Defence and Security: New Issues and Impacts

13

Andrew James

13.1 Introduction

In a previous paper (James and Teichler 2014), we observed that public domain foresight studies in Europe were characterised by a shift away from a focus on state-centric military threats to a much broader view of security risks. In the intervening years, much has changed. Many of those changes (the global financial crisis, the growth of authoritarianism and the rise of an increasingly assertive Russia using hybrid warfare including cyber) were barely mentioned in these foresight studies or (infamously in the case of the global financial crisis) not at all. The focus of today has returned to state-centric hybrid threats. Events have overtaken foresight studies.

This chapter provides a meta-analysis of some of the main themes emerging from public domain defence and security foresight studies conducted since the 9/11 attacks on the United States. There are also a number of studies undertaken that—because of the sensitivity of the subject area—have either not been published or have only been published in an abridged form. For instance, the *UK Science and Technology Strategy for Countering International Terrorism* makes reference to a scenario study conducted by the government's defence laboratory DSTL on future technological threats to the United Kingdom (see HM Government 2009). The chapter focuses mainly on studies undertaken in Europe and argues that these foresight studies reflect a shift in security thinking away from a focus on state-centric threats towards a much broader view of security risks. This expanded perspective includes risks presented by the vulnerability of European society to the failure of critical infrastructure, to pandemics, environmental change and resource-based conflicts. The chapter places a particular emphasis on the treatment of technological change in these defence and security foresight studies and argues

A. James (✉)
Manchester Institute of Innovation Research, The University of Manchester, Manchester, UK
e-mail: Andrew.James@manchester.ac.uk

D. Meissner et al. (eds.), *Emerging Technologies for Economic Development*,
Science, Technology and Innovation Studies,
https://doi.org/10.1007/978-3-030-04370-4_13

that the growing importance of dual-use technologies is likely to mean that defence will play a declining role as a sponsor and lead user of advanced technologies in the future.

The chapter is structured as follows: Sect. 13.2 presents some recent defence and security foresight exercises, highlighting who has sponsored the studies, their objectives and participation. The next five sections identify some of the main themes identified from a meta-analysis of these studies. Section 13.3 stresses the core theme that these foresight studies reflect a wider shift in security thinking away from a focus on state-centric threats towards a much broader view of security risks. Section 13.4 considers their treatment of the issue of resource-based conflicts. Section 13.5 notes the importance of the topic of technological vulnerability and the potential misuse of science. Section 13.6 notes how these foresight studies emphasise the changing nature of knowledge production and use in the future, and Sect. 13.7 emphasises how in the future defence is likely to be a technological follower rather than leader in most fields. Section 13.8 goes beyond James and Teichler (2014) to consider the meaning of "emerging technologies" in a military context and what they mean for the future of war. Section 13.9 provides some conclusions.

13.2 Recent Foresight Exercises

A number of foresight exercises on defence and security matters have been conducted in recent years and placed in the public domain. These exercises have been sponsored by agencies of national governments, international organisations as well as the European Commission.

At the national level, the UK Ministry of Defence's Defence Concepts and Doctrine Centre leads an ongoing Global Strategic Trends Programme. In France, the Ministry of Defence's Délégation Aux Affaires Stratégiques undertakes an ongoing programme of foresight studies. In Finland, the *FinnSight 2015* programme on the outlook for science, technology and society undertaken by the Academy of Finland and the Tekes innovation and technology agency considered security issues. In the United States, the National Intelligence Council (an institution supporting the Director of National Intelligence within the US intelligence community) has conducted a series of *Global Trends* studies.

Similarly, international organisations and foundations have engaged in foresight studies contributing to the discussion of future defence challenges. The United Nations and the Bertelsmann Foundation have supported studies dealing with the future of a globalised world, which also address security and defence issues (UNO 2004). Finally, NATO has more particularly addressed the defence challenges that the Atlantic community is likely to face in the coming decades (NATO 2006).

