-purpose technologies that can be used for a wide variety of both military and civilian applications. Because military innovation is becoming more capability-oriented, civilian innovation related to general-purpose technologies has become more relevant to military innovation at large. Cronin argues that we are living in a period of open innovation technology, as technological innovation is not strictly dependent on military research.⁶³ In the 60s, 70s, and 80s, state-funded research in the military field has then

been introduced in the civil field. With federal government support, the Advanced Research Projects Agency Network (ARPANET) became the Internet. Tax dollars developed the Global Positioning System (GPS) and Google and Apple (among others) have been able to innovate by exploiting the existing technological and infrastructural base originally funded by the state. Today, the private sector has become the primary locus of scientific progress, especially for what concerns automation. Companies like Microsoft, IBM, Facebook, Amazon, Apple, and Alphabet now drive research in autonomous systems and AI. Players in the IT and automotive industries are also at the forefront in advancing autonomy.⁶⁴

A key underlying factor is that the defence industry is currently being outspent on R&D: aerospace and defence companies spend less on R&D as a percentage of revenue than both software and tech companies. In 2017, Amazon became the world leader in R&D expenditure, ahead of Alphabet, Google's parent company, and Intel. With Apple and Microsoft being ranked in the American Top 5, these companies spend 76.2 billion dollars on R&D. Amazon spends more on R&D than the entire global aerospace and defence industry.⁶⁵ These developments may gradually erode the defence industry's market position, also considering the challenge associated with defence contractors' workforce, many of whom are older workers nearing retirement. Young talents in IT and engineering are more attracted to the civil sector and the technology platform companies, which ensure higher salaries and a more stimulating working environment.⁶⁶

Public authorities are also trying to adapt to these new market dynamics. In the US, the Pentagon explicitly aims to adopt a venture capital model of development by partnering with the start-up business community in the Silicon Valley.⁶⁷ This would ideally allow US national security agencies to steer nascent companies' business trajectories by firms to apply their innovations to defence. A striking example is In-Q-Tel (IQT), a strategic investment firm funded by the CIA. Among other things, IQT finances also the now-famous Palantir Technologies, a data analysis agency that works very closely with US security agencies. In 2019, Palantir Technologies won an \$800 million contract for updating the US Army's software on ground systems, becoming the first Silicon Valley company "to win a defence program of record".⁶⁸

At the moment, data shows that the traditional defence industry continues to dominate the market, including in automated and autonomous combat systems. 50% of Unmanned aerial vehicles (UAVs) in the US have been contracted to Northrop Group and General Atomics, two well-established defence firms.⁶⁹ In 2020, the top 100 defence companies increased their revenues for a fourth straight year.⁷⁰ Since Apple, Amazon, Google, or Tesla (just to name a few) have not yet been embedded in the defence circuit, some have suggested that the traditional war-state infrastructure is still dominant in military innovation.⁷¹ Geist highlights that the US Department of Defence's Advanced Research

Projects Agency (DARPA) provided the bulk of funding for artificial intelligence in the US.⁷² Recently, DARPA announced a 2\$ billion campaign to develop the next wave of AI technologies and it is currently pursuing more than 20 programs to advance in autonomy-related technologies. In Europe, many calls for the establishment of a “European DARPA”, a centralized structure able to finance defence technology. The just-approved European Defence Fund and the creation of the EU Commission’s DG on Defence Industry and Space can be contextualized as first steps in this direction, given that for the first time EU funds will be used to finance the military research.⁷³

We need also to consider the structural obstacles of the spin-in (technological transfer from the civil to the military sector). More than twenty years ago, Molas Galart convincingly argued that dual-use technology transfer in the military is complicated by the degree of modifications required for defence platforms.⁷⁴ Verbruggen highlights that this factor is important in technologically driven automation, where there is a great initial overlap between civilian and military R&D, but at the later stage application and standards diverge.⁷⁵ Working with defence agencies is also complicated from a purely business perspective, especially when it comes to intellectual property rights. Civilian R&D often relies on open-source technologies where companies release incremental improvements. Military research is instead structured around confidentiality and public ownership of sensitive technologies.⁷⁶ Some civilian industries have already expressed some unease in collaborating with the defence sector, as shown by resistance from Google developers to collaborate with the Pentagon. Civil society groups are also pressuring private companies through groups like the “Campaign to Stop Killer Robots” in Europe.⁷⁷ Civilian companies seems to be worried about the negative stigma associated with working with the military ecosystem in the development of automated and autonomous systems.

