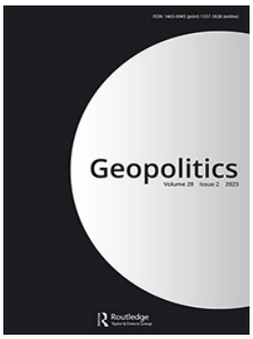

Geopolitics

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fgeo20

Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination

Raluca Csernatoni & Bruno Oliveira Martins

To cite this article: Raluca Csernatoni & Bruno Oliveira Martins (2023): Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination, Geopolitics, DOI: 10.1080/14650045.2023.2224235

To link to this article: https://doi.org/10.1080/14650045.2023.2224235

Published online: 19 Jun 2023.

GEOPOLITICS
https://doi.org/10.1080/14650045.2023.2224235

Routledge
Taylor & Francis Group

Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination

Raluca Csernatoni [a] and Bruno Oliveira Martins [b]

[a]Carnegie Europe, Brussels, Belgium; [b]Peace Research Institute Oslo

ABSTRACT

Emerging technologies are increasingly portrayed as having disruptive effects in security and defence, both in civilian and military environments. Yet, while revolutionary military technologies have always been connected to the notion of permanent techno-scientific innovation, there remains ample room for a critical enquiry on what it means to be disruptive in security and defence technology, the effects of claiming disruption and the broader socio-political contexts within which disruptive technology emerges. In this regard, the article draws theoretical insights from critical security studies, science and technology studies, and innovation studies, to propose a new analytical framework to study disruptive security and defence technologies along three analytical axes: temporality, performativity, and imagination. The notion of disruption implies a pre-existing linear, temporal dimension that is meant to be disrupted, and the mere claim of disruption is a performative act that can – although not always – trigger, enable or enact pre-imagined socio-technical futures. As the notion of disruption becomes prevalent in both civilian and military environments, the article contributes to unpacking its constitutive elements and to give it a more central position in contemporary IR debates.

Introduction

In February and March 2022, during the first weeks of the war in Ukraine, part of the international solidarity towards the government in Kiev was mediated through cutting-edge military technologies. The US personnel conducted training with Ukrainian drone pilots so that they could operate the hundreds of Switchblade tactical drones included in the armament package provided by the US. Significantly, more advanced military technology was provided since that initial stage. Germany made available missiles and other equipment to the

CONTACT Bruno Oliveira Martins brumar@prio.org PRIO, PO Box 9229 Grønland, NO-0134 Oslo, Norway

This paper is part of the special issue.
'Imaginaries of security-innovation'.
Edited by Dagmar Rychnovská (University of Sussex), Christian Haddad (Austrian Institute for International Affairs), Nina Klimburg-Witjes (University of Vienna).

Ukrainian army and announced a special EUR 100 billion fund to modernise its own armed forces and invest in new technology. The European Union (EU) channelled EUR 1 billion worth of military aid to Ukraine through its European Peace Facility instrument and declared the intention of advancing the development of disruptive military technologies. In the EU's first ever defence strategy, 'A Strategic Compass for Security and Defence', published in March 2022, emerging and disruptive technologies (EDTs), 'such as Artificial Intelligence, quantum computing, advanced propulsion, bio- and nano-technologies and new materials', are framed as re-shaping military affairs and identified as essential for 'the future battlefield' (EEAS 2022, 47–48). In January 2022, the US Department of Defense (DoD) established the Chief Digital and Artificial Intelligence Office (CDAO) to scale up Pentagon's innovative power via the closer integration of advances in AI systems, data analytics and other digital technologies across the DoD. With the CDAO, the end goal is also to mainstream the trailblazing industry experience of big corporate tech players into the DoD's activities, in order to generate value-added 'from the boardroom to the battlefield' (Department of Defense DoD 2022).

Underlying these efforts is the notion that modern, revolutionary technologies can not only provide a decisive advantage in the battlefield but also require innovative organisational changes to fully harness their disruptive potential.

Throughout history, different state and non-state actors have dedicated vast resources to acquire *that* cutting-edge weapon that would disrupt the *status quo* and provide them with decisive leverage in warfare. The US DoD's efforts on AI and data analytics are a contemporary case in point, being indicative of a commitment to foster AI and data leadership by putting forward disruptive organisational changes. However, the notion of disruption is growing central in different areas of social life beyond the military. It is the motto of Silicon Valley and the start-up venture capital business model that looks for permanent innovation and technological revolution, impacting many aspects of daily life, from the way we travel to the way we conduct our work. In the field of international relations (IR), Nicole Sunday Grove, Charmaine Chua and Louise Amoore have recently addressed what happens when disruption occurs by design and becomes the norm, rather than the exception (Amoore 2023; Chua 2023; Grove 2023), with Grove arguing that disruption draws on a 'libidinal economy that does not bend towards justice or equity' (Grove 2023, 3).

This proclaimed non-linear way of thinking that is foregrounded by disruption aims at permanently breaking up lines of continuity. Yet, does 'disruption' have the same meaning in different areas of knowledge? Can the broader societal and technological implications of both civil and military realms be equated? In a time where dual-use technologies are increasingly

important both in civilian and military settings, and where technology transfers between these sectors occur in increasingly complex ways, do the strict divisions between both areas still matter? Finally, what counts as disruption in security and military terms, and what does disruption mean in defence research and innovation policies?

The main objective of this article is to bring the concept of disruption to a more central analytical position in the fields of IR and security studies. This will be pursued through a two-stage strategy. First, we critically unpack the different meanings of 'disruption' in various academic fields that relate to discussions on security and defence technologies, namely critical security studies (CSS), science and technology studies (STS), and innovation studies (IS). Second, and as a consequence of this exercise, we highlight the core elements of 'disruption', so that a critical engagement in the field of security can ensue. As will be argued below, the ideas of temporality, performativity and imagination emerge as such core elements. Throughout the text, we will use empirical illustrations from the EU, US and recent North Atlantic Treaty Organization (NATO) efforts that promote and mainstream emerging and disruptive technologies for security and defence purposes.

We use these empirical illustrations because they can provide examples of how disruptive technological innovation is legitimised and performatively linked to regional or institutional identity-building and transformation. Long-held, institutionally entrenched socio-technological imaginaries (Jasanoff and Kim, 2015a) have had an important security and defence component, and this has implications for the politics of research and development (R&D) funding and (non)knowledge creation, circulation and legitimation surrounding disruptive innovation. Today, disruptive technologies in security and defence are often seen as core elements of national and institutional and economic growth, of strategic autonomy in security and defence, of technological and digital sovereignty as well as of international, geopolitical or regional survival (Csernatoni 2022).

The article has the underlying motivation of contributing to a widening of the field of IR through a growing dialogue between STS and critical approaches to security and military studies. It does so by zooming in on a concept of growing conceptual and policy importance in the fields of security and defence. We speak to the goals of this special issue by analysing *disruption*, a core concept in the contemporary security-innovation nexus.

Disruption: The International Politics of a Concept

For a long time, technological innovation for security and defence purposes has occupied a central position in national strategies of different countries. The current emphasis on techno-solutionism and technological superiority in military affairs is indeed not a new development. Neither is the belief that

cutting-edge technological innovations, in their own right, can solve complex security and defence problems, become force multipliers or provide either a strategic, operational or tactical edge during times of conflict. Traditionally, this instrumentalist approach has been grounded in the technology's potential to generate both security and defence advantages and in fostering innovation that would spin off and benefit society at large in different ways.