In addition, there have been a series of studies undertaken in Europe that have been sponsored directly or indirectly by the European Commission. The Seventh Framework Programme included for the first time a security research theme and within that there was a funding stream on foresight, scenarios and security as an

evolving concept. This aimed at research in broad societal foresight to capture new and emerging threats as well as other aspects of security as an evolving concept (e.g. ethical and economic aspects). The Commission has funded projects such as FORESEC on *Europe's evolving security: drivers, trends and scenarios* and FESTOS which has as its goal "to identify and assess evolving security threats posed by abuse or inadequate use of emerging technologies and new S&T knowledge, and to propose means to reduce their likelihood". Within the FP7 Social Sciences and Humanities funding stream, the Commission has also funded foresight studies. For instance, the theme *Blue Sky Research on Emerging Issues Affecting European S&T* funded Project SANDERA which focused on the future relationship between the EU science and technology policy strategy to move towards the European Research Area and those EU policies focused on the security of the European citizen in the world both through EU defence policies and EU security policies. This chapter draws on some of the insights from SANDERA which brought together academics and think tanks from eight European countries.

The Commission was also heavily involved in ESRIF (the European Security Research and Innovation Forum). ESRIF describes itself as "a European strategy group in the civil security research domain". ESRIF was established in September 2007 by the EU Member States and the European Commission with the objective to develop a mid- and long-term strategy for civil security research and innovation in Europe. ESRIF included a working group on foresight and scenarios, and its final report—delivered in 2009—includes scenarios.

In addition the European Union Council has sponsored studies discussing future defence challenges such as the European Defence Agency's *Long-Term Vision for Defence* and the EU Institute's for Security Studies *The New Global Puzzle* (European Defence Agency 2006; Gnessotto and Grevi 2006).

The purpose of these foresight studies has been to inform policy-makers, provide a basis for policy priorities and raise awareness amongst key stakeholders. Their main published outputs have been lists of drivers of change, and some studies have also developed scenarios (e.g. ESRIF and SANDERA).

In comparison to the studies sponsored by national governments, the EU reports have addressed the topics from a security rather than defence perspective. Hence, their principal focus has been on the identification of "risks" or "hazards" to security at either the national or European level. Military threats are addressed only in a strictly limited way, relating to the Petersberg Tasks and the fight against terrorism.[1] Whilst these reports, like other foresight studies, have aimed to simulate public debate, they have sought to do so in a different manner by involving stakeholders across the EU and claiming the topic of security as a responsibility of the Commission.

These defence and security foresight exercises have found it difficult to engage with civil society. The FORESEC study and final conference raised the problem that

[1]This reflects the status of defence matters in the European Union which, prior to the Lisbon treaty, were strictly intergovernmental and from which the European commission was largely excluded.

European security foresight exercises rely almost exclusively on a community of security "experts". By omission or commission, the broader European scientific community and civil society have been effectively excluded from such exercises.

The remaining sections of this chapter report a meta-analysis of these foresight exercises undertaken as part of Project SANDERA, and from that we have identified five broad themes:

- Defence and security foresight studies reflect a wider shift in security thinking away from a focus on state-centric threats towards a much broader view of security risks.
- Defence and security foresight studies emphasise that resource-based conflicts are likely to grow in importance in the future.
- Defence and security foresight studies tend to emphasise the technological vulnerability of European society and the potential for the misuse of science
- Defence and security foresight studies emphasise the changing nature of knowledge production and use in the future and how that might increase security risks to Europe.
- Defence and security foresight studies emphasise how in the future defence is likely to be a technological follower rather than a technological leader in most fields.

13.3 From "Defence" to "Security": The Emergence of a New Security Paradigm

The first point from our meta-analysis is that the focus of the defence and security foresight studies that we have reviewed is less on state-centric threats and the potential for state-on-state conflict and more on the security risks posed by intentional and unintentional human actions, technological change and environmental factors.

In this way these foresight studies reflect a broader shift in academic and policy thinking from the traditional notion of national security, which puts the emphasis on the security of the state and military threats to its territorial integrity towards a thinking in broader terms to include new types of threats (e.g. ecological, economic) to new objects of security (the human beings or the citizen, society), calling for a new means to ensure security. Several concepts have been developed to capture these or parts of these notions such as "human security", "total defence", "societal security", "security of the citizen" or the "all-hazards" approach [for a discussion see, e.g. Giegerich and Pantucci (2008)].

Many of these studies assume a shift from traditional state-centric warfare towards a much broader view of security risks. This perspective is captured in the UK Ministry of Defence's Development Concepts and Doctrine Centre (DCDC) report which observes that "Greater interdependence and intensifying competition are likely to be a defining feature of the next 30 years. This tension is likely to

heighten preoccupation with risk at every level, from the personal to the international" (DCDC 2007).

