



Innovative technologies shaping the 2040 battlefield

STUDY

Panel for the Future of Science and Technology

EPRS | European Parliamentary Research Service

Scientific Foresight Unit (STOA)

PE 690.038 – August 2021

EN

Innovative technologies shaping the 2040 battlefield

Looking towards 2040, the global innovation and technology landscape is expected to evolve significantly, driving change in the nature of warfare as well as in the capabilities, concepts and doctrines employed by actors on the battlefield. As such, there is a need to understand this technological change and explore its potential influence and impact on the future battlefield, in order to formulate policies and investment decisions that are as future-proof as possible.

Providing an assessment of the risks, challenges and opportunities relating to the new and emerging technologies that are most expected to shape the future battlefield up to 2040, this study presents the implications stemming from consideration of individual technologies, as well as cross-cutting analysis of their interactions with broader political, social, economic and environmental trends. In doing so, the study highlights a need for EU institutions and Member States to pursue a broad range of capability development initiatives in a coherent and coordinated manner, ensure the development of an agile regulatory and organisational environment, and guide investments in the technologies most relevant to the European context.

AUTHORS

This study has been written by Jacopo Bellasio, Linda Slapakova, Luke Huxtable, James Black, Theodora Ogden and Livia Dawaele of RAND Europe, at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

ADMINISTRATOR RESPONSIBLE

Gábor Zsolt Pataki, Scientific Foresight Unit (STOA)

To contact the publisher, please e-mail stoa@ep.europa.eu

LINGUISTIC VERSION

Original: EN

Manuscript completed in July 2021.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

Brussels © European Union, 2021.

PE 690.038

ISBN: 978-92-846-8399-4

doi: 10.2861/620590

QA-05-21-220-EN-N

<http://www.europarl.europa.eu/stoa> (STOA website)

<http://www.eprs.ep.parl.union.eu> (intranet)

<http://www.europarl.europa.eu/thinktank> (internet)

<http://epthinktank.eu> (blog)

Table of contents

1. Introduction	1
1.1. Context of the study	1
1.2. Scope and objectives of the study	1
1.3. Methodology and limitations	2
1.3.1. Research approach and methods used in the study	2
1.3.2. Limitations	6
1.4. Structure of this report	7
2. Evolving policy context and future strategic environment	8
2.1. The evolving strategic environment	8
2.1.1. Political trends and factors	9
2.1.2. Social trends and factors	10
2.1.3. Economic trends and factors	11
2.1.4. Environmental trends and factors	12
2.1.5. Technological trends and factors	13
2.1.6. Characteristics and views on the possible future battlefield	13
2.2. The EU regulatory and policy context for defence and new and emerging technologies	16
2.2.1. The changing role and ambition for the EU as a defence and security actor	16
2.2.2. EU focus on innovation and new and emerging technologies with a disruptive potential	18
2.2.3. Summary	20
3. Overview and assessment of new and emerging technologies shaping the 2040 battlefield	21
3.1. Overview and assessment of individual technology clusters	22
3.1.1. Artificial intelligence, machine learning and big data	22
3.1.2. Advanced robotics and autonomous systems	26
3.1.3. Biotechnology	30
3.1.4. Technologies for the delivery of novel effect	33

3.1.5. Satellites and space-based technologies and assets	36
3.1.6. Human-machine interfaces	40
3.2. Other technologies of relevance for the future battlefield	43
3.2.1. Advanced energy and power systems	43
3.2.2. Novel and advanced materials and manufacturing	43
3.2.3. Quantum technologies	44
3.2.4. Computing, data storage, and telecommunications	45
3.2.5. Sensor and radar technologies	46
4. Findings, implications and policy options for the EU	47
4.1. Cross-cutting findings and implications	47
4.1.1. The nature of impact of emerging technologies on the future battlefield	48
4.1.2. Factors shaping the impact of emerging technologies on the future battlefield	50
4.1.3. Enablers and barriers in European defence	51
4.2. Policy options	53
4.2.1. Further pursue a broad range of capability development initiatives	54
4.2.2. Ensure the development of an environment characterised by the appropriate regulatory and organisational agility and absorption capacity	56
4.2.3. Facilitate EU investments and RDT&I activities in relevant new and emerging technologies by strengthening collaboration with industry	58
Annex A: The EU policy and regulatory landscape for defence and new and emerging technologies	66
The EU regulatory and policy context for defence and for new and emerging technologies	66
EU focus on innovation and new and emerging technologies with a disruptive potential	70
Annex B: Methodology	75
WP1 Scoping and Framing	75
WP2 Identifying and selecting technologies	77
WP3 Characterising and comparing technologies	78
WP4 Implications and reporting	83

Annex C: Additional STREAM analysis	84
Comparative assessment of emerging technologies shaping the future battlefield	84
Artificial Intelligence, Machine Learning and Big Data	89
Advanced robotics and autonomous systems	92
Biotechnology	94
Technologies for the delivery of novel effect	96
Satellites and space-based technologies and assets	98
Human-machine interfaces	100
Annex D: Copy of stakeholder engagement materials	103
Materials used in expert interviews	103
Materials used in the STREAM workshop	104
Annex E: Horizon scanning technology longlist	108

List of tables

Table 1.1 – Study research questions	2
Table 2.1 – Thematic trends and factors that could contribute to shaping the 2040 battlefield	9
Table 2.2 – Potential characteristics of the future battlefield	14
Table 3.1 – Overview of key new and emerging technology clusters shaping the 2040 battlefield _	21
Table 4.1 – Overview of cross-cutting findings	47
Table B.1 – Longlist of technology clusters and definitions	76
Table B.2 – Results of technology shortlisting consultations	77
Table B.3 – List of experts consulted in WP3 interviews	79
Table B.4 – STREAM scoring criteria for impact on the EU and the CSDP	80
Table B.5 – STREAM scoring criteria for impact on future battlefield dynamics	82
Table B.6 – STREAM scoring criteria for feasibility of implementation	83
Table C.1 – Overview of the impact and implementation criteria	84

List of figures

Figure 1.1 – Overview of project tasks, underpinning activities, and resulting outputs and deliverables	3
Figure 1.2 – Technology shortlisting and selected technology clusters	5
Figure B.1 – Overview of project tasks, underpinning activities, and resulting outputs and deliverables	75
Figure B.2 – Technology shortlisting process	78
Figure B.3 – High-level overview of the STREAM methodology	80
Figure C.1 – Aggregated scores for technologies with associated error bars (+/- 1 standard deviation)	85
Figure C.2 – Aggregated scores for technologies (zoomed-in, no error bars)	86
Figure C.3 – Summary assessment of the technology clusters across the impact criteria	88
Figure C.4 – Summary assessment of the technology clusters across the implementation criteria	89
Figure C.5 – Assessment of AI, ML and Big Data on impact criteria- EU and the CSDP	90
Figure C.6 – Assessment of AI, ML and Big Data on impact criteria - future battlefield dynamics	91
Figure C.7 – Assessment of AI, ML and Big Data on implementation criteria	92
Figure C.8 – Assessment of advanced robotics and autonomous systems on impact criteria – EU and the CSDP	93
Figure C.9 – Assessment of advanced robotics and autonomous systems on impact criteria – Future battlefield dynamics	93
Figure C.10 – Assessment of advanced robotics and autonomous systems on implementation criteria	94
Figure C.11 – Assessment of biotechnology on impact criteria – EU and the CSDP	95
Figure C.12 – Assessment of biotechnology on impact criteria – Future battlefield dynamics	95
Figure C.13 – Assessment of advanced biotechnology on implementation criteria	96
Figure C.14 – Assessment of technologies for the delivery of novel effect on impact criteria – EU and the CSDP	97
Figure C.15 – Assessment of technologies for the delivery of novel effect on impact criteria – Future battlefield dynamics	97
Figure C.16 – Assessment of technologies for the delivery of novel effect on implementation criteria	98
Figure C.17 – Assessment of satellites and space-based technologies on impact criteria – EU and the CSDP	99
Figure C.18 – Assessment of satellites and space-based technologies on impact criteria – Future battlefield dynamics	99
Figure C.19 – Assessment of technologies for the delivery of novel effect on implementation criteria	100
Figure C.20 – Assessment of human-machine interfaces on impact criteria – EU and the CSDP	101
Figure C.21 – Assessment of human-machine interfaces on impact criteria – Future battlefield dynamics	101
Figure C.22 – Assessment of human-machine interfaces on implementation criteria	102

List of abbreviations

AGI	artificial general intelligence
AI	artificial intelligence
ANI	artificial narrow intelligence
ASAT	anti-satellite
ASI	artificial super-intelligence
BCI	brain-computer interface
C2	command and control
CADR	coordinated annual review on defence
CDP	capability development plan
CFFS	Centre for Futures and Foresight Studies
CSDP	common security and defence policy
DEW	directed energy weapon
DG DEFIS	Directorate-General for Defence Industry and Space
DOD	Department of Defense
EDA	European Defence Agency
EDAP	European defence action plan
EDF	European Defence Fund
EDIDP	European defence industrial development programme
EEAS	European External Action Service
ELV	expendable launch vehicle
EMS	electromagnetic spectrum
EO	earth observation
EP	European Parliament
EU	European Union
EU GSS	Global Strategy for European foreign and security policy
EUI	EU institution
FAWS	fully autonomous weapons system
GEO	geosynchronous earth orbit
GUI	graphical user interface
HADR	humanitarian assistance and disaster relief
HAPS	high-altitude pseudo-satellites
HCM	hypersonic cruise missile
HEL	high energy laser
HGD	hypersonic glide vehicle
HMI	human-machine interfaces
HMT	human-machine teaming
HR/VP	High Representative of the Union for Foreign Affairs and Security Policy
ICT	information and communications technology

IHL	international humanitarian law
IoT	internet of things
ISR	intelligence, surveillance and reconnaissance
ISTAR	intelligence, surveillance, target acquisition and reconnaissance
LAWS	lethal autonomous weapons systems
LEO	low earth orbit
LOAC	law of armed conflict
ML	machine learning
MNC	multi-national company
MPCC	Military Planning and Conduct Capability
MS	Member State
NATO	North Atlantic Treaty Organisation
NLP	natural language processing
OODA	observe, orient, decide and act
OSCE	Organization for Security and Co-operation in Europe
PADR	preparatory action for defence research
PESCO	permanent structured cooperation
PNT	positioning, navigation and timing
QKD	quantum key distribution
R&D	research and development
RDTI	research, development, technology and innovation
RI	responsible innovation
RLV	reusable launch vehicle
RQ	research question
RRI	responsible research and innovation
S&T	science and technology
SATCOM	satellite communications
SSA	space situational awareness
SSTA	single-stage-to-orbit
STOA	science and technology options assessment
STREAM	systematic technology reconnaissance, evaluation and adoption method
SWaP	size, weight and power
TRL	technology readiness level
UAV	unmanned aerial vehicle
UAS	unmanned aerial system
US	United States
UV	ultraviolet
WME	weapon of mass effect
WP	work package
WSN	wireless sensor network
WUI	web user interface

1. Introduction

1.1. Context of the study

The coming decades are expected to be a time of transition, possibly characterised by instability within and between state actors. The world is likely to face the need to address the impacts of: a changing climate, the increasing pace of innovation and technological change, rapid population growth, growing resource scarcity and global power shifts. Such trends are also likely to drive significant change in the character of warfare and the technologies used by defence organisations, allies and adversaries.

Understanding technological change and forecasting its potential impact on and shaping of the future battlefield is crucial to formulating policies and investment decisions conducive to making appropriate modifications to armaments, military operations, wartime preparations and defence budget priorities. It is therefore important to understand what technology areas are likely to lead to profound changes on the future battlefield, and how such impacts may materialise. This understanding will inform decision-making and maximise, to the extent possible, returns on investment in a context of limited resources and competing priorities.

1.2. Scope and objectives of the study

In this context, the European Parliament's Panel for the Future of Science and Technology (STOA) commissioned RAND Europe in August 2020 to conduct a study on 'Innovative technologies shaping the 2040 battlefield' (Reference: EPRS/STOA/SER/20/017). The objectives of this study were to:

1. analyse risks and challenges related to the innovative technologies that may shape the 2040 battlefield, particularly as regards designing and commissioning new types of weapons and the human-system interaction on the battlefield (including the deployment of mixed components);
2. develop several case studies to assess the possible impacts on future warfare of different technologies of particular relevance to the European Parliament's Security and Defence (SEDE) Subcommittee;
3. characterise the definitions, impacts, risks and challenges relating to new and emerging defence technologies to assess the prospects for their use in building EU resilience and strategic autonomy; and
4. formulate and propose policy options for consideration to the SEDE Subcommittee.

To meet these study objectives, RAND Europe formulated a set of research questions (RQs) that were addressed through the delivery of the study, as shown in Table 1.1.

Table 1.1 – Study research questions

Research questions	
RQ1 Understanding technology	How might new and emerging technologies be expected to have an impact on defence and shape the future battlefield in 2040?
RQ2 Technology challenges	What are the potential challenges that new and emerging technologies might present for the EU and its Member States within the context of defence and security up to 2040?
RQ3 Technology opportunities	What are the potential opportunities offered to the EU and its Member States by emerging technologies and their role in the 2040 battlefield?
RQ4 Policy implications	What are the implications arising out of the challenges and opportunities of new and emerging technologies within defence and security for EU and Member State policy and activities?

To address these RQs, the study team conducted a range of activities within four technical work packages (WPs):

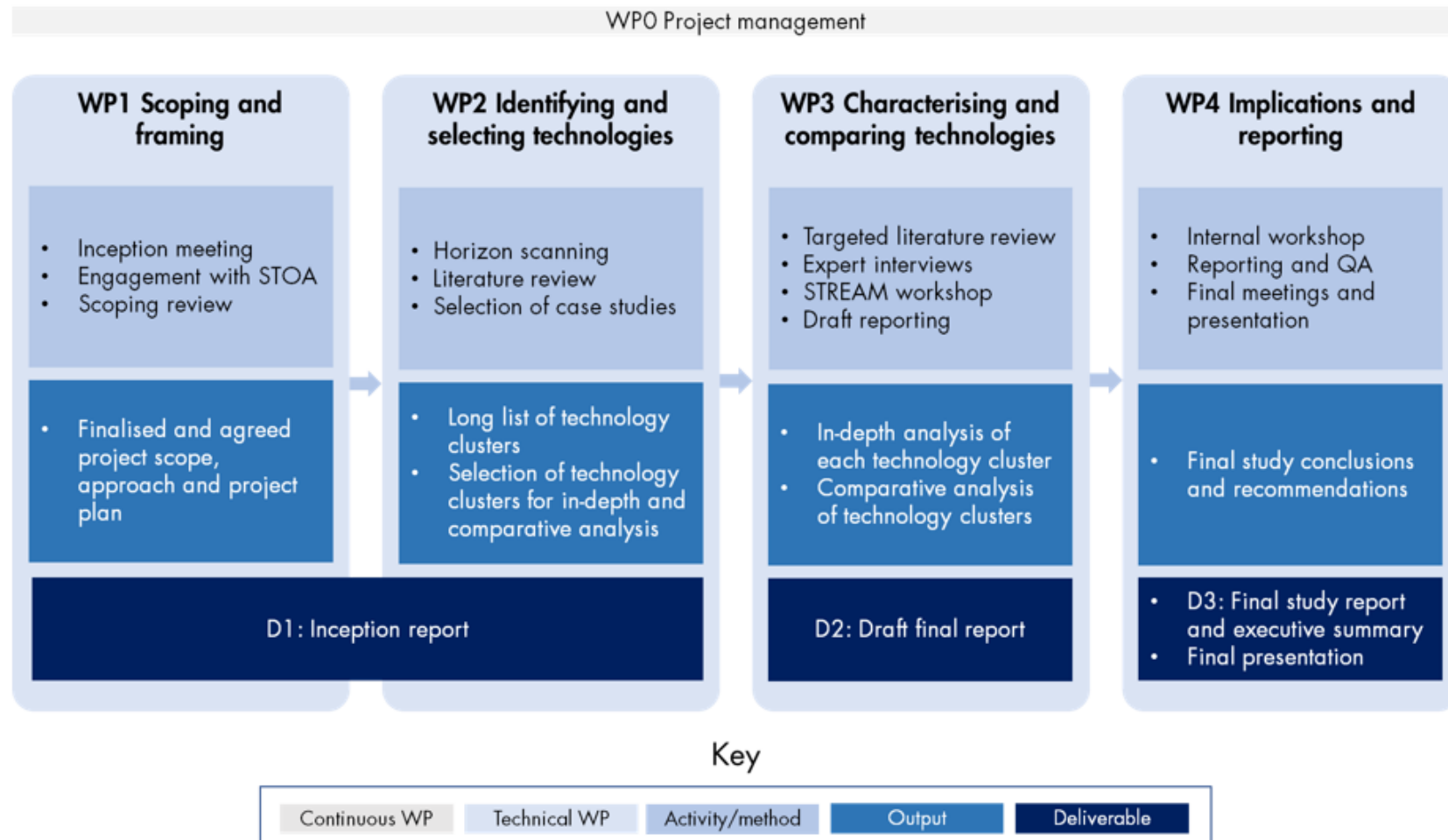
- **WP1 – scoping and framing** aimed to characterise the research context by taking stock of existing literature and to define the research scope, objectives and approach for the study;
- **WP2 – identifying and selecting technologies** further expanded in the scoping and framing activities to understand how new and emerging technologies may shape the future battlefield, while also identifying the new and emerging technologies that are most expected to do so within the 2040 timeframe (RQ1);
- **WP3 – characterising and comparing technologies** focused on providing a more in-depth understanding of the opportunities and challenges associated with those new and emerging technologies (identified in WP2) that were most expected to shape the 2040 battlefield, and providing a comparative assessment of such impacts (RQs 2 and 3); and
- **WP4 – implications and reporting** serves to identify the key policy implications for the EU and its Member States arising from the challenges identified and opportunities associated with new and emerging technologies on the 2040 battlefield (RQ4).

1.3. Methodology and limitations

1.3.1. Research approach and methods used in the study

To answer the RQs presented in Table 1.1 and meet the requirements of the study, RAND Europe adopted a structured mixed-methods research approach, as shown in Figure 1.1. **Annex B** presents a more in-depth explanation of the study methodology.

Figure 1.1 – Overview of project tasks, underpinning activities, and resulting outputs and deliverables



In the initial phase of the study, the study team conducted a range of activities to characterise the context in which new and emerging technologies may shape the 2040 battlefield. This included a review of the economic, social, political, environmental and technological trends that constitute both the future strategic environment and the evolving EU regulatory and policy contexts. The results of this scoping review are presented in **Chapter 2** of this report. The study team also engaged with STOA to establish a comprehensive understanding of the study context and refine the scope, approach and timelines for the study.

Building on the initial scoping activities, the study team combined top-down application-driven and bottom-up technology-driven data collection to compile a longlist of potential technology clusters that may be expected to have the greatest potential impact on European defence and the future battlefield. This leveraged the following methods and data collection tools:

- Literature review – Application-driven review of publicly available open-source academic and grey literature (e.g. government reports and defence news media) on new and emerging technologies with a primary focus on emerging technologies applied within a defence and security context over the next 20 years.
- Horizon scanning – Review of the RAND Europe Centre for Futures and Foresight Studies (CFFS)¹ Science and Technology (S&T) horizon scanning database to identify, understand and prioritise key emerging technology developments through a technology-driven approach. The RAND Europe horizon scanning database is developed through the collection and analysis of a broad spectrum of different sources to identify a longlist of new and emerging technologies to be considered under the study.

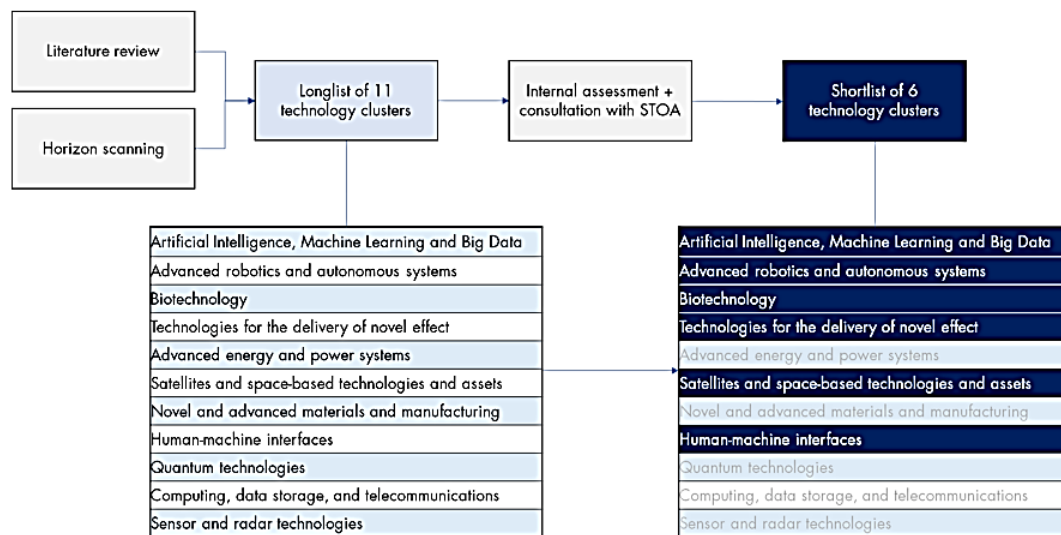
On the basis of the scoping activities, horizon scanning and literature review, the study team synthesised all data captured and categorised the technologies assessed in the reviewed sources as likely to shape the future battlefield within 11 technology clusters.² Six of those technology clusters were subsequently shortlisted for further in-depth examination and comparative analysis on the basis of internal analysis and consultations with STOA. This consultation considered two selection criteria, namely the likelihood of adoption and the extent of expected impact of the technology cluster in the battlefield context in the 2040 timeframe.³ Figure 1.2 captures the technology selection process.

¹ RAND Europe's Centre for Futures and Foresight Studies (CFFS) enables RAND Europe to help a wide range of clients to navigate the uncertain space of science and technology developments and to explore and assess possible future implications of technological change across different sectors, including defence and security. The CFFS brings together deep expertise in futures research methods along with specialist sector knowledge to help our clients make robust decisions and plans in conditions of uncertainty.

² A list of S&T items identified through the horizon scanning exercise is included in Annex E.

³ This prioritisation process is further discussed in Section 3.1 and Annex A.

Figure 1.2 – Technology shortlisting and selected technology clusters



Source: RAND Europe analysis.

To characterise further the nature of relevant technological trends and impacts of the selected technology clusters, the study team conducted an in-depth analysis of each technology cluster through targeted literature reviews and expert and stakeholder interviews.⁴ This served to establish an in-depth understanding of: 1) the relevant trends and potential impacts of each technology cluster, including relevant technological advances and future trends; 2) the potential impacts of the technology on the future battlefield, opportunities and challenges for European defence; and 3) any relevant enablers and barriers for future adoption. Findings from this analysis are presented in **Chapter 3** of this report.

To make a comparative assessment of the various impacts of the technology clusters, the study team hosted an expert and stakeholder workshop using the RAND-developed systematic technology reconnaissance, evaluation and adoption method (STREAM), which is further explained in **Annex B** of this report.⁵ Through the STREAM approach, the workshop gathered expert and stakeholder perspectives on the potential impact and future uptake of the selected technology clusters. This included a series of quantitative scoring assessments of: 1) the technology clusters with regard to their potential impact on EU Member States' military capability; 2) the ability of the EU to fulfil the objectives of the common security and defence policy (CSDP); and 3) the overall nature of future battlefield dynamics.

Participants were also asked to consider the relevance of potential technical, organisational, commercial, regulatory and other barriers to implementation that may impact the scale or pace of adoption of the technology clusters by EU Member State and potential state and non-state adversaries. **Chapter 4** of this report provides a high-level overview of findings from the comparative analysis, with further details on the quantitative findings included in **Annex C**.

To validate and provide further granularity to emerging findings regarding the implications of emerging technologies for European defence and identify relevant policy options, two internal workshops gathering RAND Europe experts were held. The workshops were designed to analyse

⁴ Annex B provides further details on the literature review and stakeholder engagement process and provides a list of interviewees.

⁵ Annex B also provides a list of workshop participants.

data gathered over the course of study activities and generate cross-cutting insights, as well as identify possible areas for future work and intervention.

1.3.2. Limitations

A number of caveats, limitations and assumptions should be considered in relation to the activities and findings presented in this study:

- **Targeted focus on a non-exhaustive list of technology clusters.** While the study is aimed at identifying and characterising the potential impacts of new and emerging technologies for European defence and the future battlefield at large, it focuses on a shortlist of six technology clusters. These technology clusters were identified in existing literature as well as through consultations with STOA as having the greatest potential impact on the future European defence context out to 2040. While the limited timeframe and resource constraints required a focused approach of the study on a selected number of technology clusters, it is recognised that other existing or hitherto underdeveloped technologies may also have a significant impact in this context. Section 3.3 provides an overview of some of these technology trends.
- **Heterogeneity of the technology clusters.** Workshop discussions as well as interviews conducted with experts and stakeholders highlighted the significant breadth and heterogeneous nature of technology clusters considered within the study. Experts consulted noted that, to a degree, this posed a challenge for generating insights on future trends and potential impacts with an adequate level of nuance. Where targeted literature reviews and expert interviews informing the in-depth technology assessments provided relevant data, the potential differences between different technologies *within* each technology cluster is highlighted throughout this report.
- **Robustness of quantitative insights of the STREAM workshop.** The expert STREAM workshop gathered a limited number of experts, with a total of 14 participants, excluding the study team. As such, quantitative insights stemming from this activity should be reviewed and understood in the context of the broader qualitative insights generated and discussed in the context of the study and report. Additionally, the findings should be interpreted with the participants' expertise and experience in mind, which, in this case, encompassed mainly the strategic impacts of new and emerging technologies in security and defence.
- **Literature review and consultation activities.** Recognising the significant breadth of the existing research base regarding the potential impacts of new and emerging technologies, and due to the project's timeframe and resource constraints, the study draws on insights from a selected number of literature sources. The study team addressed challenges stemming from the ability to engage only with a limited volume of sources by prioritising most up-to-date sources and triangulating literature review findings with insights from stakeholder engagement activities.
- **Future uncertainty.** The purpose of this study is to identify future trends in potential impacts of emerging technologies on the battlefield out to 2040. Given the pace of technological change and the inherent degree of uncertainty surrounding the future use and performance of new technologies and battlefield dynamics, the analysis and findings presented in this study should not be interpreted as predictions of specific future advances and scenarios. Rather, they should offer insights into the main trends, opportunities and challenges to allow relevant stakeholders to navigate and manage the complexity and uncertainty of technological change and design relevant flexible, forward-looking policies and investment strategies.

1.4. Structure of this report

Beyond this introductory chapter, this document features three additional chapters:

- **Chapter 2 – Evolving policy context and future strategic environment** – presents the trends and drivers expected to shape the future battlefield, as well as an overview of the policy landscape as regards European defence and technology innovation.
- **Chapter 3 – Overview and assessment of new and emerging technologies shaping the 2040 battlefield** – provides an in-depth overview of selected technology clusters considered under the study, including relevant emerging and potential future technological trends, as well as possible opportunities and challenges for European defence stemming from these.
- **Chapter 4 – Findings, implications and policy options for the EU** – presents key findings from the study stemming from a cross-cutting analysis of results, and formulates policy options for consideration by EU stakeholders and institutions.

The core report is accompanied by a full bibliography and five technical annexes:

- **Annex A** provides an in-depth discussion of the EU policy and regulatory landscape for defence and new and emerging technologies, building on insights from Chapter 2 of the main report.
- **Annex B** provides a detailed overview of the study methodology and research approach.
- **Annex C** provides a detailed overview of the quantitative findings and insights generated through the STREAM workshop, complementing the high-level summary included in Chapter 4 of the report.
- **Annex D** presents a copy of expert and stakeholder engagement materials employed for interviews and workshop activities over the course of the study.
- **Annex E** presents the full technology longlist identified through the study's horizon scanning exercise.

2. Evolving policy context and future strategic environment

This chapter provides an overview of the political, social, economic, environmental and technological trends defining the evolving strategic context out to 2040 (Section 2.1). The chapter also presents an overview of the evolving EU policy and regulatory context for addressing the opportunities and challenges provided by new and emerging technologies, particularly in a defence context (Section 2.2). A more detailed discussion of these topics is included in **Annex A**.

2.1. The evolving strategic environment

In the last decade, the global and European security environment saw a number of strategic, political, economic and technological trends consolidating and leading to greater instability and conflict.⁶ In particular, following almost two decades of relative stability in its neighbourhood, the EU was confronted with significant security challenges. Countries in its eastern neighbourhood faced a range of security threats and vulnerabilities in the military, economic, political and energy spheres. Further, the failure of a number of states across the southeastern Mediterranean region, the Sahel and sub-Saharan Africa generated a series of conflicts, crises and ungoverned spaces in which instability could breed and have further impacts on the European stage.⁷

Over the next two decades, the strategic environment is expected to be further influenced and shaped by a range of trends that will also have repercussions for the characteristics and dynamics of the future battlefield. These trends may be categorised as political, societal, economic, environmental or technological in nature. The next sections provide a thematic overview of factors and drivers expected to influence the future strategic environment. These trends were identified through a targeted review of literature on future trends and clustered in thematic groups to facilitate their discussion. Trends have been organised according to political, societal, economic, environmental and technological thematic clusters. For each cluster, the chapter provides an overview of the main drivers and factors identified by the study team and expected to have an impact on future developments, including possible implications from a defence and future battlefield standpoint. This overview captures findings from the scoping literature review conducted within WP1 (Scoping and framing) part of the study.

⁶ See European Commission (2017a).

⁷ See European Commission (2017a).

Table 2.1 – Thematic trends and factors that could contribute to shaping the 2040 battlefield

Thematic cluster	Relevant trends and factors	Section
Political	<ul style="list-style-type: none"> • Redistribution of global geopolitical and geostrategic power • Increasing great power competition and emergence of novel geopolitical rivalries • Rising influence of non-state actors and weakening state sovereignty • Growing nationalism and populism coupled with increasing public discontent 	2.1.1
Social	<ul style="list-style-type: none"> • Asymmetric demographic change and population growth • Asymmetric decline in fertility rates and population 'aging' • Urbanisation, asymmetric population growth in small-to-medium-sized cities • Increasing polarisation and fracturing of societies • Backlash against empowerment of women and minority groups 	2.1.2
Economic	<ul style="list-style-type: none"> • Increasing interconnectedness in global financial and economic systems • Increasing global inequalities • Shifting workforces and diminishing productivity gains • Decrease in economic opportunities and increase in youth unemployment • Trade nationalism and protectionism • Intensifying competition over natural resources and increasing energy consumption 	2.1.3
Environmental	<ul style="list-style-type: none"> • Environmental, economic and political impacts of climate change • Increasing water and food scarcity, intensifying competition over resources and changing migratory flows • Higher risks of infectious diseases and decreased capacity to address global health risks • Increasing occurrence of natural disasters • Increasing risk to cities and coastal areas from rising sea levels 	2.1.4
Technological	<ul style="list-style-type: none"> • Increased social, economic and military reliance on ICT networks • Rapid rate and increasing complexity of technological innovation • Democratisation of technology • Decreasing state monopoly on technology development vis a vis non-state actors (including MNCs) • Increased reliance of defence on commercial technology 	2.1.5

Source: RAND Europe analysis.

2.1.1. Political trends and factors

Out to 2040, several domestic and inter-state political trends and factors are expected to shape the international security and strategic environment and thus influence the future battlefield. Such political trends include structural political developments in the form of redistribution of global

geopolitical and geostrategic power.⁸ Redistribution is likely to include a shift in global balance of economic and military power towards Asia through trends such as the rise of China and other states in the Indo-Pacific region.⁹ Increasing great power competition and emergence of novel geopolitical rivalries, particularly in the Indo-Pacific, are also frequently identified as likely developments.¹⁰ Such rivalries may contribute to the spread of an increasing range of lethal, disruptive technologies, increasing the risk of wide-spread societal disruption.¹¹

Further to the redistribution of global geopolitical and geostrategic power, the role of the state in international politics may diminish. Correspondingly, the role and influence of non-state actors including non-state armed groups and multi-national corporations (MNCs) is likely to increase.¹² As such, a broader range of actors ranging from small grassroots movements to large well-connected organisations is likely to present a challenge to states in relation to national and international governance. The democratisation of technology may further expand the range of players who may attempt to block or otherwise pose a challenge to political action.¹³

Further to these structural political trends and developments in the international geopolitical and geostrategic environment, national political developments may also have a significant impact on the future battlefield. Growing nationalism and divergent threat perceptions at the national level are likely to correspond to increasing potential for confrontation and conflict as well as challenge established international governance structures for the management of international crises. Populism and nationalism may also be increasingly used to influence and mobilise the public.¹⁴ Public discontent and increasing demands on governments to deliver security and prosperity in an increasingly contested international environment may also challenge existing national and international governance frameworks.

Increasing global interconnectedness and connectivity, as well as polycentrism (i.e. the development of a global system that contains many different centres of political authority, influence, or control) are likely to present further challenge to global governance. Amid weak economic growth, increasing global connectivity may incentivise increasing tensions within and between societies; while a reliance on 'seamless and ubiquitous connectivity' may increase the vulnerability of information networks and critical national infrastructure to kinetic or non-kinetic disruption.¹⁵

2.1.2. Social trends and factors

A number of social and societal trends will complement the above-described political developments in transforming global governance and the global strategic environment out to 2040. These trends include asymmetric demographic change in the form of population growth, with current estimates predicting the global population to reach 9.7 billion in 2050.¹⁶ This population growth is likely to be concentrated in some regions more than others, with largest population growth expected among African, Middle Eastern, Central and South Asian countries.¹⁷ Further asymmetries are likely to be

⁸ See NATO (2017).

⁹ See Cohen et al. (2020a).

¹⁰ See Cohen et al. (2020a).

¹¹ See NIC (2017).

¹² See UK MOD (2017).

¹³ See NIC (2017).

¹⁴ See Cohen et al (2020a), TRADOC G-2 (2017).

¹⁵ See NATO S&T (2020).

¹⁶ See UN (2019).

¹⁷ See NATO (2017), UK MOD (2017).

caused by declining fertility rates and increasing population 'aging', with wealthy Western societies disproportionately affected.¹⁸

In addition to uneven population growth, increasing urbanisation is likely to define the structural features of future societies and, consequently, the nature and dynamics of conflict out to 2040.¹⁹ Two-thirds of the global population are expected to live in cities by 2030, with small-to-medium-sized cities growing particularly fast in population.²⁰ Where cities, particularly those of small and medium size, have insufficient access to capital and resources to manage increase in population growth and establish or strengthen governance structures and institutions, this may present significant security challenges and potentially lead to instability and conflict, as well as environmental degradation.²¹

Increasing polarisation and the trends of national and international governance described above are likely to compound an increasing fracturing of societies. Western societies are identified as particularly vulnerable to the effects of polarisation. While polarisation may emerge through political, social as well as economic denominators, factors such as unemployment, lack of economic opportunities, asymmetric demographic change or a backlash against the increased empowerment of women and minority groups may combine to cause an increased risk of civil unrest.²²

2.1.3. Economic trends and factors

Globalisation has, and is, likely to continue to produce not only political and societal changes, but also shifts in economic power whilst intensifying international economic integration. This is likely to further enhance global interconnectedness and connectivity in global financial and economic systems. In conjunction with other wider shifts in the global economy, globalisation and intensifying interconnected may produce further social and political backlash in the form of increased populism and anti-globalisation, as well as economic nationalism and protectionism.²³

Societal trends, such as ageing populations, intersect with economic trends in the form of shifting workforces and diminishing productivity gains in major global economies. Out to 2040, such trends may, in conjunction with weak economic growth, produce novel tensions and potential conflict dynamics through the reduction of economic opportunities and increasing youth unemployment.²⁴ Rising powers such as China, may also face slowing economic growth which may, consequently, produce intensifying economic pressures on the regime and incentivise a more aggressive pursuit of key foreign policy and strategic interests.²⁵ Among Western countries, slowing economic growth may also produce pressures on defence budgets that may further influence how emerging threats are managed on the future battlefield.²⁶

The economic impacts of climate change may also intensify tensions over natural resources and increase global inequalities, further compounding the trends described above, which may result in increased instability and likelihood of conflict.²⁷ Significant and periodic rises in global energy consumption – expected to increase by 1.7% annually, predominantly in rising economies – may

¹⁸ See NIC (2017).

¹⁹ See Cohen et al. (2020b).

²⁰ See UN (2018).

²¹ See Gaub (2019), UK MOD (2017).

²² See NATO (2017).

²³ See NATO (2017).

²⁴ See NIC (2017).

²⁵ See Cohen et al. (2020a).

²⁶ See NATO (2017).

²⁷ See UK MOD (2015).

also contribute to increasing environmental degradation due to corresponding rises in greenhouse gas emissions, exacerbating the future economic fallout of the changing climate.²⁸

The role of national governments and states may also be challenged with regard to providing economic governance and managing new and potential future threats in relation to financial and economic trends. The rise of alternative currencies, including cryptocurrencies, represents one such trend, with challenges in relation to the ability of governments to freeze financial assets or impose economic sanctions already emerging in today's strategic environment.²⁹

2.1.4. Environmental trends and factors

As described in the previous sections, environmental trends are likely to be the causative factors for many wider societal and political transformations. Out to 2040, climate change is likely to result in increased occurrence of natural disasters, food and water scarcity, as well as rising sea levels and the physical destruction of urban centres and coastal areas.³⁰ Rising temperatures may also have significant strategic effects, with reduced economic productivity leading to weakening governance structures and exacerbating existing tensions among populations (e.g. along ethnic or sectarian divides). This may particularly concern the future of conflict in regions where tensions related to the distribution of natural resources are already present, such as the greater Middle East region and East Africa.³¹

In combination with population growth, increasing food and water scarcity as well as environmental degradation may also result in increasing risk of famine and disease.³² Increasing levels of international travel in combination with poor or degrading health infrastructure may make infectious diseases and other global health challenges arising out of climate change more difficult to manage.³³ Such trends may, in turn, produce further secondary effects such as increase in global migratory flows, social unrest and instability, and ultimately increase the risk of wide-spread conflict.

Resource shortages and water scarcity may also alter the types of operations Western and European militaries will likely engage in. Climate change may for example create greater demand for humanitarian assistance and disaster relief (HADR) operations, thereby transforming the role of the military and changing its future value proposition.³⁴ Exploration into remote and challenging environments for natural resources may also result in the need for military engagement to protect such exploration areas as well as relevant transportation and communication networks.³⁵

The effects of environmental trends on the future strategic and operational context also include various direct impacts on the military and service members fighting on the future battlefield. Rising temperatures may, for example, pose serious health risks to military personnel as well as produce maintenance challenges for military bases and capabilities.³⁶ The need to operate in remote areas or extreme environments may also increase the need for technologies for human physical or cognitive advancement, thereby enhancing the significance of such technologies on the future battlefield.

²⁸ See Gaub (2019).

²⁹ See NIC (2017), Van Woensel and Archer (2015).

³⁰ See Gaub (2019).

³¹ See Cohen et al. (2020b).

³² See UK MOD (2015).

³³ See NIC (2017).

³⁴ See NATO (2017).

³⁵ See UK MOD (2015).

³⁶ See Cohen et al. (2020b).

2.1.5. Technological trends and factors

Technology is a key driver for exponential change in the world, likely to result in 'game-changing' developments for society. Advanced technologies, including the Internet of Things (IoT), advanced manufacturing, robotics and Artificial Intelligence (AI) present considerable opportunities for both economic growth in Europe and the ability to address many contemporary national and international governance challenges.³⁷ Many new and emerging technologies are also integral to the defence sector and may present operational benefits to the armed forces and more efficient processes in defence more widely (e.g. through automating and optimising logistics systems).³⁸

The scope of opportunities associated with technological advancement are incentivising a rapid rate of technological innovation and democratising technology (i.e. access of an increasing number of actors to technology). The increased access to emerging and potentially disruptive technologies by state and non-state actors may produce a range of challenges and potential threats for defence. More broadly, the strategic environment out to 2040 is likely to feature decreasing technology monopoly of state powers vis-à-vis non-state actors, including MNCs, as well as a predominance of the private sector in technological innovation, enhancing the reliance of defence on commercial technology.