'Revolution' and 'innovation' have equally been important mobilising concepts in writings on security and defence. Technology, both as a strategic enabler and as a source of innovation in military affairs, has a long history, with accounts of technologically induced strategic ruptures dating as far back as Thucydides. The emergence of technologies so disruptive that they can revolutionise strategic, operational and tactical concepts in security and defence has thus long captured the imagination of strategic study researchers, culminating with the crystallisation of concepts such as the Revolution in Military Affairs (RMA). The following paragraphs aim to provide a non-exhaustive overview of RMA while underlying the importance of correlative notions, such as 'Revolution' and 'innovation' that contribute to a technopolitical imaginary around new technologies.

Indeed, based on technological developments that occurred from the 1970s, the concept of RMA captures the impact of new technology on military doctrines and organisation. Hundley (1999, 9) describes an RMA as 'a paradigm shift in the nature and conduct of military operations which either renders obsolete or irrelevant one or more core competencies of a dominant player, and/or creates one or more new core competencies, in some new dimension of warfare'. Conversely, according to Andrew Krepinevich, an RMA occurs when the application of 'new technologies into a significant number of systems combines with innovative operational concepts and organisational adaptation in a way that fundamentally alters the character and conduct of conflict' (Krepinevich 1994, 30). In this definition, emphasis is given to new technologies as triggers of organisational and operational change, which will presumably determine vital ontological transformations in the very nature of conflicts. Krepinevich argued that such technologies produce a 'dramatic increase' in the combat capacity and military effectiveness of the armed forces.

The 1990s and early 2000s saw a renewed interest in the notion of a coming RMA brought about by new technologies, namely information and communication technologies and their association with military doctrines, such as network-centric warfare (Cebrowski and Garstka 1998). Nowadays, another RMA is arguably under way, powered by advances and fusions in technologies, such as AI, autonomous systems, quantum computing and advanced additive manufacturing, to name a few. However, as military historian Max Boot wrote in a history of military innovation since the 1500s, technology is just one side of the story that sets the 'parameters of the possible and creates the potential

for military revolution' (Boot 2006, 10). In other words, other factors play an equally important role in inducing seismic shifts in warfare, such as the ability of the militaries to recognise and capitalise on the opportunities inherent in new weapons systems, as well as the capacity to re-organise structures and the ability to deploy forces.

Irrespective of the preferred explanatory variables of choice mobilised to construct models of (revolutionary) military-technological innovation, broader scientific frameworks and socio-technical imaginaries, as well as concrete technologies, are often portrayed as contextual, black-boxed and their materiality taken as a given. Or, from an instrumentalist perspective, technologies are underpinned as mere tools of power projection. This is mostly due to the applied bent of most of the RMA scholarship and the realist and neorealist approaches still dominating the field of military innovation studies (Griffin 2016). In contrast, the work of Antoine Bousquet (2022) on RMA has eschewed traditional accounts of technological change in war, by instead focusing on scientific conceptual frameworks applied to the theoretical understanding of war. This has made possible the exploration of modern and networked warfare as the constitution of increasingly complex social assemblages of bodies and machines (Bousquet 2022, 4). According to Bousquet, while technology plays an important role in such social assemblages of war, it is the impact of broader scientific conceptual frameworks and their corpus of ideas that shape contemporary theories and practices of warfare in the Western world. How then to situate EDTs such as AI systems, swarming drones and data analytics within current scientific theories applied to 'warfare in its totality'? Bousquet argues that the scientific rationalities, techniques and interpretation frameworks of 'chaos' and 'complexity' that have emerged in recent decades are best suited to capture the current 'scientific way of warfare', in what the author calls *chaoplexic warfare* (Bousquet 2022).

This interpretation also points towards the fact that scientific and socio-technical contexts foreground broader processes of technological innovations (or disruptions) in security and defence. They are indeed linking past, present and future scientific ideas and R&D programmes and initiatives, which require further scholarly attention. In this respect, Brett Edwards argues that contemporary science 'creates a significant demand for resources', this being 'reflected in the politics which has surrounded the major national and international "big" scientific projects' that 'have emphasised different visions about if and how scientific innovation should be integrated with industry and military institutions' (Edwards 2019, 17–18). Edwards showcases the important role that advocates of military and weapons technology have in legitimising the value of developing and adopting new technologies based on not only national and international security arguments but also humanitarian ones, by for instance expanding US efforts in the area of lethal autonomous weapons systems. Such

advocates, and in line with Hilgartner and colleagues, are 'sociotechnical vanguards' who play a significant role in the creation of socio-technical imaginaries around new technologies, including in the case of military institutions (Hilgartner, Miller, and Hagendijk 2015). Accordingly, 'vanguards', a group of stakeholders leading the way in new ideas and developments, play an active role in proactively promoting their ideas of innovation to make them more durable and to embed them into organisational cultures, institutions and materialities, and whereby the 'merely imagined is converted into the solidity of identities and the durability of routines and things' (Jasanoff and Kim 2015b, 323). Furthermore, this empowers various stakeholders, from tech experts, policymakers, to the military, to perform various 'discretionary decisions that ultimately constitute the sovereign decision' (Bourne, Johnson, and Lisle 2015, 308) framing what comprises the 'right' technology for warfare. In relation to the current age of chaos and complexity, materialised in the emergence and fusion of EDTs across civil and military affairs, is it engendering what Dillon and Reid (2001) have long identified as a 'new strategic imaginary'?

To illustrate, recently, NATO has embraced a new strategic imaginary on emerging and disruptive technologies, which, according to the Alliance, are increasingly permeating all aspects of life, while also having a 'profound impact on security' and providing 'new opportunities for NATO militaries, helping them become more effective, resilient, cost-efficient and sustainable' (NATO 2022). In this respect and to maintain its technological edge, NATO has put forward several flagship initiatives focused on EDTs: from the 'Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies'; the launch of the Defence Innovation Accelerator for the North Atlantic (DIANA) to create a transatlantic innovation platform; to the establishment of the first multi-sovereign venture capital fund, the NATO Innovation Fund, to provide strategic investments in start-ups developing dual-use deep-tech.

Another illustrative example is of how the EU is mobilising political and financial capital to promote disruptive security and defence technologies under the European Defence Fund (EDF), the ground-breaking investment programme in the areas of security and defence that addresses both the EU's capabilities-expectations and technological-innovation gaps in Europe (Csernatoni 2021b; Martins and Mawdsley 2021). Out of the Fund's EUR 8 billion for the period 2021–2027, between 4% and 8% is dedicated to targeted breakthrough innovation, disruptive technologies and innovative equipment. The funding from the EDF for disruptive military technologies is aimed at fostering high-risk and high-reward technological innovation in the European defence sector, with, according to the EU, an expected potential spin-off effect in the civilian domain. Like in NATO's case, when it comes to EDTs, the end goal is to 'showcase innovative ideas and to facilitate the crossfertilisation of

innovation between the civil and defence domains' (European Commission 2021, 13).

The above illustrations reflect a propensity to legitimise the design of overarching strategies aimed at harnessing the potential of EDTs for security and defence, with special consideration being given to 'fostering a coherent approach to the development and adoption of dual-use technologies (i.e., technologies that are focused on commercial markets and uses, but may also have defence and security applications)' (NATO 2022). Indeed, these dynamics are exemplifying not only the impact of the present governance of dual-use innovation programmes (Martins and Ahmad 2020) but also the necessity to project ideas into how the future will be organised in a logic of co-production, namely simultaneous processes and practices via which societies create their epistemic and normative knowledge of the world (Hilgartner, Miller, and Hagendijk 2015; Jasanoff 2004; Jasanoff and Kim 2015b).