In this respect, it is interesting to note the similarities between the constraints on the privatization of combat and the legal and normative barriers to develop and eventually employ lethal autonomous weapon systems. From a legal point of view, there are similar discussions between ensuring public accountability of private contractors and the regulation of autonomous weapon systems.⁷⁸ From a normative standpoint, both private contractors and autonomous weapon systems are problematic to justify for nation-states that have anchored their political legitimacy and sovereignty on upholding a monopoly of violence and maintaining publicly funded armed forces.⁷⁹ Public and media attention on the role of PMSCs like Blackwater is currently preventing systematic recruitment of private contractors on the battlefield.⁸⁰ PMSCs also have learned that the stigma attached to conducting offensive security tasks may be bad for business, and are currently wary of participating in activities that may involve them in direct, physical conflict with enemy forces.⁸¹ PMSCs are also incentivized to shift their range of operations to smaller countries with less democratic oversight, where they can offer customised services, technologies and trained specialist personnel for operational planning and

training support. This is, in turn, useful for small states to close the discrepancy between ambitious strategic objectives and available in-house capacity and capability.⁸² For instance, some analyses have reported on the business operations of the former CEO of Blackwater Erik Prince in the UAE and the activities of major Western PMSCs in Saudi Arabia.⁸³ An interesting recent trend is represented by big private equity firms that are buying and controlling PMSCs and directly rent their services to small states or private firms.⁸⁴

4. Privatization, Automation and Armed Forces

What will be the impact of privatization and automation on the armed forces? Can we envisage a foreseeable future in which states will systematically rely on PMSCs on the battlefield? Will automated and autonomous systems or robots eventually replace soldiers and private military contractors?

Scholarly works revealed how outsourcing missions to PMSCs tend to decrease military effectiveness and negatively impact the severity of armed conflicts in weak states.⁸⁵ Evidence on the cost-effectiveness of contracting is also mixed.⁸⁶ Nevertheless, the use of PMSCs is likely to continue increasing due to their political rather than merely financial convenience, linked to the dispersion of risks, discretion, deniability and the overall desire to affect the military balance without being directly involved in a conflict.⁸⁷ Moreover, private contractors will arguably be increasingly involved in taking government activities related to advisory role in failing states⁸⁸, as well as low-intensity military policing tasks, such as ensuring security for diplomatic premises and personnel.⁸⁹ Recent studies have highlighted states' outsourcing of cyber-operations and the growing importance of cyber "boutique firms" offering offensive cyber security services to law enforcement and national security organisations. Some relevant examples of this trend are Hacking Team, a company that was based in Italy but offered cyber services to public and private entities around the world, and Endgame, dubbed – not by chance - as "Blackwater of hacking".⁹⁰ Journalistic sources have also reported about "Project Raven" and the activities of former US intelligence operatives recruited by UAE for vulnerabilities hunting in the computer systems of foreign governments.⁹¹ It is certainly difficult to draw a clear line of demarcation between PMSCs and groups of hackers, due to their ambiguous relationship with state structures. For instance, Russian cyber-operations rely on disparate groups of hackers and have employed advanced techniques for cyber intrusion and evasion to prevent hackers identification and possible attribution to Moscow.⁹² Recent scholarly works by Egloff and Maurer on, respectively, semi-state actors and state proxies have developed relevant analytical categories to investigate this phenomenon.⁹³ Another important point in this discussion on cyber-operations' outsourcing is related

to the legal aspects of cyber-attacks attribution, which needs to be contextualized in a complex environment that must necessarily balance domestic and international law with geopolitical and cost-opportunity implications.⁹⁴

As argued above, privatization has been often associated with financial incentives. Since the 80s, steered defence budgets towards research & development and procurement created a need to cut personnel costs. Defence budgetary restrictions and growing costs (and technological complexity) of military procurement are positively correlated with the structural involvement of the private sector.⁹⁵ Technological progress inevitably leads to the creation of new professionals who are not immediately available among armed forces' personnel but who can be recruited by the private sector. At the same time – as currently exemplified by the Joint Strike Fighter – the procurement of sophisticated weapon systems has transformed into the provision of a service rather than the purchase of an asset to be operated and maintained by uniformed personnel. To make another example, in the current discussion on the next European sixth-generation fighter, the two competing projects (the British with “Tempest” and the Franco-German “Future Combat Air System”) are based around structural links between national governments and defence industries throughout the procurement cycle, from initial studies to maintenance.⁹⁶ Similar considerations are also valid for logistics, services and other non-core security tasks. Publicly-funded armed forces are no longer able to successfully self-perform and are dependent on external capacity and capability to manage the globalized supply-chain of war.

The privatization of security has already been impacted by the growing automation of security technologies. For instance, the systematic use of drones on the battlefield has led to the creation of new professional figures specifically dealing with functions such as take-off and landing. These tasks have been entrusted to private contractors' expertise, as the armed forces do not currently have in-house expertise to manage them.⁹⁷ Scholarly works are also currently speculating on whether warrior machines or robots will directly supplant soldiers on the battlefield.⁹⁸ Military autonomy has evolved to a point where it is possible to contemplate conflicts in which human beings are no longer directly engaged in combat. This may eventually negatively impact PMSCs because if more non-core security tasks will be automated, there will be less and less need for private contractors. At the moment, robots have tended to replace humans in repetitive but precise tasks, while humans do many skilled activities.⁹⁹ Consequently, many of the tasks currently performed by PMSCs, like driving, catering, and cleaning, construction, and static security, are among the easiest to automate. However, increasing automation will primarily depend on these systems' costs and reliability. At the moment, predictions that automation would supplant humans in complex tasks are not entirely accurate because these kinds of robots remain costly.¹⁰⁰ In this discussion, we need also to consider how automated and autonomous systems will be actually integrated into armed forces' practice and routine. Lindsay

has convincingly argued the need to carefully investigate how practitioners use technology in actual operations.¹⁰¹ It is therefore difficult to predict how automation and autonomy will eventually impact armed forces without taking into account how different military structures in different countries and regions adopt and integrate these technologies. Most likely, each armed force will find a different balance between machines and humans.