In addition to the many benefits provided by emerging technology, advanced technologies present numerous challenges for the management of the future battlefield. Further to increasing technological dependencies and the democratisation of potentially disruptive technologies, the electrification and digitalisation of global governance as well as increased social, economic and military reliance on ICT networks also exacerbate the risk of cybersecurity incidents. These risks may be intentional or accidental, but all have the potential to incur a serious disruption to essential services. This risk is further compounded by the complexity and rapid pace of technological developments, as well as the high levels of uncertainty about the pace and nature of future technological advances.

2.1.6. Characteristics and views on the possible future battlefield

The various political, social, economic, environmental and technological trends discussed in the previous section may shape the future battlefield in different ways. The interaction of the above-described trends and the associated impacts on the characteristics of the future battlefield can be categorised by several key factors, including: adversaries, mission types, terrains, weather and climatic conditions and timeliness requirements. Collectively, these factors shape the spectrum of operations in which new and emerging technologies may be utilised by the European armed forces.

³⁷ See European Commission (n.d.a).

³⁸ See EDA (2017); EDA (2020).

Table 2.2 – Potential characteristics of the future battlefield

Factor	Relevant trends out to 2040
Adversaries	<ul style="list-style-type: none"> Continued presence and relevance of high-end state peer and near-peer adversaries, state-sponsored hybrid adversaries, and low-end non-state irregular forces Increasing relevance of proxy warfare to the future battlefield Increasing role of non-state actors with technology used to augment low-end capabilities to increase lethality and mobility
Mission type	<ul style="list-style-type: none"> Combination of national (territorial) defence operations in a national or multi-national setting, expeditionary counterterrorism and counterinsurgency operations, and expeditionary peacekeeping, peace enforcement and conflict resolution interventions
Terrain	<ul style="list-style-type: none"> Impacts of climate change and environmental degradation on urban terrains Increasing prevalence of urban warfare and operations in complex urban environments as a result of urbanisation
Weather and climatic conditions	<ul style="list-style-type: none"> Requirement to operate in increasing extremes (e.g. temperature, humidity) Prevalence of hot and dry or extreme hot and dry environments for expeditionary operations
Operational pace	<ul style="list-style-type: none"> Increased requirement for military forces to react rapidly to regional and global events as result of globalisation, including rapid deployments at long range and short notice Need for rapid decision-making and information-sharing

Source: RAND Europe analysis.

Adversaries

The European armed forces may face a range of adversaries on the 2040 battlefield across the spectrum of operations. These can be categorised as:³⁹

- High-end state peer or near-peer adversaries, largely organised in larger-size hierarchical formations with centralised command and control (C2) and employing sophisticated high-end conventional and non-conventional capabilities;
- State-sponsored hybrid adversaries, with a wide spectrum of capabilities including small arms and standoff capabilities deployed in decentralised, conventional and unconventional lines of operation;
- Low-end, non-state irregular forces, with decentralised C2 structures and formations, largely utilising low-end capabilities with potential exploitation of dual-use technologies to increase lethality and mobility on the battlefield.

As discussed in the previous sections, non-state actors are likely to have an increasing influence in the future strategic environment, with hybrid adversaries and irregular forces likely featuring more prominently on the future battlefield. This may include an increasing use of proxy forces and increasing prevalence of 'wars by proxy'.⁴⁰

³⁹ See Johnson (2016).

⁴⁰ See Kepe et al. (2018).

Mission

The 2040 battlefield may be characterised for EU MS Armed Forces by the undertaking of a range of missions in line with the different strategic and national security priorities. The various mission types can be categorised as:

- National defence, including territorial defence in a national or multinational context
- Expeditionary counterterrorism and counterinsurgency operations, including EU-led CSDP missions
- Expeditionary peacekeeping, conflict prevention and peace enforcement missions, including EU-led CSDP missions.

New and emerging technologies may be of varying utility depending on the mission type and the corresponding capability requirements.

Terrain

Environmental trends and climate change may significantly shape the natural physical topography of the future battlefield. It is likely that future battlefield will span different terrains within extremely remote areas and environmental extremes.⁴¹ The effects of climate change, particularly on coastal areas, may produce various impacts for future capability requirements and the extent to which emerging technologies are utilised in various domains. For example, the maritime and air domains may gain strategic importance due to increased urbanisation in coastal areas and increasing reliance on unmanned aircraft.⁴² Additionally, phenomena such as rising sea levels, risks of flooding and rising temperatures may cause disruption to military installations and civilian infrastructure impeding the movement of personnel and equipment.⁴³

Perspectives from existing literature also highlight that man-made urban areas are likely to be an increasingly central environment for military operations in Europe and globally in light of increasing urbanisation. As such, conflict and battlefield interactions are increasingly likely to take place in densely populated or restricted urban areas, with restrictions for intelligence, observation and movement of forces.

Weather and climate

The future battlefield may span various weather and climatic conditions, from extreme cold to extremely hot and dry environments. The different mission types featuring on the 2040 battlefield may correspond with different climatic environments. For example, territorial defence missions may be carried out predominantly in intermediate to intermediate cold environments. In contrast, expeditionary operations may take place in a wider range of climatic conditions, particularly hot dry as well as extreme hot dry climatic contexts (e.g. the Mediterranean, Sahel, Central Africa). The effects of climate change and environmental degradation indicate that future uses of new and emerging military technologies may be influenced by the need to operate in increasingly extreme environments (e.g. high or low temperatures, high humidity).

Operational pace

Capability requirements in the future battlefield environment may be characterised by the timeliness for the availability of specific capabilities. As the pace and complexity of decision-making may increase with the integration of new and emerging technologies such as AI on the battlefield,

⁴¹ See Brosig et al. (2020).

⁴² See Kepe et al. (2018).

⁴³ See Cox et al. (2020).

the timeliness factor may be key in ensuring efficiency and operational effectiveness on the battlefield.

As noted in existing research on future strategic trends, increased globalisation and interconnectedness may increase the requirement for rapid response and the ability of military forces to respond to rapidly unfolding regional and global developments.⁴⁴ The future battlefield may therefore include requirements for rapid decision-making and information sharing as well as capabilities for real-time situational awareness and capability to deploy forces at long range at a short notice.⁴⁵

2.2. The EU regulatory and policy context for defence and new and emerging technologies

2.2.1. The changing role and ambition for the EU as a defence and security actor

Increased recognition of the trends discussed in Section 2.1 of this report has led in recent years to a sustained call for a stronger EU in the areas of security and defence at the highest political levels. At a practical level, commitments to a greater role for the EU in the areas of common security and defence translated into a number of concrete policies that have a direct impact on European defence. These are discussed in the following paragraphs.

The EU Global Strategy puts the EU on a path towards strategic autonomy and the development of full spectrum defence capabilities. Following a strategic review of changes in the global environment conducted by the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP) in consultations with EU MS, the European Union launched its 'Global Strategy for European Foreign and Security Policy' (EU GSS) in June 2016. The EU GSS recognises that ongoing crises and conflicts in the EU's neighbourhood pose a threat to the Union. As such, the EU GSS sets out an ambitious vision of policies, instruments, and capabilities towards achieving strategic autonomy.⁴⁶ To achieve its vision, the EU GSS calls for collective investment into the development of a credible, responsive and interlinked Union. Among other actions, it stresses the urgency of investment in security and defence and the importance of developing full spectrum defence capabilities to respond to external crises and guarantee the Union's safety.

The shift in the EU approach for security and defence towards enhanced integration was also displayed in the adoption of initiatives to tackle hybrid threats.⁴⁷ In parallel to the process leading to the adoption of the EU GSS, the events of the 2014 Ukrainian crisis highlighted the growing challenge posed both internally and externally to the EU by the increasing use of hybrid threats and tactics by state and non-state actors. In response to the growing number of such threats in the European and global context, with support from the European Defence Agency (EDA) and MS, the HR/VP designed a 'Joint Framework on countering hybrid threats'.⁴⁸ The Framework is to be considered part of EU efforts towards developing a more integrated approach to security and

⁴⁴ See MOD (2015).

⁴⁵ See Kepe et al. (2018).

⁴⁶ See EEAS (2016).

⁴⁷ The EC defines hybrid threats as 'a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare', European Commission (2016a). Actors employing hybrid tactics seek to exploit the vulnerabilities of a target to generate uncertainty and hinder decision making processes.

⁴⁸ See European Commission (2016a).

defence. As such, the framework calls for close coordination of its implementation alongside other EU frameworks and efforts.⁴⁹

Amid crises and instability, a new impetus was also given to joint capability development and cooperation with NATO. The 2016 *Joint Declaration* by the President of the European Council, the President of the European Commission, and the Secretary General of NATO gave a new impetus to EU-NATO cooperation.⁵⁰ This came in recognition of the need to find new means of cooperation, as well as an enhanced level of ambition in response to the common challenges faced by both organisations in the current security context.

Furthermore, following approval of the EU GSS, sectoral plans for implementing the Strategy were prepared by HR/VP with support from relevant stakeholders. In November 2016, an 'Implementation Plan on Security and Defence' was approved, placing significant emphasis on investing and developing defence capabilities through collaborative approaches for both military and civilian aspects of CSDP. Overall, three key tenets underpin the Implementation Plan focusing on Security and Defence:⁵¹

1. Responding to external conflicts and crises when they arise;
2. Building the capacities of partners;
3. Protecting the EU and its citizens through external action.

The Implementation Plan translates these into a number of concrete actions, including:⁵²

1. Work to deepen defence cooperation to identify the capabilities that are needed, notably through a review of the EDA Capability Development Plan (CDP);
2. Establish the Coordinated Annual Review on Defence (CARD);
3. Explore the possibility of a Permanent Structured Cooperation (PESCO);
4. Establish a new permanent operational planning and conduct capability within the European External Action Service for non-executive military missions, the Military Planning and Conduct Capability (MPCC);
5. Review priorities and increase responsiveness of civilian missions;
6. Strengthen cooperation with UN, NATO, African Union and the Organization for Security and Co-operation in Europe (OSCE).

Finally, as indicated in the EU GSS, it is necessary for the European defence industrial base to be able to meet the EU's current and future security needs, contributing to the achievement of strategic autonomy for the EU towards the proposed vision of strategic autonomy. Amid shrinking public spending, the EU and its MS must focus on creating conditions conducive to further defence cooperation, maximising the output and efficiency of defence spending.⁵³ To this end, the European Defence Action Plan (EDAP) launched in 2016 builds on the vision of the EU GSS by enabling the sustainment and growth of the European defence industrial base. In this regard, among the initiatives implemented as part of the EDAP, the European Defence Fund (EDF) stands out, due to its goals to coordinate, supplement and amplify national MS investments in collaborative defence.

⁴⁹ See European Commission (2016a).

⁵⁰ See NATO (2016).

⁵¹ See Council of the European Union (2016).

⁵² See Council of the European Union (2016).

⁵³ See European Commission (2016a).

2.2.2. EU focus on innovation and new and emerging technologies with a disruptive potential

The EU policy and regulatory context on emerging technologies in security and defence is currently shaped by a comprehensive agenda on innovation and harnessing the benefits of digital and advanced technologies, while proactively guarding against possible risks. The European Commission spearheaded this agenda through the 2011 adoption of the 'Innovation Union' a flagship initiative of the Europe 2020 strategy.⁵⁴ More recently, the EU's agenda on innovation and emerging technologies has seen advancement via the April 2019 'digital package'.⁵⁵ This package detailed the Commission's recommendations for the EU approach towards harnessing the benefits of advanced technologies, including:

- A European data strategy⁵⁶
- Policy options for human-centric development of AI⁵⁷
- Graphene Flagship, focusing on transferring graphene innovation into commercial applications⁵⁸
- Quantum Flagship, supporting the development of quantum research and innovation activities.⁵⁹

These initiatives constitute part of a broader effort by the European Commission to foster Europe's technological sovereignty, a concept explained as 'having European technological alternatives in vital areas where [it is] currently dependant [on others]'.⁶⁰ Such technological sovereignty is envisioned via cooperation in 'areas of strategic importance such as defence, space, and key technologies such as 5G and quantum [computing]', facilitated through the European Single Market, and contributing to Europe's gradual emergence as 'a digital, technological and industrial leader'.⁶¹ The EU also hopes that emerging as a key digital player will project European values onto the international stage, inspiring more countries to pursue similar digital governance models.⁶²

Recent initiatives also reflect the European Commission's promotion of the concept of responsible innovation (RI), often discussed in relation to the wider concept of Responsible Research and Innovation (RRI). Embedded primarily within the Commission's FP7 and Horizon 2020 programmes, the RI and RRI concepts emphasise the idea of innovation as a 'transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability, and societal desirability of the innovation process and its marketable products'.⁶³ Along with other definitions of RI and RRI, this acknowledges the uncertainty inherent in innovation processes, as well as a corresponding need for transparent and cautious approaches to research and innovation across all policy areas.⁶⁴

⁵⁴ See European Commission (2011).

⁵⁵ See European Commission (2020a).

⁵⁶ See European Commission (n.d.a).

⁵⁷ See European Commission (2020c).

⁵⁸ See Graphene Flagship (n.d.).

⁵⁹ See Quantum Flagship (n.d.).

⁶⁰ See European Parliament (2019).

⁶¹ See European Parliament (2019).

⁶² See European Commission. (n.d.b).

⁶³ See Von Schomberg (2011).

⁶⁴ See Silfversten et al. (2017).

A food for thought paper published by a collection of EU MS⁶⁵ recognised the need for EU action on the digitalisation of defence,⁶⁶ highlighting the central role of digitalisation and advanced technologies, particularly AI, for future capability development. The key topics for discussion on future EU action set out in the paper are further outlined in **Annex A**.

Current efforts driving the EU's digital agenda were preceded by various initiatives addressing innovation and emerging technologies in EU's foreign and security policy. In May 2018, for example, the EEAS and High Representative Federica Mogherini launched the Global Tech Panel, gathering key industry, private sector, academia and civil society stakeholders to 'foster new types of cooperation between diplomacy and technology'.⁶⁷ Intended to serve as a forum to discuss practical steps to address challenges of innovation and technology for foreign and security policy, the Global Tech Panel has focused on four initial work streams:⁶⁸

- Regulating Lethal Autonomous Weapons Systems (LAWS) in relation to international security and law.⁶⁹ LAWS have been described as 'a top priority file where the EU is seeking to promote a common understanding on a global legal and ethical framework'.⁷⁰
- Increasing economic competitiveness through digital technologies and innovation, while boosting digital skills and jobs for human development.⁷¹ The panel's work in this area has corresponded with the EU's Digital4Development policy framework.⁷²
- Examining the global ethics aspects of applied machine learning in the fields of surveillance, justice and security.
- Discussing the 'future frontiers in cyber security'.⁷³

Enhancing cooperation in the security and defence-related aspects of the Panel's agenda connects to broader efforts to strengthen European cooperation on security and defence.

These efforts show that there have been considerable measures taken towards strengthening European cooperation on defence and security, including defence innovation and managing the impact of advanced technologies. For example, out of the 17 new EDF projects announced by the European Commission in June 2020, three projects have been dedicated to disruptive technologies, corresponding to 8% of the EDF.⁷⁴ The new initiatives under the EDF build on previous programmes oriented towards strengthening European capability in innovative technologies within the defence context under the Preparatory Action for Defence Research (PADR) and European Defence Industrial Development Programme (EDIDP).⁷⁵

Existing research, however, indicates a number of challenges for EU action in this area. Military uses of AI have, according to Franke, received 'too little attention' among EU MS⁷⁶. Despite the creation

⁶⁵ These were Finland, Estonia, France, Germany and the Netherlands.

⁶⁶ EU2019.fi (2019a).

⁶⁷ See EEAS (2018a).

⁶⁸ See EEAS (2018b).

⁶⁹ See EEAS (2018c).

⁷⁰ See EEAS (2019).

⁷¹ See EEAS (2018c).

⁷² See Viola (2017).

⁷³ See EEAS (2018b).

⁷⁴ See European Commission (2020b).

⁷⁵ See EDA (2017).

⁷⁶ See Franke (2019).

of new defence innovation funding streams, uncertainties remain around the future availability of EU defence funding and support for the EDF.⁷⁷

2.2.3. Summary

Historical and present-day developments in the strategic and operational environments indicate a number of takeaways concerning the future battlefield and possible implications for its associated capabilities requirements. The future battlefield will likely require EU MS Armed Forces and allies to operate in a wide range of terrain, weather and climate types including a need to adapt to increasing extreme conditions brought about by ongoing climate change and environmental degradation. Furthermore, in addition to a diversification in the typology of operational environments, future missions and operations will also vary in their purpose and requirements, ranging from counter-insurgency operations and other forms of asymmetric conflicts, to area control and denial and high-intensity manoeuvre warfare. This will require the development of multi-purpose capabilities, integrating new and emerging technologies and leveraging their potential as part of broader system of systems under new concepts of operations and doctrinal approaches. Technological advances and the proliferation of new systems, platforms and tools are also expected to raise challenges as regards interoperability, an aspect that EU MS will need to proactively manage as new technologies are deployed and embedded in the functioning and capabilities of their armed forces.

Technological advances, however, are unlikely to result in a full obsolescence of previous technologies and requirements. As such, military planners will be required to consider not only cutting-edge, high-end technologies but also the specific challenges and opportunities arising from the battlefield use of older technologies and analogue systems, or the combination of old technologies with novel tactics and capabilities. Furthermore, the impact of trends presented above may also result in a continued growth and diversification in sub-threshold activities. These could leverage the potential of new and emerging technologies in ways that will require addressing to ensure that such approaches cannot be employed to weaken or unravel the fabric of societies, institutions, and alliances upon which European MS build and rely on also in a defence context.

In this context, the European policy framework relevant to security, defence, as well as to innovation and new and emerging technologies has undergone significant changes and developments in the past decade. Overall, greater emphasis has been placed on the pursuit of strategic autonomy, including by means of developing greater autonomy, resilience, and superiority in the context of a wide array of military capability areas, as well as new and emerging technologies.

⁷⁷ See Wilkinson (2020).

3. Overview and assessment of new and emerging technologies shaping the 2040 battlefield

This chapter presents an overview of selected new and emerging technologies expected to significantly shape the nature of the future battlefield out to 2040. As discussed in Section 1.3, the technology clusters were selected through internal analysis of the data gathered through horizon scanning and the WP2 literature review and consultations with the STOA from a broader list of technology clusters. The internal analysis and consultations with STOA aimed at prioritising technologies based on the following factors:

- **Likelihood of adoption:** the extent to which a given technology cluster is expected to be widely used and adopted, or not, in the battlefield context in the 2040 timeframe.
- **Expected impact:** the extent to which a technology cluster is expected to significantly shape the future battlefield out to 2040, considering both the opportunities and challenges associated with the relevant technological advances.

Table 3.1 provides an overview of the shortlisted technology clusters.

Table 3.1 – Overview of key new and emerging technology clusters shaping the 2040 battlefield

Technology cluster	Definition
Artificial intelligence, machine learning and big data	Software technologies that are able to perform advanced computing to analyse and interpret large quantities of data.
Advanced robotics and autonomous systems	Technologies that constitute or enable the operation of unmanned vehicles with advanced capabilities, including in the area of operating without human supervision or control.
Biotechnology	Technologies that leverage biological systems or innovations in biological sciences to develop systems with advanced properties and levels of performance.
Technologies for the delivery of novel effect	Technologies, including weapons and sub-systems, that enable the delivery of novel kinetic and non-kinetic effect or the delivery of conventional effect in novel ways.
Satellites and space-based technologies and assets	Technologies that enable access to space or technologies that are space-based and facilitate terrestrial or space-based operations.
Human-machine interfaces	Technologies that facilitate human-machine interactions or human-machine teaming, including information transfer.

Source: RAND Europe analysis.


As previously discussed in Section 1.3, the nature and scope of impact of the prioritised technology clusters on the future battlefield was subsequently explored through targeted literature reviews and key informant interviews with technology experts.

The remainder of this chapter focuses on an overview and assessment of the potential impacts of individual technology clusters, including a discussion of relevant emerging and potential future technological trends, as well as key impacts on the future battlefield and associated opportunities and challenges for European defence. Chapter 4 then provides a comparative assessment of the technology clusters and discusses cross-cutting findings from the scoring exercise and workshop inputs.

3.1. Overview and assessment of individual technology clusters

3.1.1. Artificial intelligence, machine learning and big data

Figure 3.1 – Overview of the Artificial Intelligence, Machine Learning and Big Data technology cluster

 <h3>Artificial Intelligence, Machine Learning and Big Data</h3>	
Definition	Software technologies that are able to perform advanced computing to analyse and interpret large quantities of data.
Future trends	<ul style="list-style-type: none"> • Increasing maturity of AI and ML systems and ability to address ambiguous, complex situations and deal with asymmetric information • Advances in data science (e.g. advanced unsupervised 'deep learning' systems) and increased ability to learn from unstructured or unfamiliar data • Increased breadth of AI, ML and Big Data applications across public and private sectors
Key impacts on the future battlefield	<ul style="list-style-type: none"> • Opportunities to gain strategic advantage through information control and data access management • Increased speed of decision-making on the battlefield Increased stealth and rapid analysis capabilities for defensive systems • Increased challenges of attack attribution (e.g. AI-enabled cyber attacks)

Source: RAND Europe analysis.

Technology overview and future trends

While there is no universally accepted definition of AI, it generally refers to computer systems that can perform tasks with some degree of autonomy, underpinned by capabilities for data acquisition, interpretation of data, reasoning and information processing.⁷⁸ AI spans a wide range of systems with different levels of sophistication, autonomy and Technology Readiness Level (TLR). Such systems are commonly classified as:

- Artificial Narrow Intelligence (ANI), which includes systems that are able to autonomously perform a narrow range of task through pre-programmed competencies;
- Artificial General Intelligence (AGI), referring to systems that are able to replicate human intelligence and autonomously perform multi-functional capabilities through human-like learning, perception, understanding and functional competencies;
- Artificial Superintelligence (ASI), encompassing systems able to develop competencies that exceed human comprehension.⁷⁹

AI encompasses a range of different sub-systems and techniques, including Machine Learning (ML), which refers to systems able to perform supervised or unsupervised learning when exposed to training data.⁸⁰ AI and ML systems can generally be used to automate tasks or provide cognitive

⁷⁸ See AI HLEG (2019), Wong et al. (2020).

⁷⁹ See Joshi (2019).

⁸⁰ See van Duin and Bakhshi (2018). Supervised machine learning includes models that are developed to process and learn from labelled data only (i.e. data that is tagged with pieces of relevant information, such as name or type of an object). In contrast, unsupervised machine learning comprises algorithms that are able to learn from unlabelled data.

insight through the analysis of large quantities of data, or cognitive engagement (i.e. when a system engages or interacts with its environment, such as chatbots).⁸¹

Big Data refers to sophisticated data-gathering techniques and machine-based analytics (i.e. the gathering and processing of data), which can be used to provide insight from large quantities of structured or unstructured data.⁸²

Though AI is already present in various forms and applications on the contemporary battlefield, AI-based systems may significantly evolve out to 2040 in relation to the capabilities and maturity of AI. This includes increasing capacity of AI and ML systems to learn autonomously with little training data input and to 'cope with ambiguous and asymmetric information'.⁸³ Despite ongoing interest in the development of AGI, workshop participants noted that the adoption of AGI currently appears unrealistic in the 2040 timeframe.⁸⁴

Advances in data science are likely to drive significant improvements in computing technologies such as AI, ML and Big Data. This includes advances in the development of unsupervised 'deep learning' systems that are able to process and learn from unstructured and unfamiliar data, or AI techniques such as natural language processing (NLP) and computer vision.⁸⁵ An increasing interest in the uses of AI, ML and Big Data across the public and private sector, underpinned by the need to collect and process increasing amounts of data, are also likely to incentive increasing breadth of applications of such technologies.

Opportunities and challenges on the future battlefield

AI, ML and Big Data have numerous applications in security and defence, including providing decision support in contexts such as nuclear security.⁸⁶ AI, ML and Big Data may provide several potential general opportunities for defence:

- The control of information flows and access to information may provide a significant advantage to any actor in the context of the future battlefield. As such, AI, ML and Big Data systems present significant opportunities for EU MS to establish a strategic advantage in data access and management over a potential adversary as well as breaking through an adversary's Observe, Orient, Decide and Act (OODA) loop.⁸⁷
- At the strategic level, the capacity of AI, ML and Big Data for rapid data processing and inference may produce a qualitative edge for decision-makers. For example, strategic-level AI may support decision-making through challenging accepted wisdom concerning relationships between various factors relevant to strategy-making or identifying key vulnerabilities in an adversary.⁸⁸

⁸¹ See Davenport and Ronanki (2018).

⁸² See Patrizio (2018).

⁸³ See Payne (2018).

⁸⁴ RAND Europe workshop (October 2020).

⁸⁵ Deep learning refers to ML applications that carry out unsupervised learning methods (i.e. methods not relying on training through historic data), Babuta et al. (2018).

⁸⁶ See Geist and Lohn (2018).

⁸⁷ RAND Europe workshop (October 2020). The OODA loop represents an iterative feedback model representing four steps of decision-making processes, from an observation of information relevant to the decision-making process, filtering through the information to allow an actor to orient themselves on the information, deciding on an appropriate course of action, and acting on the decision.

⁸⁸ See Payne (2018).

- Through enabling autonomy, AI and ML bring opportunities for defence through increased stealth and rapid analysis for defensive action on the battlefield.⁸⁹
- AI can provide opportunities for improving organisational innovativeness and the adaptability of public sector organisations, including defence, to fast-paced changes in the socio-economic, geo-political and security environment.⁹⁰

In addition to these general opportunities, specific examples of AI, ML and Big Data military applications can be identified, particularly in the areas of ISR, decision-support, command-and-control and logistics.

The ability, however, of AI, ML and Big Data systems to rapidly process and make inferences from large amounts of data also indicate various challenges for future defence. The speed of decision-making may substantially increase in the event of wide-spread uses of AI and ML-enabled systems on the future battlefield. In particular, the employment of networked agents with autonomous decision-making abilities may enable 'extremely rapid sequential action, even in uncertain operating environments.'⁹¹

AI and ML are also being integrated across many offensive and defensive weapons and cyber-physical systems. This includes the integration of AI into offensive cyber capabilities, as well as advanced remote sensing, precision-guided munitions and hypersonic weapons.⁹² The integration of AI with advanced weapons systems, including systems based on biotechnologies and systems for the delivery of non-kinetic effects, could significantly advance the potency of weapons systems as well as their lethality and speed of decision-making concerning their deployment.⁹³

While AI may improve the ability of EU MS forces to establish an understanding of adversary actions and capabilities, AI may also challenge the attribution of attacks or hostile action.⁹⁴ AI applications to programming automation may, for example, lead to uses of AI-generated malicious code, which would be significantly more difficult to trace and attribute. When being used for covert purposes or influence operations, AI and ML may be used to create 'deep fake' images and videos or operation of sophisticated social media 'bots', challenging the ability of armed forces to navigate an increasingly complex information environment.⁹⁵

Future trends with regards to uses of AI on the future battlefield may be underpinned by the potential of AI to spark unmitigated arms race-like escalations in military AI, including AI-enabled weapons systems. Existing literature points to the inherent nature of military technology investments as creating situations of a security dilemma, fostering uncertainty and incentivising increased investment in increasingly autonomous systems resulting in an armament spiral.⁹⁶

While its development and adoption remains highly unlikely in the 2040 timeframe, if actualised, AGI would present additional and far-reaching challenges in the battlefield context as well as for societal resilience more broadly. This is due particularly to the uncertainty as to the alignment of an AGI agent with established human values and intentions, including ethical standards and commonly accepted norms of conduct. The ability of AGI to replicate human-like learning abilities may also drastically magnify the challenges associated with inexplicability of AI models, significantly reducing

⁸⁹ See Franke (2019).

⁹⁰ See Accenture (2018).

⁹¹ See Payne (2018).

⁹² See Johnson (2019), Johnson and Krabill (2020).

⁹³ RAND Europe interview (INT03, October 2020).

⁹⁴ RAND Europe workshop (October 2020).

⁹⁵ See Caldwell et al. (2020).

⁹⁶ See Franke (2019), RAND Europe interview (INT03, October 2020).

predictability and increasing the risk of accidental or maliciously-induced conflicts or collisions involving artificial agents.

Enablers and barriers for future adoption

Despite the significant opportunities that AI and ML may represent for defence, workshop participants noted that the limitations of AI and ML should not be disregarded. Despite cognitive and heuristic limitations of the human mind, humans may be naturally better pre-disposed to address certain scenarios within a battlefield context, including situations with high levels of uncertainty and new kinds of situations that require generalisation and application of transferrable heuristics.⁹⁷ Similarly, the technological maturity of current systems and the nature of current technological trends indicate that strictly digital systems may provide opportunities to automate certain defence-related tasks, allowing incremental gains in military operations rather than a truly decisive advantage in a battlefield context.⁹⁸ Technological advances and implementation of sensors represent an additional factor influencing future uptake and capability of AI and ML systems on the battlefield, due to the integral part of data in such systems.⁹⁹

Workshop discussions indicated that ethical concerns represent a significant barrier for future update of AI, ML and Big Data in battlefield contexts, though the extent of these concerns depends on the type of system as well as related practices. For example, AGI signals significantly greater ethical concerns due to higher levels of independence and autonomy from the decision-maker. Similarly, ethical concerns may arise not only from the nature of the technological system itself, but rather the practices through which such systems are applied, including e.g. predictive enforcement practices that may perpetuate pre-existing biases.¹⁰⁰ Such challenges may be exacerbated by two challenges associated with AI, ML and Big Data systems at large:

- Many AI and ML systems are designed as 'black boxes' – meaning that systems are frequently programmed so that the systems' inference and decision-making processes are incomprehensible to programmers themselves.¹⁰¹ This introduces significant political and ethical challenges in relation to accountability and liability.¹⁰² In defence environments, such challenges may exacerbate existing barriers to adoption of AI-based systems in relation to quality assurance, testing and accreditation requirements.
- Many AI and ML systems are also susceptible to reproducing or amplify biases present in training data. The political and ethical challenges associated with such biases have contributed to divestment of private sector stakeholders from certain AI and ML applications, such as facial recognition, and may also undermine public trust in AI and ML systems at large.¹⁰³

Several barriers also exist in the European context, including deficiencies in the innovation ecosystem and lack of incentives provided by European universities and research institutions, hampering innovation and R&D efforts.¹⁰⁴ The existing literature also highlights the fact that military applications of AI have largely been overlooked. This is despite an increasing interest in the European community for understanding the economic and societal implications of a wider uptake

⁹⁷ RAND Europe workshop (October 2020).

⁹⁸ RAND Europe workshop (October 2020).

⁹⁹ RAND Europe workshop (October 2020).

¹⁰⁰ RAND Europe workshop (October 2020).

¹⁰¹ See Bathee (2018).

¹⁰² See Franke (2019).


¹⁰³ See Franke (2019), RAND Europe interview (INT03, October 2020).

¹⁰⁴ RAND Europe interview (INT03, October 2020).

of AI technologies. More widely, literature on the military applications of AI has largely focused on the US, China and Russia.¹⁰⁵

3.1.2. Advanced robotics and autonomous systems

Figure 3.2 – Overview of the advanced robotics and autonomous systems technology cluster

 <h2>Advanced robotics and autonomous systems</h2>	
Definition	Technologies that constitute or enable the operation of unmanned systems with advanced capabilities, including in the area of operating without human supervision or control.
Future trends	<ul style="list-style-type: none"> • Advances in propulsion, precision take-off and landing, and navigation in remote and autonomous systems; • Increased breadth of functions performed by remote and autonomous systems, especially in Intelligence, Surveillance and Reconnaissance (ISR); • Advances in interoperability and swarm control;
Key impacts on the future battlefield	<ul style="list-style-type: none"> • Opportunities for rapid reaction, extended reach and coverage (e.g. in ISR), increased mission flexibility, precision-strike and reduced risk of collateral damage on the battlefield • Risk of proliferation of low-cost, off-the-shelf systems to non-state and hybrid adversaries

Source: RAND Europe analysis.

Technology overview and future trends

Advanced robotics refers to robotic systems that have 'superior perception, integrability, adaptability and mobility' allowing 'faster setup, commissioning and reconfiguration, as well as more efficient and stable operations'.¹⁰⁶ In relation to security and defence, advanced robotics is particularly relevant in relation to the design, production and operation of unmanned systems, including unmanned aerial vehicles (UAVs) and exoskeletons.¹⁰⁷

Advanced robotics relate closely to autonomous systems in that advanced robotic systems are increasingly able to perform functions with enhanced autonomy. Autonomous systems integrate advances in robotics with autonomy enabled by AI technologies, which enables autonomous systems to perform functions or tasks with varying degrees of human oversight or control. In military contexts, this includes systems with varying degrees of human control. Autonomous systems are thus commonly categorised as systems with humans either:

- 'In the loop': systems in which an AI can make autonomous decisions, including those relating to the deployment of lethal force, but with a human carrying out monitoring and supervision duties;¹⁰⁸

¹⁰⁵ See Franke (2019).

¹⁰⁶ See Kupper et al. (2019).

¹⁰⁷ Exoskeletons are wearable robotic 'suits' utilised for physical enhancement, including for soldiers in combat, Tucker (2018).

¹⁰⁸ See Wong et al. (2020).

- 'On the loop': systems in which an AI can make autonomous decisions, including those relating to the deployment of lethal force, but with a human carrying out monitoring and supervision duties;¹⁰⁹
- 'Out of the loop': systems in which an AI has extensive autonomous decision-making authority without human control or supervision. This includes decision-making authority in scenarios of lethal force deployment.¹¹⁰

Autonomous systems include a wide range of capabilities including aerial, ground, surface or underwater vehicle, as well as heterogeneous systems (i.e. networked systems of a variety of unmanned assets, including aerial, ground, surface or underwater vehicles) and autonomous swarms.¹¹¹

Robotic and autonomous systems are being improved in several ways, including through advances in propulsion, precision take-off and landing, and navigation capabilities. These advances are supported by the development of advanced computer vision systems and radar technologies. Integration of advanced sensor technologies in robotics and autonomous systems is likely to enable such systems to perform a greater range of functions, particularly with respect to ISR.¹¹²

Advances in vehicle interoperability, as well as the design of remote control units, often enabled by AI or other technologies, are also driving improvements in systems consisting of multiple vehicles being controlled by a single operator. Workshop participants noted that overall, the maturing of AI and ML technologies and the extent to which such technologies are integrated in robotic systems will be a key determinant of future trends in this area.¹¹³

Opportunities and challenges on the future battlefield

Advanced robotics and autonomous technologies will give way to performance optimisations, cost reductions and completely new operational concepts for militaries to exploit.¹¹⁴ Technological advances within these fields could act to fill multiple requirements at once and achieve desirable effects in less time, acting as a force-multiplier by increasing operative output as well as the relative firepower of forces.¹¹⁵ Additional opportunities include:¹¹⁶

- **Speed:** Leveraging autonomous systems to improve reaction times, decision-making speed and rapid movement across land, air and sea may give forces strategic advantages over a potential adversary.
- **Extended reach and coverage:** In comparison to human combatants or even tethered systems, autonomous systems may enhance the available points of presence for surveillance, intelligence, reconnaissance and weapons systems.
- **Mission flexibility:** Autonomous systems can be deployed on a variety of missions operate under a wide range of conditions (e.g. climate, weather and terrain). Increased flexibility and adaptability in robotic systems to novel types of mission and operational contexts may provide further strategic opportunities for their deployment.

¹⁰⁹ See Wong et al. (2020).

¹¹⁰ See Wong et al. (2020).

¹¹¹ Ekelhof and Persi Paoli (2020), Miskovic et al. (2014).

¹¹² See RAND Europe workshop (October 2020).

¹¹³ See RAND Europe workshop (October 2020).

¹¹⁴ See Andås (2020).

¹¹⁵ See Andås (2020).

¹¹⁶ See Torossian (2020).

- Accuracy: The accuracy of autonomous systems may provide opportunities for precision strike, as well as reducing collateral damage on the battlefield. Advances in fields such as AI-enabled object and facial recognition capabilities in autonomous systems may greatly increase accuracy across various mission contexts.

Workshop participants and interviewees noted that advances in robotics and autonomous systems may present various EU-specific opportunities. The development of a common platform for autonomous systems, mirroring similar concepts developed by international partners (e.g. Australia), could present a significant opportunity for EU MS capabilities increasing interoperability and facilitating plug-and-play use of systems from different MS in the context of joint missions and operations under CSDP.¹¹⁷ Further to advances in efforts to exploit opportunities provided by autonomous systems in the military context, there may also be significant opportunity for the EU to provide greater leadership in international multilateral efforts to strengthen safeguards against the proliferation and use of autonomous systems without meaningful human control, discussed further below.¹¹⁸

While future defence forces and establishments may increasingly leverage autonomous systems for various tasks, existing research as well as expert and stakeholder consultations highlighted a number of challenges associated with advanced robotics and autonomous systems:

- Cyber-physical systems, including the communication and data links between vehicles in a networked system or between the system and a human operator may be vulnerable to attack.¹¹⁹ While wireless signalling over Bluetooth, Wi-Fi, radio or infrared may be well applied in controlled environments, in theatre these forms of communication may have various vulnerabilities to electronic warfare attacks such as jamming, spoofing or hacking.¹²⁰
- The deployment of autonomous systems may threaten crisis stability and lead to escalatory dynamics due to factors such as increased speed of decision-making and increased risk of miscalculation and misperception. Existing research also highlights that increased force protection provided by greater opportunities to deploy autonomous systems instead of human warfighter may present risks to crisis stability due to the fact that the presence of humans in a theatre decreases the incentives to use force.¹²¹
- Remote and autonomous systems present a relatively low-cost capability and the proliferation of dual-use, off-the-shelf systems may present challenges in terms of systems being exploited by an increasing number of state as well as non-state adversaries.¹²²

Enablers and barriers for future adoption

Workshop participants noted that despite ongoing developments in the maturity of robotics and autonomous systems, there are significant technological barriers for future uptake in European defence contexts. This includes challenges in sensing and computing as well as the size, weight and power (SWaP) elements of advanced autonomous systems. Additional technological barriers to broader uptake of advanced robotics and autonomous systems on the future battlefield relate to

¹¹⁷ RAND Europe workshop (October 2020).

¹¹⁸ RAND Europe interview (INT06, October 2020).

¹¹⁹ See Ekelhof and Persi Paoli (2020).

¹²⁰ See Ekelhof and Persi Paoli (2020).

¹²¹ See Wong et al. (2020).

¹²² RAND Europe interview (INT06, October 2020).

edge computing performance, bandwidth limitations, and susceptibility of cyber-physical systems to electronic and cyber countermeasures.¹²³

Ethics and human rights protections represent a crucial factor in the context of future development and uptake of autonomous systems. Existing research documents various ethical considerations relating to autonomous weapons systems raised by International Humanitarian Law (IHL) and the Law of Armed Conflict (LOAC). These considerations include potential challenges pertaining to:

- The principles of distinction (i.e. distinguishing between combatants and civilians in the battlefield);
- Proportionality (i.e. balance of the loss of life and damage in relation to the expected military advantage)
- Military necessity (i.e. inflicting damage on an enemy only in pursuit of military objectives);
- Unnecessary suffering (i.e. prohibiting systems or weapons causing excessive injury or unnecessary suffering).

Future development and uptake of autonomous systems in the European context is likely to be determined by the extent to which systems are able to comply with these principles. Autonomous systems raise a serious ethical challenge for decision making on the use of force, as the consequences of the use of autonomous systems are generally less predictable, with the links between intention and consequences appearing more diluted or removed.¹²⁴

These factors underpin emerging international consensus on the necessity to establish and ensure meaningful human control.¹²⁵ Relevant technological specifications for autonomous systems with meaningful human control include predictability of behaviour of an autonomous system by an operator, maintaining operator ability to intervene and alter the behaviour of a system, and the speed at which commands provided by an operator are processed and actions.¹²⁶ The ability of operators to understand how autonomous systems interpret data and formulate corresponding actions is also key; though this is a potentially significant challenge particularly for highly complex systems.¹²⁷

¹²³ RAND Europe workshop (October 2020).