Almost every one of these foresight studies places an emphasis on the increasing interdependence of large parts of the world economy. In the future, the world is seen as one characterised by interdependencies through supply chains, financial flows as well as knowledge flows. These studies are agreed that the twenty-first century will be "the Asian century" (Délégation aux affaires stratégiques 2008; DCDC 2007). They also emphasise how almost ubiquitous communications technologies are likely to strengthen that sense of interdependence. What is striking is how the world has changed in ways not anticipated by these foresight studies. The emergence of authoritarianism and anti-globalisation, not least with the election of President Donald Trump, raises profound and worrying questions about these easy assumptions about growing interdependence that have been commonplace in many foresight studies (although for balance it ought to be noted that the DCDC future reports warn of the tensions arising from globalisation).

There is an emphasis on competition in this new globalised and multipolar world. This competition is seen not only in economic terms although this is recognised as important. Equally, attention is paid to the nature of political competition in a world where the United States is likely to face near-peer competitors such as China and India and in which Europe struggles to retain its position in the world. The competition is also seen in terms of a competition between the state and the emergence of new actors and the importance of non-state terrorist groups and disaffected individuals. Competition also takes the form of competition between competing identities, ideologies and religious world views.

The emphasis on risk also means that these foresight studies consider the consequences for European society of unintended dangers such as natural or man-made disasters. Interdependence means that Europe will become more vulnerable to pandemics no matter whether a virus is spread by tourists, terrorists or both. Equally, food security, energy security and so forth are matters of concern as well as increasingly frequent and violent weather events as a consequence of climate change.

13.4 The Rise of Resource-Based Conflicts

The second observation from our meta-analysis is that defence and security foresight studies emphasise that resource-based conflicts are likely to grow in importance in the future.

Climate change is seen as likely to exacerbate existing conflict situations by intensifying already stressed security situations, particularly in regions with weak institutions that are not able to mitigate or adapt to the changed climatic circumstances (Academy of Finland and Tekes 2006; NIC 2008). The role of climate change in spurring an increase in uncontrolled migration is also emphasised not least from Africa as the sub-Saharan region experiences increasingly prolonged droughts and famines. There is likely to be an increasing prevalence and frequency of human

and animal pathogens as a consequence of climate change, international flows of people and sociocultural change, and this is likely to lead to an increasing number of global pandemics (Délégation aux affaires stratégiques 2008).

Some of these foresight studies also note that demographic developments may have security implications. Asia, Africa and Latin America will account for virtually all population growth over the next 20 years amounting to 1.2 billion more people by 2025 (UNO 2004). In combination with continued economic growth, this will significantly increase demand for energy, food and water resources and amplify the problem of climate change. In countries with significantly more young males than females ("youth bulge"), economic and social institutions need to develop in order to avoid that these countries (in particular Afghanistan, Nigeria, Pakistan and Yemen) continue to be prone to instability and internal conflict (DCDC 2007; National Intelligence Council 2008).

Geopolitical struggles over material and energy resources are also identified as a potential source of growing interstate tensions in the future (DCDC 2007; Délégation aux Affaires Stratégiques 2008). This may take three forms: first, states might use their control over energy resources for political coercion and influence. Second, terrorists and pirates might pose threats to transit routes calling for military protection of those routes, a situation we witness currently at the coast of Somalia. Finally, domestic instability and conflict within strategic energy-producing states could trigger intervention from outside (National Intelligence Council 2008).

13.5 Dangerous Knowledge: Technological Vulnerability and the Misuse of Science

Another theme that we have identified is that defence and security foresight studies tend to emphasise the vulnerability of European society due to its growing dependence on technology and the potential for the misuse of science and technology.

A common theme is that in the future, cyberspace is likely to be a key area for conflict and that security will need to be ensured in this domain. A number of security foresight studies note how critical infrastructures including energy supply, transport and water may be vulnerable to deliberate or accidental failure due to their dependence on networked information and communication technologies (Academy of Finland and Tekes 2006; NIC 2008).