If automated technologies will become cheaper and more reliable, eventually threatening armed forces' jobs, it is also plausible to expect resistance from the armed forces themselves. Automation does not come conflict-free. De Vore has shown that the US Air Force's and Naval aviation's pilot-dominated hierarchies never prioritized drones over manned aircraft.¹⁰² Military disruptive technologies like automated UAVs threaten a person's role and identity within the armed forces.¹⁰³ On this point, the RAND corporation found that AI adoption among armed forces has been hampered so far by "inherent resistance to change...concerns about the potential loss of an individual's value to the organization", and a general lack of trust in the technology itself.¹⁰⁴ Such services and individuals may therefore resist automation, perhaps by leveraging both strategic concerns (the spread of these technologies might erode Western military superiority and favor non-state actors), tactical risks (software failure and risk of hacking), as well as international law and norms (automated lethal platforms are unaccountable and they violate international humanitarian law). The scholarship on military innovation has long emphasized that innovation in military doctrine requires the presence of advocates for change.¹⁰⁵ In this context, automated and autonomous systems may prove to be either so cheap to be permanently integrated in non-core security tasks or so reliable and effective on the battlefield that they will inevitably lead to pressures for top-down change. It is also interesting to note how some emerging dynamics in the field of automation were already experienced by private contractors. Military organizations tended to resist giving up to contractors those tasks that they see as central to their mission or essence, but easily accept or even encourage the delegation to private actors of those that they see as peripheral.¹⁰⁶ We can therefore expect the behaviour of military organizations to be similar vis-à-vis both privatization and automation: armed forces should welcome both the privatization and the automation of support tasks that are seen as peripheral but are likely to resist both the privatization or the automation of tasks that they see as crucial to their mission and identity, most notably combat.

Overall, much will depend on how automation and autonomy – for instance, linked to AI, machine learning, and big data – will prove to be enabling or labour replacing technologies. Frey has shown how historically labour-replacing technologies have generated opposition while enabling technologies have been more easily embraced.¹⁰⁷ Automation does not necessarily imply indeed the replacement of human personnel. Technological progress always triggers an increasing demand for

complements and a reallocation of tasks between humans and machines. So far, automation has been usually accompanied by new tasks necessary to enable it. For instance, Fino noted how the use of guided missiles in F-4 fighter jets led to a need for a second human in the cockpit to operate the radar.¹⁰⁸ Additional automation has historically been developed primarily to alleviate traditional burdensome tasks. Once the pilots accepted that these developments would improve their professionalism rather than undermine their role and identity, they began to accept them.¹⁰⁹ A recent report found defense research into AI is focused “not on displacing humans but assisting them in ways that adapt to how humans think and process information”.¹¹⁰ Recent studies have shown that the use of drones is not – at the moment - positively correlated with a reduction of personnel.¹¹¹ Highly skilled remotely crewed platforms are critical for the successful employment of drones on the battlefield. These considerations raise important questions about the future composition of armed forces. It is indeed likely the army of the future will be composed of soldiers with a different skill set to effectively integrate humans and machines. In a recent study, Asoni et al noted that in the US the change in technology, tactics, operations, and doctrines observed over the past decades has called for the recruitment of more skilled individuals.¹¹² Greater automation of the armed forces is inextricably linked to more-capital intensive personnel. At this stage, it is difficult to predict whether this would encourage the use of more specialized PMSCs or more in-house expertise. In the future, technology might directly replace many private contractors, as automation is most likely to affect those repetitive and peripheral tasks that are currently the bulk of the activities performed by contractors. In any case, education, recruitment, and training will probably be critical to integrate humans (both soldiers and contractors) and machines in armed forces’ organizations.

5. Conclusions

The article provides an original analysis on the interplay between the privatization of security tasks and technologically driven automation. Notwithstanding privatization and automation have been often treated separately, they are more interlinked than it is usually portrayed. This work shows that privatization and automation are both inextricably related to the externalization of the burden of war, political benefits and costs, and international security competition. Both privatization and automation are also inhibited by the same legal and normative barriers related to accountability. Technological progress has created the need for private contractors to maintain and operate platforms that armed forces do not have the expertise to run. The defence industry has also undoubtedly benefiting from the privatization of security tasks, especially in IT, service and logistics. However, automated and autonomous systems might directly replace many contractors, as automation is most likely to affect

many of the non-core functions and repetitive tasks that are currently performed by private contractors. Armed forces have also traditionally resisted the privatisation of core security tasks and they are having a similar negative reaction to the systematic use of automated and autonomous systems on the battlefield. Privatisation and automation will therefore remain, at least in the short term, systematically employed in non-core-security functions. This may change if automated and autonomous systems will be so effective on the battlefield to induce top-down change and if there will be internal advocates for change at the political or military level.