¹²⁴ See Boulanin et al. (2020).

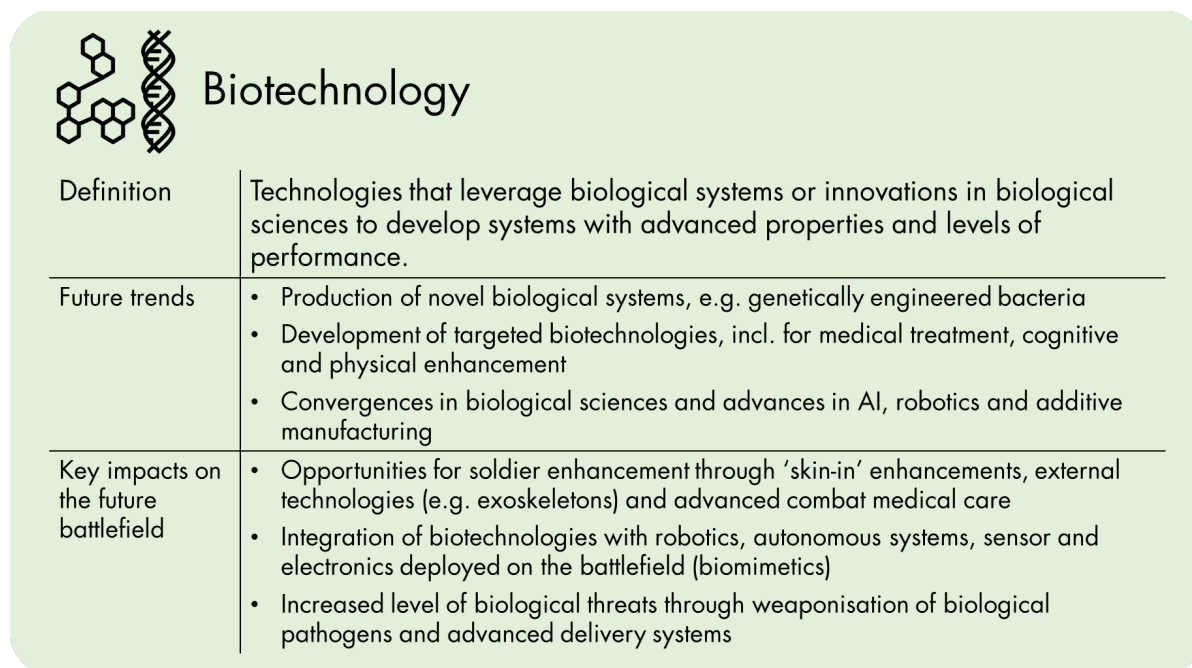
¹²⁵ RAND Europe interview (INT06, 27 October 2020).

¹²⁶ See Ekelhof and Persi Paoli (2020).

¹²⁷ See Torossian (2020).

3.1.3. Biotechnology

Figure 3.3 – Overview of the technology cluster



Source: RAND Europe analysis.

Technology overview and future trends

Biotechnology represents a wide range of scientific and technological advances, including in the fields of synthetic biology, i.e. the 'redesigning organisms for useful purposes by engineering them to have new abilities'.¹²⁸ Biotechnology applications in the context of Defence include:

- Physical or cognitive enhancement for soldiers on the battlefield, leveraging methods such as gene editing, pharmaceuticals and the application of biotechnologies in advanced combat medical care.¹²⁹ Further to physical or genitive enhancement, biotechnologies are also being applied to trauma care for wounded military personnel.¹³⁰
- Integration of biotechnology with robotics, autonomous systems, sensors and electronics. This includes biomimetic robotics or biomimetics, comprising the design and development of robots through the mimicking of biological systems.¹³¹ Biomolecular engineering applications to sensors and electronics (including microelectronics) includes biosensors (i.e. sensors with a biological recognition element) and bioelectronics (i.e. the integration of biological materials such as biological fuel cells and electronics for information processing, data storage, and actuators). Biosensors and bioelectronics can significantly augment capabilities for recognising biological threats to various physiological targets.¹³² Offensive use of biotechnologies in the form of biological weapons that generally consist of a weaponised biological agent and a corresponding delivery system that facilitates the 'appropriate dissemination and dispersion of the agent in a way that makes the target

¹²⁸ See NIH (2019a).

¹²⁹ Gene editing comprises the use of various technologies for the transformation of an organism's DNA, leading to changes in an organism's physical traits. See Armstrong et al. (2010), NIH (2019b).

¹³⁰ See Armstrong et al. (2010).

¹³¹ See Nathan (2015).

¹³² See Armstrong et al. (2010).

susceptible to its effect'.¹³³ Further to direct risks to the armed forces operating on the battlefield and the civilian population, weaponisation of biological pathogens and 'gene drives' can also be exploited to spread rapidly through animal and plant populations.¹³⁴

Out to 2040, significant advances may be achieved in biotechnology with regard to genetic modification of organisms enabling the production of novel types of biological systems, such as genetically engineered bacteria. Advances in related fields (e.g. neurology and pharmaceutical research) may also be relevant in this field. While such advances may produce significant opportunities (e.g. for soldier enhancement), they also carry inherent risk with regard to potential exploitation through weaponisation of advanced pathogens, including e.g. targeted biological agents designed to target populations with particular genetic backgrounds ('ethic weapons').¹³⁵

Existing research highlights that there is also a growing convergence of biological sciences with technological advances in computer science, engineering and emerging technologies such as AI, additive manufacturing and robotics.¹³⁶ Potential future trends in this cross-technological field and developments could include the development of entirely novel bioweapons as well as lower barriers to entry through the potential of non-state actors gaining access to advanced biotechnological and delivery systems.

Opportunities and challenges on the future battlefield

Advances in biotechnology may provide significant opportunities for defence establishments in general and European defence in particular. In particular, these include the application of advanced biotechnologies for soldier enhancement, which, as workshop participants noted, may be particularly relevant to European defence due to the perceived reliance of many EU MS on land forces.¹³⁷

Enhancements can be separated into 'skin-in' enhancements – internal adjustments manipulating the soldier's own biology – and external ('skin-out') technologies such as exo-skeletons.¹³⁸ Both of these modes of application improve soldier performance, in kinetic and non-kinetic functions, e.g. through improving alertness and learning capabilities as well as improving digestive health and cognition more broadly.¹³⁹ Biotechnology-enabled applications for cognitive enhancement may also assist in decision making processes, particularly in stressful or high-pressure environments such as crisis scenarios. For example, Modafinil, an attention-enhancing drug is designed to enhance situational awareness and decision making.¹⁴⁰ Trauma-blocking drugs, such as Propranolol, can prevent post-traumatic stress disorder (PTSD) and keep soldiers alert and in combat for days on end.¹⁴¹ In addition, soldiers may have access to tailored medicine through genome engineering, with human gene therapy allowing soldiers to be 'pre-screened for potential vulnerabilities and diseases so that accurate treatments can be available'.¹⁴²

¹³³ This can include genetically engineered pathogens, midspectrum agents (e.g. toxins, biological regulators), vectors capable of delivering genetic material into human genomes, and novel chemical agents, See Armstrong et al. (2010), Brockmann et al. (2019).

¹³⁴ See Brockmann et al. (2019).

¹³⁵ RAND Europe interview (INT02, October 2020).

¹³⁶ See Brockmann et al. (2019).

¹³⁷ RAND Europe workshop (October 2020).

¹³⁸ Skin-in enhancements include Peak Soldier Performance, the Metabolically Dominant Soldier. Skin-out enhancements include the Land Warrior, Objective Force Warrior and Future Force Warrior suite of programmes. See Bickford (2020).

¹³⁹ See Dieulis (2018).

¹⁴⁰ See Bickford (2020).

¹⁴¹ See Bickford (2020).

¹⁴² See Perkins and Steevens (2015).

Advances in biotechnology may pose significant challenges for security and defence, particularly through the development of novel types of biological weapons, weaponisation of gene editing technologies, or advances in weaponised biomimetics.

The potential development of novel types of weapons have dominated discussions about the potential challenges posed by advanced biotechnologies. Similar to chemical weapons, the current threat of biological weapons is defined by the risk of adversarial actors being able to access hazardous biological agents or exploit advances in the fields of synthetic biology and gene editing. Despite international bans and treaties (e.g. the Biological Weapons Convention) as well as a number of international organisations and mechanisms that serve to prevent the development, testing, proliferation and operational use of biological weapons, frameworks including the Biological Weapons Convention may face pressures to adapt its infrastructure and mechanisms to a rapidly changing technological landscape.¹⁴³

Enablers and barriers for future adoption

The enablers and barriers for future adoption may vary significantly depending on the assumed application of biotechnology. The legal, ethical and regulatory barriers associated with the adoption of weaponised biotechnologies greatly exceed those associated with biotechnology-based human enhancements. There may also be significant international variation in relation to the regulatory and ethical barriers for military uses of biotechnologies. Differences in the levels of ethical and regulatory constraints on the use of biotechnology may represent a challenge for European forces and their ability to respond to existing and potential new adversaries.

Several barriers have been noted in relation to the potential uptake of biotechnologies for human enhancement:

- Existing literature documents significant concerns that many emerging biotechnologies are susceptible to single points of failure for essential components.¹⁴⁴ For example, while the bioengineering of silkworms to generate 'dragon silk' could produce advanced body armour, silkworms survive on mulberry leaves, and would require over 6,000 acres of mulberry trees for large-scale production. Current examples of such production processes, such as those pursued by the US Department of Defence (DOD), highlight the reliance of the production process on farming cooperatives in Vietnam, which require international contracts, embassy approvals and a complex supply chain, representing a potential single-source point of failure.¹⁴⁵
- Inequality of access represents a further potential barrier for the adoption of biotechnological advances such as gene editing. Within the military, uniformity is used as a mechanism to instil discipline and garner compliance with rules and directions, which is intrinsically tied to the chain of command structure.¹⁴⁶ Making some human enhancement technologies available to some, but not others (e.g. special forces personnel only) may lead to dissent, potentially allowing soldiers to refuse deployment on the basis that they have not been afforded the same protection as others.¹⁴⁷

Despite these challenges, ongoing efforts to adapt bioeconomy strategies may support biotechnology innovation across a wide range of sectors.¹⁴⁸ In particular, efforts are ongoing to integrate codes of conduct and norms to address potential security concerns, encourage

¹⁴³ RAND Europe interview (INT02, October 2020).

¹⁴⁴ See Dieulis (2018).

¹⁴⁵ See Dieulis (2018).

¹⁴⁶ See Greene and Master (2018).

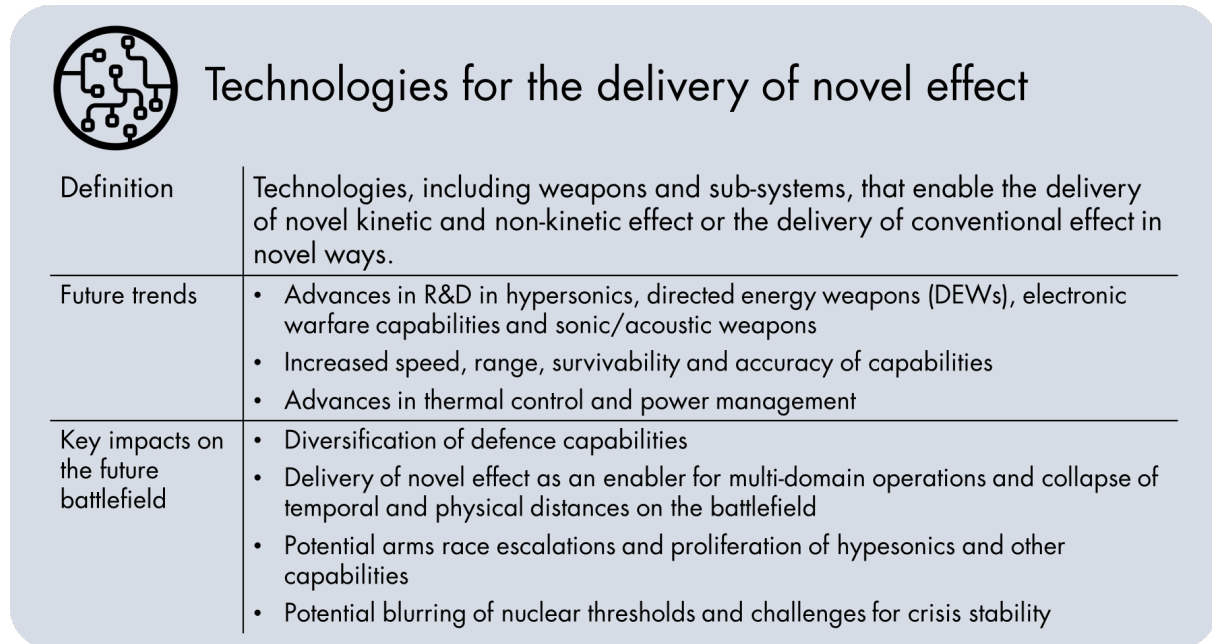
¹⁴⁷ See Greene and Master (2018).

¹⁴⁸ See Dieulis (2018).

developments by ensuring transparency, and coordinate government investments and building public trust.¹⁴⁹

3.1.4. Technologies for the delivery of novel effect

Figure 3.4 – Overview of the cluster of technologies for the delivery of novel effect



Source: RAND Europe analysis.

Technology overview and future trends

Technologies for the delivery of novel effects can be defined as technologies, including weapons and sub-systems, that enable the delivery of novel kinetic and non-kinetic effect or the delivery of conventional effect in novel ways. This encompasses a range of technologies and capabilities, including:

- Directed Energy Weapons (DEWs), encompassing weapons systems that utilise 'concentrated electromagnetic energy or atomic or subatomic particles' as a means to deliver effect and include capabilities relying on laser energy, such as High Energy Lasers (HELs).¹⁵⁰
- Sonic and acoustic weapons, which utilise the propagation of sound to deliver non-lethal or less-lethal effect. This includes capabilities conceptualised to operate at ultrasound (above 20 kHz), infrasound (below 20 Hz) or low frequencies (below 100 Hz).¹⁵¹
- Hypersonic weapons defined by their ability to achieve flight at speeds of Mach 5 and above. Current trends in the development of hypersonic capabilities concern two types of hypersonic technology: Hypersonic glide vehicles (HGVs), which mirror the principles of ballistic missile technologies with an initial launch and subsequent release along the upper atmosphere; and Hypersonic cruise missiles (HCMs), which utilise advanced jet engines and/or rockets for greater speed (compared to conventional, subsonic, cruise missile technology). Though hypersonic weapons do not travel faster than some more traditional

¹⁴⁹ See Dieulis (2018).

¹⁵⁰ See Wheeler (2017).

¹⁵¹ See Article36 (2018).

systems (e.g. intercontinental and submarine-launched ballistic missiles), they provide greater manoeuvrability than more traditional capabilities allowing hypersonics to potentially evade current missile defence systems.¹⁵²

- Electronic warfare capabilities that may be used to 'degrade, neutralise, or destroy enemy equipment, facilities or personnel, and can include jamming or spoofing of the enemy's own use of the electromagnetic spectrum (EMS)'.¹⁵³

A number of nations, including China, Russia, and the US, have sought to advance the development of hypersonic and other capabilities to achieve novel kinetic and non-kinetic effects with greater speed, survivability, accuracy, and range.¹⁵⁴

Hypersonic technologies have seen rapid advances over the last few decades, including in the development of high-speed supersonic scramjet engines and advanced materials able to withstand the high heat loads of hypersonic flights, improving survivability of hypersonic vehicles.¹⁵⁵ Future advances in this area may also include increasing integration with enabling AI and other technologies. For example, electronic warfare capabilities as well as hypersonic technologies are likely to feature applications of autonomy and AI-enabled networked C2.¹⁵⁶

Opportunities and challenges on the future battlefield

Technologies to deliver novel effects may provide a range of opportunities for addressing tactical as well as strategic challenges in future battlefield contexts. Workshop participants, however, highlighted that there is significant variation among the technologies within this cluster in terms of the associated opportunities and challenges they present for the future battlefield.

The delivery of novel effects, such as directed energy, may increasingly be used to provide support for air and missile defence systems, including countering ballistic missile and UAS threats. DEWs and HELs have been explored in relation to various offensive and defensive applications in this context, including in combination with autonomous and advanced robotic systems (e.g. HELs mounted on autonomous UAVs).¹⁵⁷ The opportunities associated with DEWs in particular relevant for applications against targets sensitive to localised optical radiation (i.e. targets that 'can be neutralised by (over)heating a small area on its surface').¹⁵⁸ The very limited time of strike of DEWs also increases the vulnerability of such targets due to the limited time allowed to avoid a strike.¹⁵⁹ Advances in the precision of capabilities to deliver kinetic and non-kinetic effects may also allow actors on the battlefield to avoid or minimise collateral damage.

Workshop discussions noted that despite variations within the technology cluster, a common impact shared by technologies in this area may be their role in facilitating multi-domain operations. This is achieved through the use of technologies to collapse temporal and physical distances to deliver effects at sufficient range and speed, disrupting C2 and breaking through an adversary's OODA loop. This serves to achieve military advantage through fragmenting the adversary forces and reducing capacity for effective and efficient manoeuvre within the future battlefield. As such, existing and emerging concepts for multi-domain operations, such as the Chinese concept of

¹⁵² Terry and Cone (2020).

¹⁵³ See O'Connell (2018).

¹⁵⁴ See Speier et al. (2017), Barrie (2019).

¹⁵⁵ See Terry and Cone (2020).

¹⁵⁶ RAND Europe workshop (October 2020).

¹⁵⁷ Gunzinger and Dougherty (2012).

¹⁵⁸ See Pudo and Galuga (2017).

¹⁵⁹ See Pudo and Galuga (2017).

systems attack and the Russian concept of disorganisation and reflexive control, frequently rely on the uses of capabilities in this technology cluster.¹⁶⁰

While there may be opportunities provided by technologies to deliver novel effect for defensive systems, such efforts may incentivise investments in advanced offensive capabilities by potential adversaries. This is due to the perceived imperative to adopt more potent capabilities (including hypersonic weapons) to break through enemy defences, which may use novel technologies to augment traditional defence systems (including missile defences).

Hypersonic weapons were noted by workshop participants to have a greater effect in comparison to other technologies on the future battlefield, particularly with regard to potential arms race as well as conflict escalations. Hypersonic capabilities, through their delivery of greater speed and survivability, challenge options for detection and counter-strike.¹⁶¹ The corresponding increasing speed of battlefield interactions may inherently challenge crisis stability. Relatedly, technologies such as hypersonic missiles may contribute to an increasing blurring of the nuclear thresholds. In addition to the increasingly pronounced role of nuclear capabilities in national security strategies, technological advances and the integration of technologies to deliver novel effect may thus pose considerable risk through potential nuclear crisis escalations.¹⁶²

Enablers and barriers for future adoption

While some technologies such as hypersonic missiles, DEWs and sonic weapons may feature more prominently on the future battlefield, workshop participants also noted that such capabilities are unlikely to replace more traditional capabilities to deliver kinetic effects.¹⁶³ This is due, in part, to considerable uncertainty about the extent to which novel weapons systems in fact yield significant capability improvements in the battlefield context.¹⁶⁴ Historically, this uncertainty has emerged out of significant costs and delays in R&D programmes, which ultimately failed to produce viable operational capabilities.¹⁶⁵ The potential occurrence of unforeseen technical failures of novel technologies encountered during development have further limited the potential actualisation of an operationally viable system. Additionally, similar to other technology clusters, the adoption of technologies in this area may be prohibited by insufficient adaptation of existing concepts of operations.¹⁶⁶

¹⁶⁰ RAND Europe workshop (October 2020).

¹⁶¹ See Speier et al. (2017).

¹⁶² RAND Europe interview (INT05, October 2020).

¹⁶³ RAND Europe workshop (October 2020).

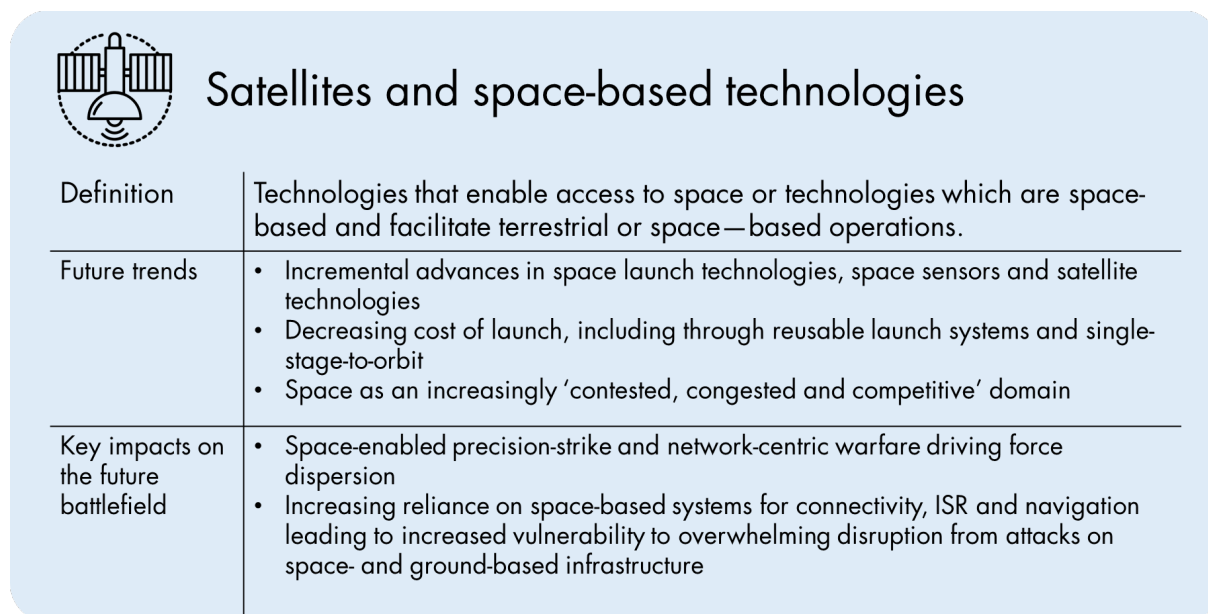
¹⁶⁴ RAND Europe workshop (October 2020).

¹⁶⁵ See Pudo and Galuga (2017).

¹⁶⁶ See Rossiter (2019).

3.1.5. Satellites and space-based technologies and assets

Figure 3.5 – Overview of the satellites and space-based technologies and assets cluster



Source: RAND Europe analysis.

Technology overview and future trends

Space has emerged as an increasingly crucial domain for security and defence, including through the provision of space-enabled communications, navigation and Earth Observation (EO) services. The future battlefield may include applications of technologies that facilitate access to space in support of space-based or ground-based operations. New and emerging technologies in this area may be categorised as:

- Space launch technologies (i.e. technologies that facilitate access to space). This includes advanced launch vehicles, as well as reusable launch vehicles (RLVs), which, in contrast to expendable launch vehicles (ELVs), allow some or all of the components of the system to be recovered following launch. This enables the re-use of a system for multiple launches, which is expected to have significant impact on the uses of space across civil and military domains due to the significant reductions in launch costs.¹⁶⁷ Other relevant technologies include responsive space launch capabilities.¹⁶⁸
- Space sensors and technologies for space-based surveillance and **space-based Space Situational Awareness (SSA)**, including optical sensors, satellite-based hyperspectral imaging satellites, advanced sensors mounted on nanosatellites or CubeSats, integrated space-based sensor networks and AI-enabled data processing capabilities.¹⁶⁹
- Communications satellites and technologies supporting space-based communications, including technologies for advanced communications security (e.g. satellite-based

¹⁶⁷ See Matignon (2019).

¹⁶⁸ Responsive space launch aims at providing 'assured space access to enable the rapid proliferation, disaggregation and replacement of satellite systems to meet real-time operational needs in response to adversarial action' Moore (2019).

¹⁶⁹ See Moore (2019).

quantum cryptography), optical communications technologies and LEO-to-GEO communications technologies, and high-altitude pseudo-satellites (HAPS).¹⁷⁰

- Space-based technologies to deliver kinetic or non-kinetic effects. Satellites and space-based technologies may also include counterspace and anti-satellite (ASAT) capabilities. Electronic methods of ASAT attack include: the disruption of satellite communications through the creation of 'noise' in radiofrequency bands to intervene with radiofrequency communications ('jamming'), emission of a false signal by a malicious device to downlink data from a target satellite ('spoofing'), or 'blinding' of satellites with laser power ('dazzling').¹⁷¹ Other modes of ASAT attack include: anti-satellite missiles, close-proximity operations or the use of space-based interceptors.

Due to the increasingly central role of space-based technologies, not only for security and defence but also a wider range of services within the terrestrial economy, space-based technologies are likely to significantly advance in the future through civil, commercial and military research and development programmes. Examples of likely future advances include further development of reusable launch systems and single-stage-to-orbit (SSTO) technologies.

Future trends, however, in the adoption and use of space-based technologies are likely to be largely influenced by incremental technological advances or improvements in the uses of existing technological solutions.¹⁷² Future improvements of space-based technologies, particularly in the military context, may include efforts to increase the resilience and reliability of space-based services as well as technological advances to facilitate low-cost access to space.¹⁷³ Technological advances in other technology clusters may also serve as important enablers for the future uses of space-based technologies in the battlefield context. This includes, for example, additive manufacturing (3D printing) and technologies enabling the miniaturisation of space-based assets or on-orbit assembly.¹⁷⁴

Lastly, technological advances are also likely to occur in capabilities that provide space-like services without operating in the atmosphere itself (i.e. near-space capabilities such as High-Altitude Pseudo Satellites). The use of remotely operated aircraft in the stratosphere could, in the future, provide an alternative to space-based EO services.¹⁷⁵ This could also contribute to a perceived blurring of the distinction between the space domain and near-space (i.e. terrestrial) areas of operation.¹⁷⁶

Opportunities and challenges on the future battlefield

Space-based assets have become increasingly crucial in the context of enabling terrestrial operations in and across the air, land, sea and cyber domains. Already, space-based technologies have served as critical enablers for the emergence of network-centric and precision-strike warfare. Out to 2040, the need to adapt to space-enabled precision-strike through force dispersion may further increase reliance of military forces on space-enabled C2 and ISR.¹⁷⁷

The falling cost of access to space is also likely to further increase the use of space-based services such as Earth Observation (EO), Positioning, Navigation and Timing (PNT) and Satellite

¹⁷⁰ HAPS are 'unmanned vehicles that take advantage of weak stratospheric winds and solar energy to operate without interfering with commercial aviation and with enough endurance to provide long-term services as satellites do' Gonzalo et al. (2018), Moore (2019).

¹⁷¹ See Livingstone and Lewis (2016), Suzuki (2016).

¹⁷² RAND Europe interview (INT04, October 2020).

¹⁷³ RAND Europe interview (INT04, October 2020).

¹⁷⁴ RAND Europe interview (INT05, October 2020).

¹⁷⁵ For example, Coulon and Johnson (2017).

¹⁷⁶ RAND Europe workshop (November 2020).

¹⁷⁷ RAND Europe interview (INT04, October 2020), RAND Europe workshop (October 2020).

Communications (SATCOM) to enable terrestrial military operations, particularly for C2 and ISR. Space-based technologies may also serve as enablers for air and missile defence, including through the use of space-based interceptors or the use of new satellite technologies for the tracking of ballistic and long-range missiles.¹⁷⁸ Detection of tests or uses of weapons of mass effect (WME) such as biological and chemical weapons, may also be assisted or enabled by space-based services. DARPA's 'Atmosphere as a Sensor' programme has, for example, been discussed as an opportunity for detecting the testing of nuclear weapons.¹⁷⁹

The proliferation of and rapid advances in space-based technologies at large are likely to increase the role of space as an enabler in future battlefield interactions as well as further increase the spectrum of space-based services applied in the future battlefield. This extends to the uses of space-based technologies to enable the uses of other new and emerging technologies in a battlefield context, for example through providing intelligence and connectivity for human-machine teaming.¹⁸⁰ The increasing reliance, however, of military operations on space-based services is also likely corresponds to increasing risks due to the extensive impacts produced by a potential attack against the ground- or space-based infrastructure for the provision of space-based services. Attacks on satellite services, including through jamming, spoofing, dazzling of satellites or direct attacks on downlink and uplink data transmission may produce extensive damages to military operations. Similarly, attacks against ground-based infrastructure, including ground installations, which support the operation of space-based services, present significant vulnerabilities to actors on the future battlefield.¹⁸¹

While workshop participants noted that a wider use of satellites and space-based technologies for the direct delivery of kinetic or non-kinetic effect remains unlikely in the near future, there are several challenges associated with the increasing reliance on space-based assets:

- Space has increasingly been characterised as 'contested, congested and competitive'.¹⁸² The falling cost of launch and corresponding proliferation of objects and actors in space are likely to exacerbate the challenges associated with increasing space congestion, including potential for accidental collisions or disruptions to space-based services caused by damages from space debris.
- The increasing congested-ness of space also increases the number of potentially valuable targets for a potential adversary.¹⁸³ The proliferation of technologies aimed at defeating or disrupting satellite communications, including anti-satellite missiles, may also feature in this evolving threat landscape.¹⁸⁴
- The increasing reliance on space-based assets for terrestrial military operations may incentivise states to seek ever-improving military space capabilities in order to maintain superiority in the space domain.¹⁸⁵ This may, in turn, contribute to the characterisation of space itself as a warfighting domain and a potential battlefield out to 2040.
- Nevertheless, challenges related to the potential exploitation of space-based technologies to deliver kinetic attacks are exacerbated by the lack of definition as to what represents a

¹⁷⁸ See O'Hanlon (2018).

¹⁷⁹ See Peck (2020).

¹⁸⁰ RAND Europe workshop (October 2020).

¹⁸¹ RAND Europe workshop (October 2020).

¹⁸² See Schulte (2011).

¹⁸³ RAND Europe workshop (October 2020).

¹⁸⁴ The US, Russia, China and India have all carried out anti-satellite missile tests in recent years. See, for example, Kan (2007), Miglani and Das (2019), Gordon (2020).

¹⁸⁵ See Air Force Space Command (2019).

'space weapon'. For example, technologies for space debris management may be misused to cause damage to space-based assets.¹⁸⁶ This poses challenges for efforts to develop more effective codes of conduct with regards to the uses of space by commercial, civil as well as military actors.

The potential of conflict and warfighting extending to the space domain poses the question of how space-to-space kinetic engagements would take place, given the inherent physical differences of the space domain. Existing research points to several constraints arising out of orbital mechanics that would shape the nature of such engagements:¹⁸⁷

- Satellites can move quickly but predictably due to the interconnectedness between a satellite's speed, altitude and orbit shape (i.e. direction of movement through space). The constraints of a satellite's orbit imposed by the Earth's gravitational pull also mean that any physical approximation of two satellites being deployed as weapons systems would require extensive planning to perform successful phasing, flyby or intercept manoeuvres against another satellite.
- Further to the mechanical constraints imposed on a satellite's manoeuvrability through space, the extensiveness of the space domain is an important factor when considering the potential nature of space-to-space kinetic engagements. The volume of space between Low and Geosynchronous Earth Orbits (LEO and GEO) comprising approximately 200 trillion cubic kilometres – 190 times more than the volume of Earth. As such, the manoeuvring of objects such as satellites through space requires the investment of significant energy and resources.

Enablers and barriers for future adoption

High costs of launch and access to space remain a significant barrier for space-based operations, particularly in relation to any efforts to advance the militarisation of space or the use of space-based weapons for terrestrial defence purposes. In combination with the need for space-based weapons systems to be employed at considerable scale, the high costs associated with the use of space-based weapons systems make their proliferation or increased uses unlikely in the 2040 timeframe.¹⁸⁸

The changing nature of the space economy, including increasing commercialisation and reliance on public-private sector partnerships, may provide opportunities through incentivising innovation and further decreasing the costs of launch and access to space. There are, however, disagreements as to the precise impacts of commercialisation and public-private sector ventures on innovations in military space-based technologies. While some perspectives note that the growth of the commercial space sector is leading to an effective end to the government-led space race, others highlight the ongoing significance of civil and military funding for the space economy.¹⁸⁹

In the European defence context, the heterogeneity of national policy and strategy frameworks in relation to the space domain may pose challenges for future European cooperation on space-based technologies in defence. Recent initiatives, however, to strengthen EU's roles and competencies in relation to security and defence discussed in Section 2.2 as well as the establishment of a new Directorate-General for Defence Industry and Space (DG DEFIS) may provide opportunities for facilitating such cooperation. This includes areas such as development and acquisition of space-

¹⁸⁶ RAND Europe interview (INT05, October 2020).

¹⁸⁷ See Reesman and Wilson (2020).

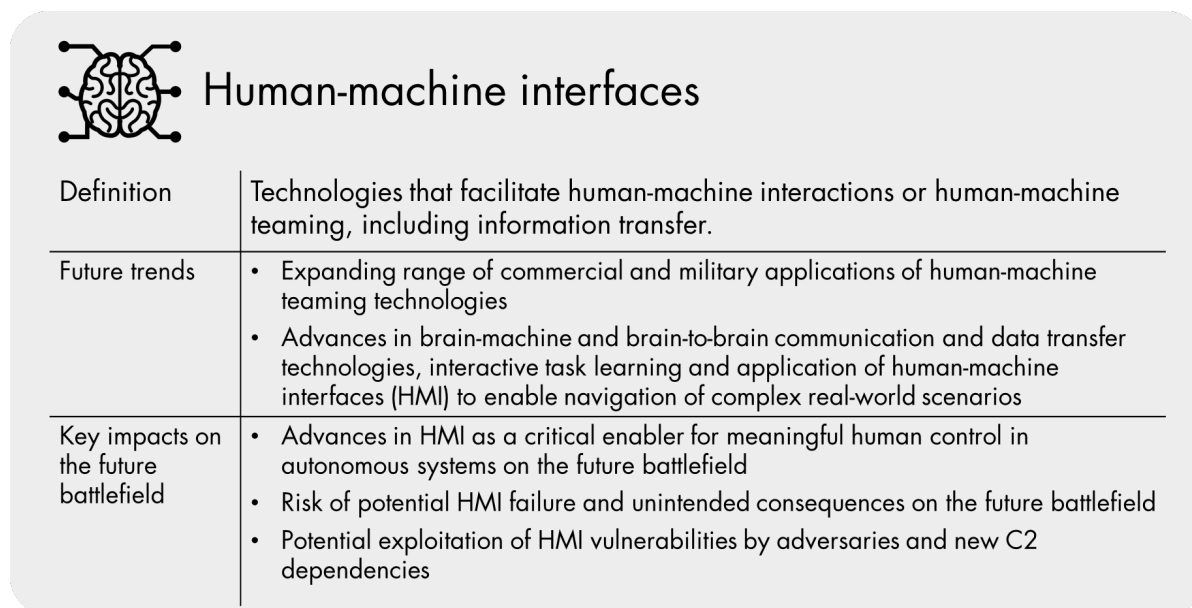
¹⁸⁸ RAND Europe interview (INT04, October 2020).

¹⁸⁹ RAND Europe interview (INT04, October 2020), RAND Europe workshop (October 2020).

based technologies and enhancing existing synergies between defence-oriented space technology applications and the wider EU space programme.¹⁹⁰

3.1.6. Human-machine interfaces

Figure 3.6 – Overview of the human-machine interfaces technology cluster



Source: RAND Europe analysis.

Technology overview and future trends

Human-machine interfaces (HMI) include technologies and devices that facilitate human-machine interactions or human-machine teaming (HMT), including processes such as delivering information from a computer system to a human.¹⁹¹ Based on their technical specifications, human-machine interfaces are commonly categorised as:

- Graphical user interfaces (GUI), which are interfaces that 'accept input via input devices and provide articulated graphical display on the output devices';
- Web user interfaces (WUI), which accept input and provide output by generating web pages that are transmitted via the Internet and viewed by the user via a web page'.¹⁹²

Advanced forms of HMT may include brain-computer interfaces (BCIs), technologies that provide 'a direct communication pathway between an enhanced or wired brain and an external device, with bidirectional information flow'.¹⁹³ New and emerging technologies in the context of HMT also include devices such as robotic limbs and neural prostheses that may restore human motor or cognitive functions following physical injury or neural damage.

Technologies enabling HMT are likely to significantly evolve out to 2040 in relation to an expanding array of operational and commercial applications. Improvements in HMT technologies are being made in various aspects, including technologies for 'data transfer from the brain; direct systems control; prosthetics and paralysis treatment; cortically coupled AI (for training or running AI

¹⁹⁰ See ESPI (2020).

¹⁹¹ See Gonzales (2015).

¹⁹² See Zhang (2010).

¹⁹³ See Binnedijk et al. (2020).

systems), and data transfer to the brain, and brain-to-brain communication'.¹⁹⁴ Future advances in these areas may also be derived from non-military fields, such as the healthcare sector in relation to the development of BCIs and prosthetics with direct systems control.

In the near to medium term (5-10) years, advances are expected in areas such as the development of minimally invasive sensors to measure neural activity in real-time, interactive task learning based on human-robot interaction, and improvement of HMI systems to comprehend natural language and better navigate more complex and uncertain real-world scenarios.¹⁹⁵ In the longer term (10-20 years), HMI technologies may advance in areas such as actively seeking information via directed data links to human operators, or navigating scenarios that require multiple goals to be addressed through sequencing and combining task representations. This advancement may be underpinned by developments in the modelling and decoding of human brain activity and the understanding of real-time human-system interactions.¹⁹⁶

Opportunities and challenges on the future battlefield

In line with the advancing applications of AI-enabled and autonomous systems on the future battlefield, HMT is expected to represent an increasingly important characteristic of future warfare. Existing research identifies a number of ways in which HMI technologies may provide opportunities for forces navigating the future battlefield. Advanced HMI technologies may allow forces to process and synthesise large amounts of data produced by 'an extensive network of humans and machines' more effectively and efficiently.¹⁹⁷ Additionally, HMI technologies may facilitate faster decision making, integrating advances in AI and autonomy. Advances in HMT are generally considered crucial for the effective integration of robotics including swarm technologies on the future battlefield while ensuring meaningful human control.¹⁹⁸

Workshop participants noted that a coordinated development of HMI technologies or a common HMI platform in the EU context could provide significant opportunities to European defence specifically. These include better integration of platforms and weapons systems, enhanced interoperability, as well as lower costs and ensuring compliance with relevant ethical and legal safeguards.¹⁹⁹

Further to these impacts, future uptake of HMI may produce several challenges for European defence, if not well executed. Such challenges include:

- Potential failure of HMI technologies carries considerable risk of unintended engagements and other undesirable effects. Workshop participants highlighted that the achievement of effective HMT represents a highly technical endeavour, a failure of which may impose significant costs.²⁰⁰
- New risks and dependencies for C2, in particular an increasing dependence on cyber and electromagnetic defences for resilience.²⁰¹
- New requirements for training and staff expertise, for example ensuring that staff are practised in reversionary modes of operating.²⁰²

¹⁹⁴ See Binnedijk et al. (2020).

¹⁹⁵ See DOD (2020).

¹⁹⁶ See DOD (2020).

¹⁹⁷ See Binnedijk et al. (2020).

¹⁹⁸ RAND Europe interview (INT06, October 2020).

¹⁹⁹ RAND Europe workshop (October 2020).

²⁰⁰ RAND Europe workshop (October 2020).

²⁰¹ See MOD (2018).

²⁰² See MOD (2018).