Another theme is the potential for misuse of science and technology. A number of the foresight studies emphasise that there is likely to be accelerating convergence and interaction between major enabling technologies such as information technologies, biotechnologies, nanotechnologies and neuro- and cognitive sciences (Institute of the Future 2005; James et al. 2008). These converging technologies could have a profound transformative impact on European societies and are seen as presenting significant economic, social, cultural and ethical opportunities and challenges. Military application of nanotechnology is seen by some as having potentially destabilising effects, and there may be spillovers from the military use

of converging technologies to crime and terrorism (Nordmann 2008). Thus, ESRIF's final report says:

> There is no doubt that rapid evolution in ICT/cyber security and its misuse will continue and even accelerate. Some technologies already identified as candidates for misuse are nano-technology, artificial intelligence and 'synthetic biology' (i.e., the use of DNA technology to 'engineer' living organisms). These threats will have to be continually monitored and countered. (ESRIF 2009: 25)

13.6 Beyond the Military-Industrial-Scientific Complex: The Changing Nature of Knowledge Production and Use

A further theme emphasised by defence and security foresight studies is the changing nature of knowledge production and use in the future and how that might increase security risks to Europe. The globalisation process is likely to further weaken the ability of states to control research, production and exportation of sensitive technologies and goods, and even maintaining secrecy about sensitive technologies and systems will be extremely difficult (DCDC 2007). These studies suggest that technological innovation will continue to be predominantly commercially led, and commercial dynamics mean that companies will seek to exploit technologies in as many new applications and markets as possible (DCDC 2007). Global capital flows and cross-border ownership will mean that the ownership of companies will become increasingly complex (Délégation aux affaires stratégiques 2008). This may provoke tensions with the security community who are likely to regard the proliferation of some scientific and technological knowledge as a threat its potential to offer terrorists an increasing access to sensitive technologies (National Intelligence Council 2008).

They also emphasise that we are likely to see the emergence of new scientific superpowers. Science in the twenty-first century will be more like a network, with multiple, linked centres of excellence. The United States, Britain and other current leaders will still be important centres of research and innovation but will be joined by India and, probably, China. A host of small countries or regions, including South Korea, Taiwan, Israel and Brazil, will also develop world-class capabilities in strategic specialties or interdisciplinary areas, building targeted programmes that fuse global scientific knowledge with local technical, natural or even cultural resources (Institute for the Future 2005).

A further element in these studies is that we are likely to see new knowledge circulation patterns. The globalisation of scientific and technological activity is likely to continue. There will be increasing information exchange across borders, and we are likely to move "from brain drain to brain circulation (Institute for the Future 2005). This circulation is likely to be driven by the growth of research and entrepreneurial opportunities in emerging countries, the general lowering of global barriers to migration and the erosion of the standard career model in business and academia (Institute for the Future 2005).

These foresight studies also suggest that an increasing body of scientific and technological knowledge and technique is likely to be widely available as a consequence of the emergence of new scientific superpowers and the diffusion of knowledge. This is likely to be facilitated by modern means of communication (mainly, but not only, the Internet) (Délégation aux affaires stratégiques 2008). The Internet and information technologies have broadened access to scientific knowledge and are starting to lower the barriers to participation in scientific research. In the next decades, the spread of pervasive computing technologies, low-cost sensors, flexible electronics and desktop manufacturing tools, combined with commons-based, peer-reviewed scientific production systems, will broaden the range of opportunities for wider participation in science and technology (Institute for the Future 2005).

These trends and technologies, some of the studies suggest, will lower the barriers to participation in science for individuals, groups and emerging countries (Institute for the Future 2005). The result may be the growth of "amateur science", new scientific and technical centres of excellence in developing countries and a more global distribution of world-class scientists and technologists (DCDC 2007).

There is a concern in the defence and security communities that the pace of change in many science and technology domains may exceed the speed at which governments can respond and that the spread of scientific knowledge and technological capabilities may become able to outperform states who can be constrained by their decision-making processes, technological path dependencies and commercial and political factors (DCDC 2007).

This is an emerging trend, and such developments may be regarded as a threat to the security community since it has the potential to widen the tools available to both small terrorist groups and to emerging countries seeking to increase their ability to wage war by both old and new means (DCDC 2007). The diffusion of the knowledge underpinning weapons of mass destruction and of dual-use knowledge in the life sciences that has the potential to be applied to biological weapons is frequently noted and discussed (DCDC 2007; Délégation aux affaires stratégiques 2008). In addition, terrorists and/or criminals might abuse new emerging technologies for their purposes, in particular the output of robotics, nanotechnology in combination with medicine, cognitive science, sensors, networks and smart materials (Délégation aux affaires stratégiques 2008). This driver is supported also by a trend that innovation, research and development will originate from more international and diffuse sources and will proliferate widely, making regulation and control of novel technologies more challenging (DCDC 2007).