The article opens fruitful avenues for future research: first, the scholarship on defence technology and privatization should further investigate the relations between automation and privatization of security tasks. More should be written on how technologically driven automation will impact on the deployment of private contractors both in non-core security tasks and on the battlefield. Second, it would be interesting to make a systematic examination on how defence budgets are currently balancing the need for increasingly sophisticated and expensive procurement of automated and autonomous systems with expenses for private contractors. This point is inextricably linked to the future composition of armed forces, where it will be crucial to find a balance between a more capital-intensive military and a more automated and eventually privatized support system. Finally, this work needs also to be complemented by specific analyses on the evolving role of the state. Both privatization and automation are linked to a special emphasis on private industries and enterprises. However, great power competition, the growing politicization of value chains, and exogenous events such as COVID-19 are leading the state to (re-)assume a central role in economic and security policy. This will probably have a major impact both on privatization and automation and on the broader understanding of the changing character of warfare.

¹ Krishnan, *War as business*.

² Singer, *Corporate Warriors*; Avant, *The market for force*; Cusumano & Kinsey, *Bureaucratic interests*.

³ Cusumano, *Bridging the gap*, 110.

⁴ Commission on Wartime Contracting in Iraq and Afghanistan, *At What Risk?*.

⁵ Mahoney, *United States defence contractors*, 4.

⁶ Peltier, *The Growth of "Camo Economy"*

⁷ Marten, *Russia's semi-state security*; See Østensen, *Private Military Companies – Russian great power politics on the cheap?* on this special issue

⁸ Swed and Crosbie, *Private security military contractors*; see Yuan, *China's Private Security Companies and the Protection of Chinese Economic Interests Abroad* on this special issue

⁹ Krahmann, *States, citizens and privatization*; Cusumano and Ruzza, *Piracy and the Privatisation*.

¹⁰ Avant, *The market for force*

¹¹ Leander, *Commercialising security in Europe*

¹² Percy, *Mercenaries*; see Olsen, *The Social Construction of Mercenaries*

¹³ Singer, *Corporate Warriors*

¹⁴ Schwartz, *Department of defense contractors*.

¹⁵ La Porte, *Balancing Act*; Krieg, *Defining Remote Warfare*.

¹⁶ Moore, *US military logistics*, 9

¹⁷ Singer, *Corporate warriors*, Avant, *The market of force*; Erbel and Kinsey, *Think again—supplying war*.

¹⁸ Calcara, *European Defence Decision-making*.

¹⁹ Bury, *Conceptualising the quiet revolution*.