- Potential for adversaries gaining significant tactical advantages through advanced adversarial applications of human-machine interfaces. The actors able to optimise their human-machine decision-making will considerably benefit from speed at the tactical level. As militaries seek to leverage the detection, recognition, optimisation and efficiency advantages of AI in the OODA loop, EU MS forces may be put at a disadvantage.²⁰³ Increased reliance on HMI technologies may also increase vulnerability of EU MS armed forces by offering new opportunities for an adversary to deny access to the technology.²⁰⁴

Enablers and barriers for future adoption

The proliferation of cyber-physical systems on the future battlefield and advances in remote and autonomous capabilities are likely to drive future uptake of human-machine interface technologies on the battlefield. In addition to the increasing requirement for effective human-machine teaming solutions, military growth and modernisation could see ground forces evolve as militaries exploit human-machine interface systems, seeking to gain the strategic advantage over their adversaries.²⁰⁵

Though human-machine teaming may feature increasingly prominently on the future battlefield, several barriers for future adoption can be identified:²⁰⁶

- Trust deficit. There is a need to build trust among military personnel in human-machine interfaces to become effectively integrated into teams. Heavy vetting and testing, as well as an initial focus on non-invasive measures could facilitate adoption of emerging technologies.
- Ethical constraints. The adoption of advanced AI and robotics integrated into human-machine interface systems could raise significant ethical challenges, particularly with reference to responsibility for actions and lowering the threshold of the use of force.
- Civil-military relations. The relationship between militaries and societies may become stressed if military personnel receive augmentation. Mechanical and (eventually) cognitive human enhancement will be expensive and beyond the means of the average person, raising questions about equality.
- Institutional culture. Some militaries may have an institutional culture of a people-centric approach, resisting the adoption of new ideas, techniques and technologies such as human-machine interface technologies.

Collaborative private-public sector approaches that leverage advances in the private sector may serve to address some of these challenges, particularly through improving trust gaps in the military.²⁰⁷ Workshop participants also highlighted that a continuous involvement of operators throughout the cycle of development, testing, adoption and use of new systems was crucial to mitigate risks associated with HMI technologies.²⁰⁸ Advances in AI research, particularly with regard to natural intelligence – cognitive capabilities – as well as human-AI teaming experiments may also serve as technological enablers for future uptake of human-machine interface technologies.²⁰⁹

²⁰³ See MOD (2018).

²⁰⁴ See Binnedijk et al. (2020).

²⁰⁵ See Ryan (2018).

²⁰⁶ See Binnedijk et al. (2020).

²⁰⁷ See Binnedijk et al. (2020).

²⁰⁸ RAND Europe workshop (October 2020).

²⁰⁹ See DOD (2020).

3.2. Other technologies of relevance for the future battlefield

This section provides a brief overview of additional technology clusters that were identified in existing literature and the S&T horizon scanning as potentially shaping the future battlefield. These clusters were reviewed in lesser detail due to lesser certainty concerning the scope and nature of the impact of these technologies as well as the timelines and extent of future uptake, as highlighted during the study team's consultations with STOA.

3.2.1. Advanced energy and power systems

Advances in energy and power systems encompass a range of new and emerging technologies used for the production, transmission, conversion and storage of energy and power. These include:

- Propulsion technologies and engines harnessing hypersonic, electric, hybrid-electric and other forms of energy as well as fuel-efficient propulsion solutions. Novel propulsion and engine technologies may include high-efficiency thrusters (e.g. ion thrusters) to propel aircraft and other capabilities.²¹⁰
- New technologies for the conversion and transmission of novel and traditional sources of energy, including fossil fuels, fuel cells, nuclear power, renewable energy (e.g. solar and wind). This may include wireless energy transmission, power lines and networks, fuel cell- and advanced composite-based energy transmission solutions.²¹¹
- Energy storage and management technologies that may include next-generation batteries, smart energy management technologies and microgrids, and energy-efficient equipment.²¹²

Future advances in this field may be directed at the development of renewable and green energy solutions for defence and security.²¹³ Improvements may also be directed at addressing prevailing limitations in the capacity, efficiency and weight of conventional energy storage and transmission technologies used in the military to improve energy security, resilience and military readiness.²¹⁴

Advanced energy and power systems represent critical enablers for defence, including in relation to military logistics and the operation of military bases. Defence energy demands, however, are increasing through the proliferation of advanced electronics onboard military capabilities and 'electrification of the battlefield'.²¹⁵ Additionally, energy and power demands are increasing with the proliferation of advanced and computing capabilities as well as other trends. Along with high energy and power demands of military operations, these increased demands have incentivised investment in the development of innovative energy and power system solutions.

3.2.2. Novel and advanced materials and manufacturing

Novel and advanced materials include materials with unique functionalities or advancing the performance of traditional materials in terms of properties such as strength-weight ratios, thermal stability or resilience against corrosion.²¹⁶ Of particular relevance to defence and security are nanotechnologies, graphene and advanced composite materials.²¹⁷ Nanotechnology is typically

²¹⁰ See MIT (2013).

²¹¹ See Robyn and Marqusee (2019).

²¹² See Army Technology (2016).

²¹³ For example, Gardner (2017).

²¹⁴ See EDA (2012).

²¹⁵ See Robyn and Marqusee (2019).

²¹⁶ See Kennedy et al. (2019)

²¹⁷ See Freedberg (2020).

defined as technology involving the manipulation of matter on a scale of 1 to 100 nanometres.²¹⁸ This has applications across a vast array of fields, potentially including the production of nanoweapons or weaponised nanoparticles.²¹⁹ Other relevant categories of advanced materials include graphene (including carbon nanotubes)²²⁰ and advanced composite materials such as metal-, ceramic- and polymer matrix composites.

Further to novel materials, advance techniques for manufacturing have also been of increasing relevance in defence and security. This includes primarily additive manufacturing, including 3D printing, which consists of the building of objects through layering of materials, usually with the use of a 3D modelling software and specialised machine equipment such as a 3D printer.²²¹

Though advanced materials and manufacturing techniques present myriad opportunities for defence, e.g. through the development and production of better military equipment, they also represent potential threats. In addition to potentially leading to new types of biological threats, advanced materials such as nanotechnology may change the nature the systems used for the delivery of biological weapons, expand their potential attack surface, and increase the difficulty of detection and attribution.²²² While the offensive use of nanotechnology is still at the concept stage, nanotechnology may therefore create new pathways to formulation, delivery and evasion of detection for chemical and biological weapons.²²³ As highlighted in Section 3.1.3, the potential application of additive manufacturing to the 'printing' of laboratory equipment, delivery equipment (or component parts) as well as the bioprinting of potentially dangerous chemicals and biomaterials may also lower barriers for the acquisition of chemical and biological weapons.²²⁴

3.2.3. Quantum technologies

Quantum technologies encompass a range of applications and capabilities connected to the field of quantum mechanics - the 'physics of sub-atomic particles'.²²⁵ This includes the following technologies:²²⁶

- Quantum computing or the use of quantum computers to perform highly complex calculations much faster and energy-efficiently than conventional computing through the utilisation of subatomic particles (qubits);
- Quantum sensors, which harness the sensitivity of quantum states for technologies to detect light, gravity and magnetic fields;
- Quantum communications, the use of quantum technology for secure, high-speed and long-range communications;
- Quantum cryptography, which may provide highly secure communications and render traditional cryptography obsolete;
- Quantum clocks, which could replace atomic clocks in providing time-critical products and services and support next-generation navigation systems.

²¹⁸ See NNI (n.d.).

²¹⁹ See Brockmann et al. (2019).

²²⁰ Carbon nanotubes are carbon materials shaped in tubes with nanometer-scale diameters. They have been explored in relation to replacing silicon-based semiconductors in electronics, Freedberg (2020).

²²¹ See Additive Manufacturing (n.d.).

²²² See Caves and Carus (2014).

²²³ See Brockmann et al. (2019).

²²⁴ See Brockmann et al. (2019).

²²⁵ See Martin (n.d.).

²²⁶ See Murray (2016).

Quantum technology overall has extensive applications in defence and security through enabling more accurate, faster and more time-efficient processing of larger amounts of data and thus providing advanced analytics capabilities. Existing research also points to a number of implications of quantum technologies including quantum key distribution (QKD), quantum cryptanalysis and quantum sensing on offensive as well as defensive capabilities.²²⁷ For example, while use of quantum encryption through the transmission of QKDs may provide an advantage to defence, quantum cryptanalysis is seen as an 'inherently offensive capability'.²²⁸ Quantum technologies will also likely enable advances in field relevant to defence and thus have an indirect impact on the future battlefield, e.g. through quantum-enabled development of advanced materials.²²⁹

Despite continuing advances in the development of quantum computing, current estimates suggest that quantum computers may still take a decade or longer to develop, with the timeframe for their potential broader uptake reaching beyond 2040.²³⁰

3.2.4. Computing, data storage, and telecommunications

There are various new and emerging technologies of relevance to providing computing, data storage and telecommunications capabilities. Innovative computing technologies include not only quantum computers, but also cloud AI²³¹ and edge AI computing.²³² Advanced supercomputers,²³³ semiconductors²³⁴ and semi-processors²³⁵ also represent important technological advances in computing. Technologies such as high-density low-energy consumption data storage solutions and holographic data storage, among others, are enabling improved capacities for the storing of data. Telecommunications includes solutions for the analogue or digital transmission of information through technologies such as **5G** and advanced fibre optic technologies.

The development of advanced military capabilities and solutions for the future battlefield relies on the availability of a large amount of computational resources and high-performance computing solutions. Future advances in computing are likely to focus on increasing the speed and energy efficiency of computing as well as reducing latency. Telecommunications services are also increasingly important for civil, military and commercial stakeholders, while advanced telecommunications technologies such as 5G may also pose challenges for defence and security and constitute new or potential future national security threats.²³⁶ Consultations with the STOA indicated that as computing, data storage and telecommunications technologies are already in use

²²⁷ See IISS (2019).

²²⁸ See IISS (2019).

²²⁹ See Murray (2016).

²³⁰ See Greenemeier (2018).

²³¹ Cloud AI computing refers to the layering of AI and cloud computing solutions, with cloud computing defined as the 'on-demand delivery of IT resources over the Internet with pay-as-you-go pricing'. In security and defence contexts, cloud AI computing may encompass advanced networks of remote Internet servers as a data storage and processing solution, AWS (n.d.), Cuthbertson (2019).

²³² Edge AI computing describes the 'concept of storing data and computing data directly at the location where it is needed'. This enables improved personalisation as well as increased latency and reduced security risks in data transfer processes, Wu (2020).

²³³ Supercomputers are distinguished from conventional (personal) computers through the capacity to provide significantly higher computing power, ASC Community (2018).

²³⁴ Semiconductors are materials that can function both as an electric conductor and insulator in various contexts, GCS (2018).

²³⁵ Holographic data storage devices include technologies that can store information as 3D holograms, including holographic versatile discs (HVDs), drives and cards. Holographic devices may improve the density of data storage, data reading and writing speeds as well as resilience of devices, Irving (2018).

²³⁶ For example, Hoehn and Sayler (2020).

in the European defence context, with incremental improvements expected out to 2040, the cumulative impact of these technologies may be smaller than that of other technologies.

3.2.5. Sensor and radar technologies

Military capabilities conventionally include a range of sensor and radar technologies used as analytical devices for the detection or measurement of physical and environmental indicators such as the presence, direction, speed of movement of objects or chemical and biological substances. Among next-generation sensors, innovative technologies may include advanced optical, infrared and UV, sound, sonar and motion sensors. Additionally, various analytical devices may be used as chemical and biological sensors for the detection of the use of chemical or biological substances. Sensor technologies may also be used to provide persistent sensing, i.e. continuous surveillance or monitoring of a defined area, or be integrated into so-called 'smart dust' or wireless sensor networks (WSNs).²³⁷

The development of advanced sensor and radar technologies provides various opportunities for defence through increasing the range of indicators that can be captured and measured, as well as improving the precision of such measurements. This may, for example, facilitate faster and improved detection of chemical or biological weapons uses, as well as advance air and missile defences.²³⁸

Advances in sensor and radar technologies are also crucial for ensuring sufficient coverage and effectiveness of intelligence, surveillance, target acquisition and reconnaissance (ISTAR) capabilities in future battlefield contexts. Next-generation sensor and radar technologies are also considered integral for the development and operation of advanced robotics and autonomous systems as well as other military capabilities.

The development and proliferation, however, of advanced sensors and radars may also pose risks and security challenges. For example, new sensors able to capture a wider range and new types of data may present data and information security challenges for military as well as civilian stakeholders. The proliferation of smart sensors and radars also increases computational power, energy and data storage demands that militaries need to meet to efficiently utilise such technologies.

²³⁷ WSNs can be defined as 'self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed' Matin and Islam (2012).

²³⁸ For example, Erwin (2019).

4. Findings, implications and policy options for the EU

This chapter presents a cross-cutting analysis of the issues and challenges stemming from new and emerging technologies, discussed in previous chapters, in relation to the 2040 battlefield (Section 4.1). The chapter also discusses cross-cutting implications for the EU and formulates policy options for addressing them (Section 4.2). Insights informing this chapter were derived from data collection and analysis activities carried out in the context of this study, including the literature review, horizon scanning, expert interviews, internal workshops, and STREAM workshop activities.

4.1. Cross-cutting findings and implications

Table 4.1 provides an overview of the key cross-cutting findings of the study in relation to the impact of new and emerging technologies on the future battlefield.

Table 4.1 – Overview of cross-cutting findings

Category	Key findings
Nature of impact of emerging technologies on the future battlefield	<ul style="list-style-type: none"> • Access to and control of data will represent a key enabler on the future battlefield as a range of new and emerging technologies will provide new opportunities for collecting, managing, and analysing data to achieve superiority on the battlefield. • Emerging future technologies both exacerbate complexity of future battlefield interactions and offer ways to mitigate that complexity. • Emerging technologies are expected to shape both conventional and unconventional warfare, potentially further mudding boundaries between the two and requiring an equal focus on the impact of technologies on above- and sub-threshold activities. • Technological advances and the magnitude of their expected impact may suggest an emphasis on qualitative improvement of future forces. Considerations, however, should be made as regards the resilience and ability of forces to rebuild quantitatively in the event of a loss of technological superiority. • An increased reliance on technological solutions may increase risk of systemic disruption caused by single points of failures and vulnerabilities that may need to be managed also through non-technological approaches to fostering resilience. • Pervasive technological change is not expected to diminish the importance of human factors or significantly reduce the uncertainty and unpredictability of the nature of war.
Factors shaping the impact of emerging technologies on the future battlefield	<ul style="list-style-type: none"> • Characterising the impact of new and emerging technologies should go beyond considering isolated technological advances. Rather, it should consider interactions among technological trends. • The extent and manner in which new and emerging technologies may be employed by EU MS armed forces in a defence context will depend also on whether and how technologies are adopted by adversaries. • Organisational adaptation and wider socioeconomic and cultural factors (e.g. flexibility in strategic mindsets and organisational culture) will act as enablers or barriers for the uptake and use of new and emerging technologies.
Enablers and barriers in European defence	<ul style="list-style-type: none"> • The ability of the EU and its MS to effectively navigate an increasingly complex technology and innovation landscape represents a key enabler to achieve superiority on the battlefield. To foster and retain this, EU MS should continue efforts to attract technological expertise,

Category	Key findings
	<p>foster innovation, and establishing relevant policy and regulatory mechanisms to guide investments in technological R&D.</p> <ul style="list-style-type: none"> • Divergences in access to new and emerging technologies, financial and cost-related barriers, as well as differing strategic mindsets among EU MS may shape national adoption pathways.

Source: RAND Europe analysis.

4.1.1. The nature of impact of emerging technologies on the future battlefield

The rapid pace of technological change as well as advances in individual technological fields are likely to significantly shape both the battlefield context and the wider socio-cultural context in which future conflicts take place. Continuous technological developments may foster an over-reliance on technological systems due to overly optimistic perceptions of the efficacy of technological solutions for complex policy issues among populations and policymakers. Additionally, the rapid global proliferation of technology may create opportunities for technologies such as offensive cyber tools, biological weapons and weapons of mass destruction may become increasingly affordable and accessible to adversaries, particularly non-state actors.²³⁹ The proliferation of advanced technologies to a greater number of actors may thus fundamentally shape the nature of future battlefield interactions and who the key actors on the 2040 battlefield are.

This study provides several cross-cutting insights on the way in which new and emerging technologies may shape the future battlefield. The collected evidence base suggests that interactions on the future battlefield will likely be shaped by an overarching importance of data in light of the increasing quantity of information that actors on the battlefield will have access to but will also need to store, aggregate and process.²⁴⁰ As such, the ability of actors to fully exploit opportunities provided by emerging technologies in the battlefield context may fundamentally depend on the capacity of actors to establish and maintain data access, ownership and control. Sufficient quantity and quality of data is considered key not only for systems such as AI, ML and Big Data but also for the development and adoption of other technology clusters, including biotechnologies. Security of data will also be pivotal to ensuring resilience and mitigating against vulnerabilities and threats stemming from adversarial access to sensitive data. It was, for example, noted that the potential for a state actor to gain access to highly sensitive data (e.g. DNA data) may enable the monopolisation of pharmaceuticals relevant to peer actors or the design of highly targeted potentially weaponised pathogens.²⁴¹

While access to and control of data represents a cross-cutting factor shaping the development and use of emerging technologies, some technology clusters are also considered crucial enablers for the processing of increasing quantities of increasingly complex data. AI, ML and Big Data in particular offer significant opportunities for actors on the future battlefield in this regard. The relevance of AI, ML and Big Data for the management of the data layer of the future battlefield includes a substantial impact on speed and complexity of decision-making on the battlefield.²⁴² This is due to the enabling role of AI for systems to react significantly faster than those relying on manual operational input, navigate exponential increases in the quantity of data processed for operational analysis, and help decision-makers to more rapidly navigate uncertain and complex environments.²⁴³

²³⁹ See Kepe et al. (2018).

²⁴⁰ RAND Europe workshop (October 2020).

²⁴¹ RAND Europe workshop (October 2020).

²⁴² RAND Europe workshop (October 2020).

²⁴³ For example, Payne (2018), Sayler (2020).

As such, while new and emerging technologies add a layer of complexity to the future battlefield, they also provide opportunities for making sense of such complexity. This concerns particularly the opportunities provided by technologies such as AI, as well as autonomous systems, to establish a more accurate and comprehensive understanding of an adversary's capabilities and actions through applications to ISR as well as advanced and predictive analytics. Automation, however, as well as the integration of AI with technologies delivering non-kinetic effects, may increase the challenges of attribution.

As technology develops, so too will the dynamics of conflict. Existing research indicates that future conflicts are likely to be characterised by a disintegration of the boundaries between conventional and unconventional or asymmetric warfare and between the states of war and peace.²⁴⁴ The possibility of interstate conflicts will persist, but their conduct may be diversified through elements of hybrid warfare, proxy wars, offensive and defensive use of cyber capabilities and strategic attacks to disrupt critical. Conflicts are anticipated to take place in all physical (land, air, sea and space) and virtual (cyber) domains. Rather than being limited to one domain at any one time, actors are likely to shift between domains, seeking to leverage those that provide them with the biggest advantage or where they have superior capabilities.²⁴⁵

Emerging technologies could play a significant role in shaping these evolving boundaries between conventional and unconventional, symmetric and asymmetric, as well as above- and sub-threshold conflict. Technologies such as AI and ML may, for example, augment existing capabilities of malicious actors to achieve strategic goals by exploiting vulnerabilities in societal resilience through manipulation of the social media layer of the information environment to instigate widespread societal disruption. Exploitation of emerging technologies on the future battlefield is therefore likely to span the full continuum of conflict. While maintaining military-technological superiority in above-threshold battlefield scenarios may be prioritised, the failure to maintain such superiority in the sub-threshold space may also result in vulnerabilities being exploited by future adversaries below the conventional conflict threshold.²⁴⁶

The ability to establish and maintain military-technological superiority has conventionally been considered as an offset to a quantitative disadvantage by Western militaries.²⁴⁷ This has informed a focus on achieving qualitative operational and strategic advantages over an assumed adversary through a general pursuit of technological advancements.²⁴⁸ The proliferation, however, of advanced emerging technologies on the future battlefield may require the EU MS to consider how armed forces can achieve mass more rapidly in the event of technological superiority being undermined or limited by means of unexpected vulnerabilities or adversarial breakthroughs. As such, there is a need to better understand the possible impacts of a potential future loss of technological edges against a potential adversary, particularly in relation to the speed with which military forces can be reconstituted and rebuilt.²⁴⁹

As described throughout Chapter 3, technologies such as those providing space-based services as well as AI, ML and Big Data are likely to be increasingly relevant for defence. This indicates a likely shift towards increasing reliance within defence on such technologies thus increasing vulnerabilities to potential wide-spread disruption caused by attacks against single points of failure. As such, future policy-making should consider the benefits of developing non-technological solutions to maintaining societal resilience in the event of wide-spread disruption to complex technological

²⁴⁴ See Kepe et al. (2018), Winkler et al. (2019).

²⁴⁵ See Kepe et al. (2018)

²⁴⁶ RAND Europe workshop (November 2020).

²⁴⁷ See Kepe et al (2018).

²⁴⁸ See Winkler et al (2019).

²⁴⁹ RAND Europe workshop (November 2020).

networks underpinning the provision of many public as well as defence- and security-related services.²⁵⁰

Lastly, while emerging technologies may significantly shape the future character of conflict through defining the techniques of war, historical scholarship points to the prevalence of the fundamentals of war despite technological change.²⁵¹ These fundamentals include emotive factors such as fear, ambition, and opportunism, which shape interactions among actors on the battlefield; as well as uncertainty and unpredictability of such interactions. As such, future policy and strategy may need to account for the impacts of technological change as well as the fact that such change, however pervasive it may be, is unlikely to change the need for actors on the future battlefield to navigate human dimensions of armed conflict.²⁵²

4.1.2. Factors shaping the impact of emerging technologies on the future battlefield

While some impacts of emerging technologies can be clearly delineated, factors including the interaction among technological advances, actors on the battlefield, and non-technological factors can significantly shape how technologies impact European defence or future battlefield dynamics.

This being the case, characterising the impact of new and emerging technologies on European defence and future battlefield dynamics ought to go beyond considering isolated technological advances. Rather, interactions *among* technologies need to be taken into account as those may produce additional, novel effects or magnify the impacts of individual technologies. Equally, limitations and shortfalls in one technology area may constrain the adoption and deployment of other technologies (e.g. impossibility to deploy a new AI/ML algorithm due to limits in computing power).²⁵³ This includes, in particular, the interaction of AI, ML and Big Data technologies with other technology clusters such as biotechnology and technologies for the delivery of novel effect. This is due to the application of AI, ML and Big Data across different systems, with existing research noting that advances in these technologies should be explicitly considered as advances in *AI-enabled* applications.²⁵⁴ Further, advances in one technology area may serve as enablers for improvements in other technological areas, particularly with regard to the role of AI and ML in autonomous systems and human-machine interfaces.

The impact of emerging technologies on the future battlefield will also ultimately be shaped by interactions among actors on the future battlefield. As conflicts remain actor-centric phenomena, the extent and manner in which new and emerging technologies may be applied by EU MS armed forces in a defence context is shaped by whether and how certain technologies are adopted by adversaries. For example, the extent to which AI and ML may add complexity and speed to decision-making processes on the future battlefield depends on an assumption that both, or all, parties utilise AI and ML-based systems.

Similarly, the degree to which certain technologies may facilitate escalation or arms race-type dynamics is a function of reactions and interactions among actors on the future battlefield, rather than the capabilities or motivations of individual actors.²⁵⁵ As such, while there may be a risk of technological arms race dynamics emerging in the form of a 'race to develop the most capable [technology] and to translate this into economic dominance by capturing markets, users, data and customers', the framing of technological developments as potential arms races may run the risk of

²⁵⁰ RAND Europe workshop (November 2020).

²⁵¹ For example, Herberg-Rothe (2009).

²⁵² RAND Europe workshop (November 2020).

²⁵³ RAND Europe workshop (October 2020).

²⁵⁴ For example, Franke (2019).

²⁵⁵ See Franke (2019), RAND Europe workshop (October 2020).

such dynamics becoming self-fulfilling prophecies.²⁵⁶ This is due to the inherent uncertainty characterising future technology development and adoption, and perceived incentives by policy-makers to rapidly implement often untried and untested new technologies due to the risk of losing strategic advantage.²⁵⁷

Further to the impact of individual technologies being amplified by interactions among various technological advances, non-technological factors may play an important role in inducing systemic shifts in future defence and battlefield contexts. Organisational adaptation and wider socioeconomic and cultural factors may serve as crucial enablers or barriers for the uptake and use of new and emerging technologies. These factors are encapsulated in the concept of organisational absorptive capacity and include:²⁵⁸

- Flexibility in strategic mindsets and organisational culture, including the ability of militaries to recognise and capitalise on the opportunities inherent in new technologies in military applications so as to create a strategic advantage;
- Organisational capacity to adapt and exploit opportunities provided by technological advances, including through the revision of organisational processes and procedures, doctrine, policy and ethics guidelines;
- Organisational ability to foster innovation and relevant expertise across all leadership and personnel levels, including through education, training as well as recruitment processes;
- Capacity to harness innovation from non-Defence and civilian R&D efforts, including through the adaptation of acquisition processes.

The evolution of legal, ethical and regulatory frameworks represents an additional factor shaping the ability of organisations to harness technological advances out to 2040. These frameworks may evolve in a way so as to significantly diverge nationally and regionally, with adversaries potentially facing lower legal, regulatory and ethical constraints for R&D as well as deployment of certain new and emerging technologies. In combination with evolving concepts and doctrines, the evolution of national and international legal, ethical and regulatory frameworks as well as potential future divergences could significantly shape battlefield interactions as well as the previously-described blurring of delineations between war and sub-threshold conflict.²⁵⁹

Overall, therefore, technological advances ought not be considered in isolation, but rather through the lens of the effects that such advances produce for organisational and operational change. This corroborates perspectives from existing research emphasising that changes in how technologies are used and employed by military organisations, rather than technological advances themselves, are likely to lead to fundamental or revolutionary shifts in military tactics and the character of conflict.²⁶⁰

4.1.3. Enablers and barriers in European defence

The future impact of emerging technologies on the battlefield may be shaped by various enablers and barriers that are specific to the European defence context. This includes the ability of the EU and its MS to effectively navigate an increasingly complex technology and innovation landscape.

Technological innovation is projected to occur primarily in the private sector and in the context of companies that may be reluctant to support defence programmes and applications. Furthermore,

²⁵⁶ See Asaro (2019), RAND Europe workshop (October 2020).

²⁵⁷ RAND Europe workshop (October 2020).

²⁵⁸ RAND Europe workshop (October 2020).

²⁵⁹ RAND Europe workshop (November 2020).

²⁶⁰ For example, Cohen (2015).

innovation may occur largely through companies located outside of the EU, raising challenges for the monitoring and assessing of supply-chain security, as well as the pursuit of European strategic autonomy. In addition, technological advances are each expected to occur at a different pace, resulting in challenges for forecasting the interaction of different technologies in increasingly complex supply chains.

Effectively navigating this landscape will be key for the EU's ability to fully exploit the opportunities provided by emerging technologies for military efficiency and effectiveness and ensuring that such technologies are developed and employed in line with relevant ethical, regulatory and legal safeguards. This includes overcoming existing policy hurdles that exist in the European policymaking context. For example, as battles start to unfold at faster paces, automated decision making may become a necessity, as human commanders are unable to keep up with the pace of warfare.²⁶¹ Europe would thus be faced with the challenge of integrating automation capabilities into policy. A degree of resistance to automated decision making already exists, reflected, for example, in Art. 22(1) GDPR, which prohibits decision making on the data of natural persons based solely on automated processing. Yet, as such technology progresses and becomes more reliable, there will be a need to adapt policy to take advantage of this and other emerging technologies.

Additional enablers for the EU's ability to navigate the evolving technology landscape to the benefit of European defence include:

- Developing a capability to detect potentially important S&T developments so as to enable early action (e.g. through a horizon scanning and early warning system);
- Ensuring the ability of European universities and research organisations to attract leading talent in technological R&D and associated incentives for harnessing cutting edge innovation;
- Establishing relevant policy and regulatory mechanisms to guide investments in technological R&D in the application of emerging technologies within defence and military contexts in compliance with relevant ethical and normative standards (e.g. meaningful human control);²⁶²
- Focusing R&D to strengthen capabilities to mitigate potentially disruptive effects of emerging technologies within defence contexts, such as investments in AI-enabled and autonomous systems for counter-UAS applications;²⁶³
- Strengthening the capacity of the EU and its MS to shape the international regulatory and governance context with regard to the ethical and normative standards for the uses of emerging technologies employed within defence and battlefield contexts. The issue of Lethal or Fully Autonomous Weapons Systems (LAWS/FAWS) was highlighted as an issue of significant concern for the EU.²⁶⁴

Further to these cross-cutting enablers, adoption pathways for new and emerging technologies may significantly vary among the EU MS. Varying levels of access to new and emerging technologies, financial and cost-related barriers, as well as differing strategic mindsets may play a role in such variations.²⁶⁵ Additionally, heterogeneity in national policy and regulatory contexts should be taken into account, particularly when considering the relative weight of regulatory barriers on the future development and uptake of various emerging technologies in European defence.

²⁶¹ See Economist (2018).

²⁶² RAND Europe interview (INT06, October 2020).

²⁶³ RAND Europe interview (INT06, October 2020).

²⁶⁴ RAND Europe interview (INT01, October 2020).

²⁶⁵ RAND Europe workshop (October 2020), Franke (2019).

4.2. Policy options

As discussed in detail in Section 4.1, technological trends and broader political, social, economic, and environmental trends may result in a future marked by uncertainty, complexity and rapid change. This could exacerbate current trends characterising contemporary defence and military dynamics or perhaps initiate new dynamic, opportunities and challenges. This section presents policy options for EU and MS institutions to consider in their ongoing efforts to prepare for and shape this rapidly evolving landscape. It does so by setting out three broad policy options for EUs and MS that have been developed by the RAND Europe study team. These include:

- Pursuing a broad range of capability development initiatives;
- Ensuring the development of an environment characterised by the necessary regulatory and organisational agility and absorption capacity;
- Facilitate EU investments and research, development, technology and innovation (RDT&I) activities in relevant new and emerging technologies by strengthening collaboration with industry.

These policy options build on the overall study findings presented in the previous chapters and have been developed on the basis of the study's STREAM workshop insights, and internal expert workshops. While these policy options seek to outline initial options for capitalising on the opportunities or mitigating the challenges of technological change, further analysis of their practical implementation or associated resource requirements should be conducted in the event of their adoption and implementation. Each of these policy options emphasises a distinct type of intervention required to create a more holistic approach to fostering innovation and facilitating technology uptake and absorption across EU MS armed forces.

In addition to the individual policy options, the following principles should be considered by policy- and decision-makers when developing and pursuing initiatives concerning the impact that technological developments may have on the future battlefield:

- **Adopting a broad range of initiatives.** Regardless of which technologies ultimately have the largest impact on the future battlefield out to 2040, it is likely that EU MS armed forces will require to adopt a wide array of strategic and policy measures to adequately prepare to foster, absorb, and leverage technological innovation. The policy options provided in the following sections are neither exhaustive, nor mutually exclusive, nor is any of them sufficient if taken on its own. Rather, a key aspect of future decision-making will pertain to the identification of suitable combination of, ideally, mutually reinforcing initiatives and policies to achieve desired outcomes.
- **Placing emphasis on technology-agnostic approaches where possible.** While the study focused on a subset of technology clusters, the policy options presented below are typically agnostic to technologies. Indeed, the policy options presented could be adapted to cater and address challenges stemming from different technologies than those considered in this study and that could surface or advance at a different pace of development than currently expected (e.g. quantum technologies). This is not to suggest that technology-specific initiatives should be discounted, but rather that they should be integrated in the context of broader efforts aimed at fostering preparedness, resilience, and adaptability from a general innovation standpoint. An approach that is grounded, as much as possible, in technology-agnostic solutions has the added benefit of providing greater resilience and adaptability to deal with multiple possible futures. Such possible futures would include those in which today's projections of the future uptake or impact of any given single technology prove to be incorrect.

- **Prioritising resource use and investments according to a clear intervention logic.** The technology trends discussed in this report may have a profound impact on the future battlefield and societies more broadly. While different policy approaches and initiatives could be implemented, in a context of resource constraints and finite opportunities for action EU Institutions (EUIs) and MS will be required to make choices and balance different trade-offs. Future policies and initiatives should be accompanied by adequate planning and ex ante analyses, as well as be supported throughout their lifecycle and implementation by adequate monitoring and evaluation activities. These activities should be aimed at ensuring that the initiatives and policies being implemented are relevant, coherent, effective and efficient, as well as linked to a clear overarching intervention logic.
- **Adopting approaches and initiatives that are cognisant and reflective of changing realities concerning technological innovation and advances in the context of defence.** As discussed in previous sections of this report, dynamics concerning the science and technology landscape, as well as how and where innovation occurs in a context of defence, have changed significantly in recent years. Now, a great deal of innovation occurs outside of the defence industry, at a pace that is poorly compatible with traditional defence procurement cycles. In this context, any initiatives or investments that are made should be cognisant of and able to adhere to requirements stemming from these challenges. For instance, this might involve facilitating participation in procurement and R&D activities by companies not traditionally involved with defence industry. More broadly, the pace and breadth of technological developments suggest that traditional concepts of technological superiority should be nuanced (to reflect realities stemming from an increasingly complex threat landscape) and inform efforts supporting any ambition to pursue this. Indeed, the use of a variety of technologies into platforms and capabilities linked in complex systems of systems will result in the potential embedding of vulnerabilities. These vulnerabilities could then be leveraged by adversaries and malicious actors that do not have access to similar technologies, emphasising a need to consider vulnerabilities and threats stemming from technologies even when superiority in a given field is achieved.

With these considerations in mind, the following sections provide a more detailed overview of each of the policy options and their supporting actions to help inform future decision making and allocation of resources by EUIs and MS.

4.2.1. Further pursue a broad range of capability development initiatives

As discussed in Chapter 2 of this report, the future battlefield will likely require EU MS Armed Forces and allies to conduct a variety of missions and operations in a wide range of terrain, weather and climate conditions. This will require the development of multi-purpose capabilities, integrating new and emerging technologies and leveraging their potential as part of a broader system of systems under new concepts of operations and doctrinal approaches. For example, developing capabilities to augment the situational awareness of individual soldiers on the battlefield may be achieved through real time collation and analysis of data collected by sensors embedded across different platforms and processed by different algorithmic tools.

Technological developments may render obsolete existing capabilities and generate requirements for fostering and sustaining new skills, systems, and approaches. Technological advances, however, are unlikely to result in a full obsolescence of existing technologies and requirements. As such, military planners will be required to consider not only cutting-edge, high-end technologies but also the specific challenges and opportunities arising from the use of existing technologies, or the combination of existing technologies with novel tactics and capabilities. For instance, vulnerabilities associated with human factors are unlikely to be fully mitigated by technological augmentations in the context of the future battlefield.

Future technological developments may also result in a broader spectrum of sub-threshold activities. This will require EUs and MS to prepare so that such approaches may not be leveraged to degrade and unravel the cohesion of the EU and of MS societies and institutions, as well as those of its broader alliances and partnerships.

Within this context, EUs and MS should continue to pursue a broad range of capability development investments concerning new and emerging technologies that may have an impact on the future battlefield including as regards sub-threshold activities. Such investments should encompass a variety of activities including early stage research, technology, development, and innovation (RDT&I) related to the development, implementation, assurance, and testing of new and emerging technologies. This could entail investment in university research and other RDT&I efforts related to the development, implementation, security, assurance, and testing of emerging technologies.

Equally, in order for the EU and its MS to be in a position to adequately respond to challenges and benefit from opportunities posed by new and emerging technologies on the future battlefield, there must be capability to understand these at the technical level. As such, adequate skills and competences must be fostered and retained to understand and work with new and emerging technologies. This is not just at the level of RDT&I activities, but also at the level of senior decision-makers, planners, and general staff of EU MS armed forces.

While emphasis should be placed on technology-agnostic interventions, as noted above, a number of technology clusters and developments will also require tailored investments and initiatives including due to the complex ethical, technological, and legal challenges and implications that stem from them (e.g. AI, autonomous systems and weapons, biotechnology). For further details on the relevance, significance, and challenges associated with specific technology areas please refer to Chapter 3 of this document.

In this context, the following principles and supporting actions should be considered when pursuing a broad range of capability development initiatives:

- **Continue to monitor science and technology developments to assess opportunities and threats stemming from these.** In order to be able to detect potentially relevant S&T developments and enable early action where necessary, efforts should be made to conduct rolling horizon scanning and threat assessment activities. These should be conducted on a continuous basis to take stock of new and emerging technology developments and their associated opportunities and threats. Additionally, analysis should go beyond the narrow confines of traditional security and defence with a view to assessing not just how technological capabilities and advances could be employed to support EU MS Armed Forces on the future battlefield but also to enhance the resilience of the EU and its MS vis-à-vis sub-threshold activities. Results stemming from horizon scanning and threat assessment activities could provide different actors and stakeholders with a common baseline of knowledge and understanding of future challenges and opportunities. They could also be leveraged to inform and support decision-making activities as regards priority technology areas to be pursued through capability development initiatives. With a view to ensuring a common situational awareness and understanding of S&T developments across EU MS, there may be merit in exploring options for this activity to be implemented at the EU level through the work of EDA.
- **Identify priority areas for capability development to be pursued through joint initiatives to facilitate EU cooperation and interoperability.** As noted above, the technological advances discussed in this report may have a profound impact on the future battlefield and on requirements for EU MS armed forces. In the context of finite resources, priority areas for capability development will need to be identified. This is not only to effectively prioritise investments, but also to ensure that initiatives are designed and implemented in the fora that enable impact and overall efficiency to be maximised. In this

regard, care should be taken in identifying those technologies and capabilities that would best benefit from joint development efforts across the EU to guarantee a high degree of interoperability in the context of future missions and operations under CSDP. Ensuring interoperability in key areas of capability development (e.g. command and control) and increasing the efficiency and effectiveness of defence spending by avoiding duplication and enhancing readiness, should be balanced with fully exploiting national expertise and specialist skills.

For those technologies and requirements that would most benefit from the development of an interoperable-by-default capability through joint efforts at the level of EU MS and through consortia of European industrial actors, existing initiatives and platforms to facilitate these should be considered. Indeed, a number of existing programmes could be exploited for these purposes. The recent launch of PESCO and the EDF and European Defence Industrial Development Programme (EDIDP) have opened up new opportunities for EU MS and European industry to improve cooperation in the area of research and capability development. Any further initiatives could also build on lessons learned through prior efforts delivered in the space of joint capability development efforts by the EDA to facilitate joint procurements and overcome the political, cultural and practical barriers to successful multinational programmes in areas of defence.

- **Identify continued areas for strengthening cooperation and coordination with NATO and key EU allies.** Looking beyond the EU policy and institutional landscape, efforts should be made to strengthen working-level and programme-level cooperation and coordination between relevant EU and NATO actors to maximise synergies and coherence of approach in the area of capability development. This should be done with respect to the spirit and mandate of the 2016 Joint Declaration and its implementation plans. In this regard, EDA should continue to play a facilitating role in identifying and pursuing synergies and cooperation with relevant NATO counterparts. Similarly, the fostering of European strategic autonomy should not preclude an exploitation of the opportunities provided by emerging technologies coherently with initiatives being pursued by NATO or key EU allies, such as the US.

4.2.2. Ensure the development of an environment characterised by the appropriate regulatory and organisational agility and absorption capacity

As discussed in Section 4.1 above and elsewhere in this report, technological advances and developments are expected to occur over the next decades at such a pace, and have such wide-ranging impact, that EU MS and their armed forces could struggle to cope with them. If the advances discussed in this report occur as envisioned, they are likely to have profound implications and require that initiatives and changes are implemented. Initiatives should not touch on procurement aspects alone, but more widely aim to ensure the establishment of an environment conducive to the leveraging and exploitation of technological advances. This should be done in a manner that maximises the positive impacts of new technologies and manages and minimises their associated vulnerabilities and nefarious effects. Additionally, flexibility will be required also to account and consider for past technologies and capabilities.

In this context, EUs and MS should work towards ensuring that EU MS Armed Forces and the structures and processes envisioned under CSDP are agile and suited to prepare for, respond to, and exploit as appropriate any technology developments and advances occurring in the next decades of the kind considered in this report. EU MS Armed Forces and the broader institutional and organisational frameworks within which they operate should develop the capacity and agility required to harness technological advances, mitigate against their use by adversaries, and manage any vulnerabilities. To achieve this, complex systems characterised by several interacting factors should be leveraged.