At the same time, such developments may also be seen as an opportunity by the defence and security communities, and they will increasingly seek to access the potential of "democratised innovation" as part of a move towards an open innovation model for defence. This may stimulate efforts on the part of the defence and security policy communities to build closer and cooperative relationships with the wider civil research community although how that civil research community may respond is an open question as we will see in the next section.

13.7 Defence as a Technological Follower Rather than a Technological Leader

Defence and security foresight studies emphasise how in the future defence is likely to be a technological follower rather than a technological leader in most fields.

Defence has played an important role as a sponsor and lead user of some advanced technologies at some stages in their development. The growing emphasis of defence science and technology policy on accessing commercial off-the-shelf technologies as well as a move towards an open innovation model that will depend upon accessing globally available technological knowledge suggests that defence may play a declining role as a sponsor of advanced technologies in the future. Equally, defence procurement has declined in absolute terms in Europe and also when compared to the size of other (civilian) markets (James et al. 2008). This is a continuation of past trends, and defence and security science and technology research may be of declining importance in the European science policy mix.

The rapid pace of nondefence origin technological change and the likelihood that absolute defence R&D spending in Europe will continue to decline (or at best remain stable) are likely to impact the way that governments and industry conduct defence R&D. The role of defence R&D is already shifting from the development of new technologies in large specialised defence research establishments to partnerships that can access and exploit technologies that are the product of commercially funded research. This trend is likely to continue (James et al. 2008).

Specific national government R&D investment in in-house expertise and technology development is likely to continue where there is no civilian equivalent and where there are particular concerns about the need to retain national operational sovereignty, for example, in some critical defence and security technologies, such as cryptography, nuclear, counterterrorism and chemical, biological, radiological and nuclear (CBRN) defence (DCDC 2007). In other fields, however, governments are already developing R&D programmes that draw on the increasingly diverse global science and technology base in industry, SMEs and universities and adapt and apply that knowledge for military use. This approach is likely to broaden and deepen.

The pace of this move towards an open innovation approach is likely to depend in the ability of the civil and military research communities to work together. On the other hand, it will require the willingness of those nontraditional sources of scientific and technological knowledge to engage with the defence sector. There are major cultural differences between universities and the defence sector. On the other, traditional defence firms will need to embrace new business models and marketing practices reflecting the different dynamics of value creation in civilian markets and requirements linked to commercial customers.

13.8 Emerging Technologies and the Future of War

So far this chapter has closely followed an earlier journal paper (James and Teichler 2014). This section goes beyond that earlier paper to consider the meaning of "emerging technologies" in a military context and what they mean for the future of war.

This question is important because radical technological change is back on the military's agenda. In his last major address as Defence Secretary, Chuck Hagel announced the Defence Innovation Initiative, aimed at fostering a third "game-changing" offset strategy. Eisenhower's "New Look" doctrine in the 1950s led to the development of new types of nuclear weapons, long-range delivery systems and active and passive defences to offset the Soviet Union's quantitative force advantage. The offset strategy of the 1970s and 1980s led to leap-ahead capabilities like standoff precision strike, stealth, wide-area surveillance and networked forces. The Defence Innovation Initiative calls for "a new Long-Range Research and Development Planning Program [that] will help identify, develop and field breakthroughs from the most cutting-edge technologies and systems, especially in robotics, autonomous systems, miniaturization, big data and advanced manufacturing, including 3-D printing".[2] At the time of writing, it was not possible to judge the Trump administration's view of the Defence Innovation Initiative although the President's 2017 budget request had included a proposed substantial increase in spending of defence research and development.

13.8.1 Emerging Technologies in the Military Context

This chapter has already shown that visions of the military future almost always have a strong technological element. Emerging technologies feature prominently in foresight studies. They identify a host of emerging technologies that may have implications for security, military capability and—in some cases—the conduct of future war. These include:

- **Autonomous systems and artificial intelligence**: self-thinking, deciding and organising partially sentient devices that mimic aspects of human intelligence and decision-making are being developed and may move/reduce the need for human input and reduce the manpower burden.
- **"Big data"** information analysis and exploitation may lead to better decision-making and enhanced intelligence analytic capability.
- **Developments in nanotechnology and microsystems** promise sensors of small size and improved performance.