-
- ²⁰ Krahmann, *States, citizens and privatization*; Leander, *Commercialising security in Europe*
- ²¹ Erbel, *Underlying causes military outsourcing*, 137
- ²² Moore, *US military logistics*
- ²³ La Porte, *Balancing Act*
- ²⁴ Cusumano, *Bridging the gap*
- ²⁵ Krieg and Rickli, *Surrogate warfare*
- ²⁶ Marten, Russia's semi-state security, see Krieg, Call in the Mercenaries - Externalizing Warfare to Corporate Warriors in the Middle East on this special issue
- ²⁷ Krishnan, *War as business*; Kinsey and Patterson, *Contractors and War*
- ²⁸ Mahoney, *United States defence contractors*
- ²⁹ Chin, *Technology, war and the state*, 767
- ³⁰ Horowitz, *The diffusion of military power*
- ³¹ Jervis, *Meaning of nuclear revolution*
- ³² McAfee and Brynjolfsson, *Human work robotic future*
- ³³ Schwab, *The Fourth Industrial Revolution*.
- ³⁴ Sechser, Narang and Talmadge, *Emerging technologies and strategic stability*; Brose, *The Kill Chain*
- ³⁵ Horowitz, *Artificial Intelligence, International Competition*
- ³⁶ Calcara, Csernatononi and Lavallée, *Emerging Security Technologies*
- ³⁷ Rossiter, *The impact of robotics*
- ³⁸ Scharre, *Opportunity and challenge autonomous systems*, 10
- ³⁹ Cummings, *Artificial intelligence*, 3
- ⁴⁰ Scharre and Horowitz, *Introduction Autonomy Weapon Systems*, 5
- ⁴¹ Horowitz, *When speed kills*
- ⁴² Gibney, *Google AI algorithm*
- ⁴³ Scharre and Horowitz, *Introduction Autonomy Weapon Systems*, 16
- ⁴⁴ Altmann and Sauer, *Autonomous weapon systems*, 118
- ⁴⁵ Brose, *The Kill Chain*
- ⁴⁶ Horowitz, *When speed kills*
- ⁴⁷ Ayoub and Payne, *Strategy Artificial Intelligence*
- ⁴⁸ Scharre and Horowitz, *Introduction Autonomy Weapon Systems*; Cummings, *Artificial intelligence*
- ⁴⁹ Ayoub and Payne, *Strategy Artificial Intelligence*
- ⁵⁰ Boulanin and Verbruggen, *Mapping Development of Autonomy*, 26
- ⁵¹ Leys, *Autonomous weapon systems*
- ⁵² Haas and Fischer, *Evolution of targeted killing practices*, 289
- ⁵³ Zegart, *Cheap fights*
- ⁵⁴ Gartzke, *Blood and Robots*
- ⁵⁵ Calcara, *European Defence Decision-making*
- ⁵⁶ Krishnan, *War as business*, 4
- ⁵⁷ Gholz, *Systems integration*
- ⁵⁸ Mahoney, *United States defence contractors*
- ⁵⁹ Bellais, *Technology and the defense industry*, 73
- ⁶⁰ Schilde, *Political Economy European Security*
- ⁶¹ Molas-Gallart, *Which Way to Go?*; Krishnan, *War as business*
- ⁶² Verbruggen, *The Role of Civilian Innovation*
- ⁶³ Cronin, *Power to the People*
- ⁶⁴ Brynjolfsson, Rock and Syverso, *Artificial Intelligence*
- ⁶⁵ PWC, *Defence trends 2020*
- ⁶⁶ Taubman, *Defense Industry's Brain Drain*; PWC, *Defence trends 2020*
- ⁶⁷ Mahoney, *United States defence contractors*, 2
- ⁶⁸ Chan, *Palantir US army*
- ⁶⁹ Mahoney, *United States defence contractors*
- ⁷⁰ Gould, *Arms trade momentum*
- ⁷¹ Chin, *Technology, war and the state*
- ⁷² Geist, *AI arms race*
- ⁷³ Calcara, Csernatononi, and Lavallée, *Emerging Security Technologies*
- ⁷⁴ Molas-Gallart, *Which Way to Go?*
- ⁷⁵ Verbruggen, *The Role of Civilian Innovation*
- ⁷⁶ Bellais and Guichard, *Defense Innovation, Technology Transfers*
- ⁷⁷ Carpenter, *Rethinking the political/-science/-fiction nexus*
- ⁷⁸ Bode, *Norm-making Global South*
- ⁷⁹ Tilly, *National states in Western Europe*

-
- ⁸⁰ Cusumano, *Private military and security companies' logos*
⁸¹ Mahoney, *United States defence contractors*, 2
⁸² Krieg, *UAE's dogs of war*
⁸³ Mason, *Breaking the mold*, 101; Stinchfield, *Small groups*, 119-122
⁸⁴ Stinchfield, *Small groups*
⁸⁵ Dunigan, *Future US military contracting*, Petersohn, *Private military and security companies*
⁸⁶ Cusumano, *Contractor Support Economic Perspective*.
⁸⁷ Krieg, *Defining Remote Warfare*; Marten, *Russia's semi-state security*
⁸⁸ Mahoney, *United States defence contractors*, 7-9; See Weiss, A 'brave new industry': From civilian service provider to cybersecurity warriors? on this special issue
⁸⁹ Cusumano and Kinsey, *Diplomatic Security*
⁹⁰ Lobato, *Unraveling cyber security*, 104-105
⁹¹ Bing and Schectman, *Secret Hacking Team*
⁹² Jasper, *Russian Cyber Operations*
⁹³ Egloff, *Cybersecurity and Non-State Actors*; Maurer, *Cyber Mercenaries*
⁹⁴ Egloff and Smeets, *Publicly attributing cyber attacks*
⁹⁵ Krishnan, *War as business*.
⁹⁶ Bellais, *Combat Air Systems*
⁹⁷ Dickinson, *Drones Automated Weapons*
⁹⁸ Gartzke, *Blood and robots*; Williams, *Asymmetric arms control*
⁹⁹ Rossiter, *The impact of robotics*
¹⁰⁰ Gartzke, *Blood and robots*, 7
¹⁰¹ Lindsay, *Information Technology and Military Power*
¹⁰² DeVore, *Reluctant innovators?*
¹⁰³ Fino, *Tiger Check*
¹⁰⁴ Tarraf, *Defense Posture for Artificial Intelligence*
¹⁰⁵ Posen, *The sources of military doctrine*
¹⁰⁶ Cusumano, *Scope of military privatization*; Cusumano and Ruzza, *Piracy and Privatisation*
¹⁰⁷ Frey, *The technology trap*
¹⁰⁸ Fino, *Tiger Check*
¹⁰⁹ Ibid.
¹¹⁰ Konaev, *U.S. Military Investments in Autonomy*
¹¹¹ Harrison, *Remotely Crewed Systems*
¹¹² Asoni et al, *Mercenary army of the poor*

Bibliography

Altmann, Jürgen, and Frank Sauer. "Autonomous weapon systems and strategic stability." *Survival* 59, no. 5 (2017): 117-142.