Previous RAND research has identified a number of factors of innovation systems in defence that enables innovation and transformation.²⁶⁶ Innovation can be conceptualised as comprising and being enabled by a mix of provisions concerning organisations expected to deliver and harness this. Such factors include considerations about tools and systems employed; organisational knowledge; staff skills and behaviours; and processes that enable the delivery of specific outputs and outcomes. This approach, or alternative ones, could be used by EUs and MS when considering whether and how to best adapt their organisation, structures, and culture to forecast, prepare for and harness technological advancements.

To formulate specific policy options for an architecture and approach for achieving this at the EU and MS level falls beyond the scope of this project. Several specific aspects and challenges, however, should be considered when addressing this policy option:

- **Contribute to the development and uptake of norms, regulation and appropriate legislation for the use of different technologies in a defence context, including for those technologies emerging from outside the EU.** A number of ethical and legal concerns in relation to new and emerging technologies considered under this study were noted in Chapter 3 of the report. Similarly, concerns as to the possible legal and ethical implications of the use of different technologies were raised by experts and stakeholders consulted over the course of this study. EUs and MS should therefore explore options for identifying legal and regulatory standards for the use of different technologies both within the EU and globally.

Efforts should be made to assess technology areas and their associated advances to determine whether and how any regulatory and legal adjustments are necessary. Equally, this should entail a review of existing treaties and instruments that may already provide adequate frameworks and provisions for envisioned advances. EUs and MS should seek to contribute to such discussions and efforts also at an international level, facilitating the adoption of common approaches and commitments that resonate with EU values.

More broadly, EUs and MS should work to developing guidance on how different technologies could be employed and standardised in the context of EU MS Armed Forces with a view to ensure ethical and legal compliance and interoperability.

- **Ensure the fostering and retention of an adequate skills base for harnessing technological advances both within EU MS Armed Forces and broader defence industry.** EUs and MS should ensure the fostering and retention of an adequate skills base to facilitate the adoption and exploitation of new and emerging technologies. This would entail focusing on the development of skills both within EU MS Armed Forces and institutions, as well as across broader EU defence industry.

As regards EUs and EU MS Armed Forces and institutions, efforts should be made to promote the development of common training approaches and resources. For instance, this could entail the development of standardised training curricula and courses through the European Security and Defence College.

As regards defence industrial skills, RAND Europe has previously identified a range of strategic objectives and supporting actions for fostering and retaining defence industrial skills and competences. This could entail improving communication between EUs, MS, industry and the education and training sector by establishing fora for strategic dialogue around industrial skills issues. This policy option could be implemented by leveraging existing coordination and cooperation mechanisms and aim to inter alia develop joint skills profiles encompassing a focus on new and emerging technologies that could be transferred

²⁶⁶ See Freeman et al. (2015).

within the defence industry and between defence and other high-tech industries to ensure their sustainability. Moreover, coordination fora linking industry, the education and training sector, MS, and EUs could be leveraged to better match supply with demand for defence-relevant skills.²⁶⁷

- **Consider the impact that new and emerging technologies will have on concepts of operations.** As noted in previous sections of this report, technological advances will require for the flexible adaptation of existing structure, processes, and culture characterising EU MS Armed Forces. Equally, military planners will be required to consider not only cutting-edge, high-end technologies but also the specific challenges and opportunities arising from the battlefield use of older technologies, or the combination of old technologies with novel tactics and capabilities. In addition, efforts should be made to investigate wider implications stemming from technological advances, including, as regards logistics and through-life-support of different platforms, tools and products. In this context, EUs and MS should consider working to experiment with, design and update tactics and concepts of operations in light of technological advancements and wider strategic developments. This could include gaming, modelling and experimentation activities in order to develop and refine innovative new ideas for how to address the impact and vulnerabilities of technologies and address future battlefield threats.

4.2.3. Facilitate EU investments and RDT&I activities in relevant new and emerging technologies by strengthening collaboration with industry

As discussed in Section 4.1 of this report, RDT&I in the technology areas considered in this study are primarily driven by private sector actors, often originating from outside the traditional defence industrial base. In this context, EU MS and their defence establishments have been faced with increasing challenges in terms of harnessing and adapting to technological advances that occur at a fast pace, are globally accessible, and fall outside their direct or exclusive control. In addition to requirements for greater organisational absorptive capacity, agility and flexibility discussed in Section 4.2.2, these trends put an increasing pressure on governments to invest in a wide array of developing technologies and ensuring access to these in a manner that facilitates their harnessing in a defence context. In this context, the following actions should be considered for implementation by EUs and MS governments and Armed Forces.

- **Identify means for providing industry with clear guidance on future military requirements in order to help incentivise and guide investments in relevant RDT&I and capability development initiatives.** Industry lacks certainty and clear directions concerning key military requirements for the future platforms, weapons, and overarching systems envisioned to leverage them. EUs and MS should consider strengthening fora and mechanisms for providing industry with access to clear guidance on future military requirements. This could help incentivise and guide investments in relevant RDT&I activities within industry. This entails developing and maintaining partnerships that go beyond traditional customer-supplier relationships and should involve structures for innovation where inventors, investors and industry can partner across a wide range of technology areas. These activities could also entail exploring measures to simplify and reduce procurement and regulatory burdens that limit the ability of industry actors to operate across different MS.

²⁶⁷ Further details on the operationalisation of possible actions and approaches pertaining to this recommendation can be found in the European Commission's European vision on defence-related skills and supporting actions to solve the skills gap today and tomorrow in Europe.

- **Explore ways for broadening and sustaining engagement with companies developing dual use technologies.** In addition to strengthening and broadening engagement with defence industry, efforts should be made to establishing new partnerships and deeper collaboration mechanisms with companies developing dual-use technologies. As discussed in Section 4.1 of this report, much of the innovation and developments envisioned as potentially having an impact on the future battlefield will occur outside of defence industry and sector. EUs and MS should therefore work to: (i) broaden their engagement and mutual understanding with non-defence private sector actors developing technologies expected to have an impact on the future battlefield; (ii) better communicate their needs and requirements to non-traditional defence suppliers; and (iii) identify ways of generating incentives for such companies to invest in RDT&I, focusing on possible defence applications.

REFERENCES

- Accenture. [Realising the Economic and Societal Potential of Responsible Artificial Intelligence in the UK](#). Accenture Applied Intelligence, 2018.
- Additive Manufacturing. [What is Additive Manufacturing?](#). Additive Manufacturing website, n.d.
- Amazon Web Service (AWS). [What is cloud computing?](#). AWS. Amazon website, n.d.
- Andås, H. [Emerging technology trends for defence and security](#), Norwegian Defence Research Establishment, April 2020.
- Armstrong, R., Drapeau, M., Loeb, C. and Valdes, J. (Eds.), [Bio-inspired innovation and national security](#), Centre for Technology and National Security Policy, Washington D.C., 2010.
- Army Technology. [Put to the test: smart energy solutions for the military](#). Army Technology website, February 2016.
- Article36. [Acoustic Weapons](#). Discussion paper for the Convention on Certain Conventional Weapons (CCW). Article36 website, November 2018.
- ASC Community. [Development and Application of Supercomputing](#). *The Student Supercomputer Challenge Guide*, Springer online, March 2018, pp. 3-19. doi: 10.1007/978-981-10-3731-3_1
- Asaro, P. [What is an 'Artificial Intelligence Arms Race' Anyway?](#) *Journal of Law and Policy for the Information Society*, 2019.
- Babuta, A., Marion O. and Rinik, C. [Machine Learning Algorithms and Police Decision making](#): Legal, Ethical, and Regulatory Challenges, RUSI Whitehall Report 3-18, September 2018.
- Barrie, D. [Unstable at speed](#): hypersonics and arms control. IISS website, October 2019.
- Bathee, Y. [The Artificial Intelligence Black Box and the Failure of Intent and Causation](#). *Harvard Journal of Law and Technology*, Vol. 31(2), Harvard University Press online, 2018, pp. 890-938.
- Bickford, A. [Chemical Heroes: Pharmacological Supersoldiers in the US Military](#). Duke University Press, 2020.
- Binnendijk, A., Marler, T. and Bartels, E. [Brain-Computer Interfaces](#): US military applications and implications, Rand Report RR-2996-RC, Rand Corporation, 2020.
- Bordin, G., Hristova, M. and Luque-Perez, E. [JRC horizon scanning on dual-use civil and military research](#), JRC Science for Policy Report, European Commission, 2020.
- Boulanin, V., Davidson, N., Goussac, N. and Carlsson, M. [Limits on Autonomy in Weapon Systems](#): Identifying Practical Elements of Human Control, Stockholm International Peace Research Institute, June 2020.
- Brockmann, K., Sibylle B. and Vincent B. [Bio Plus X](#): Arms Control and the Convergence of Biology and Emerging Technologies, Stockholm International Peace Research Institute, March 2019.
- Brosig, M., Frawley, P., Hill, A., Jahn, M., Marsicek, M., Paris, A., Rose, M., Shambaljamts, A. and Thomas, N. [Implications of Climate Change](#) for the U.S. Army, United States Army War College, 2020.
- Caldwell, M., Andrews, J., Tanay, T. and Griffin, L. [AI-enabled future crime](#). *Crime Science*, Vol. 9:14, Biomedical Central Publications, 2020, pp. 1-13.
doi: 10.1186/s40163-020-00123-8
- Caves, J. P. and Carus, W. S. [The Future of Weapons of Mass Destruction: Their Nature and Role in 2030](#). Centre for the Study of Weapons of Mass Destruction, June 2014.
- Cohen, E. [Technology and Warfare](#). *Strategy in the Contemporary World: An Introduction to Strategic Studies*, edited by Baylis, J., Wirtz, J. and Gray, C., Oxford University Press, 2015, pp. 236-253.

- Cohen, R., Chandler, N., Efron, S., Frederick, B., Han, E., Klein, K., Morgan, F., Rhoades, A., Shatz, H. and Shokh, Y. [The Future of Warfare in 2030](#): Project Overview and Conclusions, RAND Report RR-2849/1-AF, RAND Corporation, 2020a.
- Cohen, R., Han, E. and Rhoades, A. [Geopolitical trends and the future of Warfare](#): The changing global environment and its implications for the US Air Force, RAND Report RR-2849/2-AF, RAND Corporation, 2020b.
- Coulon, A. and Johnson, S. [Using High-Altitude Pseudo Satellites as an innovative technology platform for climate measurements](#), American Geophysical Union, Fall Meeting 2017, abstract #A31L-03, December 2017.
- Council of the European Union. [Implementation Plan on Security and Defence](#), Note 14392/16 to the Council, Council of the European Union, November 2016.
- Cox, K., Knack, A., Robson, M., Adger, N., Paille, P., Freeman, J., Black, J., Harris, R. [A Changing Climate](#): Exploring the Implications of Climate Change for UK Defence and Security, RAND Report RR-A487-1, RAND Corporation, 2020.
- Cuthbertson, A. [War Cloud](#): Why is the US Military Building a Vast AI System and How Will it Change the Battlefield of the Future?. The Independent, Wednesday 10 July 2019.
- Davenport, T. and Ronanki, R. [Artificial Intelligence for the Real World](#). *Harvard Business Review*, January-February 2018.
- Dieulis, D. [Biotechnology for the Battlefield](#): In Need of a Strategy. War on the Rocks website, 27 November 2018.
- Department of Defense (DOD). [Future Directions in Human Machine Teaming Workshop](#), Department of Defense Research and Engineering Enterprise website, Archive for January 2020.
- Economist. [Getting to grips with military robotics](#), the Economist, 25 January 2018.
- Ekelhof, M. & Paoli, G. P. Swarm Robotics: Technical and Operational Overview of the next Generation of Autonomous Systems United Nations Institute for Disarmament Research, 2020.
- Erwin, S. [Next steps](#) for the Pentagon's new space sensors for missile defense. Space News website, 21 January 2019.
- EU2019.fi. [Digitalization and Artificial Intelligence in Defence: Food for Thought paper by Finland, Estonia, France, Germany, and the Netherlands](#), 2019(a).
- _____. [Sustainable Europe – Sustainable Future: Finland's Presidency Programme](#), 2019(b).
- European Commission (EC). [Foreign Policy](#), Policy Outreach and International Affairs (Unit D.3), European Commission website, n.d.(a)
- _____. [European Data Strategy](#), European Commission website. n.d.(b).
- _____. [Europe 2020 Flagship Initiative: Innovation Union](#), European Commission website, 2011.
- _____. [Joint Framework on countering hybrid threats](#). Joint Communication to the European Parliament and the Council, 2016(a).
- _____. [European Defence Action Plan: Towards a European Defence Fund](#). European Commission website, 2016(b).
- _____. [The European Defence Fund](#): Questions and Answers, European Commission website, 2017(a).
- _____. Reflection Paper on the Future of European Defence, [COM\(2017\) 315](#), European Commission, 7 June 2017(b).
- _____. [Antitrust](#): Commission launches sector inquiry into the consumer Internet of Things (IoT). European Commission website, 16 July 2020a.

- . [European Defence Fund](#): €205 million to boost the EU's strategic autonomy and industrial competitiveness. European Commission website, 15 June 2020b.
- . [White Paper: On Artificial Intelligence – A European approach to excellence and trust](#). European Commission website, 2020c.
- European Defence Agency (EDA). [Military Green](#): Energy & Environment at the European Defence Agency', European Defence Agency, 2012.
- . [EDF](#): Opening New 'Windows' for Defence Support, European Defence Agency, 2017.
- . [Research & Technology](#), European Defence Agency, 2020.
- European External Action Service (EEAS). [Shared Vision, Common Action: A Stronger Europe](#). Global Strategy for the European Union's Foreign and Security Policy, 2016.
- . [Global Tech Panel: Mogherini starts debate with tech leaders](#). European External Action Service website, 2018(a).
- . [About the Global Tech Panel](#). European External Action Service website, 2018(b).
- . [Digital for Development](#). European External Action Service website, 2018©.
- . [EU pushes for global cooperation on lethal autonomous weapons and to use tech for mediation](#). European External Action Service website, 2019.
- European Parliament (EP). [Questionnaire to the Commissioner-Designate Thierry Breton](#), European Parliament website, 2019.
- European Space Policy Institute (ESPI). [ESPI Report 72](#) - Europe, Space and Defence - Full Report, European Space Policy Institute, February 2020.
- Fiott, D., Missiroli, A. and Tardy, T. [Permanent Structured Cooperation: What's in a Name?](#) European Union Institute for Security Studies, Chaillot Papers, 2017.
- Franke, U. [Not smart enough](#): The poverty of European military thinking on Artificial Intelligence. Policy Brief, European Council on Foreign Relations Report ECFR/311, European Council on Foreign Relations, December 2019.
- Freedberg, S. [Carbon Nanotubes](#) & Quantum Dots: Army Thinks VERY Small. Breaking Defense website, 7 January 2020.
- Freeman, J., Hellgren, T., Mastroeni, M., Persi Paoli, G., Cox, K., Black, J. [Innovation Models: Enabling new defence solutions and enhanced benefits from science and technology](#). RAND Corporation, 2015.
- Gardner, T. [U.S. military marches forward on green energy, despite Trump](#). Reuters website, 1 March 2017.
- Gaub, F. [Global Trends to 2030](#): Challenges and Choices for Europe, European Strategy and Policy Analysis System, April 2019.
- Gauss Centre for Supercomputing (GCS). [Advancing Next-Generation Semiconductors](#)'. Technology Networks website, 9 March 2018.
- Geist, E. and Lohn, A. [How Might Artificial Intelligence Affect the Risk of Nuclear War?](#) RAND Corporation, 2018.
- Gonzalo, J., Lopez, D., Dominguez, D., Garcia A. and Escapa, A. [On the capabilities and limitations of high altitude pseudo-satellites](#). *Progress in Aerospace Sciences*, Vol. 98(April), Elsevier, 2018, pp. 37-56.
- Gordon, M. [Russia Tests an Anti-Satellite Weapon](#), U.S. Officials Say. *The Wall Street Journal*, 23 July 2020.
- Graphene Flagship. [The Graphene Flagship is research, innovation and collaboration](#). Graphene Flagship website, n.d.
- Greene, M. and Master, Z. [Ethical Issues of Using CRISPR Technologies for Research on Military Enhancement](#), *Journal of Bioethical Inquiry* 15, 2018, pp. 327-335.

- Greenemeier, L. [How Close Are We](#)—Really—to Building a Quantum Computer?. *Scientific American*, 30 May 2018.
- Gunzinger, M. and Dougherty, C. [Changing the Game: the Promise of Directed-Energy Weapons](#), 2012.
- High-Level Expert Group on Artificial Intelligence (AI HLEG). [A definition of Artificial Intelligence](#): Main capabilities and scientific disciplines. European Commission website, 8 April 2019.
- Hoehn, J. and Saylor, K. [National Security Implications](#) of Fifth Generation (5G) Mobile Technologies, Congressional Research Service Report IF11251, Congressional Research Service, 2020.
- Irving, M. [Holographic data storage](#) could cram 1,000 DVDs onto a 4-in square film. New Atlas website, 9 April 2018.
- International Institute for Strategic Studies (IISS). [Quantum Computing and defence](#). *The Military Balance 2019* edited by the IISS. Routledge, 2019, pp. 18-20.
- Johnson, D. [The Challenges of the 'Now' and Their Implications for the U.S. Army](#), RAND Perspectives PE184, RAND Corporation, 2016.
- Johnson, J. [The AI-cyber nexus](#): implications for military escalation, deterrence and strategic stability. *Journal of CyberPolicy*, Vol. 4(3), Taylor & Francis online, 2019, pp. 442-460.
- Johnson, J. [Artificial Intelligence](#): A Threat to Strategic Stability. *Strategic Studies Quarterly*, Vol. 14(1), Air University Press, 2020, pp. 16-39.
- Johnson, J. and Krabill, E. [AI, Cyberspace, and Nuclear Weapons](#). War on the Rocks website, 31 January 2020.
- Joshi, N. [7 Types Of Artificial Intelligence](#). Forbes website, 19 June 2019.
- Kan, S. [China's Anti-Satellite Weapon Test](#), Congressional Research Service Report for Congress RS22652, Congressional Research Service, 2007.
- Kennedy, A., Brame, J., Rycroft, T., Wood, M., Zemba, V., Weiss, C., Hull, M., Hill, C., Geraci, C., Linkov, I. [A Definition and Categorization System for Advanced Materials](#): The Foundation for Risk-Informed Environmental Health and Safety Testing. *Risk Analysis*, Vol. 39(8), Wiley online, 2019, pp. 1783-1795.
- Kepe, M., Black, J., Meling, J. and Plumridge, J. [Exploring Europe's capability requirements for 2035 and Beyond](#): Insights from the 2018 update of the long-term strand of the Capability Development Plan, RAND Europe Report for the European Defence Agency, European Defence Agency, 2018.
- Kupper, D., Lorenz, M., Knizek, C., Kuhlmann, K., Maue, A., Lassig, R. and Buchner, T. [Advanced Robotics in the Factory of the Future](#). BCG website, 27 March 2019.
- Kurrer, C. and Tarlton, J. (Eds.). [Ten more technologies which could change our lives](#), Report PE 598.626, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), 2017.
- Livingstone, D. and Lewis, P. [Space, the Final Frontier for Cybersecurity?](#), Chatham House Research Paper, International Security Department, Chatham House, September 2016.
- Martin, P. [What is quantum technology?](#). PA Consulting website, n.d.
- Massachusetts Institute of Technology (MIT). [Ionic thrusters generate efficient propulsion in air](#). Science Daily website, 3 April 2013.
- Matin, M. and Islam, M. [Overview of Wireless Sensor Networks](#). *Wireless Sensor Networks: Technology and Protocols* edited by Islam, M. IntechOpen, 2012.
- Matignon, L. [The History of Reusable Launch Systems](#). Space Legal Issues website, 29 May 2019.
- Miglani, S. and Das, K. [Modi hails India as military space power after anti-satellite missile test](#). Reuters website, 27 March 2019.

- Miskovic, N., Bogdan, S., Petrovic, I. and Vukic, Z. [Cooperative Control of Heterogeneous Robotic Systems](#). *37th International Convention on Information and Communication Technology, Electronics and Microelectronics*. Croatian Society for Information and Communication Technology and Microelectronics (MIPRO), Petar Biljanovic, 2014, pp. 982-986.
- Ministry of Defence (MOD). [Future Operating Environment 2035 – First Edition](#), Development, Concepts and Doctrine Centre, 2015.
- _____. [Industry for Defence and a Prosperous Britain: Refreshing Defence Industrial Policy](#), 2017.
- _____. [Human-Machine Teaming](#), Joint Concept Note 1/18. Development, Concepts and Doctrine Centre, UK Ministry of Defence, 2018.
- Moore, D. [Space technologies insights paper](#). NoeticGroup and Defence Science and Technology (DST), 2019.
- Murray, R. [What's going on in quantum technologies?](#). Innovate UK website, 20 July 2016.
- Nathan, S. [Forces of nature](#): Biomimicry in robotics. The Engineer website, 13 July 2015.
- National Nanotechnology Initiative (NNI) [What is nanotechnology?](#). Nano.gov website, n.d.
- National Human Genome Research Institute (NIH). [Synthetic biology](#). Genome.gov website, 2019a.
- _____. [What is genome editing?](#). Genome.gov website, 2019b.
- National Intelligence Council (NIC). [Global Trends](#): Paradox of Progress, National Intelligence Council, 2017.
- North Atlantic Treaty Organization (NATO). [Joint declaration](#) by the President of the European Council, the resident of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, Press Release (2016) 119. NATO website, 8 July 2016.
- _____. [Strategic Foresight Analysis](#), 2017 Report, Allied Command Transformation, North Atlantic Treaty Organization, 2017.
- _____. [Framework for Future Alliance Operations](#), Allied Command Transformation, North Atlantic Treaty Organization, 2018.
- NATO Science & Technology Organization. [Science & Technology Trends 2020-2040](#): Exploring the S&T Edge, NATO Science & Technology Organization, March 2020.
- O'Connell, G. [The future of electronic warfare in Europe](#). Global Defence Technology website, 2018.
- O'Hanlon, M. [Forecasting Change in Military Technology, 2020-2040](#). Brookings website, September 2018.
- Patrizio, A. [Big Data vs Artificial Intelligence](#). Datamation website, 30 May 2018.
- Payne, K. [Artificial Intelligence: A Revolution in Strategic Affairs?](#). *Survival*, Vol. 60(5), Taylor & Francis online, 2018, pp. 7-32.
- Peck, M. [Why Does DARPA Want To Turn Earth's Atmosphere Into a Surveillance Sensor?](#). The National Interest website, 29 February 2020.
- Perkins, E. and Steevens, J. [Future Applications of Biotechnology](#). *Small Wars Journal*, 22 October 2015.
- Permanent Structured Corporation (PESCO). [About PESCO](#). PESCO website, n.d.
- Pudo, D. and Galuga, J. [High Energy Laser Weapon Systems](#): Evolution, Analysis and Perspectives. *Canadian Military Journal*, Vol. 17(3), 2017, pp. 53-60.
- Robyn, D. and Marqusee, J. [The Clean Energy Dividend](#): Military Investment in Energy Technology and What It Means for Civilian Energy Innovation, Information Technology & Innovation Foundation, March 2019.

- Rossiter, A. High-Energy Laser Weapons: Overpromising Readiness. *Parameters, The US Army War College Quarterly*, Vol. 48(4), 2019, pp. 33-44.
- Ryan, M. [Human-machine teaming for future Ground Forces](#), Center for Strategic and Budgetary Assessments, 2018.
- Schulte, G. [A New Strategy for New Challenges in Space](#), Remarks to the National Space Symposium, US Department of Defence, 2011.
- Silfversten, E., Knack, A., Flint, R., Altenhofer, M. and Paoli, G. P. Studies for Innovation in Defence: Strand A. Non-Public Report, 2017.
- Speier, R., Nacouzi, G., Lee, C. Moore, R. [Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons](#). RAND Corporation, 2017.
- Suzuki, K. [Satellites, the floating targets](#). Chatham House website, 12 February 2016.
- Terry, N. B. and Cone, P. P. [Hypersonic Technology: An Evolution in Nuclear Weapons?](#) *Strategic Studies Quarterly*, Vol. 14(2), 2020, pp. 74-99.
- Torossian, B., Bekkers, F., Sweijts, T., Roelen, M., Hristov, A. and Atalla, S. [The Military Applicability of Robotic and Autonomous Systems](#). The Hague Centre for Strategic Studies (HCSS), Security, 2020.
- Tucker, P. [Russia, US Are In a Military Exoskeleton Race](#). Defense One website, 30 August 2018.
- United Nations (UN). [World Urbanization Prospects 2018](#), United Nations Department of Economic and Social Affairs, United Nations, 2018.
- . [Growing at a slower pace](#), world population is expected to reach 9.7 billion in 2050 and could peak at nearly 11 billion around 2100, United Nations Department of Economic and Social Affairs, United Nations, 2019.
- US Army Training and Doctrine Command (TRADOC) G-2. [The Operational Environment and the Changing Character of Future Warfare](#), Training and Doctrine Command, 2017.
- Van Duin, S. and Bakhshi, N. [Artificial Intelligence](#). Deloitte website, March 2018.
- Van Woensel, L. and Archer, G. [Ten technologies which could change our lives](#). European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), 2015.
- Viola, R. [DIGITAL4DEVELOPMENT: A new approach in the EU's development tool kit](#). European Commission website, 2017.
- Von Schomberg, R. [Prospects for Technology Assessment in a framework of responsible research and innovation](#). Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methoden, edited Dusseldorp, M. & Beecroft, R, 2011, pp. 39–61.
- Wheeler, A. [Directed Energy Weapons, Discussion paper for the Convention on Certain Chemical Weapons](#) (CCW) Article36 website, November 2017.
- Wilkinson, B. [The EU's Defence Technological and Industrial Base](#). Directorate General for External Policies of the Union, January 2020.
- Winkler, J. D., Marler, T., Posard, M. N., Cohen, R. S. and Smith, M. L. [Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense](#), RAND Corporation, 2019.
- Wong, Y., Yurchak, J., Button, R., Frank, A., Laird, B., Osoba, O., Steeb, R., Harris, B. and Sebastian, J. [Deterrence in the Age of Thinking Machines](#), RAND Report RR2797, RAND Corporation, 2020.
- Wu, J. [Edge AI Is The Future, Intel And Udacity Are Teaming Up To Train Developers](#). Forbes website, 16 April 2020.
- Zhang, P. [Human-machine interfaces](#). *Advanced Industrial Control Technology*, Elsevier, 2010, pp. 527-555.

Annex A: The EU policy and regulatory landscape for defence and new and emerging technologies

The EU regulatory and policy context for defence and for new and emerging technologies

The changing role and ambition of the EU as a defence and security actor

Increased recognition of the trends discussed in Section 2.1 of this report has led, in recent years, to a sustained call for a stronger EU in the areas of security and defence at the highest political levels. After coming into office in 2014, the Juncker Commission indicated, within the Political Guidelines issued for the 2014-2019 period, that Europe would become a stronger global actor, with security and defence as one of its ten priorities. The Commission emphasised taking steps towards the development of a European security and defence union, a call that was further reiterated at regular intervals through State of the Union Addresses made by President Juncker.²⁶⁸ Equally, EU MS support was echoed in conclusions and statements from the Council of the European Union. These pledged to work towards strengthening the EU's common security and defence, enabling the creation of a more competitive defence industry and working in partnership with NATO.²⁶⁹ Similarly, the European Parliament welcomed efforts towards framing a stronger European defence stance in its 2017 annual report on the implementation of CSDP.²⁷⁰

At a practical level, commitments to a greater role for the EU in the areas of common security and defence translated into a number of concrete policies that have a direct impact on European defence. These are discussed in the following sections.

EU Global Strategy

The EU Global Strategy puts the EU on a path towards strategic autonomy and the development of full spectrum defence capabilities. Following a strategic review of changes in the global environment conducted by HR/VP in consultations with EU MS, the European Union launched its 'Global Strategy for European Foreign and Security Policy' (EU GSS) in June 2016. The EU GSS recognises that ongoing crises and conflicts in the EU's neighbourhood pose a threat to the Union. As such, the EU GSS sets out an ambitious vision of policies, instruments, and capabilities towards achieving strategic autonomy.²⁷¹

To achieve its vision, the EU GSS calls for collective investment into the development of a credible, responsive and interlinked Union. Among other actions, it stresses the urgency of investment in security and defence and the importance of developing full spectrum defence capabilities to respond to external crises and guarantee the Union's safety. To achieve this, the EU GSS recognises that defence cooperation should become more established, committing to encourage defence cooperation and establish a solid European defence industry. In addition, the Strategy emphasises that CSDP must become more rapid and effective regarding its capacity for rapid response, for instance, via the deployment of EU Battlegroups and improved civilian missions. Finally, the EU GSS places significant emphasis on the cyber domain, where it calls for the EU to solidify its role as a forward-looking player.²⁷²

²⁶⁸ See European Commission (2016), Bendiek (2017).

²⁶⁹ See Council of the European Union (2015);

²⁷⁰ See European Parliament (2017)

²⁷¹ See EEAS (2016).

²⁷² See EEAS (2016).

The shift in the EU approach for security and defence towards enhanced integration was also displayed in the adoption of initiatives to tackle hybrid threats. In parallel to the process leading to the adoption of the EU GSS, the events of the 2014 Ukrainian crisis highlighted the growing challenge posed both internally and externally to the Union by the increasing use of hybrid threats and tactics by state and non-state actors. International actors and organisations have put forward several definitions of *hybrid threats* in recent years. The EC defines these as 'a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare'.²⁷³ Actors employing hybrid tactics seek to exploit the vulnerabilities of a target to generate uncertainty and hinder decision making processes.²⁷⁴

In response to the growing number of such threats in the European and global context, with support from the EDA and MS, the HR/VP designed a 'Joint Framework on countering hybrid threats'.²⁷⁵ The Framework is to be considered part of EU efforts towards developing a more integrated approach to security and defence. As such, the framework calls for close coordination of its implementation alongside other EU frameworks and efforts, including the EU CSS.²⁷⁶

Enhanced EU-NATO cooperation

Amid crises and instability, a new impetus was given to joint capability development and cooperation with NATO. Across several of the policy documents reviewed above, including the EU GSS and the Joint Framework on Hybrid Threats, EU policymakers and decision-makers have called for enhanced defence capability development within an international cooperation framework.

In 2001, the EU Presidency and the NATO Secretary General exchanged letters on the definition of the scope of cooperation between the two organisations, initiating the first steps in the EU-NATO partnership.²⁷⁷ Soon after, the so-called 'Berlin Plus Agreement' was signed in 2002. This granted the EU access to NATO's collective assets and capabilities for carrying out EU-led missions where NATO has no interest in conducting such missions or operations.²⁷⁸

Since 2013, the signing of the 2016 *Joint Declaration* by the President of the European Council, the President of the European Commission, and the Secretary General of NATO boosted EU-NATO cooperation significantly.²⁷⁹ The Joint Declaration gave new impetus and substance to the strategic EU-NATO partnership. There was a recognition of the need to find new means of cooperation, as well as an enhanced level of ambition in response to the common challenges faced by both organisations in the current security context. To this end, the Declaration identifies seven priority areas for strategic cooperation:²⁸⁰

1. Hybrid threats present the need to enhance resilience by cooperating on analysis, prevention and early detection, as well as coordinated procedures, strategic communication and response, in addition to sharing intelligence;

²⁷³ See European Commission (2016a).

²⁷⁴ See European Commission (2016a).

²⁷⁵ See European Commission (2016a).

²⁷⁶ See European Commission (2016a).

²⁷⁷ See Kurrer & Tarlton (2017).

²⁷⁸ See Kurrer & Tarlton (2017), Robinson et al (2013).

²⁷⁹ See NATO (2016).

²⁸⁰ See NATO (2016).

2. Operational cooperation at sea prioritises sharing maritime awareness, including on migration, in addition to enhanced coordination and mutual reinforcement of NATO activities in the Mediterranean;
3. Cyber security and defence joint exercises, training and education would enhance cooperation in this domain;
4. Defence capabilities require greater coherence and interoperability among EU MS and NATO allies;
5. Defence industry and research requires strengthening and cooperation within Europe and across the Atlantic;
6. Coordinated exercises, including on hybrid, are important towards facilitating cooperation;
7. Building resilience among partners in the East and South is essential towards strengthening the defence and security capacity among individual recipient countries.

Further initiatives in support of the EU GSS

Following approval of the EU GSS, sectoral plans for implementing the Strategy were prepared by HR/VP with support from relevant stakeholders. In November 2016, an 'Implementation Plan on Security and Defence' was approved, placing significant emphasis on investing and developing defence capabilities through collaborative approaches for both military and civilian aspects of CSDP. Overall, three key tenets underpin the Implementation Plan focusing on Security and Defence:²⁸¹

1. Responding to external conflicts and crises when they arise;
2. Building the capacities of partners;
3. Protecting the EU and its citizens through external action.

The Implementation Plan translates these into a number of concrete actions, including:²⁸²

1. Work to deepen defence cooperation to identify what capabilities are needed, notably through a review of the European Defence Agency Capability Development Plan (CDP);
2. Establish the Coordinated Annual Review on Defence (CARD);
3. Explore the possibility of a Permanent Structured Cooperation (PESCO);
4. Establish a new permanent operational planning and conduct capability within the EEAS for non-executive military missions, the MPCC;
5. Review priorities and increase responsiveness of civilian missions;
6. Strengthen cooperation with UN, NATO, African Union and the Organization for Security and Co-operation in Europe (OSCE).

The coordinated annual review on defence

One of the ambitions of the EU GSS in the field of defence is to lead to the gradual synchronisation and mutual adaptation of national defence planning cycles and capability development practices, with a view to facilitate defence cooperation among EU MS.²⁸³ As such, HR/VP and the Head of EDA proposed the implementation of the Coordinated Annual Review on Defence (CARD), a voluntary mechanism designed to facilitate the sharing of relevant national information on defence expenditure and expenditure planning. CARD aims to provide better identification of capability shortfalls and enable MS to address them through cooperation, as well as the improved

²⁸¹ See Council of the European Union (2016).

²⁸² See Council of the European Union (2016).

²⁸³ See Council of the European Union (2016).

transparency and political visibility around European defence capabilities generated by this mechanism. In sum, CARD can facilitate joint capability development and the operationalisation of the EDA CDP and accompanying Strategic Context Cases (SCCs).

Permanent structured cooperation

The EDA CDP, its accompanying SCCs, and CARD can be seen as instruments facilitating common priority setting and the identification of gaps and opportunities for cooperation among MS respectively. In conjunction with these mechanisms, with a view to enable common planning and the implementation of joint projects and capability development activities, the EU GSS called on MS to consider the possibility of establishing the Permanent Structured Cooperation (PESCO). PESCO provides MS with a binding framework, which deepens defence cooperation and joint capability development and use.

The dispositions enabling PESCO had long been enshrined in the Treaty of the European Union but had not been implemented. In recent years, developments in the European and global security context generated new incentives for the implementation of PESCO, encouraging the adoption of this mechanism by MS in December 2017.²⁸⁴

PESCO is a Treaty-based framework and process designed to deepen defence cooperation amongst EU MS who are capable and willing to do so. PESCO remains distinct from other policy initiatives due to its binding nature.²⁸⁵ Twenty-five EU MS have joined PESCO, pledging to invest, plan, develop and operate defence capabilities within the EU framework and in close cooperation with one another.²⁸⁶ Until now, 47 projects are being developed in the context of PESCO, covering areas that include land, maritime, air, cyber and space.²⁸⁷

The European defence action plan

As indicated in the EU GSS, it is necessary for the European defence industrial base to be able to meet the EU's current and future security needs, and thus contribute to the achievement of strategic autonomy for the EU towards the proposed vision of strategic autonomy. Amid shrinking public spending, the EU and its MS must focus on creating conditions conducive to further defence cooperation, maximising the output and efficiency of defence spending.²⁸⁸

Launched by the European Commission in 2016, the European Defence Action Plan (EDAP) builds on the EU GSS and its Implementation Plan on Security and Defence.²⁸⁹ The EDAP is also closely linked with a number of other key European defence and security initiatives, including the EU-NATO Joint Declaration, and the Joint Framework to counter hybrid threats. EDAP contributes to the vision of the EU GSS by enabling the sustainment and growth of the European defence industrial base. Through the EDAP, the Commission aims to:²⁹⁰

1. Establish a European Defence Fund to support investment in joint research and the joint development of defence equipment and technologies;
2. Foster investment in defence supply chains, by providing access to finance for small and medium enterprises (SMEs) and other suppliers to the defence industry, through the European Structural and Investment Funds (ESIF);

²⁸⁴ See Fiott et al. (2017).

²⁸⁵ See Fiott et al. (2017)

²⁸⁶ See PESCO (n.d.).

²⁸⁷ See PESCO (n.d.).

²⁸⁸ See European Commission (2016b).

²⁸⁹ See European Commission (2016b).

²⁹⁰ See European Commission (2016b).

3. Strengthen the single market for defence by enhancing conditions for an open and competitive defence market in Europe via the application of the two Directives on defence and security procurement and on EU transfers;
4. Maximise civil-military synergies across EU policies to enhance the coherence and synergies between defence issues and other relevant Union policies and sectors.

The European Defence Fund

Within the dispositions that were implemented as part of the EDAP, the European Defence Fund (EDF) stands out due to its goals to coordinate, supplement and amplify national MS investments in defence. The EDF consists of two complementary phases – or 'windows' – that implement distinct financing structures.²⁹¹

1. A research window, whereby the EU offers funding for collaborative defence research projects at EU-level;
2. A capability window, which focuses on the joint development commonly agreed by MS.

Activities under both strands are coordinated by a *Coordination Board* comprising of the Commission, HR/VP, MS, EDA and, where appropriate, industry. This Board is tasked with ensuring a degree of coherence and consistency between the research and capability windows. From 2020, funding from both the Commission and MS could generate a total of €5.5 billion per year for both windows.²⁹²

Most importantly, via co-financing from the EU budget, the EDF provides financial incentives for MS to foster defence cooperation, from research to the development phase of capabilities, including prototypes. In particular, it is expected that PESCO projects may benefit from increased EU co-financing from the EDF, with the EU share of budget covering 30 per cent of costs, instead of 20 per cent.

EU focus on innovation and new and emerging technologies with a disruptive potential

Europe's technological sovereignty and 'responsible innovation'

The EU policy and regulatory context on emerging technologies in security and defence is currently shaped by a comprehensive agenda on innovation and harnessing the benefits of digital and advanced technologies, while proactively guarding against possible risks. The European Commission spearheaded this agenda through the 2011 adoption of the 'Innovation Union' a flagship initiative of the Europe 2020 strategy.²⁹³ More recently, the EU's agenda on innovation and emerging technologies has seen advancement via the April 2019 'digital package'.²⁹⁴ This package detailed the Commission's recommendations for the EU approach towards harnessing the benefits of advanced technologies. These included:

- A European data strategy. The Commission projects that by 2025, the value of the data economy in the EU27 could total €829 billion, marking a 530 per cent increase from the volume of global data in 2018.²⁹⁵ The Commission's European strategy for data proposed the establishment of a new regulatory framework for data governance, including access,

²⁹¹ See European Commission (2017a).

²⁹² See European Commission (2017a).

²⁹³ See European Commission (2011).

²⁹⁴ See European Commission (2020a).