In this respect, the modalities of knowledge production about technological presents and futures are at the same time creating socio-political orders, which in turn have performative effects in shaping scientific and technological innovation trajectories, including in military affairs. For example, by exploring the US' history of global military supremacy since the second world war, Paul Edwards engages with a specific technopolitical imaginary while advancing the metaphor of the 'closed world' or 'dome of global technological oversight' (Edwards 1997) to portray an ideological stance that has now culminated in 'a computationally based military machine devoted to command and control' (Suchman 2022).

Namely, this imaginary is reflected in an 'imaginary of omniscience' made possible by new technologies automating intelligence (Suchman 2022), in both 'the engineering and the politics of closed-world discourse centred around problems of human-machine integration: building weapons, systems and strategies whose human and machine components could function as a seamless web, even on the global scales' (Edwards 1997, 1–2). It is also possible to argue that developments in the field of AI science are currently also fuelling an 'arms race' in dual-use AI systems, autonomy and human-machine teaming, with an impact on current and future warfare. Such developments have prompted defence experts across the globe to envision AI-powered security and defence technologies as revolutionary or disruptive. Indeed, this emerging technology creates military-strategic dilemmas and projections at the heart of institutional and national defence ecosystems that already impact the threat landscape and an increasingly automated, complex and highly dynamic physical and non-physical battlespace of the future.

Despite these and other different contributions to the literature over the years, conceptual uncertainty surrounding the nature of disruptive security technologies abounds. How can we account for the concept of disruption in the field of security and defence technology? What are the discourses, interests

and normative expectations attached to *disruption* in these fields? In the same vein, what is the role of institutional, regional and national technological innovation imaginaries in the areas of security and defence? And what can we learn from how different fields of knowledge have studied this phenomenon?

Studying Technology and Security: Materiality, Imagination and Speed

The discipline of STS has a long-standing tradition of unpacking the social and political dimensions of scientific and technological systems, thus shedding light on the governance practices and knowledge-production processes surrounding them. At the same time, however, STS has rarely engaged in a sustained and systematic manner with IR scholarship, particularly in the field of security *per se* (for exceptions, see Suchman 2020; Kathleen 2017 and the literature analysis in the introduction to this special issue). Indeed, STS offers a conceptually rich and fertile ground to understanding EDTs. STS provides a more substantive analysis of such technologies as forms of power, as socially constructed, mediated processes which involve a complex interplay between actors, infrastructures, interests, norms, discourses, technologies and practices (Bijker, Hughes, and Pinch 1987; Feenberg 2017; Jasanoff and Kim 2015b; Latour 2005; Verbeek 2011).

In recent years, as the study of technology and its entanglement with security has become increasingly prominent within the IR discipline, IR scholars have mobilised a variety of theoretical approaches and methodologies from STS (Aradau and Blanke 2015; Calcara, Csernatoni, and Lavallée 2020; Leander 2013; Salter and Walters 2016). Approaches and concepts from STS have enriched some CSS studies, yielding actor-network theory (Balzacq and Cavelty 2017), co-production (Bellanova and de Goede 2021; Jacobsen and Monses 2019; Martins and Jumbert 2022), materiality (Aradau 2010; Walters 2014), technological agency (Hoijtink and Leese 2019), socio-technical imaginaries (Klimburg-Witjes 2023; Martins and Mawdsley 2021) and performativity Amicelle, Aradau, and Jeandesboz 2015; Csernatoni 2022, 2021a, 2020; see also Hoijtink and Leese 2019; McCarthy 2017).

Within the STS literature, the focus on socio-technical imaginaries (Jasanoff and Kim 2015b) is particularly relevant in the context of disruption, given the hyped utopian promises or dystopian futures that surround many new and emerging technologies in war and security. Socio-technical imaginaries refer to 'collectively held and performed visions of desirable futures [. . .] animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology' (Jasanoff and Kim 2015b, 25). The conceptual potential of socio-technical imaginaries for the field of defence has recently been explored by Martins and Mawdsley (2021) in an analysis of recent EU initiatives in the field of defence R&D,

namely the EDF. In this respect, a focus on discourses and imaginaries that shape, and are shaped by, disruptive security and defence technologies directs attention to the international, institutional and national politics of socio-technical knowledge production. Such entrenched knowledge production is aimed at underpinning and legitimising technological development trajectories or the funding of technoscientific projects, both within specific collectives of experts and among wider publics.

Technology has been profoundly reconfiguring the material fabric of social life (Zammuto et al. 2007), and EDTs are now broadly recognised as not only purely mediators or 'tools' but also highly performative and deeply entangled in socio-material infrastructures, platforms and fabrics of human activity from various fields (Orlikowski and Scott 2008; Suchman 2007), including security and defence. For new materialism theorists, technologies are no longer a passive substrate 'out there' instrumentalised by humans, but an active and dynamic agent that is generative, resisting, lively and vital (Barad 2007; Bennett 2010; Braidotti 2002; Coole and Frost 2010; DeLanda 2016). By following Merleau-Ponty's existential phenomenology, this character of technology is also what Caroline Holmqvist has suggested with regard to material objects in war, like drone technologies, as having 'agentic capacities', which in turn 'must have a bearing on our reading of the ontology of war' (Holmqvist 2013, 538).

However, as far as disruption is concerned, there seems to be a gap in describing how it (re)configures the socio-material fabric and the 'blurring of corporeal and incorporeal in contemporary' wars (Holmqvist 2013, 538–539), as brought about by disruptive technologies like AI systems in specific socio-technical contexts, especially in the Western/European-centric or Northern transatlantic ones. Key to explaining the changes triggered by such technologies could rest in understanding the materiality of a broad range of technology-related phenomena within wider socio-technical imaginaries, as well as institutional and regional settings. Additionally, another level of complexity comes from the fact that many emerging and disruptive technologies deployed in the battlefield are digital or heavily reliant on digital components, such as AI systems, complex algorithms or machine learning models, which are central to their agentic capacities. This further begs the question of untangling not only the materiality of contemporary warfare but also the relationship between the material, digital or virtual.

Consequently, different perspectives on imaginaries and materiality may help develop explanations for the complex changes happening due to technologically or digitally induced disruption and innovation in the fields of security and defence. For instance, in the US, it could be argued that the big tech companies are increasingly involved in imaginary-building practices around cultures of 'disruption', by more and more powering the DoD's war machine, or what Suchman (2022, 14) has termed 'the long pitch of the Silicon Valley-

military industrial complex and its embrace' by tech promoters. Such an emerging imaginary is in line with 'utopian futures of profit and a conjured spectre of disaster' (2022, 14), especially regarding the need to mitigate perceived gaps in new AI and data-driven technologies to keep the US' technological leadership in the context of a rising geopolitical and high-tech rivalry with China. The close rapprochement between the Pentagon and key executives from Google, Facebook and Microsoft, most notably former Google CEO, Eric Schmidt, points towards a new impetus to mainstream new AI and data-powered technologies into the work of the DoD, coupled by a transfer of Silicon-Valley 'best practices' (Suchman 2022) regarding both the research and development of EDTs and market-tested entrepreneurship models into the DoD's processes and practices. However, this transfer is not unilateral, due to the fact that amid rising tensions and growing geopolitical competition with China in EDTs, the private sector is also increasingly starting to share a common threat perception to that of national security and strategic concerns, as exemplified by the ongoing war in Ukraine and the growing role played by tech companies in the conflict. As with the above-mentioned NATO's venture capital Innovation Fund, private venture capital processes are indeed progressively fuelling the technopolitical imaginary of an emerging commercial-military complex, prioritising the research, development and innovation of critical dual-use technologies for national security.