Asoni, Andrea, Andrea Gilli, Mauro Gilli, and Tino Sanandaj,. "A mercenary army of the poor? Technological change and the demographic composition of the post-9/11 US military." *Journal of Strategic Studies* (2020): 1-47.

Avant, Deborah, *The market for force: the consequences of privatizing security*. Cambridge: Cambridge University Press, 2005.

Ayoub, Kareem, and Kenneth Payne. "Strategy in the age of artificial intelligence." *Journal of strategic studies* 39, no. 5-6 (2016): 793-819.

Bellais, Renaud. "Technology and the defense industry: real threats, bad habits, or new (market) opportunities?." *Journal of Innovation Economics Management*, no. 2 (2013): 59-78.

Bellais, Renaud. "Combat Air Systems for the 21st Century: A Shared Stake for Europe". *EGMONT Institute. Security Policy Brief* No.131, 2020.

Bellais, Renaud, and Renelle Guichard. "Defense innovation, technology transfers and public policy." *Defence and peace economics* 17, no. 3 (2006): 273-286.

Bing, Christopher and Joel Schectman, "Inside the UAE's Secret Hacking Team of American Mercenaries", *Reuters*, January 30, 2019.

Bode, Ingvild. "Norm-making and the Global South: Attempts to Regulate Lethal Autonomous Weapons Systems." *Global Policy* 10, no. 3 (2019): 359-364.

Boulanin, Vincent & Maaïke Verbruggen, "Mapping the Development of Autonomy in Weapon Systems", *Stockholm International Peace Research Institute*, November 2017. <https://www.sipri.org/publications/2017/other-publications/mapping-development-autonomy-weapon-systems>

Brose, Christian. *The kill chain: Defending America in the future of high-tech warfare*. London: Hachette UK, 2020.

Brynjolfsson, Erik, Daniel Rock, and Chad Syverson. "Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics." *The economics of artificial intelligence: An agenda*. Chicago: University of Chicago Press, 2018. 23-57.

Bury, Patrick. "Conceptualising the quiet revolution: the post-Fordist revolution in western military logistics." *European Security* 30, no. 1, (2021): 112-136.

Calcara, Antonio. *European defence decision-making: dilemmas of collaborative arms procurement*. Abingdon: Routledge, 2020.

Calcara, Antonio, Raluca Csernaton, and Chantal Lavallée, eds. *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*. Abingdon: Routledge, 2020.

Carpenter, Charli. "Rethinking the political/-science/-fiction nexus: Global policy making and the campaign to stop killer robots." *Perspectives on Politics* 14, no.1 (2016): 53-69.

Chan, Rosalie, "Palantir has won an \$800 million contract with the US Army to build a system that helps soldiers fighting in remote areas". *Business Insider*. March 2020.

Chin, Warren. "Technology, war and the state: past, present and future." *International Affairs* 95, no. 4, (2019): 765-783.

Commission on Wartime Contracting in Iraq and Afghanistan. "At What Risk? Correcting Over-Reliance on Contractors in Contingency Operations," Second interim report to congress, Washington, 2011.

Cronin, Audrey Kurth. *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford: Oxford University Press, 2019.

Cummings, Missy. *Artificial intelligence and the future of warfare*. London: Chatham House for the Royal Institute of International Affairs, 2017.

Cusumano, Eugenio. "The scope of military privatisation: Military role conceptions and contractor support in the United States and the United Kingdom." *International Relations* 29, no.2 (2015): 219-241.

Cusumano, Eugenio. "Bridging the gap: Mobilisation constraints and contractor support to US and UK military operations." *Journal of strategic studies* 39, no. 1 (2016): 94-119.

Cusumano, Eugenio, Contractor Support from an Economic Perspective. In Berndtsson, Joakim, and Christopher Kinsey. *The Routledge research companion to security outsourcing*. Abingdon: Routledge, 2016.

Cusumano, Eugenio. "Private military and security companies' logos: Between camouflaging and corporate socialization." *Security Dialogue*, 52, no.2, (2021): 135–155,

Cusumano, Eugenio, and Christopher Kinsey. "Bureaucratic interests and the outsourcing of security: The privatization of diplomatic protection in the United States and the United Kingdom." *Armed Forces & Society* 41, no. 4 (2015): 591-615

Cusumano, Eugenio, and Christopher Kinsey, eds. *Diplomatic Security: A Comparative Analysis*. Stanford: Stanford University Press, 2019.

Cusumano, Eugenio, and Stefano Ruzza. *Piracy and the privatisation of maritime security: vessel protection policies compared*. Cham: Palgrave Macmillan, 2020.

DeVore, Marc R. "Reluctant innovators? Inter-organizational conflict and the USA's route to becoming a drone power." *Small Wars & Insurgencies* 31, no.4 (2020): 701-729.

Dickinson, Laura. "Drones, Automated Weapons, and Private Military Contractors." *New technologies for human rights law and practice* (2018): 93-124.