²⁹⁵ See European Commission (n.d.a).

use and sharing of data. This seeks to facilitate the establishment of a European data space, or a 'single market for data' within the EU.²⁹⁶ The Commission states that this initiative could facilitate the flow of data within the EU and across sectors, establishing clear laws for privacy, data protection and competition law, as well as fair rules for the access and use of data.²⁹⁷

- Policy options for human-centric development of AI. The Commission's White Paper on AI emphasised the need to: (1) enhance public and private sector partnerships to 'mobilise resources' to achieve an 'ecosystem of excellence' along the entire 'value chain'; and (2) establish a regulatory framework to generate an 'ecosystem of trust', which seeks to foster confidence and trust in the future adoption of AI-enabled technologies.²⁹⁸

These initiatives constitute part of a broader effort by the European Commission to **foster Europe's technological sovereignty**, a concept explained as 'having European technological alternatives in vital areas where [it is] current dependant [on others]'.²⁹⁹ Such technological sovereignty is envisioned via cooperation in 'areas of strategic importance such as defence, space, and key technologies such as 5G and quantum [computing]', facilitated through the European Single Market, and contributing to Europe's gradual emergence as 'a digital, technological and industrial leader'.³⁰⁰ The EU also hopes that emerging as a key digital player will project European values onto the international stage, inspiring more countries to pursue similar digital governance models.³⁰¹

Recent initiatives also reflect the European Commission's promotion of the concept of **responsible innovation (RI)**, often discussed in relation to the wider concept of Responsible Research and Innovation (RRI). Embedded primarily within the Commission's FP7 and Horizon 2020 programmes, the RI and RRI concepts emphasise the idea of innovation as a 'transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability, and societal desirability of the innovation process and its marketable products'.³⁰² Along with other definitions of RI and RRI, this acknowledges the uncertainty inherent in innovation processes, as well as a corresponding need for transparent and cautious approaches to research and innovation across all policy areas.³⁰³

In July 2020, the Commission launched an antitrust competition inquiry into the sector of Internet of Things (IoT), focusing on consumer-related products and services connected to a network and controlled at a distance, such as smart home devices or wearable technologies.³⁰⁴ In anticipation of projected growth in this sector, the enquiry seeks to develop an in-depth understanding of the effects of potential competition problems, such as restrictions of data access and interoperability, as well as the emergence of dominant digital ecosystems and gatekeepers.³⁰⁵ Any initiatives following this inquiry would seek to ensure fair competition, particularly for SMEs and smaller innovators, by pursuing adherence to EU rules on restrictive business practices and abuse of dominant market positions.³⁰⁶

²⁹⁶ See European Commission (2020b).

²⁹⁷ See European Commission (n.d.a).

²⁹⁸ See European Commission (2020c).

²⁹⁹ See European Parliament (2019).

³⁰⁰ See European Parliament (2019).

³⁰¹ See European Commission. (n.d.b).

³⁰² See Von Schomberg (2011).

³⁰³ See Silfversten et al. (2017).

³⁰⁴ See European Commission (2020a).

³⁰⁵ See European Commission (2020a).

³⁰⁶ See European Commission (2020a).

A food for thought paper published by a collection of EU MS³⁰⁷ recognised the **need for EU action on the digitalisation of defence**,³⁰⁸ highlighting the central role of digitalisation and advanced technologies, particularly AI, for future capability development. The key topics for discussion on future EU action set out in the paper are outlined in Box A.1.

Box A.1 - Summary of the 2019 Food for Thought Paper on Digitalisation and Artificial Intelligence in Defence

Finland's agenda for its Presidency of the Council of the EU included a range of priorities for strengthening security and defence cooperation as well as preventing and countering hybrid threats.³⁰⁹ In this context, a Food for Thought Paper on digitalisation and AI in defence was presented by Finland, Estonia, France, Germany, and the Netherlands, laying out the following priorities for EU action:³¹⁰

Exploring the opportunities and threats, including **potential for future disruption and transformation in security and defence**, associated with digitalisation and advanced technologies. The paper highlighted utilising existing EU structures such as the EDF and PESCO to advance relevant research and development.

Examining the impacts of digitalisation and advanced technologies on **military capabilities** and determining relevant areas for **European, as well as EU-NATO cooperation, in AI and digital defence**.

Strengthening European awareness of the **regulatory requirements** related to digitalisation and AI in defence, including examining the impacts of advanced technologies in different operational environments and military organisational levels.

Source: RAND Europe analysis.

Current efforts driving the EU's digital agenda were preceded by various initiatives addressing innovation and emerging technologies in EU's foreign and security policy. In May 2018, for example, the EEAS and High Representative Federica Mogherini launched the **Global Tech Panel**, gathering key industry, private sector, academia and civil society stakeholders to 'foster new types of cooperation between diplomacy and technology'.³¹¹ Intended to serve as a forum to discuss practical steps to address challenges of innovation and technology for foreign and security policy, the Global Tech Panel has focused on four initial work streams:³¹²

1. Regulating Lethal Autonomous Weapons Systems (LAWS) in relation to international security and law.³¹³ LAWS have been described as 'a top priority file where the EU is seeking to promote a common understanding on a global legal and ethical framework'.³¹⁴

³⁰⁷ These were Finland, Estonia, France, Germany and the Netherlands.

³⁰⁸ EU2019.fi (2019a).

³⁰⁹ EU2019.fi (2019b).

³¹⁰ EU2019.fi (2019a).

³¹¹ See EEAS (2018a).

³¹² See EEAS (2018b).

³¹³ See EEAS (2018c).

³¹⁴ See EEAS (2019).

2. Increasing economic competitiveness through digital technologies and innovation, while boosting digital skills and jobs for human development.³¹⁵ The panel's work in this area has corresponded with the EU's Digital4Development policy framework.³¹⁶
3. Examining the global ethics aspects of applied machine learning in the fields of surveillance, justice and security.
4. Discussing the 'future frontiers in cyber security'.³¹⁷

Enhancing cooperation in the security and defence-related aspects of the Panel's agenda connects to broader efforts to strengthen European cooperation on security and defence.

Table A.1 – Overview of EU defence innovation funding mechanisms

Fund	Value	Summary
EDF (2021-2027)	€13bn Research: €4.1bn Capability development: €8.9bn	Streamlining the PADR and EDIDP. The EDF will provide support throughout the industrial development Lifecycle, from research to prototype development up until certification. Projects developed through the PESCO framework may receive additional co-financing of 10 per cent (the PESCO bonus)
EDIDF (2019-2020)	€500m	A 'capability' strand to build on the research and development phase and create incentives for MS to cooperate on joint development and the acquisition of defence equipment and technology, so as to reduce costs.
PADR (2017-2019)	€900m	PADR was a genuine test-bed to prove the relevance of European defence research and lay the foundations for the EDF.
Pilot Project (2015-2016)	€1.4m	The pilot project was introduced in the 2015 and 2016 EU budgets with the aim to test funding concepts.

Source: Wilkinson (2020).

These efforts show that there have been considerable measures taken towards strengthening European cooperation on defence and security, including defence innovation and managing the impact of advanced technologies. Existing research, however, indicates a number of challenges for EU action in this area. Military uses of AI have, according to Franke, received 'too little attention' among EU MS³¹⁸. Despite the creation of new defence innovation funding streams, uncertainties remain around the future availability of EU defence funding and support for the EDF.³¹⁹

³¹⁵ See EEAS (2018c).

³¹⁶ See Viola (2017).

³¹⁷ See EEAS (2018b).

³¹⁸ See Franke (2019).

³¹⁹ See Wilkinson (2020).

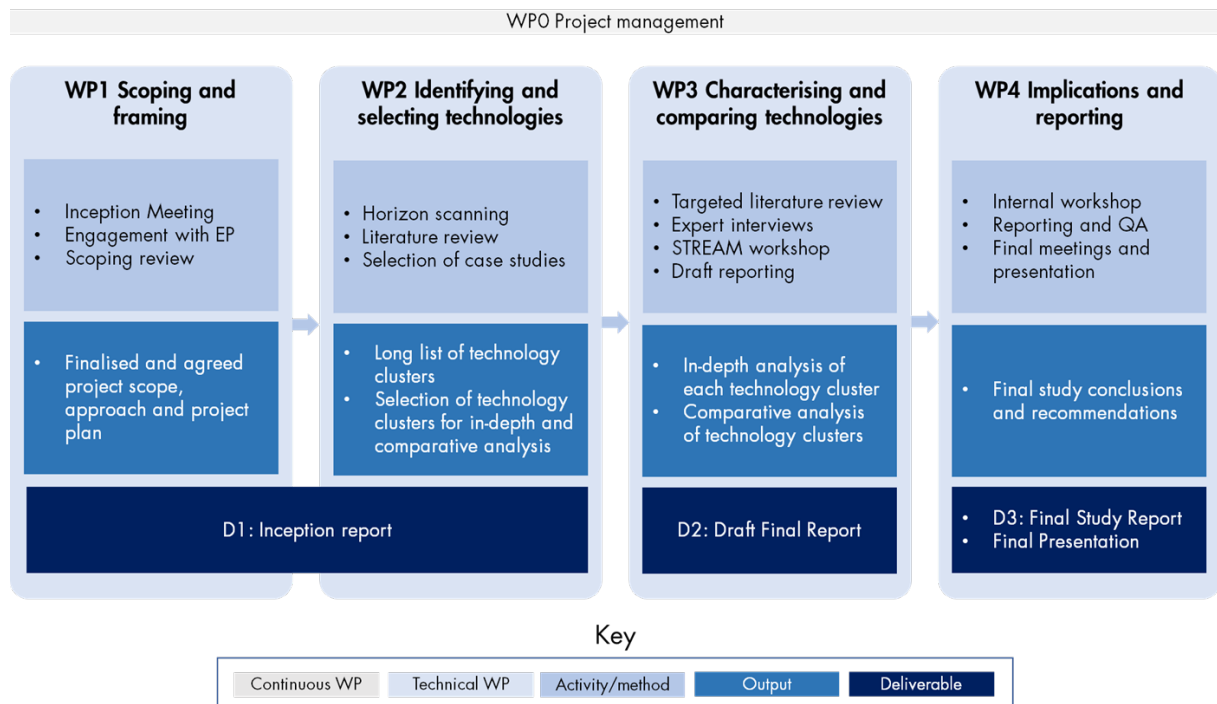
Table A.2 – Overview of key recent EU policy and regulation on advanced technologies in security and defence

Date	Author	Title
February 2013	European Commission	Cybersecurity Strategy for the European Union: An Open, Safe and Secure Cyberspace
July 2013	European Commission	Communication: Towards a more competitive and efficient defence and security sector
August 2013	European Parliament and the Council	Directive on Attacks against Information Systems
June 2014	European Commission	Report: A New Deal for European Defence
April 2016	European Commission	Joint Framework on Countering Hybrid Threats
June 2016	HRVP	A Global Strategy for the European Union's Foreign and Security Policy
July 2016	European Parliament and the Council	EU Network and Information Security (NIS) Directive
November 2016	European Commission	European Defence Action Plan
November 2016	HRVP	EU Implementation Plan on Security and Defence
June 2017	European Commission	Communication Launching the European Defence Fund
April 2018	European Commission	EU AI Strategy (AI for Europe)
June 2018	European Commission	Joint Communication – Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats
December 2018	European Commission	Coordinated Plan on AI
December 2018	European Commission	Action Plan against Disinformation
April 2019	AI HLEG	Ethics Guidelines for Trustworthy AI
April 2019	European Commission	EU Cybersecurity Act
May 2019	Finland, Estonia, France, Germany, the Netherlands	Digitalization and AI in Defence – Food for Thought Paper
June 2019	European Parliament and the Council	The Open Data Directive
June 2019	AI HLEG	Policy and Investment Recommendations for Trustworthy AI
February 2020	European Commission	White Paper on AI – A European approach to excellence and trust
February 2020	European Commission	European Data Strategy

Annex B: Methodology

This Annex outlines in greater detail the research approach adopted in the four technical WPs forming this study. The structure of the study including the WPs and corresponding methods, outputs and deliverables is captured in Figure B.1.

Figure B.1 – Overview of project tasks, underpinning activities, and resulting outputs and deliverables



Source: RAND Europe.

WP1 Scoping and Framing

In the initial phase of the study, the study team conducted initial engagement with the STOA in the form of an inception meeting involving the study team and relevant representatives of the EP and the STOA Unit. The discussion focused on clarifying and confirming the research questions, objectives of the study, research approach and workplan.

Additionally, WP1 involved a scoping review and horizon scanning to characterise the context in which new and emerging technologies may impact the future battlefield and develop a longlist of technology clusters that may shape the 2040 battlefield. The scoping review consisted of a review of previous RAND studies and strategic trend reports to:

- Characterise the evolving strategic environment, including identifying the key economic, political, environmental, social and technological trends that are likely to shape the future strategic environment out to 2040.
- Characterise the current and evolving EU regulatory and policy context for addressing the opportunities and challenges provided by new and emerging technologies.
- Identify the key technological trends or technology clusters that may shape the future battlefield, as well as potential impacts, implications, use cases, drivers, enablers or barriers for future development and adoption.

As part of the scoping review, the study team selected the most relevant previous RAND studies and 15 strategic trend reports for an in-depth data extraction. Sources were selected on the basis of their relevance to the study RQs and timeliness. Data extracted from the selected sources identified:

- Contextual source information (author/institution/organisation)
- Publication purpose
- Scope and approach of the study/report
- Main findings and conclusions pertaining the themes, drivers and factors defining the future strategic environment and EU policy and regulatory context
- Main findings on the key technologies that may shape the 2040 battlefield and the relevant impacts and implications.

On the basis of the scoping review, 11 technology clusters were identified by the study team. Table B.1 captures these technologies and their definitions.

Table B.1 – Longlist of technology clusters and definitions

Technology Cluster	Definition
Artificial Intelligence, Machine Learning and Big Data	Software technologies that are able to perform advanced computing to analyse and interpret large quantities of data.
Advanced robotics and autonomous systems	Technologies that constitute or enable the operation of unmanned vehicles with advanced capabilities, including in the area of operating without human supervision or control.
Biotechnology	Technologies that leverage biological systems or innovations in biological sciences to develop systems with advanced properties and levels of performance.
Technologies for the delivery of novel effect	Technologies, including weapons and sub-systems, that enable the delivery of novel kinetic and non-kinetic effect or the delivery of conventional effect in novel ways.
Advanced energy and power systems	Technologies that enable the production, transmission, conversion and storage of energy and power in a way that improves the system's efficiency, reliability or durability.
Satellites and space-based technologies and assets	Technologies that enable access to space or technologies, which are space-based and facilitate terrestrial or space-based operations.
Novel and advanced materials and manufacturing	Technologies that constitute or enable the production of materials with advanced properties or novel characteristics.
Human-machine interfaces	Technologies that facilitate human-machine interactions or human-machine teaming, including information transfer.
Quantum technologies	Technologies that leverage quantum mechanics to achieve advanced properties and levels of performance not achievable with conventional means.
Computing, data storage, and telecommunications	Technologies that enable the storage, processing and transfer of large quantities of data in analogue or digital form.
Sensor and radar technologies	Technologies that enable the detection or measurement of physical and environmental indicators such as the presence,

Technology Cluster	Definition
	direction, and speed of movement of objects or chemical and biological substances.

Source: RAND Europe.

WP2 Identifying and selecting technologies

Building on the scoping review, WP2 aimed at identifying technologies most likely to significantly shape the 2040 battlefield through an initial assessment of the longlist of technology clusters and shortlisting of six technology clusters for further analysis. This consisted of an initial characterisation of the longlisted technology clusters through a targeted literature review and horizons scanning, and consultation with the STOA.

To establish a baseline of understanding of the key technology trends and potential impacts of the various technology clusters, the study team conducted the following activities:

- Targeted literature reviews examining available open-source academic and grey literature (e.g. government reports and defence news media) on new and emerging technologies with a primary focus on emerging technologies in a defence and security context over the next twenty years. This literature aimed to further characterise each identified technology cluster in terms of the nature of key technologies, potential use cases on the future battlefield, and potential impacts and implications.
- A review of the RAND Europe CFFS S&T horizon scanning database to identify relevant S&T developments and use cases relevant to the identified technology clusters. This consisted of the use of key words related to the technology clusters (e.g. artificial, robot*, biotech*, energy, satellite, space, manufactur*, interface, quantum, comput*, data, sensor, radar) and the identification of examples of relevant recent S&T developments in each technology cluster. Overall, the study team identified 154 relevant items, which are included in **Annex D**.

The full longlist of technology clusters, including relevant technology use cases, was subsequently discussed in a formal consultation process with the STOA. This included an initial evaluation of the technology clusters on the basis of their likelihood of adoption in the 2040 timeframe and expected impact on the future battlefield. Figure B.1 captures the results of this consultation process.

Table B.2 – Results of technology shortlisting consultations

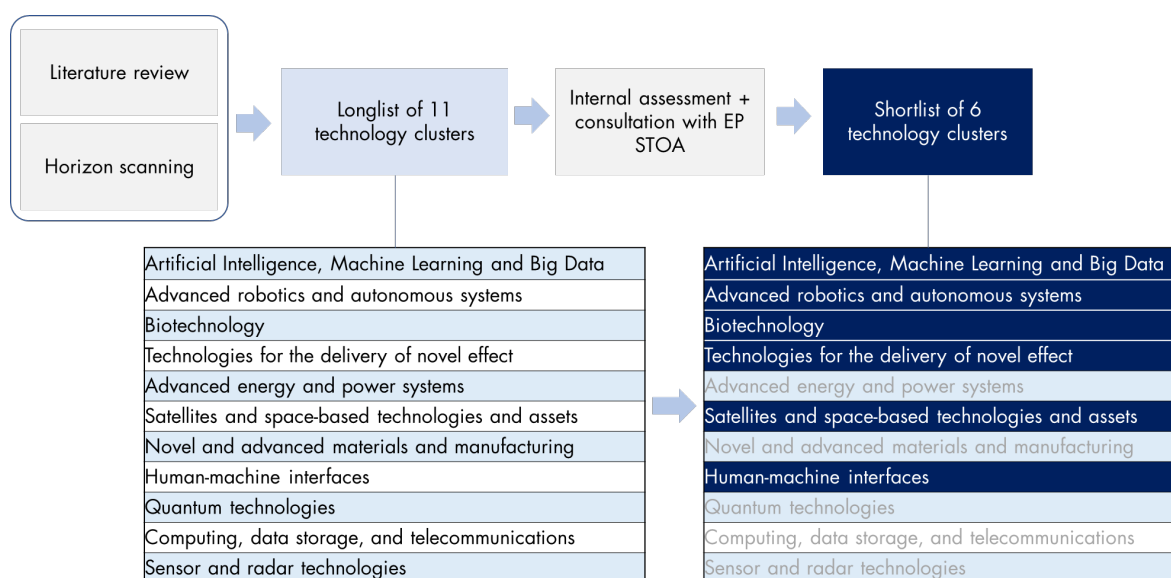
Technology cluster	Likelihood of adoption	Impact
Artificial Intelligence, Machine Learning and Big Data	High	High
Advanced robotics and autonomous systems	Medium	High
Biotechnology	Medium	Medium
Technologies for the delivery of novel effect	High	High
Advanced energy and power systems	Medium	Low
Satellites and space-based technologies and assets	High	High
Novel and advanced materials and manufacturing	Medium	Medium

Human-machine interfaces	High	High
Quantum technologies	Medium	High
Computing, data storage, and telecommunications	High	Medium
Sensor and radar technologies	High	Medium

Source: RAND Europe.

Based on the results of the consultation process, six technology clusters were selected for in-depth and comparative analysis in WP3. Figure B.2 summarises the technology shortlisting process.

Figure B.2 – Technology shortlisting process



Source: RAND Europe.

WP3 Characterising and comparing technologies

To develop a more in-depth understanding of the shortlisted technology clusters, including evolving nature of the technology cluster and relevant impacts on the future battlefield, the study team conducted in-depth analysis of each cluster through a targeted literature review and expert interviews. The targeted literature reviews focused on reviewing open source academic and grey literature discussing recent, ongoing and potential future technology trends as well as key impacts.

The interviews included consultations with experts from academia and other research institutions. The study team aimed to identify and consult one to two experts for each technology cluster, with experts being identified on the basis of their expertise and research record relevant to the technology cluster. In total, the study team carried out six semi-structured interviews.³²⁰

³²⁰ Annex C provides a copy of all stakeholder engagement materials used in the interviews, including the interview protocol.

Table B.3 – List of experts consulted in WP3 interviews

Interview date	Name and affiliation
21 October 2020	Anonymous
21 October 2020	Anonymous
23 October 2020	Anonymous
26 October 2020	Dr Bleddyn Bowen, Leicester University
26 October 2020	Anonymous
27 October 2020	Anonymous

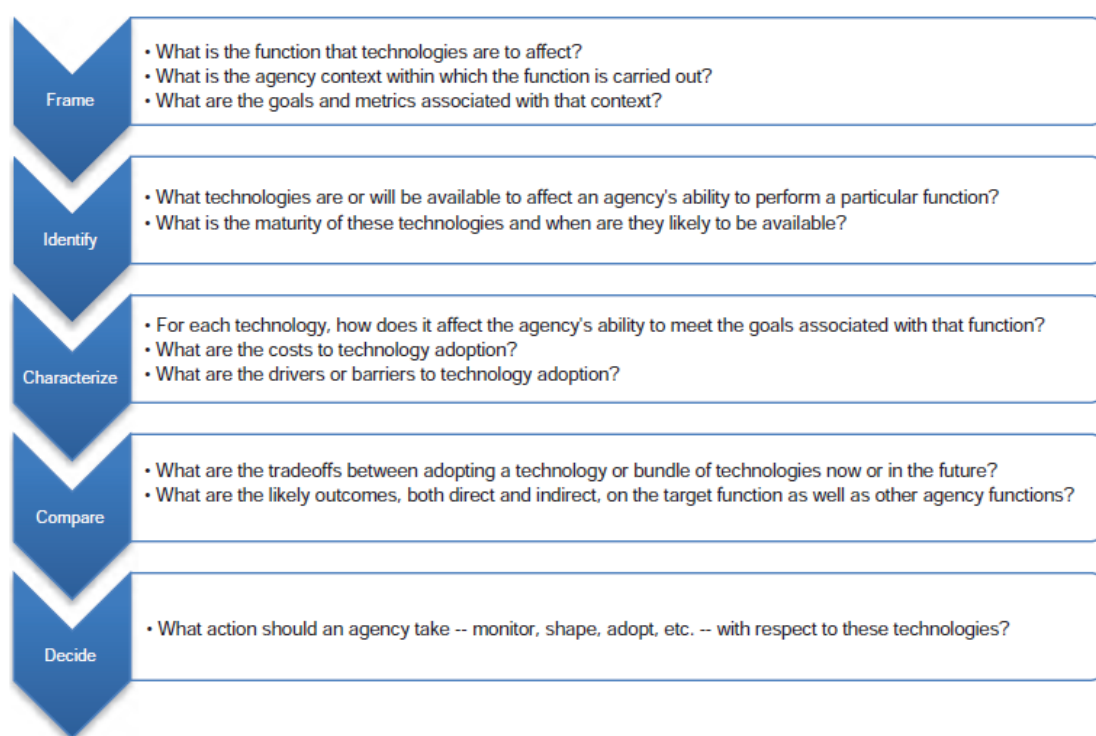
Source: RAND Europe.

Data collected through the targeted literature reviews and expert interviews was synthesised and consolidated through a structured data extraction approach, covering the following aspects:

- Definition of the technology cluster
- Overview of the technology cluster
- Examples of relevant technologies
- Summary of ongoing developments and expected future trends / developments
- Description of identified opportunities for defence
- Description of identified challenges for defence
- Description of relevant enablers and barriers for adoption
- Summary of potential impacts and implications for the EP and European defence and security.

To complement the in-depth analysis of each technology cluster, the study team conducted comparative assessment of the technology clusters through an adapted version of the RAND-developed Systematic Technology Reconnaissance, Evaluation and Adoption Method (STREAM). Figure B.33 provides a high-level overview of the STREAM methodology.

Figure B.3 – High-level overview of the STREAM methodology



Source: RAND Europe.

The STREAM methodology allows for a structured comparison of different technologies through framing of the context in which technologies may be adopted, systematically identifying the new technologies that are most relevant in the given context; assessing their potential impacts to functions or tasks relevant within the defined context; and evaluating such impacts against technical, organisational, ethical, regulatory or other barriers that may influence the uptake of the technologies. The systematic comparison serves to inform relevant policy- and decision-making with regard to potential adoption and investment decisions as well as any regulatory steps to prevent, mitigate or otherwise influence the potential impacts of new and emerging technologies.

The core of the STREAM approach is a quantitative scoring exercise in which workshop participants are asked to assess the possible impact and barriers to implementation of the different technologies. Table B.4 presents the scoring criteria that were used to capture the potential impact of technologies on the EU MS Armed Forces and their abilities to perform functions under the CSDP.

Table B.4 – STREAM scoring criteria for impact on the EU and the CSDP

#	Impact criteria	Definition
1a	EU MS military capability to prepare and respond to external conflicts and crises in the context of CSDP	The CSDP enables the EU to take a leading role in peace-keeping operations, conflict prevention and in the strengthening of the international security. The use of EU MS military capabilities to respond to external conflict and crises includes the use of military capabilities for crisis management and military missions and operations. The remit of CSDP includes the capacity for establishment and maintaining awareness and responsiveness in all phase of the conflict cycle,

#	Impact criteria	Definition
		including conflict prevention, in order to promote peace and security within a rules-based global order'. ³²¹
1b	EU MS military capability to protect the territorial integrity of the EU and its citizens	EU MS may use military capability to ensure and protect the territorial integrity of the EU, as well as the security of its citizens, by maintaining operational readiness and capacity to respond to potential threats. This includes maintaining a credible defence and deterrence posture against overt as well as sub-threshold threats and activities.
1c	Resilience of EU MS facing hostile attacks	Resilience is understood as the capacity to adapt and recover from major societal shocks, disruptions or operational setbacks (including those stemming from sub-threshold activities), including by maintaining resilient information networks and critical infrastructure.
1d	Ability to support capacity-building of EU partners and allies	Capacity-building is understood as the use of CSDP mechanisms and instruments to develop and strengthen the resources and ability of EU's partners and allies to address potential threats, conflicts, or instability.
1e	Ability to understand adversaries and attribute attacks / malicious activities	Understanding and comprehension correspond to the ability to establish situational awareness and knowledge of the intentions and capabilities of all actors within a conflict or crisis scenario. This includes the ability to attribute activities or attacks to responsible actors.

Source: RAND Europe analysis.

For each technology cluster and criteria, participants were asked to allocate the following scores (1-5):

1. Negative impact - reduction in capability or negative impact in comparison to current practices
2. No impact - negligible or no difference in comparison to current capability or practices
3. Moderate positive impact - minor improvement in comparison to current capability or practices
4. Substantial positive impact - significant improvement in comparison to current capability or practices
5. Ground-breaking positive impact - paradigm shift compared to current capability or practices (i.e. enables entirely novel approach).

While emerging technologies may contribute positively to strengthening the capabilities of EU MS and their Armed Forces, emerging technologies are also likely to influence the overall characteristics of the future battlefield and the context in which actors interact in a conflict or crisis scenario. Three additional criteria were therefore identified to capture these potential impacts. These are presented in Table B.5.

³²¹ See Council of the European Union (2016).

Table B.5 – STREAM scoring criteria for impact on future battlefield dynamics

#	Impact criteria	Definition
2a	Speed and complexity of decision-making on the battlefield	Increasing speed and complexity of decision-making on the battlefield increasing the likelihood of crisis escalation (i.e. entailing the accidental or unintended escalation of a crisis, defined as 'a confrontation between states involving a serious threat to vital national interests for both sides') with limited time available to resolve the confrontation. ³²²
2b	Likelihood of arms-race escalation	Arms-race escalation may entail a long-term dynamic in which actors are encouraged to continuously augment their forces (e.g. through commissioning new types of weapons, 'out of the fear that, in a crisis, the other side might gain a meaningful operational advantage by using weapons first'). ³²³
2c	Lethality of systems and sub-systems	Lethality refers to the capacity of weapons systems or sub-systems to cause damaging effect, including death. Increased lethality of systems and sub-systems are likely to correspond to increased levels of conflict-related violence and higher number of battlefield casualties.

Source: RAND Europe analysis.

For each technology cluster and criteria, participants were asked to allocate the following scores (1-5):

1. Negative impact - reduction in comparison to current practices / status quo
2. No impact - negligible or no difference in comparison to current capability, practices or status quo
3. Moderate impact - minor increase in comparison to current capability, practices or status quo
4. Substantial impact - significant increase in comparison to current capability, practices or status quo
5. Ground-breaking impact - paradigm shift compared to current capability, practices or status quo (i.e. enables entirely novel approach or dynamics).

Table B.6 captures the scoring criteria that were used to assess the various barriers to implementation.

³²² See Wong et al. (2020).

³²³ See Wong et al. (2020).

Table B.6 – STREAM scoring criteria for feasibility of implementation

Feasibility of implementation criteria	
3a	Unfamiliarity with technology or uncertainty concerning actual performance
3b	Financial cost to implement, operate and maintain technology
3c	Additional implementation requirements (e.g. additional requirements and barriers to develop and sustain a capability stemming from doctrine, organisation, training, materiel, leadership, personnel, facilities, or interoperability considerations)
3d	Limits on access to relevant technologies (e.g. export control restrictions, lack of European suppliers, etc.)
3e	Ethical and/or human rights protection barriers

Source: RAND Europe analysis.

For each technology, participants were asked to allocate the following scores (1–5):

1. Insurmountable barriers – barriers could not be overcome;
2. Grave concern – barriers unlikely to be overcome without major societal, organisational or economic change or disruption;
3. Significant concern – barrier could be overcome with significant change or disruption;
4. Minor concern – barriers could be overcome with only minor change or disruption;
6. Negligible or no concern – barriers could be overcome with very minor or no change or disruption.

The STREAM workshop gathered 14 experts and stakeholders from academia, research institutions and relevant European institutions. Experts and stakeholders were identified by the study team on the basis of their expertise and experience in research or policy pertaining new and emerging military technologies. Prior to the workshop, participants were provided with technology briefs, definitions of the scoring criteria as well as scoring instructions and Excel spreadsheets to record all scoring and qualitative comments. A copy of these materials is included in **Annex D**.

WP4 Implications and reporting

The final study WP focused on identifying cross-cutting implications of stemming from new and emerging technologies considered under the study, as well as the formulation of relevant policy options stemming from study findings. To inform this analysis, the study team hosted an internal workshop gathering RAND Europe experts. The workshop focused on a discussion of:

- Validating and adding additional granularity to emerging findings regarding the impacts of the selected technology clusters for European defence and future battlefield dynamics;
- Identifying additional high-level cross-cutting implications of the development and adoption of emerging technologies for the EU;
- Formulating policy options for the EU stemming from findings of the study, in light of relevant enablers, barriers and potential priorities for future EU policy- and decision-making.

The internal workshop was complemented by desk-based research to address any data gaps, as well as final reporting and Quality Assurance activities.

Annex C: Additional STREAM analysis

This Annex firstly presents a comparison of the technology clusters resulting from the quantitative STREAM workshop scoring exercise in which participants provided scoring assessments of the technology clusters in relation to specified impact and implementation criteria captured in Table C.1 further below. It then provides a more granular overview of the scoring of individual technology clusters.

The interpretation of these findings should take a view of the limitations of the STREAM workshop analysis outlined in Chapter 1 of this report. In particular, the robustness of the quantitative findings is limited due to the limited number of participants at the workshop, as well as the breadth of technology clusters.

Table C.1 – Overview of the impact and implementation criteria

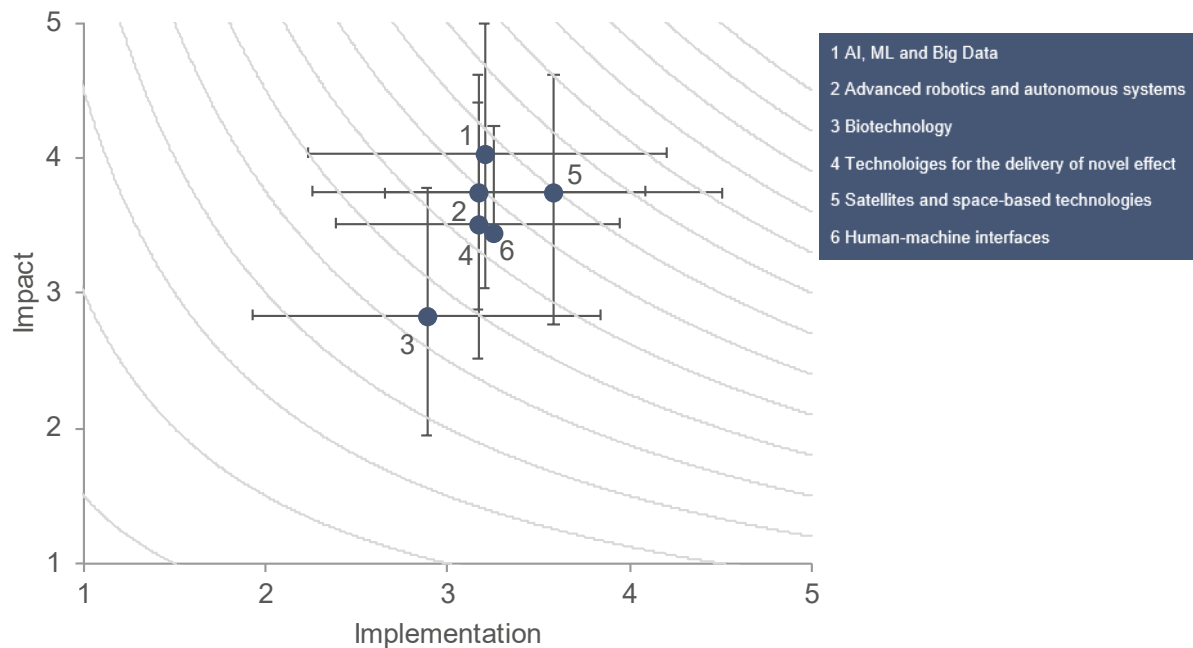
Impact criteria			
#	Impact – EU and the CSDP	#	Impact -Future battlefield dynamics
1a	EU MS military capability to prepare and respond to external conflicts and crises in the context of CSDP	2a	Speed and complexity of decision-making on the battlefield
1b	EU MS military capability to protect the territorial integrity of the EU and its citizens	2b	Likelihood of arms-race escalation
1c	Resilience of EU MS facing hostile attacks	2c	Lethality of systems and sub-systems
1d	Ability to support capacity-building of EU partners and allies		
1e	Ability to understand adversaries and attribute attacks / malicious activities		
Implementation criteria			
3a	Unfamiliarity with technology or uncertainty concerning actual performance		
3b	Financial cost to implement, operate and maintain technology		
3c	Additional implementation requirements (e.g. additional requirements and barriers to develop and sustain a capability stemming from doctrine, organisation, training, materiel, leadership, personnel, facilities, or interoperability considerations)		
3d	Limits on access to relevant technologies (e.g. export control restrictions, lack of European suppliers, etc.)		
3e	Ethical and/or human rights protection barriers		

Source: RAND Europe analysis.

Comparative assessment of emerging technologies shaping the future battlefield

To illustrate the differences between the future battlefield impacts of the six technology clusters, Figure C.1 presents the distribution of aggregated scores for all six technology clusters in terms of their average impact and the feasibility of their implementation with associated error bars. The error bars capture standard deviation of the technology scoring, visualising the variance of technology scores and therefore the levels of disagreement among participants.

Figure C.1 – Aggregated scores for technologies with associated error bars (± 1 standard deviation)



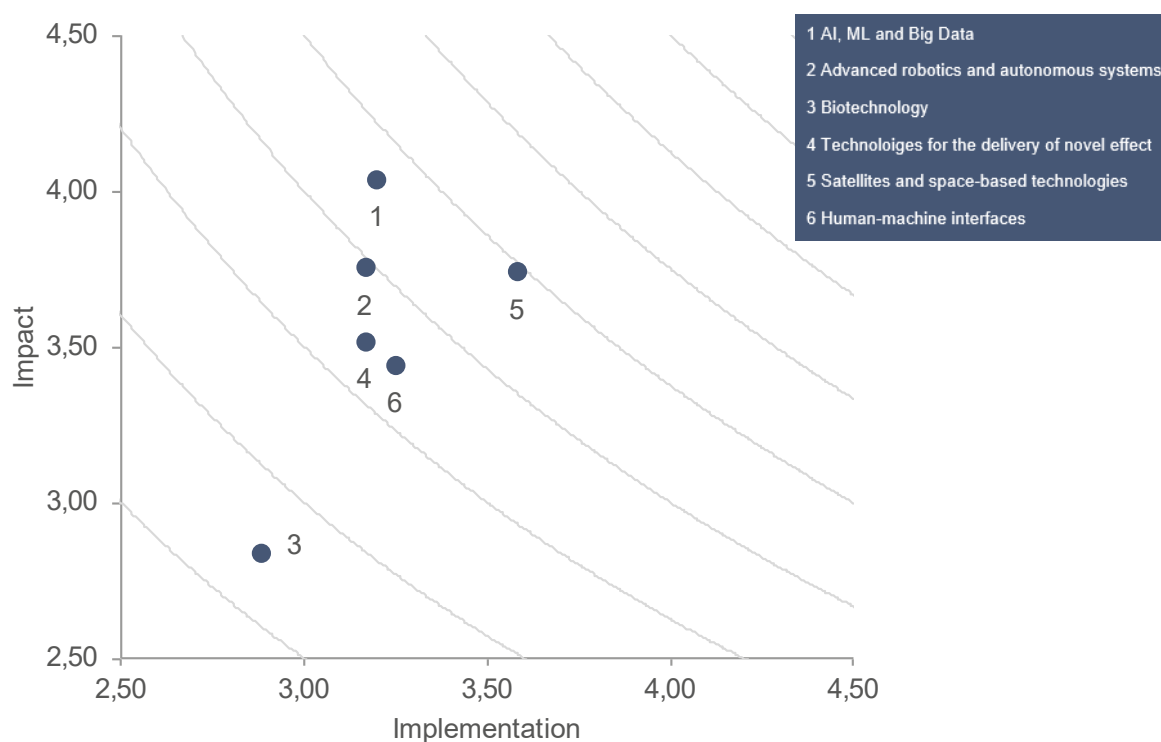
Source: RAND Europe analysis.

Note: The higher a technology is scored on the criteria, the greater the expected impact and feasibility of implementation. For impact criteria, the scale ranges from 1 (negative impact – reduction in capability compared to current practices) to 5 (ground-breaking impact – paradigm shift in capability compared to current practices). For feasibility of implementation criteria, the scale ranges from 1 (insurmountable barriers – barriers could not be overcome) to 5 (negligible or no concern about barrier – barrier could be overcome with very minor or no change or disruption). See Annex B for a full description of the STREAM scores and criteria.

Several cross-cutting insights in relation to the technology assessments can be identified from Figure C.1:

- The average scores are clustered in the middle, mainly between scores of 3 and 4 for both impact and feasibility of implementation. This is a common observation made in STREAM workshops, as there is a tendency among participants to score technologies that they may be less familiar with in the 'middle'. This may also be linked to the broad range of the technology clusters – i.e. some technologies within the clusters may be individually scored higher than others, but combined they receive a 'middle' average score.
- The error bars, representing standard deviation (SD) are fairly large in comparison to the scoring differences between some technology clusters. This is linked to significant variances among participants' scores for certain technologies. Similar to the 'middle' clustering of technology assessments, this variance of scores may be tied to the large scope of technology clusters (i.e. when scoring, participants may have focused on different technologies *within* each cluster).
- Despite the observed tendency of technologies to receive 'middle' scores for the impact and implementation criteria, the scoring results indicate significant differences in the potential impact and feasibility of implementation of some technologies. These differences are further illustrated in Figure C.2, which shows a more focused version of Figure C.1 with error bars removed to provide a clearer illustration of the scoring differences.

Figure C.2 – Aggregated scores for technologies (zoomed-in, no error bars)



Source: RAND Europe analysis.

The following key differences in technology assessments can be noted:

- The AI, ML and Big Data technology cluster was generally assessed as the most impactful technology cluster in relation to both the EU and the CSDP (avg. score 3.92) as well as future battlefield dynamics (avg. score 4.15). The technology cluster was in particular perceived to have near ground-breaking impact on speed and complexity of decision-making on the battlefield (avg. score 4.8). This result resonates with findings from existing literature, which highlights the enabling role of AI for systems to react significantly faster than those relying on operational input, navigate exponential increases in the quantity of data processed for analysis underpinning military operations, and help decision-makers to rapidly navigate uncertain and complex environments.³²⁴
- Workshop discussions also indicated that the high perceived impact of AI, ML and Big Data arises out of the role of such technologies as crucial enablers for several other technology clusters (e.g. autonomous systems), as well as the overarching crucial role of data on the future battlefield. Existing literature as well as expert interviews corroborate this view, highlighting the role of AI as an enabler for areas such as development of biotechnologies but also target recognition capabilities integrated in technologies for the delivery of novel effect (e.g. hypersonics). This includes capabilities such as AI-enabled target acquisition, tracking, guidance systems and discrimination.³²⁵
- On the opposite end of the impact and implementation spectrum, biotechnology was assessed to have the least impact of all technologies across most of the impact criteria. Similarly, it was assessed as facing the greatest barriers to implementation among all

³²⁴ For example, Payne (2018), Saylor (2020).