Another prominent approach in studying technology and agency in IR is Actor-Network Theory (ANT), which presupposes that all elements of the network are relevant for actions, allowing for more systematised understanding of non-human action (Latour 2005). William Walters, for example, has noted that materials-oriented approaches to security typically 'focus on the place of materials and objects within technologies and assemblages of governance' and rarely 'ask how materials and objects become entangled in political controversies, and how objects mediate issues of public concern' Walters (2014, 101). While ANT approaches substantially engage with the nature of the socio-technical, by bringing together the social and the material in a symmetrical way, as well as human relations with non-humans and inanimate objects, one criticism levied against them is that the networked approach makes all actions and agents (both human and non-human) seem equally empowered or disempowered, responsible or irresponsible (Jasanoff and Kim 2015b, 15–17). Hence, by eliminating subject-object boundaries and by dissolving binaries between the primacy of the social over the material, ANT perspectives also introduce a flatness within networks that may have depoliticising effects. According to Jasanoff, '[d]isrupting this flatness, revealing the topographies of power, is one aim of work on socio-technical imaginaries' (Jasanoff and Kim 2015b, 18).

A final element to highlight is how different critical researchers have engaged with the issue of time and speed when it comes to technology and

security – we believe that both time and speed are key elements to understand the logic of disruption. Here, the foundational work of Paul Virilio on speed and politics (Virilio 1977/2006), in relation to information technology and technologies of vision especially in the times of war, has been inspirational for a number of researchers that deal with issues of military and societal transformation. Already in 1998/9, James Der Derian (1999) highlighted how we could be witnessing the first of the 'integral accidents' predicted by Virilio, 'where global interconnectedness destroys the firewalls of civil society, information flows outstrip the powers of deliberation, truth is further relativised by velocity and crises spread like a contagion. The Military-Industrial-Media-Entertainment Network (MIME-NET) becomes an infrastructure of Pure Power' (Der Derian 1999, 218). For Virilio, technology accelerates time and space, and speed is crucial for the creation of wealth and power. As pointed out in Douglas Kellner's critical essay about Virilio's work on war and technology, it is grouped like the military, the state and corporations that control (information) speed and become dominant societal powers (Kellner 1999). According to Virilio's *The Information Bomb* (2000), the speed of information technology makes possible chronopolitics, i.e. a politics of time.

Virilio's vast and overwhelming intellectual production has been brought more closely to critical security studies through the work of Mark Lacy (2014). In its 2014 book *Security, Technology and Global Politics: Thinking with Virilio*, Lacy engages with some of Virilio's thinking on security matters, namely endo-colonisation, fear and the war on terror; cities and panic; cinema and war; ecological security and integral accidents and universities and ideas of progress. The idea of progress as connected to time and speed has also been explored by Paul Crogan (1999) in an essay about the way Virilio deals with the future.

The work by Virilio illuminates the understanding of the contemporary centrality of disruption to modern societies because his modernity is logistical, in the sense that 'it doesn't directly deal with war, but with everything that makes it possible' (Bratton 2006, 7). And indeed today, the possibility of war through the employment of disruptive technology requires the participation of many who are external to the war professions: computer engineers developing algorithms, university researchers working on innovative materials, collectors of semiconductor raw materials, extracting them from nature. In the processes involving these actors, speed is crucial. The processes by which speed is employed in permanent races to the top (arms races or not) are also defined by specific imaginaries of the future, and in this sense, temporality and imagination become entwined dimensions of a contemporary logic of disruption.

Furthermore, security and temporality already arise in interdisciplinary ways in security studies, most notably with the work of Tim Stevens (2015) exploring cyber security and the 'politics of time'. Accordingly, security 'is an

inherently temporal position', and in 'the modern political philosophical tradition, security is an essential bulwark against the exigencies of an unknowable future' (Stevens 2015, 1). With regard to new technologies, Stevens notes that cyber security practice and policymaking are 'forever "playing catch-up" to technological changes the uses to which information technologies are put' (Stevens 2015, 87), this security gap being manifested in a temporal lag. This is further revealed in a 'genealogy of anxiety accompanying the development of interconnected and interdependent infrastructures in modern industrial societies, worries consonant with general apprehension about the impact of new technologies on society' (Stevens 2015, 101). This chronopolitical lens can shed further light on how EDTs introduce an 'emergent sociotemporality' of nonhuman technological entities. This, in turn, further shapes the collective sociotemporality of human groups, which in turn structure political behaviours that even 'if oriented to the future', they are enacted in the present (Stevens 2015, 45).

Such a perspective provides a framework to understanding how collective anxieties and perceptions of time and speed are constructed under the impact of the nonhuman temporalities of new and disruptive technologies. This is not to say that such a perspective introduces a linear and causality-driven technological deterministic understanding of socio-technical temporal processes, under which the role of EDTs should be essentialised. Rather, by following critical technology theorist Andrew Feenberg (1995), in his collection of essays *Alternative Modernity: The Technical Turn in Philosophy and Social Theory*, it could be contended that the design and organisation of technical systems do not follow a teleological dynamic, thus rejecting the prevailing conception that technology is neutral and an unstoppable force of history shaping society and humanity's future. Conversely, he argues for a social and cultural construction of technology, by which technological design is socially relative, hence technologies may be disruptive in different ways, depending on particular social, cultural and political contexts and factors.

Accounting for Disruption in Innovation Studies

Innovation studies started to emerge as a distinct field of research in the 1960s, and much of the IS scholarly work has leaned towards cross-disciplinarity, combining different insights from several disciplines, such as economics, sociology, cognitive science, organisational science, policy studies of science, business studies and management studies (Fagerberg 2009). This reflects the fact that no single discipline can capture all aspects of innovation, the way it is organised and its technological dimensions, depending on the specific nature of the technology in question. The by now famous definition of innovation provided by Schumpeter (1934) in his *Theory of Economic Development* still constitutes an essential reference for contemporary innovation studies. The

author broadly defined innovation as a critical dimension of economic change that revolves around 'new combinations' of new or improved products, processes, markets and organisational change (Martin 2016).

Another approach, based on Schumpeter's scholarship, has been to categorise innovations depending on how radical they are as compared to existing technologies (Freeman and Soete 1997), namely by making a distinction between continuous improvements in so-called 'incremental' or 'marginal' innovations in contrast to 'radical innovations' or 'technological revolutions'. The latter two categories were considered by Schumpeter as more important, as they cover a cluster of innovations that taken together have a cumulative and far-reaching impact. However, the distinction is rather analytical because 'radical' innovations might also require a series of incremental improvements. Related to the notion of radical innovation are the correlative concepts of disruptive innovation and disruptive technology.