Dunigan, Molly. "The future of US military contracting: Current trends and future implications." *International journal* 69, no. 4 (2014): 510-524.

Egloff, Florian J. *Cybersecurity and non-state actors: a historical analogy with mercantile companies, privateers, and pirates*. PhD Dissertation, University of Oxford, 2018.

Egloff, Florian J., and Max Smeets. "Publicly attributing cyber attacks: a framework." *Journal of Strategic Studies* (2021): 1-32 (online first view).

Erbel, Mark. "The underlying causes of military outsourcing in the USA and UK: bridging the persistent gap between ends, ways and means since the beginning of the Cold War." *Defence Studies* 17, no.2 (2017): 135-155.

Erbel, Mark, and Christopher Kinsey. "Think again—supplying war: reappraising military logistics and its centrality to strategy and war." *Journal of strategic studies* 41, no. 4 (2018): 519-544

Fino, Steven A. *Tiger Check: Automating the US Air Force Fighter Pilot in Air-to-Air Combat, 1950–1980*. Washington: John Hopkins University Press, 2017

Frey, Carl Benedikt. *The technology trap: Capital, labor, and power in the age of automation*. Princeton: Princeton University Press, 2020.

Gartzke, Erik. "Blood and robots: How remotely piloted vehicles and related technologies affect the politics of violence." *Journal of Strategic Studies* (2019): 1-31 (online first view)

Geist, Edward Moore. "It's already too late to stop the AI arms race—We must manage it instead." *Bulletin of the Atomic Scientists* 72. no. 5 (2016): 318-321.

Gholz, Eugene, "Systems integration in the US defence industry: who does it and why is it important?." In *The Business of Systems Integration*, ed. Andrea Prencipe, Andrew Davies, and Michael Hobday, (Oxford: Oxford University Press, 2003), 279-306.

Gibney, Elizabeth. "Google AI algorithm masters ancient game of Go." *Nature News* 529.7587 (2016): 445

Gould, Joe, Arms trade momentum: Globalization and US defense spending drive defense industry growth. *Defense News*. August, 17, <https://www.defensenews.com/top-100/2020/08/17/arms-trade-momentum-globalization-and-us-defense-spending-drive-defense-industry-growth/>

Haas, Michael Carl, and Sophie-Charlotte Fischer. "The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order." *Contemporary Security Policy* 38, no. 2 (2017): 281-306.

Harrison, Todd (2021), "Rethinking the Role of Remotely Crewed Systems in the Future Force", *Center for Strategic & International Studies Policy Briefs*. March 2021.

Horowitz, Michael C. *The diffusion of military power: Causes and consequences for international politics*. Princeton University Press, 2010.

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

Horowitz, Michael C. "When speed kills: Lethal autonomous weapon systems, deterrence and stability." *Journal of Strategic Studies* 42, no. 6 (2019): 764-788.

Jasper, Scott. *Russian Cyber Operations: Coding the Boundaries of Conflict*. Georgetown University Press, 2020.

Jervis, Robert. *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*. Ithaca: Cornell University Press, 1989.

Kinsey, Christopher, and Malcolm Hugh Patterson, eds. *Contractors and war: The transformation of United States' expeditionary operations*. Stanford: Stanford University Press, 2012

Konaev, Margarita, U.S. Military Investments in Autonomy and AI. *CSET Policy Brief*, October 2020. <https://cset.georgetown.edu/research/u-s-military-investments-in-autonomy-and-ai-executive-summary/>

Krahmann, Elke. *States, citizens and the privatisation of security*. Cambridge: Cambridge University Press, 2010.

Krieg, Andreas. "Defining Remote Warfare: The Rise of the Private Military and Security Industry." *Oxford Research Group Briefing: Remote Warfare Programme*, Number 3, 2018

Krieg, Andreas, "The UAE's 'dogs of war': boosting a small state's regional power protection. *Small Wars & Insurgencies*, forthcoming.

Krieg, Andreas, and Jean-Marc Rickli. *Surrogate warfare: The transformation of war in the twenty-first century*. Washington: Georgetown University Press, 2019.

Krishnan, Armin. *War as business: Technological change and military service contracting*. London: Ashgate Publishing, Ltd., 2013.

LaPorte, Michael A. "Balancing Act: The US Military's Reliance on Contractors to Fulfill Operational-Level Logistical Requirements". *Naval War College Report*, May 2012.

Leander, Anna, *Commercialising Security in Europe: Political Consequences for Peace Operations*. Abingdon: Routledge, 2013.

Leys, Nathan. "Autonomous weapon systems and international crises." *Strategic Studies Quarterly* 12, no. 1 (2018): 48-73.

Lindsay, Jon R. *Information Technology and Military Power*. Ithaca: Cornell University Press, 2020.

Lobato, Luisa Cruz, Unraveling the cyber security market: the struggles among cyber security companies and the production of cyber (in)security. PhD Dissertation, Pontificia Universidade Católica do Rio de Janeiro, 2016.