³²⁵ For example, Brockmann et al. (2019), Johnson (2020).

technologies. In particular, the ethical barriers and potential human rights implications associated with biotechnology are perceived as close to insurmountable in the EU context. Workshop discussions noted that both the expected impact and feasibility of implementation may significantly differ based on the applications of biotechnology. For example, the ethical implications of biotechnology-based human augmentation may be significantly lower than the extensive ethical barriers associated with weaponised biological agents. This reiterates the challenges related to the nature of biotechnology as dual-use systems. As discussed in Section 3.1.2, while advances in fields such as synthetic biology and gene editing may create significant opportunities for defence and society at large, if weaponised or otherwise exploited, such technologies may have extremely detrimental and disruptive effects.³²⁶

- While the assessment of satellites and space-based technologies identified that they would have a comparatively lower impact than some of the other technologies, the uptake of this technology cluster in the EU context is perceived as significantly more likely than some other technologies. This is due particularly to lower ethical and human rights barriers, as well as to a relatively lower threshold of uncertainty regarding the performance of these technologies and barriers to accessing them. This finding may reflect the increasing recognition of the crucial role of space-based technologies and the increasing opportunities for strengthening European cooperation in space-based technologies (e.g. through the EDF and the newly created DG DEFIS, as well as expectations of falling cost of space launch reducing the relative weight of cost-related barriers on future development and uptake of space-based technologies).

Examining the assessment of technology impacts in relation to the impact criteria, a number of cross-cutting observations can be made. Figure C.3 presents the average scores of all technologies for each of the impact criteria illustrating these observations.

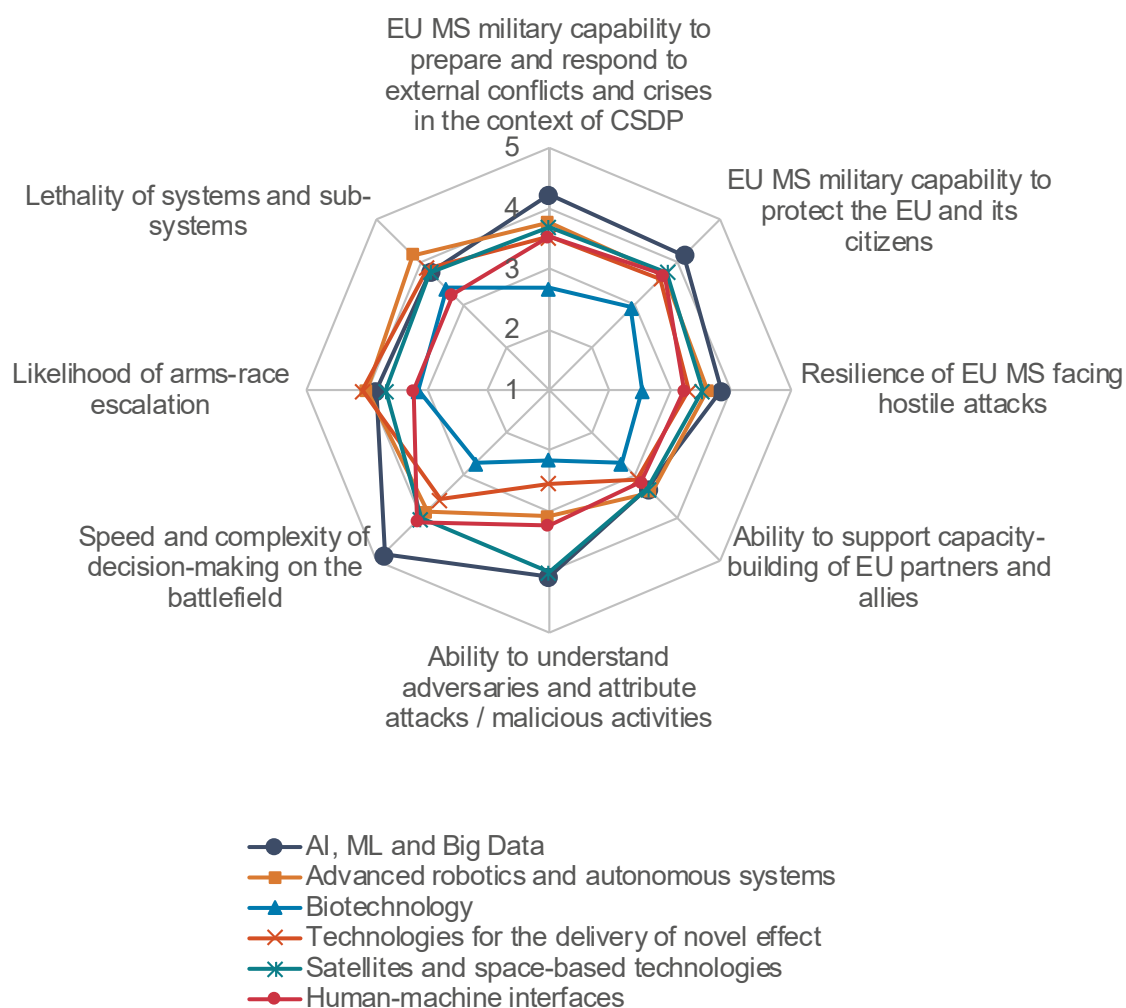
On average, the technology clusters were assessed to have the most significant impact on speed and complexity of decision-making on the battlefield. In general, technologies were assessed to have more significant impact on future battlefield dynamics (average score 3.73) than the EU and the CSDP (average score 3.4). This may indicate that overall, new and emerging technologies present greater challenges than opportunities for the EU due to their significant impact on decision-making on the battlefield, potential arms race escalations and battlefield lethality. The results, however, may also signal that the opportunities associated with new and emerging technologies for the EU in a defence or military context are less well understood. This would corroborate findings from existing research pointing to the relative lack of in-depth understanding of the opportunities presented by military technologies in the EU context.³²⁷

Among the criteria relating to the opportunities presented by emerging technologies for the EU and the CSDP, the most impact was perceived to be in relation to EU MS military capability to protect the EU and its citizens, closely followed by EU MS military capability to prepare and respond to external conflicts and crises in the context of CSDP. In contrast, emerging technologies were assessed as contributing the least potential capability improvement in relation to both the ability to support capacity-building and the ability to understand adversaries and attribute attacks. Workshop discussions, however, noted that in relation to the latter criteria, emerging technologies may improve the ability of an actor to understand an adversary's capabilities at large, while also exacerbating attribution challenges.

³²⁶ For example, Bordin et al. (2020), Brockmann et al. (2019).

³²⁷ For example, Franke (2019).

Figure C.3 – Summary assessment of the technology clusters across the impact criteria



Source: RAND Europe analysis.

Note: The higher a technology is scored on the criteria, the greater the expected impact and feasibility of implementation. For impact criteria, the scale ranges from 1 (negative impact – reduction in capability compared to current practices) to 5 (ground-breaking impact – paradigm shift in capability compared to current practices). See Annex B for a full description of the STREAM scores and criteria.

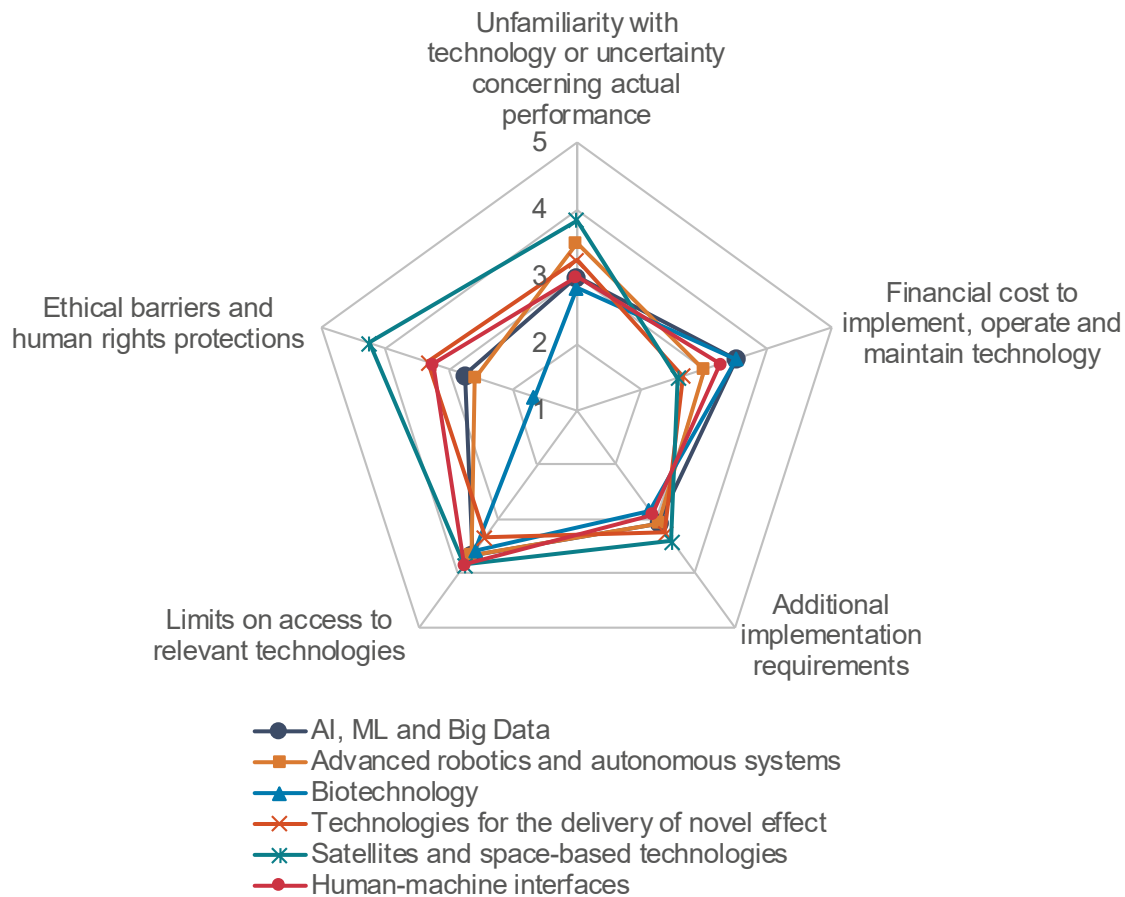
In relation to the potential uptake of each of the technology clusters, the workshop indicated the following with regards to the role of various implementation barriers. These findings are illustrated in Figure C.4, which presents the average scores of all technologies for each of the implementation criteria.

- As previously noted, significant variation can be observed among the technologies in relation to the relevance of ethical barriers and human rights protections on the uptake of technologies in European defence. While ethical barriers are considered close to insurmountable in the case of biotechnology, particularly weaponised biotechnologies, they are significantly lower in the case of space-based technologies. On average, however, ethical barriers and human rights protections were found to be the most significant factor limiting the uptake of new and emerging technologies on the future battlefield. This

highlights the significant degree of uncertainty associated with the potential ethics and the governance challenges associated with emerging technologies at large.

- In contrast, barriers to accessing relevant technologies were on average assessed as the least significant for the uptake of the selected new and emerging technologies in the European defence context. This may signify increasing confidence in growing European strategic autonomy in the area of new and emerging technologies.

Figure C.4 – Summary assessment of the technology clusters across the implementation criteria



Source: RAND Europe analysis.

Note: The higher a technology is scored on the criteria, the more positive its assessment was in relation to potential feasibility of implementation. The scale ranges from 1 (insurmountable barriers – barriers could not be overcome) to 5 (negligible or no concern about barrier – barrier could be overcome with very minor or no change or disruption). See Annex A for a full description of the STREAM scores and criteria.

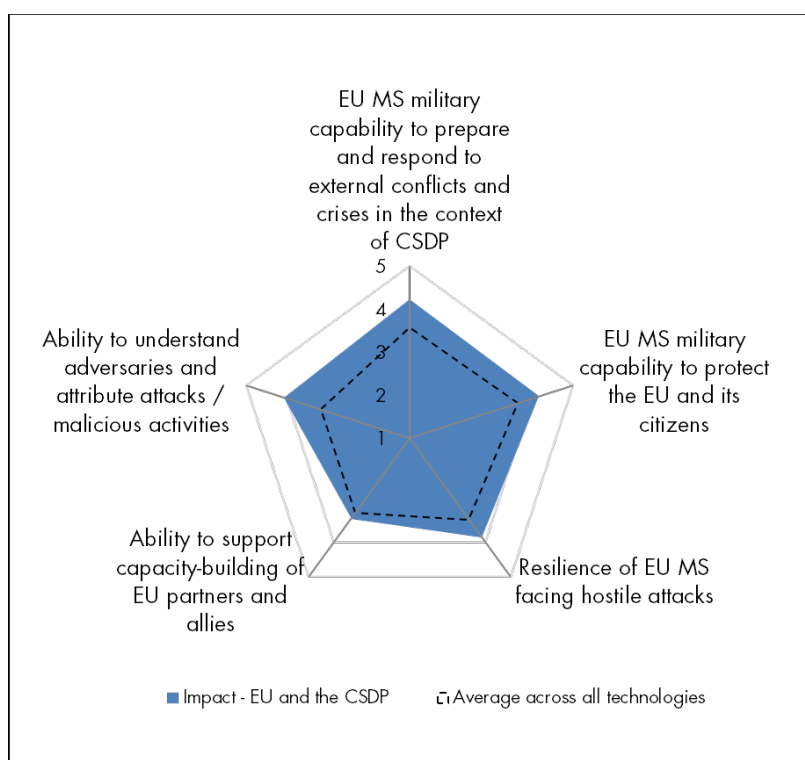
Artificial Intelligence, Machine Learning and Big Data

During the STREAM workshop, the AI, ML and Big Data technology cluster was consistently highlighted as a key enabler for advances in other technological areas as well as for future military effectiveness and efficiency on the battlefield. The scoring demonstrates that the cluster was consistently assessed to have a considerable impact across most of the impact criteria. This is captured in Figures C.1 and C.2, which illustrate the technology scores in relation to the two categories of impact criteria.

Among the opportunities for the EU and its ability to carry out functions under the CSDP, greatest impact for this technology cluster was expected to be in relation to the EU MS military capability to prepare and respond to external conflicts and crises in the context of CSDP. On the other hand, among the criteria the cluster scored the lowest in relation to ability to support capacity-building of EU partners and allies.

In relation to the future battlefield dynamics, AI, ML and Big Data were found to have near ground-breaking impact on the speed and complexity of decision-making on the battlefield. This reflects the contributions of technologies in this cluster to rapidly process large quantities of data, creating efficiency opportunities for the armed forces as well as challenges in relation to reduced decision-making and reaction timeframes.

Figure C.5 – Assessment of AI, ML and Big Data on impact criteria- EU and the CSDP



Source: RAND Europe analysis.

Figure C.6 – Assessment of AI, ML and Big Data on impact criteria - future battlefield dynamics

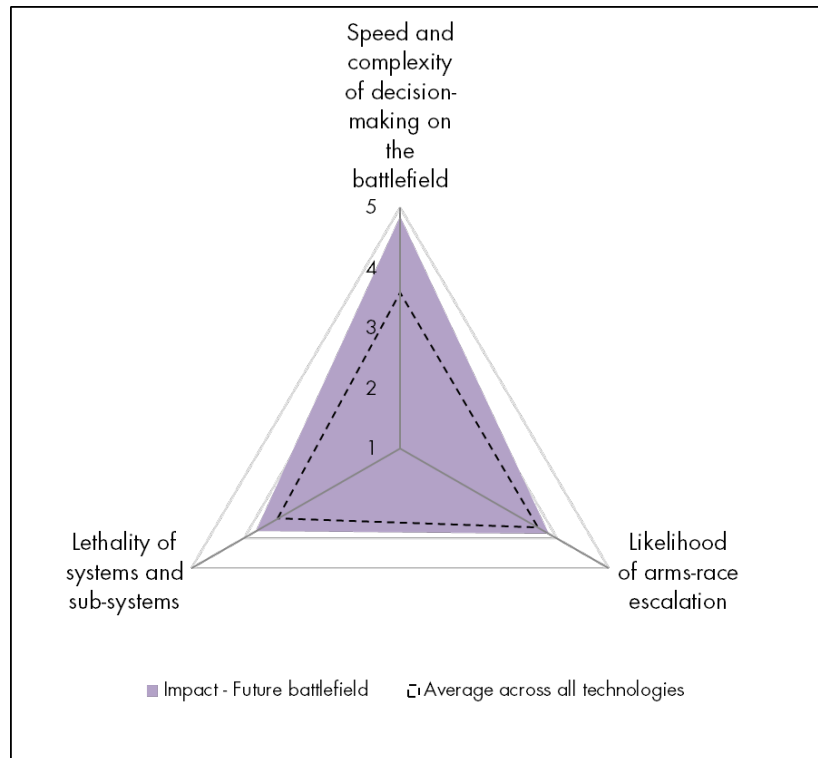
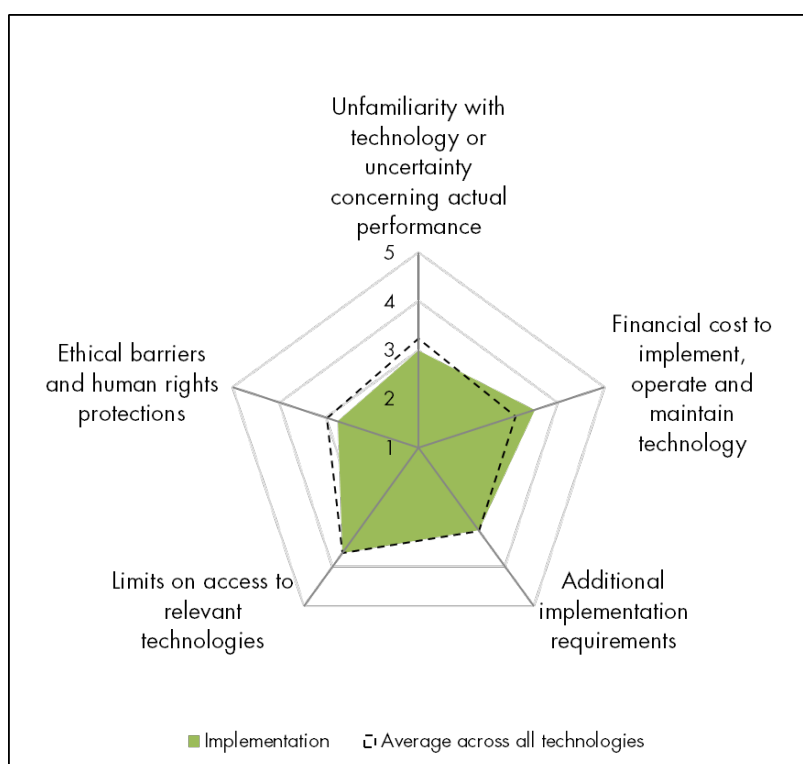


Figure C.3 provides an overview of the scoring for this technology cluster in relation to the feasibility of implementation criteria. The scoring indicates that while the financial cost of technologies in this cluster is of lesser concern as a barrier to implementation, there are more significant barriers in relation to the ethical implications of AI and ML-based systems and relevant human rights protections.

Figure C.7 – Assessment of AI, ML and Big Data on implementation criteria



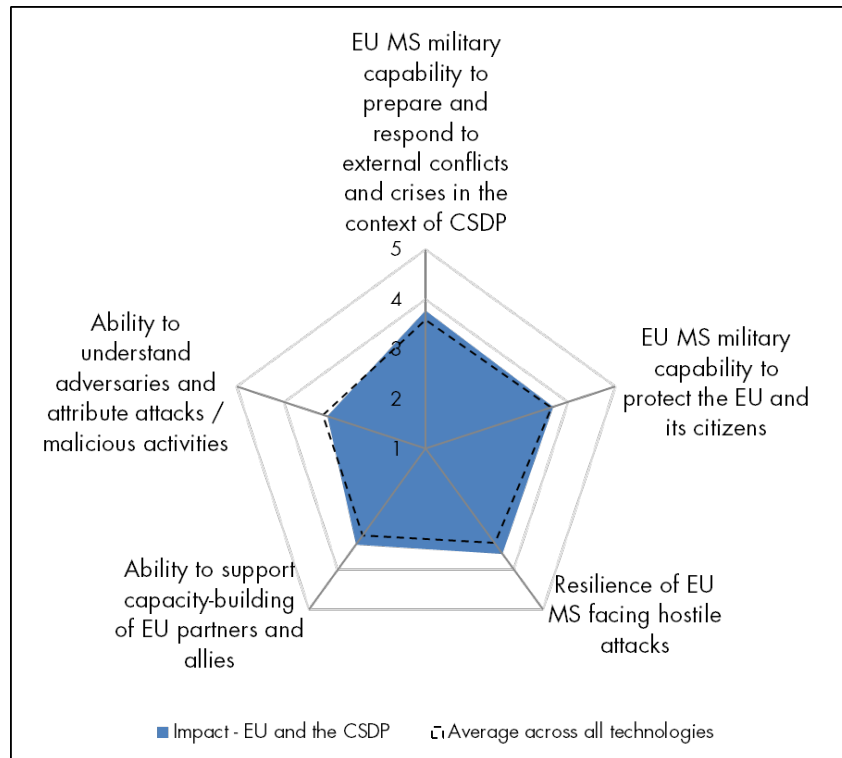
Source: RAND Europe analysis.

Advanced robotics and autonomous systems

The assessment by workshop participants of the impact of advanced robotics and autonomous systems highlighted a close link of the technology cluster with the impact of advances in AI, ML and Big Data. Workshop participants highlighted the enabling effect of AI and ML on autonomous systems in particular.

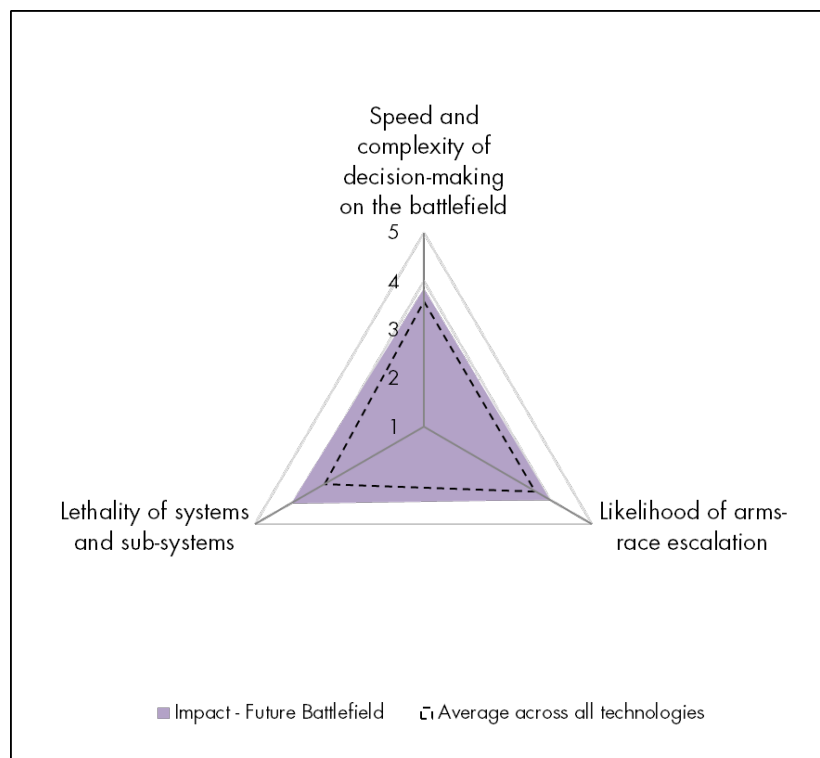
Reflecting this link, this technology cluster was assessed to have a similarly significant impact on future battlefield dynamics, though a more significant impact was expected in relation to the lethality of systems and sub-systems (Figure C.5). Among all technologies, advanced robotics and autonomous systems scored the highest on this criterion, likely reflecting the risks and challenges associated with autonomous lethal weapons systems.

Figure C.8 – Assessment of advanced robotics and autonomous systems on impact criteria – EU and the CSDP



Source: RAND Europe analysis.

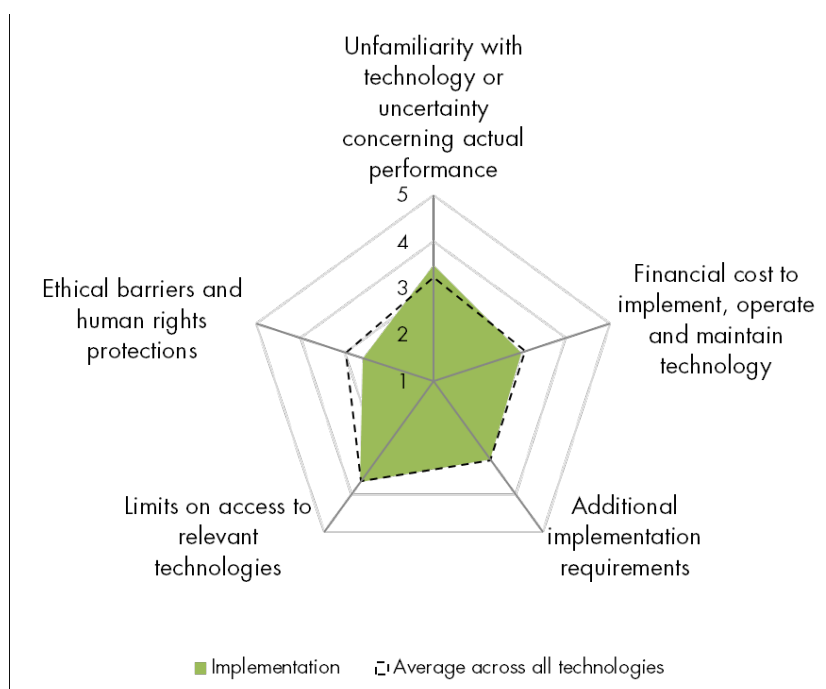
Figure C.9 – Assessment of advanced robotics and autonomous systems on impact criteria – Future battlefield dynamics



Source: RAND Europe analysis.

In relation to the feasibility of their implementation, ethical barriers and human rights protections were perceived as a similarly significant barrier in the case of advanced robotics and autonomous systems as they were in the case of AI, ML and Big Data. The technology cluster scored second lowest on this criterion, mirroring the significant ethical concerns associated with FAWs/LAWs, as well as data protection requirements in autonomous systems more widely. Despite insights from the literature indicating the potential uncertainties with regard to the performance of autonomous systems and the level of human control, unfamiliarity with technology and uncertainty with performance was not perceived as a significant barrier. This likely mirrors the increasing utilisation of autonomous systems in various Defence functions within and outside of the battlefield.

Figure C.10 – Assessment of advanced robotics and autonomous systems on implementation criteria

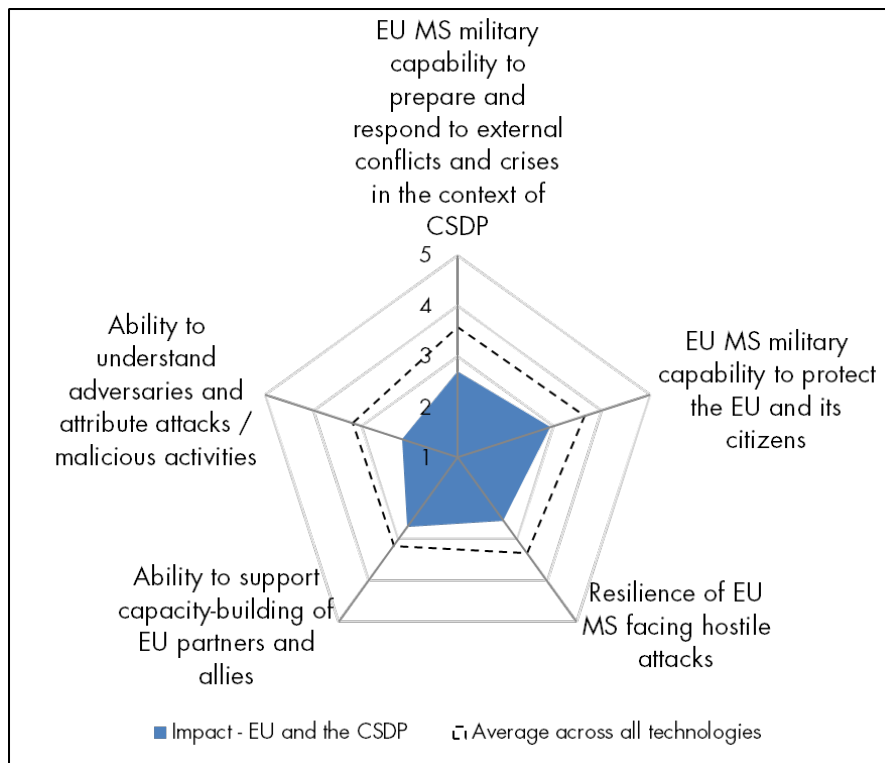


Source: RAND Europe analysis.

Biotechnology

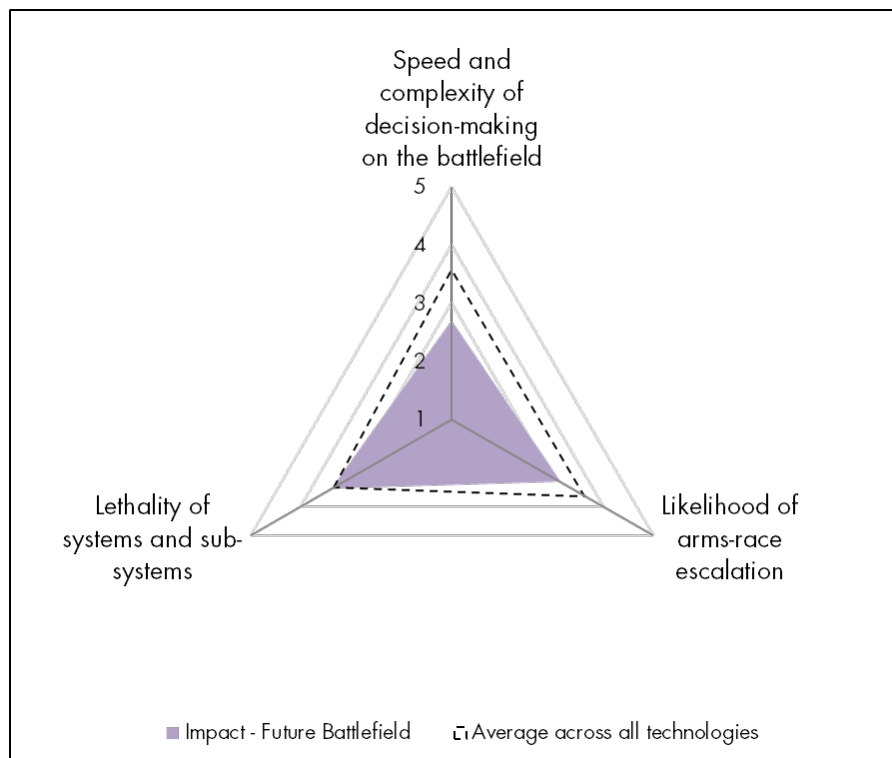
As outlined in Section 3.1.3, biotechnology has myriad applications on the future battlefield, including soldier enhancement but also weaponised applications in the form of bioweapons and the use of advanced pathogens to deliver lethal effects. Workshop discussions indicated that the potential weaponised applications of biotechnology dominated the assessments of this technology cluster. This is reflected the low impact of scoring of the technology across close to all impact criteria apart from the lethality of systems and sub-systems (see Figure C.7 and C.8).

Figure C.11 – Assessment of biotechnology on impact criteria – EU and the CSDP



Source: RAND Europe analysis.

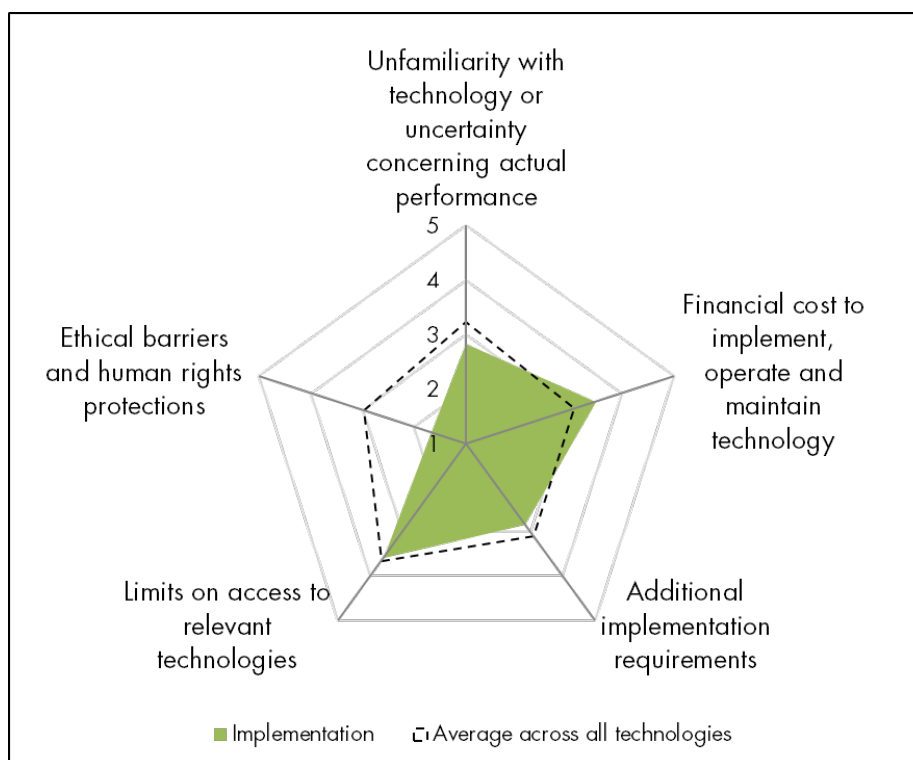
Figure C.12 – Assessment of biotechnology on impact criteria – Future battlefield dynamics



Source: RAND Europe analysis.

Assessments of the technology on the implementation criteria highlighted that the ethical and human rights implications of biotechnologies in the battlefield context were a close to insurmountable barrier for the future uptake of biotechnology. As described above, this assessment is likely focused on weaponised biotechnologies rather than biotechnology applications for soldier enhancement, biomimetic robotics or other similar applications.

Figure C.13 – Assessment of advanced biotechnology on implementation criteria



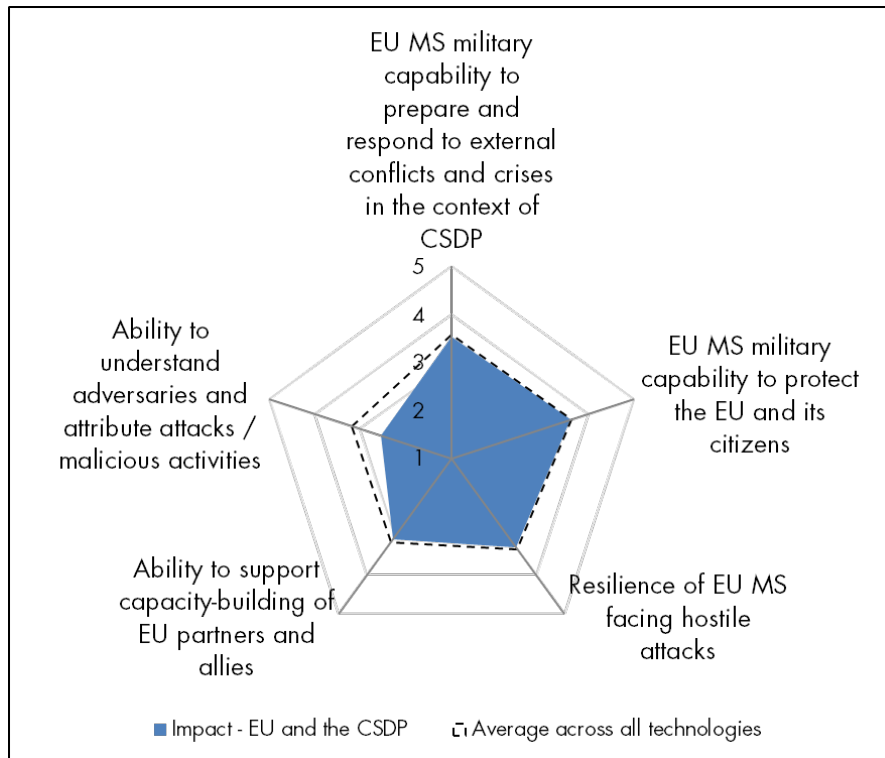
Source: RAND Europe analysis.

Technologies for the delivery of novel effect

Workshop participants highlighted significant difficulties in the scoring of this cluster due to the significant variation of technologies within the cluster. As such, the robustness of scoring for this technology cluster may be more limited in comparison to other technologies.

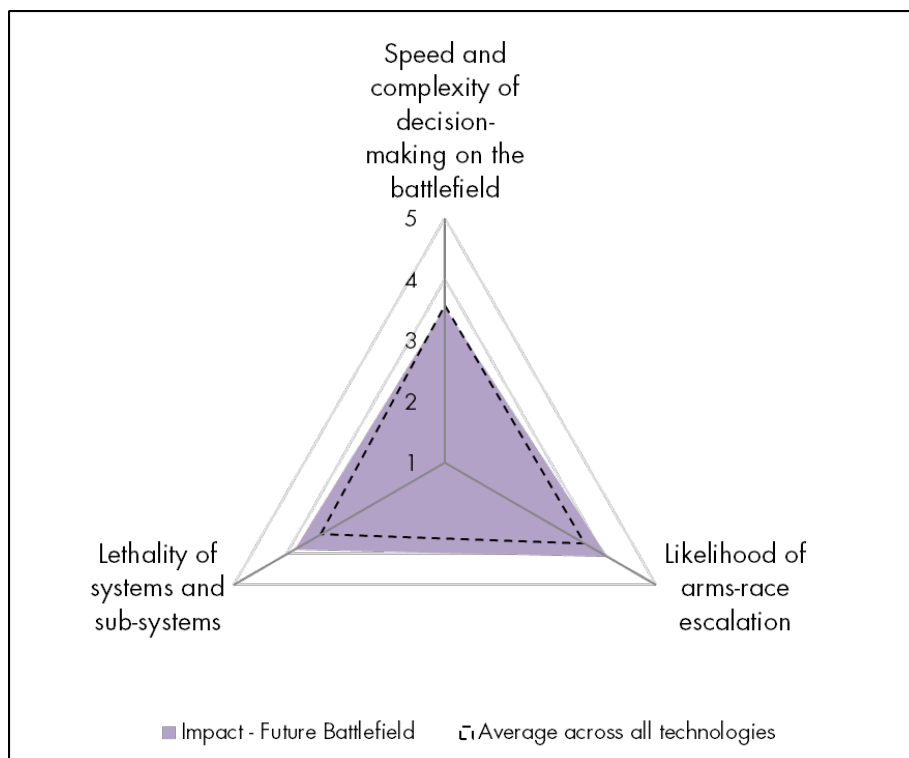
The scoring itself indicated that technologies for the delivery of novel effect were perceived as most likely among all technology clusters to result in arms race escalation (see Figure C.11). A significant impact was also recorded in relation to the lethality of systems and sub-systems, reflecting the potential applications of technologies such as hypersonics to inflict lethal effect. This likely reflects ongoing debates on the proliferation risks associated with hypersonic technologies. Workshop discussions also highlighted that technologies in this area are likely to exacerbate difficulties with attribution of attacks, reflected in the low scoring on that criteria (see Figure C.10).

Figure C.14 – Assessment of technologies for the delivery of novel effect on impact criteria – EU and the CSDP



Source: RAND Europe analysis.