The term disruptive innovation was first coined and analysed by Clayton M. Christensen (1997) in his book *The Innovator's Dilemma*, who linked it to a specific mechanism and evolution path of innovation and defined it as generating new markets and value networks that will eventually disrupt existing ones, thus displacing established market-leading companies, products and networks. The original term of disruptive innovation has gained widespread currency in various domains including security and defence, oftentimes appropriated as a buzzword by practitioners or policymakers. Nevertheless, according to its original proponent and several leading researchers, the theory's core concepts remain widely misunderstood (Christensen et al. 2018). Related to this is the phenomenon of performatively overusing and abusing disruptive innovation as a synonym for any new transformation or threat and describing any new technology that aims to revolutionise existing competitive patterns (Christensen, Raynor, and McDonald 2015). Disruptive innovation and disruptive technology also need to be further differentiated, the latter having the potential to create disruptive innovation at various levels, such as to an industry segment, an industry structure or more broadly a social system (Millar, Lockett, and Ladd 2018). Concerning disruptive technologies, Bower and Christensen (1995) are credited for introducing the term in their publication *Disruptive Technologies: Catching the Wave*, in which they classify two categories of technology in a business environment, namely as either sustaining or disruptive. Sustaining technology has the typical characteristics of incremental innovation, while disruptive technology is described as one introducing radical and very different characteristics or features that were not present previously.

For example, the European Commission's Action Plan from February 2021, the 'Three-Point Belt Plan' on synergies between civil, defence and space industries (European Commission 2021), proposes a civil-defence synergies framing and a more horizontal and cross-domain approach for boosting dual-

use research, technology development and the EU's overall innovation power. It aims to establish a structured approach and create new opportunities for innovation synergies among relevant EU-funded programmes and instruments, especially in the case of emerging and disruptive technologies (European Commission 2021, 2). This document also flags a number of critical technologies, such as AI, advanced analytics, big data, high-performance computing, quantum technologies, advanced and additive manufacturing, nanotechnologies, robotics, semiconductors, to name a few (9–10). The 17 pages-long Action Plan mentions the word 'disruptive' no less than eight times, while 'emerging' appears five times, noting that the 'pervasiveness of emerging and disruptive technologies across civil, defence and space industries creates new opportunities for synergies among EU programmes and instruments' (2). Disruptive technologies are defined as technologies 'inducing a disruption or a paradigm shift, i.e. a radical rather than an incremental change. Development of such a technology is "high risk, high potential impact", and the concept applies equally to the civil, defence and space sectors' (13). The document further clarifies that disruptive technologies for defence 'can be based on concepts or ideas originating from non-traditional defence actors and find their origins in spin-ins from the civil domain' (13). This definition seems to be inspired by Bower and Christensen's (1995) work on disruptive technologies.

Nevertheless, it does not explain what exactly a radical change is nor how to grasp a 'paradigm shift', especially in the field of security and defence, and importantly, engendered by a dual-use and enabling technology like AI. Is the 'shift' to be observed in the present or in the future, in the technologies themselves, in their research and development, in security and defence organisational or institutional structures, in defence market and innovation processes? Is the shift desirable, and if yes, what would be the positive effects, and who gets to benefit from them? Such conceptual and critical insights could feed into broader reflections of how current institutional, industrial and market-driven forces contribute to shaping and disrupting traditional governance and innovation processes in security and defence. They can help illuminate how different funding mechanisms and various types of research and innovation models stemming from the civil or private sectors, especially in the case of emerging (digital) technologies, are increasingly permeating the military sector. In this regard, in the case of military technology development, private venture capital methods are emerging as a financial engine for the development of emerging and disruptive technologies.

Temporality, Performativity and Imagination

The challenge for IR and security researchers lies indeed in connecting the dots between global systems of innovation, their impact on national and

regional systems, the agents involved and the power dynamics behind them, as well as the important science and technology policy implications for security and defence in different contexts. For instance, the distinction between invention and innovation can highlight the added value of applying a systems perspective on innovation, rather than focusing exclusively on individual inventions or innovations (Fagerberg 2009): invention is the first occurrence of an idea for a new product or process, while innovation is the first attempt to deploy it in practice, in many cases with a considerable time lag between the two interlinked processes (Rogers 1995). Consequently, what could be considered as a single technological innovation is often the result of an extensive process involving many interrelated innovations, such an interpretation thus warranting the systems perspective approach.

Indeed, less attention has been given to understanding the phenomenon of disruption as a driver of change more broadly and the socio-material nature of disruptive technologies per se. For example, most of the RMA research focuses on *how* change occurs, but less so on the *why* question. In this regard, there is an added value in mapping the trajectory of disruptive security and defence technologies from development, deployment, to adoption and uses, as well as the broader contextual socio-economic, science and technology, political, discursive and normative factors that could contribute to certain technologies gaining the label of disruptive. The development of a more interdisciplinary and critical research agenda in the IR-based military innovation scholarship could be of great benefit and provide the impetus for new understandings of innovation and disruption in security and defence.

The above discussion revealed the many complex facets to understanding disruptive innovation and technologies, as well as their context-specific, socio-technical dimension within different fields or organisations. In our understanding, the notion of disruption implies a pre-existing linear, temporal dimension that is to be radically disrupted or revolutionised, and the mere claim of disruption is a performative act that can – but not always – trigger, enable or enact a pre-imagined and desirable socio-technical future. How does this happen in reality? What is the socio-technical dynamic surrounding the materialisation of this idea, as well as the power dynamics behind it? This performativity may have both material and immaterial consequences, specifically by shaping or enacting a pre-imagined socio-technical future, either contextualised within pre-existing institutional configurations or by triggering new processes.

In this context, we highlight three elements (see Table 1) that constitute the backbone of the idea of disruption in security and defence technologies: temporality, performativity and imagination. They represent the constitutive pillars of disruption in these domains and, importantly, they have significant policy and operational implications. We propose that understanding disruption through these three elements enables both scholars and decision-makers

to unpack the notion, to potentiate the strategic benefits of technology, to understand its broader societal implications and to better prepare for its adversarial use.

Temporality refers to the notions of speed and technological evolution across time. It is also intimately linked to a sense of acceleration, combining feelings of anxiety and urgency related to the fast-paced evolution of new technologies and their impact on security and defence. At a policy and operational level, it is important to understand the continuum that is disrupted through a new technology because this enables decision makers to anticipate possible responses to its use and to envisage strategies to augment its impact. Having a sense of this time element is also necessary to govern the new technology and to devise strategies to regulate it, both domestically and internationally. The logic of anticipatory governance of new technology is particularly relevant for scientific and technological breakthroughs that are dual-use and that raise important ethical and philosophical concerns. As argued in this article, the notion of disruption foregrounds a pre-existing linear, temporal dimension that is to be radically disrupted or revolutionised, but also a sense of urgency and anticipation of the future. In other words, it consists of a specific temporal orientation that can unravel a new 'anthropology of the future' (Bryant and Knight 2019), premised on collective expectations and visions of anticipated ruptures and 'paradigmatic shifts'. This can be seen as a form of governing the future through institutions, processes and practices that rely on horizon scanning, foresight and technology forecasting to decrease potential risks or threats, but also to predict emerging technological trends (Campbell-Verduyn and Hütten 2022; Heo and Seo 2021; Rychnovská 2021). Moreover, understanding where technological development is heading, and what changes to that trajectory the disruptive technology targets, is important for operational adaptation not only from the armed forces but also from first responders and all those that have responsibilities in improving societal resilience.