[2]"Hagel Announces New Defence Innovation, Reform Efforts" http://www.defense.gov/news/newsarticle.aspx?id=123651 (last accessed 7 February 2015).

- **Human enhancement and augmentation**: a range of technologies offer considerable scope for enhancing and augmenting the physical and cognitive performance of humans, including prosthetics, drugs and genetic manipulation.
- **Synthetic biology**: the design and fabrication of biological components and systems that do not already exist in the natural world with the potential to produce to create novel threats in the form of "designer" bio-weapons.
- **Social and behavioural sciences**: developments are expected to provide additional insights into the intent and behaviour of individuals and groups leading to new opportunities to influence them.

However, before going any further, it is important to define what is—and what is not—meant by "emerging technologies". The UK's Defence Technology Plan defines emerging technologies as follows: "Emerging technologies can be characterised as: immature technologies in the early proof-of-principle stages; [and] more mature technologies but where a novel defence application has been identified". Whilst this definition appears clear and straightforward (and this chapter will use it), it is the case that a feature of much of the discussion of emerging technologies is a lack of clarity as to the subject of analysis.

"Emerging" is used variously to examine technologies that analysts regard as potentially emerging in the far future (e.g. the latest UK MOD DCDC programme report looks out to 2040 and consciously examines what technological developments *may* occur). In contrast, "emerging" is sometimes used to describe technologies that have reached a stage that we know that they *will* find application in a weapon system in the near future [e.g. many of the "emerging" IT technologies discussed by Bruce Berkowitz in his 2003 book are now in military service at least with the US military (Berkowitz 2003)]. Sometimes analysts conflate the far future and the soon to be fielded as "emerging technologies" giving the impression to the unwary that (true) emerging technologies on the technological far horizon are as certain to be fielded as those in late-stage development. This raises important questions about timing that are critical to discussions about emerging technologies. It also raises issues about uncertainty. Both issues will be discussed later in this chapter.

There is an important distinction here that is sometimes missed by military analysts of emerging technologies. The distinction is between technologies and the weapons, their delivery systems and the infrastructure that supports military capability. *Technologies* underpin *weapon systems* but are distinct from them. Thus, nanotechnologies may be important to the military, but only if they find application in weapon systems. Consequently, how emerging technologies and other factors are combined into military capability should be the critical consideration not the emerging technologies themselves.

Equally, new or improved classes of weapon rarely (if ever) comprise only new ("emerging") technologies but instead combine new technologies with mature technologies. Thinking influenced by the economist Joseph Schumpeter emphasises that innovation can be new combinations of existing technologies and stresses the potential significance of combining existing technologies in a new use. Innovation that produces modern weapon systems is increasingly based on this kind of dynamic

recombination of generic technologies which are often information technologies (Hasik 2008). The DCDC Strategic Trends study identifies the rapid asymmetric insertion and exploitation of widely available commercial technologies—GPS, low-cost unmanned aerial vehicles, mobile telephones—as a significant concern. Indeed, the experience of Iraq and Afghanistan provides graphic illustrations of how such tactics can have devastating asymmetric effects. The contrast between the rate of combinatorial innovation of this kind and the pace of developments in the traditional defence acquisition has been striking (DCDC 2014).

13.8.2 Emerging Technologies and the Future of War

Most emerging technologies represent incremental improvements to what went before and enhance the competencies of the military along dimensions that they have traditionally valued. This kind of technological development presents relatively few challenges to the military, although their insertion into existing platforms can be difficult. In contrast, it is new technologies that are radical, competence destroying and create new sources of military advantage along dimensions not traditionally valued or poorly understood by the military that tend to be the focus of attention and concern.

Fundamentally, these types of new technologies can change the environment in which military forces operate. In *The Pursuit of Power*, William H McNeill (1982) charts the consequence of technological change on the balance of power. In *War and Power in the 21st Century: The State, Military Power and the International System*, Paul Hirst (2001) analysed how new military technologies change the way that wars are fought and how power relations change as a result.

A radical new technology can change the balance of power or create new forms of insecurity. The most dramatic illustration of the impact of new technology was the Allied development of the atomic and hydrogen bombs during the Second World War and the subsequent development of similar capability by the Soviet Union. In turn, the development of inertial navigation technologies added the prospect of accuracy to devastating lethality.

It is a commonplace that today's emerging technologies may lead to the proliferation of novel disruptive threats. Many—most—of the emerging technologies are not the preserve of the military and governments. Most are emerging out of work being conducted in universities, firms and garages across the world. Some require only modest resources. For example, synthetic biology is an area of S&T that has a growing and Internet-linked "DIY community".