Mahoney, Charles W. "United States defence contractors and the future of military operations." *Defense & Security Analysis* 36, no. 2 (2020): 180-200.

Marten, Kimberly. "Russia's use of semi-state security forces: the case of the Wagner Group." *Post-Soviet Affairs* 35, no. 3 (2019): 181-204.

Mason, Robert. "Breaking the mold of small state classification? The broadening influence of United Arab Emirates foreign policy through effective military and bandwagoning strategies." *Canadian Foreign Policy Journal* 24, no. 1 (2018): 95-112.

Maurer, Tim. *Cyber mercenaries*. Cambridge: Cambridge University Press, 2018.

McAfee, Andrew, and Erik Brynjolfsson. "Human work in the robotic future: Policy for the age of automation." *Foreign Affairs* 95, no. 4 (2016): 139-150.

Molas-Gallart, Jordi. "Which way to go? Defence technology and the diversity of 'dual-use' technology transfer." *Research policy* 26, no. 3 (1997): 367-385.

Moore, Adam. "US military logistics outsourcing and the everywhere of war." *Territory, Politics, Governance* 5, no. 1 (2017): 5-27.

Peltier, Heidi, *The Growth of the "Camo Economy" and the Commercialization of the Post-9/11 Wars*. Boston University. 2020
<https://watson.brown.edu/costsofwar/files/cow/imce/papers/2020/Peltier%202020%20-%20Growth%20of%20Camo%20Economy%20-%20June%2030%202020%20-%20FINAL.pdf>

Percy, Sarah. *Mercenaries: The history of a norm in international relations*. Oxford: Oxford University Press 2007.

Petersohn, Ulrich. "Private military and security companies (PMSCs), military effectiveness, and conflict severity in weak states, 1990–2007." *Journal of conflict resolution* 61, no. 5 (2017): 1046-1072.

Posen, Barry. *The sources of military doctrine: France, Britain, and Germany between the world wars*. Ithaca: Cornell University Press, 1986.

PWC, Defence trends 2020: Investing in a digital future. *23rd Annual Global CEO Survey | Trend report*, 2020, <https://www.pwc.com/gx/en/ceo-survey/2020/trends/defence-trends-2020.pdf>

Rossiter, Ash. "The impact of robotics and autonomous systems (RAS) across the conflict spectrum." *Small Wars & Insurgencies* 31, no. 4 (2020): 691-700.

Scharre, Paul, The opportunity and challenge of autonomous systems. In Williams, Andrew and Paul Scharre (Eds.), *Autonomous systems: Issues for defence policymakers* (pp. 3–26). Norfolk, VA: NATO Allied Command Transformation, https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf

Scharre, Paul, and Michael C. Horowitz. "Autonomy in Weapon Systems." *Center for a New American Security Working Paper* (2015). http://www.cnas.org/sites/default/files/publications-pdf/Ethical%20Autonomy%20Working%20Paper_021015_v021002.pdf

Schilde, Kaija. *The political economy of European security*. Cambridge: Cambridge University Press, 2017.

Schwab, Klaus, *The Fourth Industrial Revolution*. New York: Crown Publishing Group. 2017

Schwartz, Moshe, Department of defense contractors in Iraq and Afghanistan: Background and analysis. *Congressional Research Service*. CRS R40764, 2011, <https://fas.org/sgp/crs/natsec/R40764.pdf>

Sechser, Todd S., Neil Narang, and Caitlin Talmadge. "Emerging technologies and strategic stability in peacetime, crisis, and war." *Journal of strategic studies* 42, no. 6 (2019): 727-735.

Singer, Peter, *Corporate warriors: The rise of the privatized military industry*. Ithaca: Cornell University Press, 2008.

Stinchfield, Bryan T. "Small groups of investors and their private armies: the ascendance of private equity firms and their control over private military companies as further evidence of epochal change theory." *Small Wars & Insurgencies* 31, no. 1 (2020): 106-130.

Swed, Ori, and Thomas Crosbie. "Private security and military contractors: A troubling oversight." *Sociology Compass* 11, no. 11 (2017): e12512.

Tarraf, Danielle C., et al. *The Department of Defense posture for artificial intelligence: Assessment and recommendations*. Santa Monica: Rand Corporation, 2019.

Taubman, Phillip, Efforts to Slow Defense Industry's Brain Drain. *New York Times*, June 25, 2008. <https://www.nytimes.com/2008/06/25/us/25engineercnd.html>

Tilly, Charles, *The formation of national states in Western Europe*. Princeton: Princeton University Press, 1975

Verbruggen, Maaïke. "The role of civilian innovation in the development of lethal autonomous weapon systems." *Global Policy* 10, no. 3 (2019): 338-342

Zegart, Amy. "Cheap fights, credible threats: The future of armed drones and coercion." *Journal of Strategic Studies* 43, no. 1 (2020): 6-46.

Williams, Heather. "Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles." *Journal of Strategic Studies* 42, no. 6 (2019): 789-813