Performativity refers to the power of language and symbols to produce change. In this case, it relates to the mere claim of disruption as a characteristic of a new technology, irrespective of whether it can actually produce that disruptive change in objective terms. The reason why this is important is because disruption has impacts at different levels, and the discursive dimension can itself be performative and productive of results. For example, if a particular state or non-state actor credibly announces to have acquired a new, disruptive technology that 'radically changes the rules of the game', this may produce effects at the level of the response from potential adversaries. Additionally, if, for example, a new technology emerges with a promise to produce disruptive effects, it may trigger change in society more broadly, even if these effects are different than the ones promised. A good example of this is blockchain technology, not only it has not produced

the revolutionary change it promised, but also the main product it enabled, cryptocurrencies, has had leverage to roam unregulated until its current collapse.

Imagination represents, in this context, the ideational element that triggers innovation, i.e. the conception of an ideal or desirable future and societal progress that is to be achieved and co-produced through technology and to be shared by wider collectives. As mentioned above, this notion is well captured by the concept of socio-technical imaginaries. In the context of security and military technologies, this socio-ideational element of technology is fundamental to define what objectives to pursue, how to reach them, what to prioritise, and what or who to leave behind. Acknowledging that every technology emerges out of a socio-political context, and that it will impact a socio-political reality, is fundamental to define the contours of its use and anticipate its impacts. This is even more relevant in the domain of security and military technologies because their disruptive impact can become a matter of life and death.

But who are the winners and losers of disruption in security and defence EDTs? Or, to put it differently, the notion of disruption begs the question: disruptive for whom? Several issues should be considered as regards EDTs, most importantly the compliance of research and innovation frameworks with democratic and legal requirements, social norms and ethical values. From a democratic governance point of view, there needs to be a greater representation of views and approaches, in order to determine how EDTs are designed, implemented, and meaningfully controlled, especially in sensitive areas, such as autonomous weapons, surveillance, swarming drones or any other AI-enabled security and defence practices. Most importantly, according to Andrew Feenberg (2005), the democratisation of technology is about finding new ways of privileging potentially excluded values, ideas and voices by reincorporating them in new technical arrangements, a process that he calls 'democratic rationalisation', due to the fact that it translates public demands into technically rational developments in design processes and structures. As Feenberg has argued, the technological design of the 'machine' is also an

Table 1. Elements of disruption and corresponding policy implication.

Elements of disruption	Policy implication
Temporality	• Understanding the continuum that is disrupted • Interpreting anxiety and speed • Understanding the logic of anticipatory governance of the future • Regulatory and operational adaptation
Performativity	• Understanding that disruption has impacts at different levels • Acknowledging that the discursive dimension can itself be performative • Identifying the performative roles of socio-technical advocates/vanguards of disruption
Imagination	• Focusing on ideational elements that trigger innovation • Conceptualising ideal or desirable futures (whatever the use of the technology) • Mainstreamed and collectively shared in society

inherently political process, in which power dynamics, biases and human interventions of specific stakeholders are cloaked by technological rationality and efficiency.

The choices to prioritise technical rather than moral and political solutions to crises and conflicts are highly significant from both moral and political points of view (Feenberg 2005, 49). To counteract such tendencies of subjugating 'ethics – an ultimately human activity – to techne' (Peoples 2009, 560) and limiting the access of certain groups in technological design processes by experts, corporate, military or political elites (Feenberg 2005, 52), will thus become a difficult task for the present future governance of EDTs.

Conclusion: Towards an Interdisciplinary Understanding of Disruption

This paper has highlighted the added value of theoretical insights provided by the CSS, STS and IS to expand our understanding of the meaning of disruption in the case of security and defence technologies. The paper has further identified *disruption* as a core concept in the security-innovation nexus, by providing a more nuanced account of its components, namely temporality, performativity and imagination. Furthermore, a conceptual exploration at the intersection of STS and CSS considers the social construction of disruptive technologies, their materiality, as well as a deeper understanding of the socio-technical imaginaries shaping their development and circulation. As far as the IS literature contribution to CSS is concerned, it offers systematic accounts of innovation and its market effects, by critically challenging the positive framing of innovation as an end in itself, by understanding broader innovation processes in various domains, and how they are related to and shaping social, institutional, political and security dimensions. Given that no single theoretical lens can capture the complex dynamics of disruption in security and defence, an interdisciplinary approach is warranted for a better understanding of disruptive technologies and related societal phenomena in specific contexts.

Indeed, the different meanings attached to 'disruption' are also relevant from a socio-political perspective. As argued by Chua, 'confusion over what disruption means, who exercises it, and upon whom is not a coincidence: rather, disruption's polysemy is structurally produced as a way to disguise ongoing capitalist crisis as a technical problem that market innovations can solve' (Chua 2023, 37). Imaginaries of disruption have become powerful instruments to cement both depictions of attainable futures of security and defence and prescriptions of the kinds of futures that ought to be attained by technological innovation. Yet, they are also deeply rooted in the past and in good and bad experiences, connecting the past and the future by providing a bridge within present institutional and technological structures at national, regional and international levels. Exploring these imaginaries of disruption involves paying

closer attention to how they either link or rupture the connection between the past and the future, enact certain temporal logics of emergency and necessity, enable, or for that matter curtail policy and political choices and actions around emerging security and defence technologies, as well as normalise or politicise ways of thinking about possible socio-technical worlds (Jasanoff and Kim 2015b). They draw attention to the violence and controversies involved in developing, testing and making disruptive technologies, as well as in performatively legitimising them or making them circulate by advocates or vanguards, via their deployment and uses in security and defence practices.

An interdisciplinary approach would, finally, then, contribute to a better understanding of the co-production of material and social dimensions, as well as the entanglement between innovation, security, war and global politics. This has implications for our understanding of not only security technologies but also security more broadly. Our proposal is in line with Jef Huysmans' argument that 'knowing security without centring life and matter onto security' requires approaches where (re)conceptualisations of politics and the social are given primacy over security (Huysmans in Salter et al. 2019, 15). One way of pursuing this critical research agenda is to multiply 'the actors and/or discourses beyond security-focused ones or by giving primacy to complex analytical categories through which conceptions of politics or the social are mobilised' (idem). The conceptual proposal advanced in this article is aimed at pursuing this line of inquiry.

Such an approach opens up a space for alternative imaginaries and knowledge production processes surrounding EDTs. In this respect, this article recognises that most imaginaries of disruption in technological innovation and security and defence, as well as the broader theoretical and policy reflections surrounding them, have typically been deeply rooted in North-American- and European-centric perspectives and paid less attention to the theoretical traditions, perceptions, interests, imaginaries and world views of non-Western/non-European- centric contexts. As authors of this paper, we recognise our positionality as scholars trained in, and affiliated with, European academic institutions, and we reflexively aim to avoid assuming or aspiring to universality in unpacking the notion of disruption. The examples used in this article are from North American and European realities, and further research is necessary to evaluate whether our proposed framework for understanding disruption in security and military technologies around temporality, performativity and imagination is equally relevant to understand other socio-technical processes unfolding in different socio-political realities.

Acknowledgements

Previous versions of this paper were presented at two EISA *European Workshops in International Studies*, in 2020 and 2021, as well as a workshop organised as part of this special issue. For comments that greatly improved the quality of this article, we would like to thank the participants on these events, as well as the special issue editors and the three anonymous referees.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

Research for this article was partially funded by the Norwegian Ministry of Defence for the project 'Disruptive Security Technologies: Challenges to Norway's Total Defence Concept', grant agreement 2019/2177-106/FD II 1/RAB. The project was led by the Peace Research Institute Oslo and had Carnegie Europe as a partner.