New technologies may also influence the likelihood of conflict. The emergence of the hydrogen bomb arguably reduced the threat of conflict. The increased availability and capability of remotely operated vehicles and their increasingly autonomous successors may reduce the threshold for their use by reducing the political risk of military casualties, likewise cyberwarfare. "The anonymity that cyberspace can offer reduces the risk of retribution, so may increase the attractiveness of making an attack". In *The Future of War* (2004), Christopher Coker talks about the

"re-enchantment of war in the twenty-first century". Coker argues that developed societies are likely to continue with war in the future because technological change—not least that associated with the information revolution—may make it more rational and precise than ever before. Indeed, he says: "if war is seen as merely one end on a spectrum of violence, death is not essential to it. Killing could be made redundant (though probably not optional), leaving physical coercion or the will to power by other means" (p. 141).

New technologies can redefine the way that warfare is conducted or create new types of warfare. Technology and military doctrine are closely coupled and interdependent (Alic 2007). Blitzkrieg, the AirLand Battle and Carrier Strike are but three examples of how new technologies combined with organisational and doctrinal change led to new ways of warfare (Williamson and Murray 1996). The Revolution in Military Affairs provides another example. The Internet and its widespread application have created the possibility of a new form of warfare—cyberwarfare—that was hardly imaginable 20 years ago.

Emerging technologies may also pose profound ethical and moral questions. Many areas of emerging technology will pose ethical challenges. Take the use of biotechnology, for instance. Christopher Coker (2004: 140) argues:

> by enhancing, modifying or altering our genes, we may be able to enhance the things we do well, and have always done well, as a species. One of the things we have done particularly well over the centuries has been war, and there is nothing to suggest that we will be going out of the war business—indeed quite the opposite.

In his latest book, *Warrior Geeks*, Coker (2013) warns that technological change is threatening to create a battlespace that has no place for human qualities such as courage, sacrifice or honour and even more fundamental categories such as subjectivity, agency and ethics.

13.9 Conclusion

This chapter has analysed some of the main themes emerging from public domain defence and security foresight studies conducted since the 9/11 attacks in the United States. We have emphasised how these foresight studies reflect a shift in security thinking away from a focus on state-centric threats towards a much broader view of security risks that includes risks presented by the vulnerability of European society to the failure of critical infrastructure, pandemics, environmental change and resource-based conflicts.

This chapter has also emphasised how emerging technologies may influence the future of war. This chapter has noted how the role of defence for the development of new technologies is likely to change dramatically in the future. In particular, defence and security foresight studies have emphasised that the growing importance of dual-use technologies is likely to mean that defence will play a declining role as a sponsor and lead user of advanced technologies in the future. This can be seen as the

continuation of trend developments over the last two decades. At the same time, whilst the role of defence in the creation of knowledge has changed along these dimensions, there are also continuities. "Defence", i.e. the call to protect the security of a country, its population and assets against threats or from any harm, can be expected to remain an accepted justification for extraordinary political action and the channelling of political, financial and industrial resources. We have pointed to the "securitisation" of cyberspace and of critical infrastructure, areas that have formerly been considered outside the realm of defence, governments and private actors.

This chapter concludes with a final reflection. Rémi Barré has rightly observed that "The objective, themes and content of a foresight have specific meaning and intention".[3] Nowhere is more true than in the field of defence and security foresight. Defence and security represent distinct epistemic and policy communities. Risk is the lens through which these policy communities view the world and this is reflected in the often pessimistic character of the visions of the future that emerge from defence and security foresight exercises. Many of the foresight exercises are essentially closed activities that draw upon expertise from within the policy community (although in some exercises there have been attempts to "reach out" to broader expertise). Like all policy fields, there are strong vested interests, and the proper role of defence and security in Europe is controversial and contested. The meaning and intention of security and defence foresight activities are deserving of further academic scrutiny.

Acknowledgements I wish to acknowledge the contribution of Dr Thomas Teichler to the journal paper on which parts of this chapter are based. I also wish to thank the participants in the Clements and Strauss Centers Seminar "Emerging technologies and the future of war" at the University of Texas at Austin in February 2015. Section 13.8 draws on my comments to that seminar and the useful discussion that followed. I also wish to express my thanks to all the members of the SANDERA consortium for their contribution to our thinking on these matters and in particular the participants in the SANDERA workshops in Manchester and Valencia and the contributors to the SANDERA discussion papers. All errors and omissions are entirely my responsibility.

References

Academy of Finland and Tekes (2006) FinnSight 2015 - the outlook for science, technology and society. Academy of Finland, Helsinki

Alic JA (2007) Trillions for military technology: how the pentagon innovates and why it costs so much. Palgrave MacMillan, New York

Berkowitz B (2003) The new face of war: how war will be fought in the 21st century. The Free Press, New York

Coker C (2004) The future of war: the re-enchantment with war in the twenty-first century. Blackwell, Oxford

Coker C (2013) Warrior geeks: how twenty-first century technology is changing the way we think about war. Hurst & Company, London

[3] Intervention by Rémi Barré at the AUGUR project conference Sharing Visions on Europe in 2030: Lessons from Comparative Approaches of Recent Foresight Exercises 2 June 2010, Brussels.

DAS (2008) Geostrategic prospectives for the next thirty years. Report made under the direction of the Délégation aux affaires stratégiques. Délégation aux affaires stratégiques, Paris
DCDC (UK) (2007) The DCDC's global strategic trends programme 2007–2036. Report prepared by the UK Ministry of Defence Development, Concepts and Doctrine Centre, DCDC, Shrivenham
DCDC (UK) (2014) Global strategic trends: out to 2040, 4th edn. Development, Concepts and Doctrine Centre, Ministry of Defence, London
European Defence Agency (2006) An initial long-term vision for European defence capability and capacity needs. EDA, Brussels
European Security Research and Innovation Forum (2009) Security research: final ESRIF report. European Commission, Brussels
Giegerich B, Pantucci R (2008) FORESEC deliverable 2.4 synthesis report
Gnesotto N, Grevi G (2006) The new global puzzle. EU Institute for Security Studies, Paris
Hasik J (2008) Arms and innovation: entrepreneurship and alliances in the twenty first century defense industry. University of Chicago Press, Chicago
Hirst P (2001) War and power in the 21st century: the state, military power and the international system. Polity Press, Cambridge
HM Government (UK) (2009) UK science and technology strategy for countering international terrorism. Home Office, London
Institute for the Future (2005) 2005–2055 science and technology perspectives. Institute for the Future for UK Government Office of Science & Innovation
James AD, Teichler T (2014) Defence and security: new issues and impacts. Foresight 16(2): 165–175
James AD, Hartley K, Lazaric N, Gasparini G (2008) Study on how to measure the strengths and weaknesses of the DTIB in Europe. European Defence Agency, Brussels. http://www.eda.europa.eu/documents/09-11-24/Study_on_how_to_measure_Strengths_and_Weaknesses_of_the_DTIB_in_Europe
McNeill WH (1982) The pursuit of power: technology, armed force and society since AD 1000. University of Chicago Press, Chicago
NATO (2006) Future world scenarios. North Atlantic Treaty Organisation, Brussels
NIC (2008) Global trends 2025: a transformed world. National Intelligence Council, Washington, DC
Nordmann A (2008) Converging technologies - shaping the future of European societies. European Commission, Brussels. http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBYQhgIwAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.133.2322%26rep%3Drep1%26type%3Dpdf&rct=j&q=Converging%20Technologies%3A%20Shaping%20the%20Future%20of%20European%20SocietiesNordmann%2C%202004&ei=-4EgTp6CJ4WBhQeS7KTBAw&usg=AFQjCNFQrEo7g9Qtx4hRijIuSHXInMJF4A&cad=rja. Accessed 12 Dec 2008
UNO (2004) A more secured world: our shared responsibility. Report of the high-level panel on threats, challenges and change. United Nations, New York
Williamson W, Murray AR (eds) (1996) Military innovation in the inter-war period. Cambridge University Press, Cambridge

Andrew James is Professor of Innovation Management & Policy at Alliance Manchester Business School and a former Director of the Manchester Institute of Innovation Research. His research focuses on technology and innovation management and policy in the aerospace, security and defence sectors. Between 2009 and 2011, he was the Scientific Coordinator of SANDERA (The Future Relationship between Security and Defence Policies and the European Research Area) funded under the Seventh Framework Program Socio-Economic Sciences and Humanities theme Blue Sky Research on Emerging Issues Affecting European S&T.