ORCID

Raluca Csernatoni http://orcid.org/0000-0002-1412-582X
Bruno Oliveira Martins http://orcid.org/0000-0002-0648-3627

References

Amicelle, A., C. Aradau, and J. Jeandesboz. 2015. Questioning security devices: Performativity, resistance, politics. *Security Dialogue* 46 (4):293–306. doi:10.1177/0967010615586964.

Amoore, L. 2023. Machine learning political orders. *Review of International Studies* 49 (1):20–36. doi:10.1017/S0260210522000031.

Aradau, C. 2010. Security that matters: Critical infrastructure and objects of protection. *Security Dialogue* 41 (5):491–514. doi:10.1177/0967010610382687.

Aradau, C., and T. Blanke. July-December 2015. The (big) data-security assemblage: Knowledge and critique. *Big Data & Society* 2(2):1–15. doi: 10.1177/2053951715609066.

Balzacq, T., and M. D. Cavelty. 2017. A theory of actor-network for cyber-security. *European Journal of International Security* 1 (2):176–98. doi:10.1017/eis.2016.8.

Barad, K. 2007. *Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning*. Durham: Duke University Press.

Bellanova, R., and M. de Goede. 2021. Co-producing security: Platform content moderation and European security integration. *JCMS – Journal of Common Market Studies* 60 (5):1316–34. doi:https://doi.org/10.1111/jcms.13306.

Bennett, J. 2010. *Vibrant matter: A political ecology of things*. Durham, NC: Duke University Press.

Bijker, W. E., T. P. Hughes, and T. J. Pinch, eds. 1987. *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.

Boot, M. 2006. *War made new: Technology, warfare and the course of history: 1500 to Today*. New York: Gotham Books.

Bourne, M., H. Johnson, and D. Lisle. 2015. Laboratizing the border: The production, translation and anticipation of security technologies. *Security Dialogue* 46 (4):307–25. doi:10.1177/0967010615578399.

Bousquet, A. 2022. *The scientific way of warfare: Order and chaos on the battlefields of modernity*. 2nd ed. Oxford: Oxford University Press.

Bower, J. L., and C. M. Christensen. 1995. *Disruptive technologies*: *Catching the wave*. *Harvard Business Review* 73(3):24–6. January-February .

Braidotti, R. 2002. *Metamorphoses: Towards a materialist theory of becoming*. Oxford: Blackwell.

Bratton, B. H. 2006. Logistics of habitable circulation: A brief introduction to the 2006 edition of speed and politics. In *Speed and politics*, ed. P. Virilio, 7–26. Los Angeles: Semiotexte.

Bryant, R., and D. M. Knight. 2019. *The anthropology of the future*. Cambridge: Cambridge University Press.

Calcara, A., R. Csernatoni, and C. Lavallée, eds. 2020. *Emerging security technologies and EU Governance: Actors, practices and processes*. Routledge.

Campbell-Verduyn, M., and M. Hütten. 2022. Governing techno-futures: OECD anticipation of automation and the multiplication of managerialism. *Global Society* 36 (2):240–60. doi:10.1080/13600826.2021.2021148.

Cebrowski, A. K., and J. J. Garstka. 1998. Network-centric warfare: Its origin and future. *US Naval Institute Proceedings* 124 (1):28–35.

Christensen, C. M. 1997. *The innovator's dilemma: When new technologies cause great firms to fail*. Boston, MA: Harvard Business Review Press.

Christensen, C. M., R. McDonald, E. J. Altman, and J. E. Palmer. 2018. Disruptive innovation: An intellectual history and direction for future research. *Journal of Management Studies* 55 (7):1043–78. doi:10.1111/joms.12349.

Christensen, C. M., M. E. Raynor, and R. McDonald. 2015. What is disruptive innovation? *Harvard Business Review* 93 (12):44–53.

Chua, C. 2023. Disruption from above, the middle and below: Three terrains of governance. *Review of International Studies* 49 (1):37–52. doi:10.1017/S0260210522000432.

Coole, D. H., and S. Frost, eds. 2010. *New Materialisms: Ontology, Agency, and Politics*. Duke University Press.

Crogan, P. 1999. The tendency the accident and the untimely: Paul virilio's engagement with the future. *Theory, Culture & Society* 16 (5–6):161–76. doi:10.1177/02632769922050926.

Csernatoni, R. 2020. New states of emergency: Normalizing techno-surveillance in the time of COVID-19. *Global Affairs* 6 (3):301–10. doi:10.1080/23340460.2020.1825108.

Csernatoni, R. 2021a. Between rhetoric and practice: Technological efficiency and defence cooperation in the European drone sector. *Critical Military Studies* 7 (2):212–36. doi:10.1080/23337486.2019.1585652.

Csernatoni, R. 2021b. The EU's defense ambitions: Understanding the emergence of a European defense technological and industrial complex. Working Paper, Carnegie Europe, Brussels.

Csernatoni, R. 2022. The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European Security* 31 (3):395–414. doi:10.1080/09662839.2022.2103370.

DeLanda, M. 2016. *Assemblage Theory*. Edinburgh: Edinburgh University Press.

Department of Defense (DoD). 2022. DoD announces Dr. Craig Martell as chief digital and artificial intelligence officer. Press Release, April 25. Accessed December 12, 2022. https://

www.defense.gov/News/Releases/Release/Article/3009684/dod-announces-dr-craig-martell-as-chief-digital-and-artificial-intelligence-.

Der Derian, J. 1999. The conceptual cosmology of Paul Virilio. *Theory, Culture & Society* 16 (5–6):215–27. doi:10.1177/02632769922050809.

Dillon, M., and J. Reid. 2001. Global liberal governance: Biopolitics, security and war. *Millennium: Journal of International Studies* 30 (1):41–66. doi:10.1177/03058298010300010501.

Edwards, B. 2019. *Insecurity and Emerging Biotechnology: Governing Misuse Potential*. Basingstoke: Palgrave. doi:10.1007/978-3-030-02188-7.

Edwards, P. 1997. *The closed world: computers and the politics of discourse in cold war America*. Cambridge, MA: The MIT Press. doi:10.7551/mitpress/1871.001.0001.

European Commission (2021) Action plan on Synergies between civil, defence, and space industries. Accessed January 19, 2022. https://ec.europa.eu/info/files/action-plan-synergies-between-civil-defence-and-space-industries_en.

European External Action Service (2022) 'A Strategic Compass for Security and Defence,' available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en

Fagerberg, J. 2009. Innovation: A guide to the literature. In *The oxford handbook of innovation*, ed. F. Jan and D. C. Mowery. Oxford University Press. doi:10.1093/oxfordhb/9780199286805.003.0001.

Feenberg, A. 1995. *Alternative modernity: The technical turn in philosophy and social theory*. Berkeley: University of California Press.

Feenberg, A. 2005. Critical theory of technology: An overview. *Tailoring Biotechnologies* I (I):47–64.

Feenberg, A. 2017. Critical theory of technology and STS. *Thesis Eleven* 138 (1):3–12. doi:10.1177/0725513616689388.

Freeman, C., and L. Soete. 1997. *The economics of industrial innovation*. Cambridge MA: MIT Press.

Griffin, S. 2016. Military innovation studies: Multidisciplinary or lacking discipline? *Journal of Strategic Studies*. doi:10.1080/01402390.2016.1196358.

Grove, N. 2023. Receding resilience: On the planetary moods of disruption. *Review of International Studies* 49 (1):3–19. doi:10.1017/S0260210522000456.

Heo, K., and Y. Seo. 2021. Anticipatory governance for newcomers: Lessons learned from the UK, the Netherlands, Finland, and Korea. *European Journal of Futures Research* 9 (1):1–14. doi:10.1186/s40309-021-00179-y.

Hilgartner, S., C. A. Miller, and R. Hagendijk. 2015. Introduction. In *science and democracy. Making knowledge and making power in the biosciences and beyond*, ed. S. Hilgartner, C. A. Miller, and R. Hagendijk, 1–14. New York and London: Routledge.

Hoijtink, M., and M. E. Leese. eds. 2019. *Technology and Agency in International Relations*. Oxon and New York: Routledge.

Holmqvist, C. 2013. Undoing War: War ontologies and the materiality of drone warfare. *Millennium: Journal of International Studies* 41 (3):535–52. doi:10.1177/0305829813483350.

Hundley, R. 1999. *Past revolutions, future transformation: what can history of revolutions in military affairs tell us about transforming the US Military?* Santa Monica: RAND.

Jacobsen, K. R., and L. Monses. 2019. Co-production: The study of productive processes at the level of materiality and discourse. In *Technology and Agency in International Relations*, ed. M. Hoijtink and M. E. Leese, 24–41. London/New York: Routledge.

Jasanoff, S., ed. 2004. *State of Knowledge. The co-production of science and social order*. London and New York: Routledge.

Jasanoff, S., and S.-H. Kim. 2015a. *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. University of Chicago Press.

Jasanoff, S., and S.-H. Kim. 2015b. Future imperfect: Science, technology, and the imaginations of Modernity. In *(2015)* Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power, ed. S. Jasanoff and S.-H. Kim. University of Chicago Press. 10.7208/chicago/9780226276663.001.0001

Kathleen, M. 2017. Knowledge and security. In *The handbook of science and technology studies*, ed. U. Felt, 973–1001. 4th ed. Massachusstes: MIT Press.

Kellner, D. 1999. Virilio, war and technology: Some critical reflections. *Theory, Culture & Society* 16 (5–6):103–25. doi:10.1177/02632769922050890.

Klimburg-Witjes, N. 2023. A rocket to protect? Sociotechnical imaginaries of strategic autonomy in controversies about the European rocket program. *Geopolitics* 1–28. doi:10.1080/14650045.2023.2177157.

Krepinevich, A. F. 1994. Cavalry to computer: The pattern of military revolutions. *The National Interest* (37):30–32.

Lacy, M. 2014. *Security, Technology and Global Politics: Thinking with Virilio*. 1st ed. Oxon and New York: Routledge.

Latour, B. 2005. *Reassembling the social: An introduction to actor-network-theory*. Oxford: Oxford University Press.

Leander, A. 2013. Technological agency in the co-constitution of legal expertise and the US drone program. *Leiden Journal of International Law* 26 (4):811–31. doi:10.1017/S0922156513000423.

Martin, B. R. 2016. Twenty challenges for innovation studies. *Science and Public Policy* 43 (3):432–50. doi:10.1093/scipol/scv077.

Martins, B. O., and N. Ahmad. 2020. The security politics of innovation: Sual-use technology in the EU'S security research programme. In *Emerging security technologies and EU Governance: Actors, practices and processes*, ed. A. Calcara, R. Csernatoni, and C. Lavallée, 58–73. Oxon: Routledge.

Martins, B. O., and M. G. Jumbert. 2022. EU Border technologies and the co-production of security 'problems' and 'solutions'. *Journal of Ethnic and Migration Studies* 48 (6):1430–47. doi:10.1080/1369183X.2020.1851470.

Martins, B. O., and J. Mawdsley. 2021. Sociotechnical imaginaries of EU defence: The past and the future in the European defence fund. *Journal of Common Market Studies* online first. 59 (6):1458–74. doi:10.1111/jcms.13197.

McCarthy, D., and D. R. McCarthy. 2017. *Technology and world politics: An introduction*. Oxon and New York: Routledge. doi:10.4324/9781317353836.

Millar, C., M. Lockett, and T. Ladd. 2018. Disruption: Technology, innovation and society. *Technological Forecasting and Social Change an International Journal* 129:254–60. doi:10.1016/j.techfore.2017.10.020.

North Atlantic Treaty Organization (NATO) (2022) Emerging and disruptive technologies. Accessed December 12, 2022. https://www.nato.int/cps/en/natohq/topics_184303.htm.

Orlikowski, W. J., and S. V. Scott. 2008 Sociomateriality: Challenging the separation of technology, work and organization. *The Academy of Management Annals* 2 (1):433–74. doi:10.5465/19416520802211644.

Peoples, C. 2009. Technology, philosophy and international relations. *Cambridge Review of International Affairs* 22 (4):559–61. doi:10.1080/09557570903516987.

Rogers, E. M. 1995. *Diffusion of innovations*. New York: The Free Press.

Rychnovská, D. 2021. Anticipatory governance in biobanking: Security and risk management in digital health. *Science and Engineering Ethics* 27 (3):30. doi:https://doi.org/10.1007/s11948-021-00305-w.

Salter, M., C. Cohn, A. W. Neal, A. T. Wibben, J. P. Burgess, S. Elbe, J. L. Austin, J. Huysmans, R. Walker, O. Wæver et al. 2019. Horizon scan: Critical security studies for the next 50 years. *Security Dialogue*. 50(4_suppl):9–37. doi:10.1177/0967010619862912.

Salter, M. B., and W. Walters. 2016. Bruno Latour encounters international relations: An interview. *Millennium: Journal of International Studies* 44 (3):524–46. doi:10.1177/0305829816641497.

Schumpeter, J. A. 1934. *The theory of economic development*. Cambridge MA: Harvard University Press.

Stevens, T. 2015. *Cyber security and the politics of time*. Cambridge University Press.

Suchman, L. 2007. *Human-machine reconfigurations: Plans and situated actions*. 2nd. Cambridge University Press. doi:10.1017/CBO9780511808418.

Suchman, L. 2020. Algorithmic warfare and the reinvention of accuracy. *Critical Studies on Security* 8 (2):175–18. doi:10.1080/21624887.2020.1760587.

Suchman, L. 2022. Imaginaries of omniscience: Automating intelligence in the US Department of Defense. *Social Studies of Science*. doi:https://doi.org/10.1177/03063127221104938.

Verbeek, P.-P. 2011. *Moralizing technology understanding and designing the morality of things*. Chicago and London: The University of Chicago Press. doi:10.7208/chicago/9780226852904.001.0001.

Virilio, P. 1977/2006. *Speed and politics*. Los Angeles: Semiotexte.

Virilio, P. 2000. *The information bomb*. London: Verso.

Walters, W. 2014. Drone strikes, dingpolitik and beyond: Furthering the debate on materiality and security. *Security Dialogue* 45 (2):101–18. doi:10.1177/0967010613519162.

Zammuto, R. F., T. L. Griffith, A. Majchrzak, D. J. Dougherty, and S. Faraj. 2007. Information technology and the changing fabric of organization. *Organization Science* 18 (5):749–62. doi:10.1287/orsc.1070.0307.