Figure C.15 – Assessment of technologies for the delivery of novel effect on impact criteria – Future battlefield dynamics

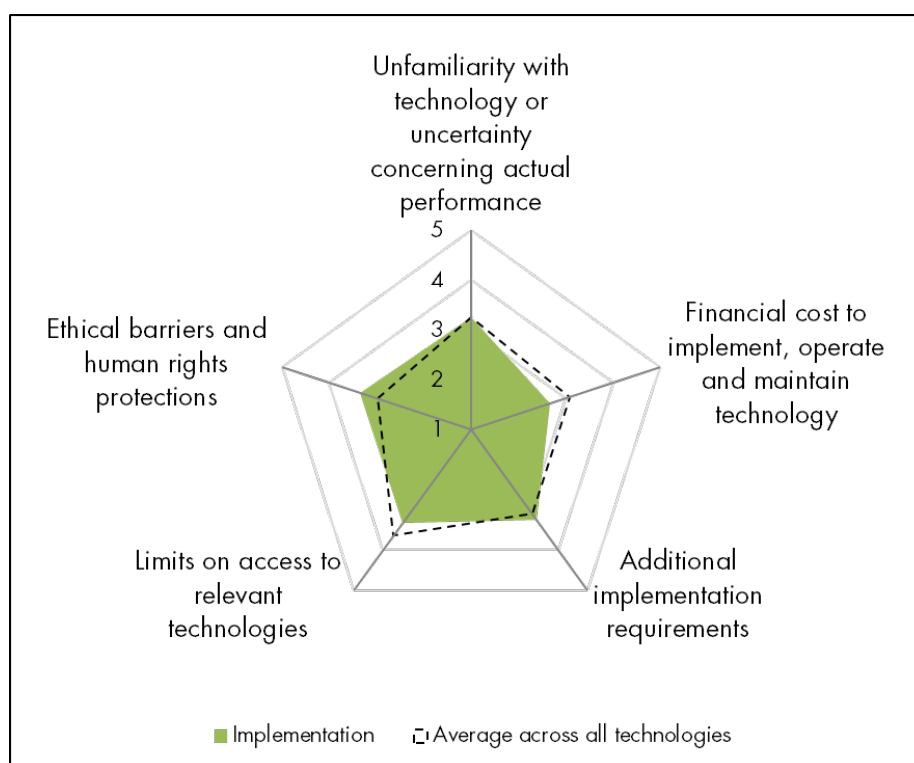


Source: RAND Europe analysis.

Noting the likely significant variation in the barriers to implementation of various technologies within this cluster, the scoring on feasibility of implementation highlighted that financial costs of implementation and access to relevant technologies represented areas of greater concern than in the case of other technologies.

Ethical barriers and human rights protections were not found to be a particularly significant barrier for this cluster, despite their expected high impact on the lethality of systems and sub-systems. The literature review and workshop discussions also noted that uncertainty concerning actual performance of technologies for the delivery of novel effect are, in practice, one of the chief barriers for the broader uptake of technologies in this cluster (see Section 3.1.4).

Figure C.16 – Assessment of technologies for the delivery of novel effect on implementation criteria

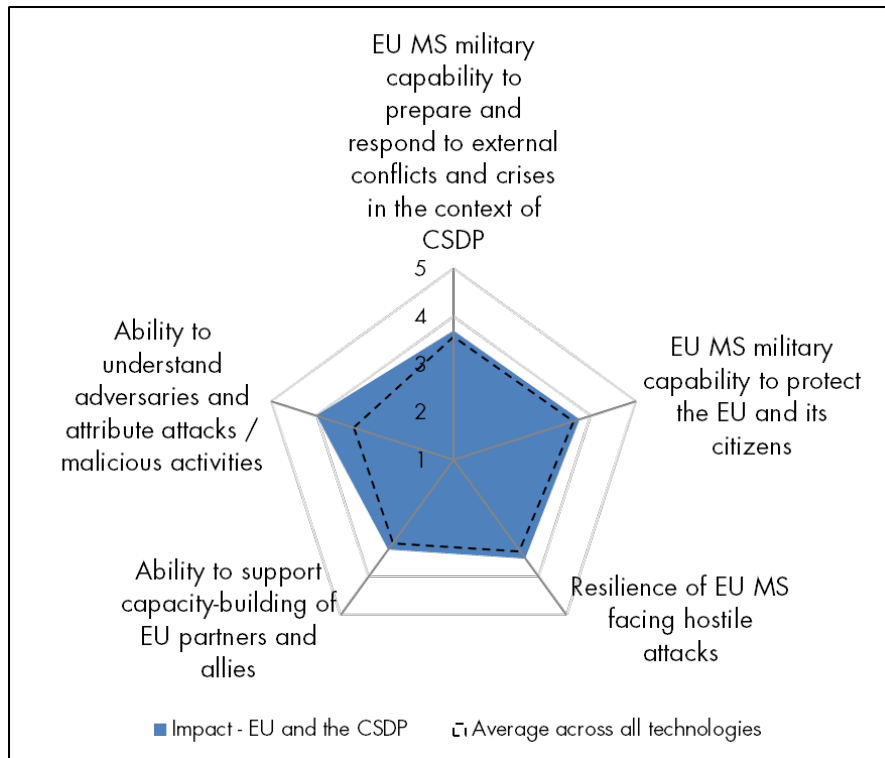


Source: RAND Europe analysis.

Satellites and space-based technologies and assets

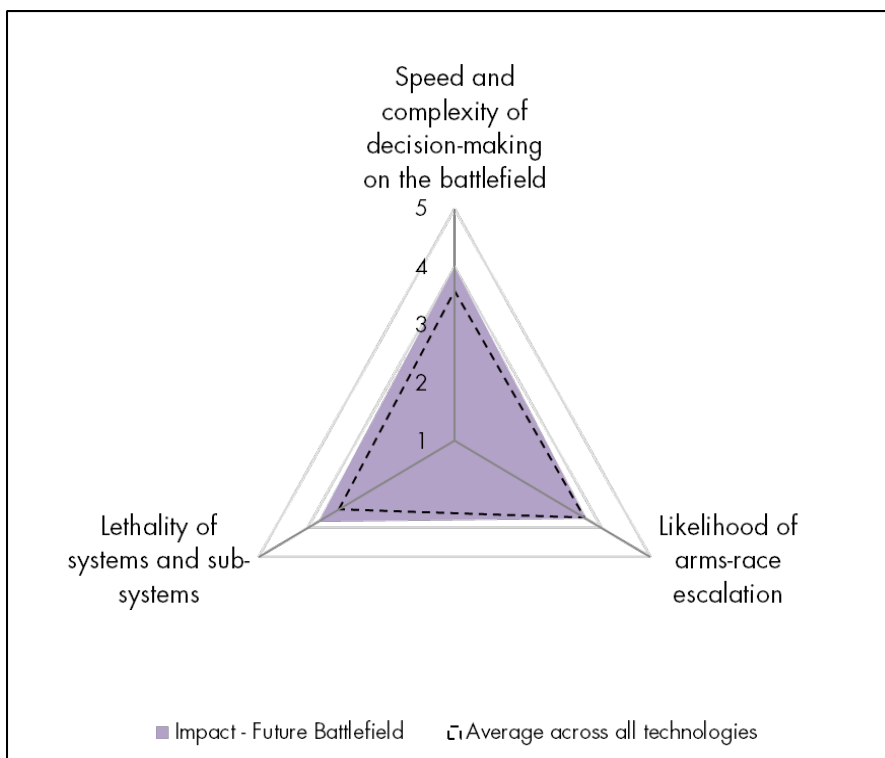
The comparative analysis presented in Chapter 4 highlighted the significant impact expected from advances in space-based technologies and satellites. Figure C.13 highlights in particular the significant opportunities associated with satellites and space-based systems for establishing an understanding of the adversary and attribute attacks and other malicious activities. This likely reflects the central role of space-based services such as EO, PNT and SATCOM in providing connectivity and supporting ISR.

Figure C.17 – Assessment of satellites and space-based technologies on impact criteria – EU and the CSDP



Source: RAND Europe analysis.

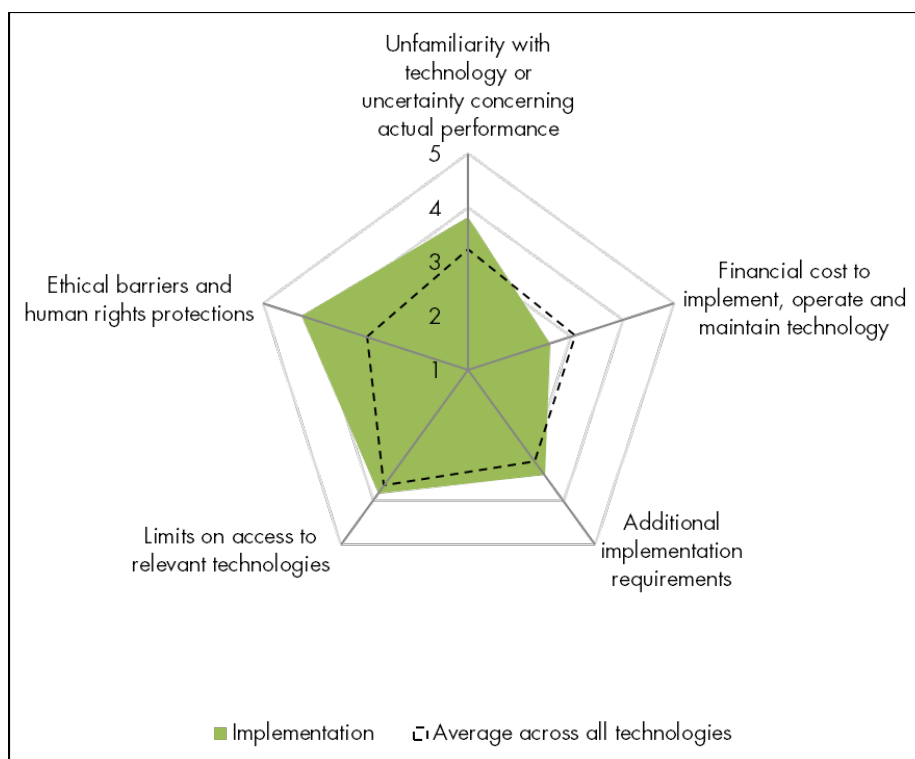
Figure C.18 – Assessment of satellites and space-based technologies on impact criteria – Future battlefield dynamics



Source: RAND Europe analysis.

In relation to the barriers of implementation, satellites and space-based technologies were scored by participants as having on average the least significant barriers to implementation. The effects of ethical barriers and human rights protections, as well as uncertainty with performance of technologies, were scored as largely negligible. Financial costs associated with the development, implementation and operation of space-based assets were assessed as more relevant in this area. This finding supports perspectives identified in the existing literature concerning the high costs of space launch as a prevalent barrier for space-based applications.

Figure C.19 – Assessment of technologies for the delivery of novel effect on implementation criteria

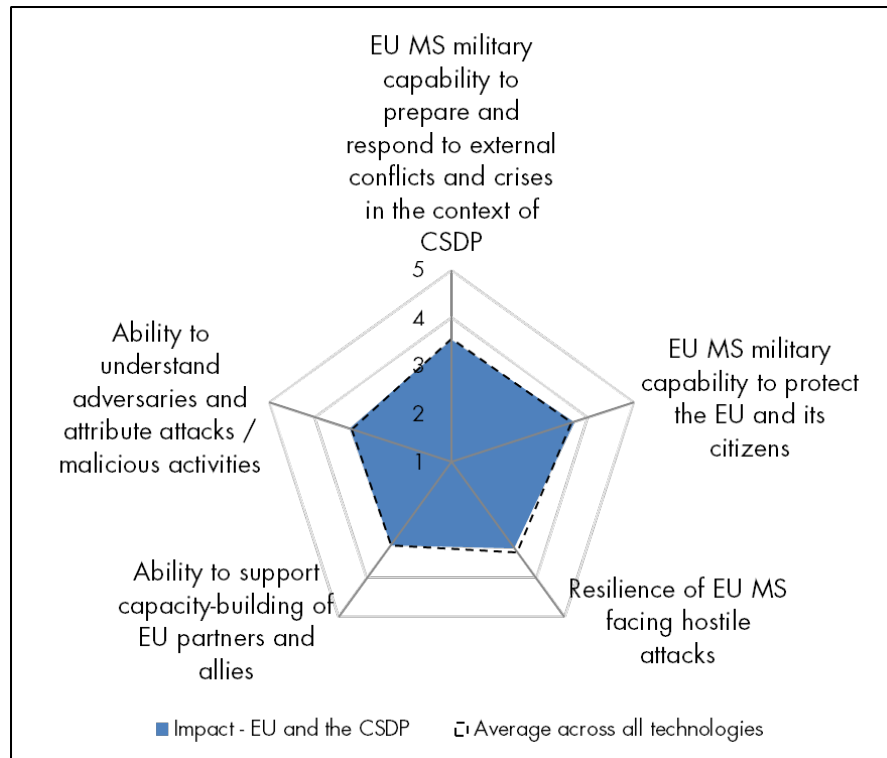


Source: RAND Europe analysis.

Human-machine interfaces

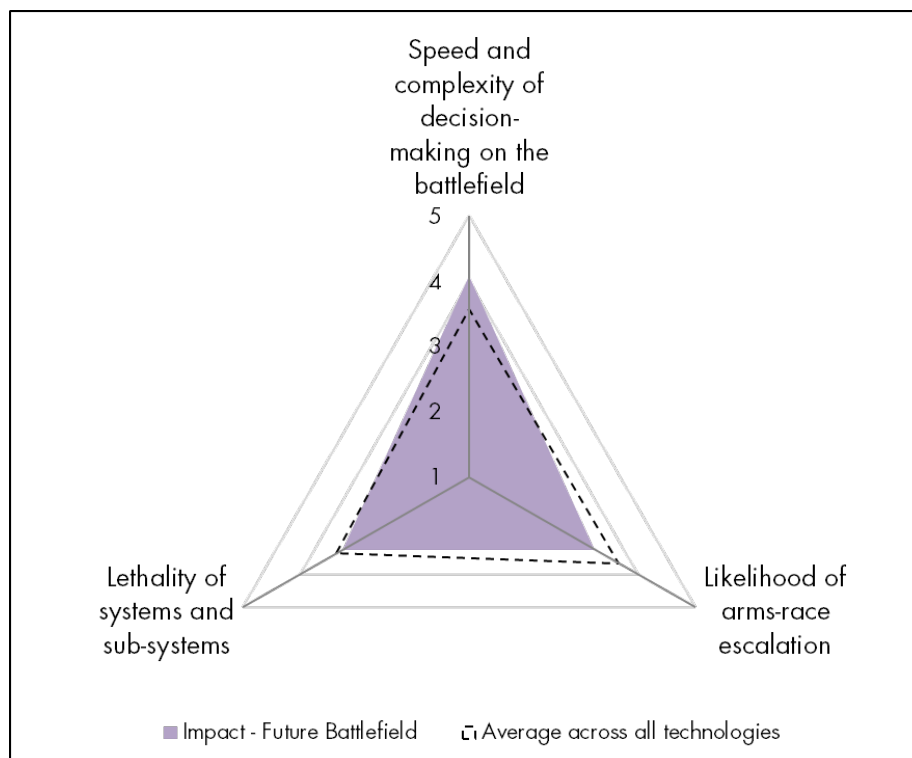
As discussed in Section 3.1.6 of the core report, human-machine interfaces encompass a range of technologies facilitating human-machine teaming on the future battlefield. In the context of the scoring exercise, human-machine interfaces were found to have a relatively average impact in terms of the opportunities for the EU and its ability to perform CSDP functions (see Figure C.16). In relation to future battlefield dynamics, the technology cluster was identified as particularly relevant in relation to the speed and complexity of decision-making on the battlefield. This likely reflects the close links between this technology cluster and advances in AI, ML and autonomous systems. Overall, workshop discussions noted a close relationship between these technology clusters.

Figure C.20 – Assessment of human-machine interfaces on impact criteria – EU and the CSDP



Source: RAND Europe analysis.

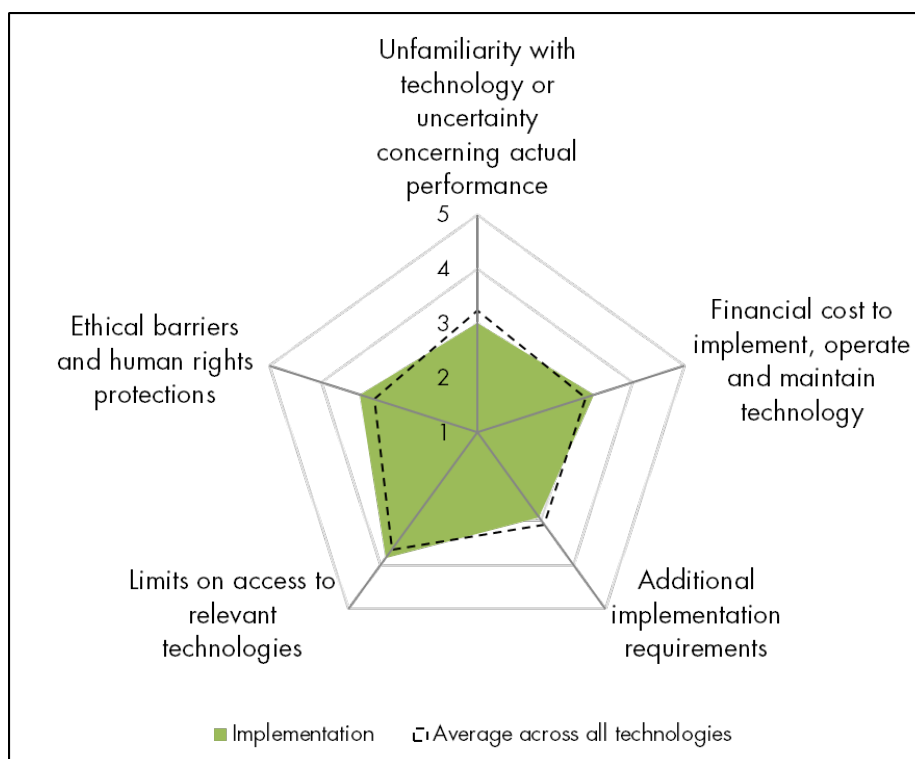
Figure C.21 – Assessment of human-machine interfaces on impact criteria – Future battlefield dynamics



Source: RAND Europe analysis.

In relation to the barriers to implementation, the technology cluster was assessed as facing relatively lower barriers to implementation stemming from ethical barriers and human rights protections. This corroborates insights from existing research on the key role of human-machine teaming technologies in addressing some of the ethical challenges associated with increasingly autonomous systems. As discussed in Section 3.1.6, this can be explained by the prevalent technical challenges associated with human-machine interfaces and the potential consequences of technical failures. This technology cluster scored comparatively higher in terms of levels of performance uncertainty and additional infrastructure requirements.

Figure C.22 – Assessment of human-machine interfaces on implementation criteria



Source: RAND Europe analysis.

Annex D: Copy of stakeholder engagement materials

Materials used in expert interviews

Interview protocol

RAND Europe has been commissioned by the European Parliament's Science and Technology Options Assessment (STOA) Panel to undertake a study examining the impact of new and emerging technologies on the future battlefield (out to 2040).

As part of the analysis, we are interviewing representatives from a number of areas, including academic experts and stakeholders from EUs. Given your relevant expertise and experience, you have been invited to take part in an interview with the project team, lasting approximately 30-45 minutes.

If at any point you feel you are unable to respond to any of these questions, simply inform the interviewer and we will move onto subsequent questions. We understand that the backgrounds and experiences of our interviewees will vary considerably, and are keen to focus on the areas where you feel able to provide commentary.

Prior to the interview, you are invited to review and sign an Information and Consent Form as well as a Privacy Notice. We will be taking notes during the interview, and – if selected in the consent form – we will record this interview for note taking purposes only. Both the recording and the notes of the interview will be stored securely in line with the EU's General Data Protection Regulation (GDPR).

Do you have any questions before we begin the interview?

Part I – Technology trends

As part of the study, we are considering a number of technology clusters that are likely to have a significant impact on the future battlefield. This includes [insert technology area].

In relation to this technology area:

- 1) What are the most prominent emerging and future trends and developments you expect will occur over the next 10-20 years for the technology area?
- 2) How do you think these technology trends and advances will impact the future battlefield and defence more broadly?
- 3) What are the key implications for defence that you expect will stem from the technology area? Are there particular trends or implications you perceive to be particularly relevant to the EU and its MS?
- 4) What key barriers and enablers may obstruct or facilitate the uptake and deployment of the technology area in a defence/battlefield context? Are there any EU-specific barriers or enablers that should be considered?

Part II - Policy options for EU and EU Member State institutions

- 5) Are there any initiatives or actions that you would suggest EUs and/or EU MS consider or prioritise as regards preparing for different new and emerging technologies that could shape the future battlefield out to 2040?
- 6) Are there any particular gaps that should be addressed in the current landscape of policy, investment, and RDT&I (i.e. research, development, technology and innovation) initiatives being pursued by EU and MS authorities?

Part III - Interview close

- 7) Is there anyone else that you would recommend us speaking with, or any documentation you would recommend us reviewing as part of our ongoing study?
- 8) Any closing remarks or questions for the study team?
- 9) If we have any further questions or clarifications, would you be happy for us to contact you again?

Materials used in the STREAM workshop

Scoring instructions

This document provides an overview of the scoring process for the RAND Europe workshop on Innovative Technologies Shaping the 2040 Battlefield that will take place on 7-9 October 2020. It includes instructions for participants on how to score each technology area, and should be read in conjunction with the Workshop Preparatory Note and Technology Briefs documents enclosed with it.

The workshop entails expert assessment of potential impacts and barriers to implementation associated with technologies in specified capability areas. This is achieved through a series of remote presentations, scoring activities and structured discussions. Participants will be asked to **independently assess and score** six shortlisted technology areas according to their potential impact on EU Member States' military capability, the ability of the EU to fulfil the objectives of the Common Security and Defence Policy (CSDP) and the overall nature of battlefield dynamics; and the feasibility of their implementation in light of technical, organisational, and other barriers to implementation that may impact the scale or pace of adoption of the technology areas by EU MS and potential state and non-state adversaries.

The following sections provide detailed definitions of the specific criteria for assessing the technologies based on their impact and feasibility of implementation. Criteria in both categories are assessed on a scale of 1-5. Definitions of each scoring option are specified below.

The scores for each technology should be recorded in the **Scoring Spreadsheet** provided by RAND Europe as part of the pre-reading materials:

- Recording scores: Participants are asked to record scores for all criteria for each of the six technology areas. Scores can be recorded through selecting from the dropdown menu on the first ('Scoring') tab of the scoring spreadsheet.
- Definitions of the criteria and technology areas: Definitions of the scoring criteria and all technology areas are also included on the spreadsheet. Definitions of the scoring criteria can be found on the 'Scoring Criteria' tab. Descriptions of the technologies are included on subsequent tabs and can also be accessed by clicking on the names of the technology case studies on the 'Scoring' tab.
- Recording additional comments and observations: Participants are encouraged to record any observations and additional comments on the technology case study at the bottom the Scoring tab of the spreadsheet.
- Submitting the spreadsheet: Once completed, participants should submit their spreadsheets via email to Ms Linda Slapakova (lslapako@randeurope.org). We ask that participants submit their initial scores at the end of the first webinar Wednesday 7 October 2020, 17:30 CET.

- Revising scores: RAND Europe will conduct initial analysis of the scoring, following this there will be a remote discussion and presentation of the results on Wednesday 20 May 2020. Participants will be able to then reassess and revise their scores for each of the technologies, and submit revised scores using the same scoring spreadsheet by Thursday 8 October 2020, 14:00 CET. Following analysis, RAND Europe will hold a remote presentation of the final results on Friday 9 October 2020.

IMPACT – EU AND THE CSDP

- Technologies may have a future impact on a range of factors defining the future context of European security and defence. To establish a comprehensive and in-depth understanding of this impact, the impact criteria considered in the workshop have been designed to enable an assessment of the EU's ability to fulfil missions and objectives concerning internal territorial integrity and resilience, as well as those stemming from the objectives of the Common Security and Defence Policy (CSDP).

If the technology were matured and implemented, what is likely to be the impact on:		
1a	EU MS military capability to prepare and respond to external conflicts and crises in the context of CSDP	The CSDP enables the EU to take a leading role in peace-keeping operations, conflict prevention and in the strengthening of the international security. The use of EU MS military capabilities to respond to external conflict and crises includes the use of military capabilities for crisis management and military missions and operations. The remit of CSDP includes the capacity for establishment and maintaining awareness and responsiveness in 'all phase of the conflict cycle, including conflict prevention, in order to promote peace and security within a rules-based global order'. ³²⁸
1b	EU MS military capability to protect the territorial integrity of the EU and its citizens	EU MS may use military capability to ensure and protect the territorial integrity of the EU, as well as the security of its citizens, by maintaining operational readiness and capacity to respond to potential threats. This includes maintaining a credible defence and deterrence posture against overt as well as sub-threshold threats and activities.
1c	Resilience of EU MS facing hostile attacks	Resilience is understood as the capacity to adapt and recover from major societal shocks, disruptions or operational setbacks (including those stemming from sub-threshold activities), including by maintaining resilient information networks and critical infrastructure.
1d	Ability to support capacity-building of EU partners and allies	Capacity-building is understood as the use of CSDP mechanisms and instruments to develop and strengthen the resources and ability of EU's partners and allies to address potential threats, conflicts, or instability.
1e	Ability to understand adversaries and attribute attacks / malicious activities	Understanding and comprehension correspond to the ability to establish situational awareness and knowledge of the intentions and capabilities of all actors within a conflict or crisis scenario. This includes the ability to attribute activities or attacks to responsible actors.

³²⁸ See Council of the European Union (2016).

For each technology area and criteria, participants are asked to allocate the following scores (1-5):

1. Negative impact - reduction in capability or negative impact in comparison to current practices;
2. No impact - negligible or no difference in comparison to current capability or practices;
3. Moderate positive impact - minor improvement in comparison to current capability or practices;
4. Substantial positive impact - significant improvement in comparison to current capability or practices;
5. Ground-breaking positive impact - paradigm shift compared to current capability or practices (i.e. enables entirely novel approach).

IMPACT – FUTURE BATTLEFIELD DYNAMICS

While emerging technologies may impact the capabilities of EU MS and their Armed Forces, emerging technologies will likely also influence the overall characteristics of the future battlefield and the context in which actors interact in a conflict or crisis scenario. Three additional criteria were identified to capture these potential impacts.

If the technology were matured and implemented, what is likely to be the impact on:		
2a	Speed and complexity of decision-making on the battlefield	Increasing speed and complexity of decision-making on the battlefield increasing the likelihood of crisis escalation (i.e. entailing the accidental or unintended escalation of a crisis, defined as 'a confrontation between states involving a serious threat to vital national interests for both sides') with limited time available to resolve the confrontation. ³²⁹
2b	Likelihood of arms-race escalation	Arms-race escalation may entail a long-term dynamic in which actors are encouraged to continuously augment their forces (e.g. through commissioning new types of weapons, 'out of the fear that, in a crisis, the other side might gain a meaningful operational advantage by using weapons first'). ³³⁰
2c	Lethality of systems and sub-systems	Lethality refers to the capacity of weapons systems or sub-systems to cause damaging effect, including death. Increased lethality of systems and sub-systems are likely to correspond to increased levels of conflict-related violence and higher number of battlefield casualties.

For each technology area and criteria, participants were asked to allocate the following scores (1-5):

1. Negative impact - reduction in comparison to current practices / status quo;
2. No impact - negligible or no difference in comparison to current capability, practices or status quo;
3. Moderate impact - minor increase in comparison to current capability, practices or status quo;

³²⁹ See Wong et al. (2020).

³³⁰ See Wong et al. (2020).

4. Substantial impact - significant increase in comparison to current capability, practices or status quo;
5. Ground-breaking impact - paradigm shift compared to current capability, practices or status quo (i.e. enables entirely novel approach or dynamics).

FEASIBILITY OF IMPLEMENTATION

The feasibility of implementation criteria are designed to assess the possible technical, organisational, commercial, regulatory or other barriers and costs to implementation. Please assess each of the technology areas on the basis of the following criteria:

How much of a concern is the following a barrier to implementation:	
3a	Unfamiliarity with technology or uncertainty concerning actual performance
3b	Financial cost to implement, operate and maintain technology
3c	Additional implementation requirements (e.g. additional requirements and barriers to develop and sustain a capability stemming from doctrine, organisation, training, materiel, leadership, personnel, facilities, or interoperability considerations)
3d	Limits on access to relevant technologies (e.g. export control restrictions, lack of European suppliers, etc.)
3e	Ethical and/or human rights protection barriers

Source: RAND Europe.

For each technology, participants were asked to allocate the following scores (1–5):

1. Insurmountable barriers – barriers could not be overcome;
2. Grave concern – barriers unlikely to be overcome without major societal, organisational or economic change or disruption;
3. Significant concern – barrier could be overcome with significant change or disruption;
4. Minor concern – barriers could be overcome with only minor change or disruption;
5. Negligible or no concern – barriers could be overcome with very minor or no change or disruption.

Annex E: Horizon scanning technology longlist

This annex presents the full technology longlist identified through the study's horizon scanning exercise.

Title	Source(s)	Technology cluster of relevance
Novel learning algorithm	https://spectrum.ieee.org/automaton/robotics/drones/deep-neural-pilot-skydio-2 https://www.skydio.com/	AI, ML and Big Data
Advanced non-line-of-sight imaging	https://www.eurekalert.org/pub_releases/2020-01/tos-dle011320.php https://www.osapublishing.org/optica/abstract.cfm?uri=optica-7-1-63	AI, ML and Big Data
New algorithm for stronger cyber defence	https://techxplore.com/news/2020-01-software-backdoor-facial-recognition.html	AI, ML and Big Data
A way to bypass Moore's law	https://www.eurekalert.org/pub_releases/2019-09/aiop-ult092419.php https://aip.scitation.org/doi/full/10.1063/1.5108912	AI, ML and Big Data
Device to improve scalability	https://www.eurekalert.org/pub_releases/2019-09/ps-bcc091219.php https://www.nature.com/articles/s41467-019-12035-6	AI, ML and Big Data
AI systems that can work as a team	https://spectrum.ieee.org/tech-talk/computing/software/deepmind-teaches-ai-teamwork http://proceedings.mlr.press/v97/jaques19a/jaques19a.pdf https://blog.goodaudience.com/a3c-what-it-is-what-i-built-6b91fe5ec09c https://www.geeksforgeeks.org/what-is-reinforcement-learning/	AI, ML and Big Data
Identifying fake text	https://arxiv.org/pdf/1907.10739.pdf https://www.seas.harvard.edu/news/2019/07/visual-forensics-to-detect-fake-text https://www.seas.harvard.edu/news/2019/07/better-way-to-train-machine-learning-models http://gltr.io/	AI, ML and Big Data

Title	Source(s)	Technology relevance	cluster	of
Chip self-learns through light	https://www.ncbi.nlm.nih.gov/pubmed/31018039 https://onlinelibrary.wiley.com/doi/full/10.1002/adfm.201901991 https://phys.org/news/2019-07-electronic-chip-mimics-brain-memories.html https://www.rmit.edu.au/news/all-news/2019/jul/electronic-chip-mimics-brain https://cosmosmagazine.com/technology/an-electronic-chip-that-makes-memories http://www.xinhuanet.com/english/2019-07/17/c_138233675.htm https://www.itnews.com.au/news/new-brain-inspired-chip-makes-light-work-of-memory-making-528398	AI, ML and Big Data		
App that tracks most populated areas	https://techcrunch.com/2019/03/08/foursquares-hypertrending-helps-you-spy-on-the-coolest-local-happenings/ https://enterprise.foursquare.com/intersections/article/introducing-hypertrending/ https://www.digitaltrends.com/social-media/foursquare-unveils-hypertrending-feature-at-sxsw-2019/ https://www.geospatialworld.net/blogs/foursquare-introduces-hypertrending/ https://www.theverge.com/tldr/2019/3/8/18256558/foursquare-hypertrending-phone-tracking-feature-sxsw-2019 https://mashable.com/article/foursquare-launches-hypertrending-sxsw/?europe=true https://enterprise.foursquare.com/intersections/article/introducing-hypertrending/ https://www.engadget.com/2019/03/10/foursquare-hypertrending-dennis-crowley-interview/ https://blog.mapbox.com/hypertrending-foursquares-real-time-view-of-all-the-cool-places-1557365eebd1	AI, ML and Big Data		
Large-scale data analytics	https://www.eurekalert.org/pub_releases/2019-06/dgi-hdp060219.php https://www.dgist.ac.kr/en/html/sub06/060202.html?mode=V&no=c678e85ac47c3981b86f080b1bf3892d https://www.sciencedirect.com/science/article/pii/S0020025518309836	AI, ML and Big Data		
Causal analysis via regression	https://blog.clearbrain.com/posts/introducing-causal-analytics https://techcrunch.com/2019/08/16/clearbrain-launches-analytics-tools-focused-connecting-cause-and-effect/	AI, ML and Big Data		
AI identification of malware	https://www.technologyreview.com/s/610881/with-this-tool-ai-could-identify-malware-as-readily-as-it-recognizes-cats/	AI, ML and Big Data		

Title	Source(s)	Technology relevance	cluster	of
Proactive AI-enabled cyber protection	https://www.baesystems.com/en/article/bae-systems-to-develop-automated-cyber-defense-tools-for-darpa http://www.foxnews.com/tech/2018/08/07/darpa-prototypes-breakthrough-cyberattack-hunting-technology.html	AI, ML and Big Data		
De-anonymising programmers through AI	https://www.defcon.org/html/defcon-26/dc-26-speakers.html#Greenstadt https://www.wired.com/story/machine-learning-identify-anonymous-code/	AI, ML and Big Data		
Ultrafast deep learning algorithm	https://www.nature.com/articles/s41598-019-48016-4 https://www.eurekalert.org/pub_releases/2019-08/bu-tb080719.php https://www1.biu.ac.il/indexE.php?id=33&pt=20&pid=117&level=2&cPath=33&type=1&news=3352 https://interestingengineering.com/a-new-type-of-ai-has-been-created-inspired-by-the-human-brain https://www.azorobotics.com/News.aspx?newsID=10768 https://www.enn.com/articles/59166-the-brain-inspires-a-new-type-of-artificial-intelligence https://cfbiu.org/news/the-brain-inspires-a-new-type-of-artificial-intelligence/	AI, ML and Big Data		
FlyJackets for drone control	https://spectrum.ieee.org/automaton/robotics/drones/epfl-flyjacket-exosuit-lets-you-control-a-drone-with-your-body	Advanced robotics and autonomous systems		
Carbon fibre artificial muscles	http://dx.doi.org/10.1088/1361-665X/aab52b https://phys.org/news/2018-04-strong-carbon-fiber-artificial-muscles.html	Advanced robotics and autonomous systems		
Superstrong artificial muscle	https://science.sciencemag.org/content/365/6449/155 https://science.sciencemag.org/content/365/6449/145 https://science.sciencemag.org/content/365/6449/150 https://www.newscientist.com/article/2209494-superstrong-artificial-muscle-can-lift-1000-times-its-own-weight/	Advanced robotics and autonomous systems		

Title	Source(s)	Technology relevance	cluster	of
	https://www.dailymail.co.uk/sciencetech/article-7241511/Artificial-muscles-created-scientists-100x-STRONGER-humans.html			
3D-printed robotic invertebrates	https://www.nanowerk.com/news2/robotics/newsid=49951.php	Advanced robotics and autonomous systems		
Electronic soft robotic skins	http://robotics.sciencemag.org/content/3/18/eaas9020 https://phys.org/news/2018-06-electronic-skins-wirelessly-fully-soft.html	Advanced robotics and autonomous systems		
Robotic skins for all objects	http://robotics.sciencemag.org/content/3/22/eaat1853 https://www.eurekalert.org/pub_releases/2018-09/you-st091418.php https://futurism.com/the-byte/robotic-skin-animate-objects	Advanced robotics and autonomous systems		
Improved drone swarm defence system	https://www.dedrone.com/blog/defending-against-drone-swarms-with-dronetracker-3-5 https://www.c4isrnet.com/unmanned/2018/09/21/dedicated-drone-tracker-can-now-detect-swarming-robots/ https://dronelife.com/2018/09/20/detecting-drone-swarms-dedrone-introduces-new-release/	Advanced robotics and autonomous systems		
Gun shoots drones from sky	https://www.defensenews.com/digital-show-dailies/navy-league/2018/04/10/this-gun-shoots-drones-out-of-the-sky/	Advanced robotics and autonomous systems		
Virtual-reality for drones	http://news.mit.edu/2018/virtual-reality-testing-ground-drones-0517 https://techxplore.com/news/2018-05-virtual-reality-ground-drones.html	Advanced robotics and autonomous systems		
Drone able to detect human violence	https://spectrum.ieee.org/tech-talk/robotics/artificial-intelligence/ai-drone-learns-to-detect-brawls	Advanced robotics and autonomous systems		
Armoured vehicle with tethered drones	https://www.defensenews.com/digital-show-dailies/eurosatory/2018/06/08/nexter-armored-vehicle-could-soon-include-tethered-drones/	Advanced robotics and autonomous systems		

Title	Source(s)	Technology cluster of relevance
Robot using echolocation	http://www.yossiyovel.com/images/PDF-Files/Eliakim2018.pdf https://www.jpost.com/Israel-News/Robat-Israeli-researchers-develop-unique-autonomous-bat-like-robot-566854 https://www.fromthegrapevine.com/innovation/breakthrough-robot-navigates-using-bat-inspired-senses	Advanced robotics and autonomous systems
Autonomous drones	https://vtnews.vt.edu/articles/2020/02/ictas-nasaraavin.html https://vpm.org/news/articles/10664/virginia-tech-researchers-testing-drones-that-detect-and-avoid-collisions https://www.therobotreport.com/drone-tests-demonstrate-autonomous-uavs-evade-air-traffic/ https://vtnews.vt.edu/articles/2019/09/ictas-upp2019.html	Advanced robotics and autonomous systems
High-speed motion planning processor	https://spectrum.ieee.org/cars-that-think/transportation/self-driving/realtime-robotics-motion-planning-chip-autonomous-cars https://hub.packtpub.com/real-time-motion-planning-for-robots-made-faster-and-efficient-with-rapidplan-processor/ https://www.therobotreport.com/realtime-robotics-shipping-rapidplan-motion-planning-processor/ https://spectrum.ieee.org/automaton/robotics/robotics-software/enabling-faster-more-capable-robots-with-real-time-motion-planning https://spectrum.ieee.org/robotics/robotics-software/motionplanning-chip-speeds-robots	Advanced robotics and autonomous systems
Aerial and shape-changing robot	https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8258850 https://spectrum.ieee.org/automaton/robotics/drones/flying-dragon-robot-transforms-itself-to-squeeze-through-gaps	Advanced robotics and autonomous systems
Computer generated genome	https://www.sciencedaily.com/releases/2019/04/190401171343.htm https://www.ncbi.nlm.nih.gov/pubmed/30936302	Biotechnology
Seawater-enabled biofuel production	https://www.manchester.ac.uk/discover/news/breakthrough-for-biofuels-that-could-be-made-from-seawater-rather-than-crude-oil/ https://www.biofuelsdigest.com/bdigest/2019/10/20/researchers-re-engineering-bacteria-to-make-higher-value-chemicals-from-seawater-based-bacteria/ https://phys.org/news/2019-10-biofuels-seawater.html	Biotechnology

Title	Source(s)	Technology relevance	cluster	of
More sensitive ultrasound sensors	https://www.nature.com/articles/s41467-018-08038-4 https://www.uq.edu.au/news/article/2019/01/ultra-ultrasound-revolutionise-technology https://www.itnews.com.au/news/uq-unveils-ultra-ultrasound-sensor-precise-enough-to-hear-a-cell-breathe-517896	Biotechnology		
New method to build infrared camera	https://www.nature.com/articles/s41566-019-0362-1 https://news.uchicago.edu/story/breakthrough-could-enable-infrared-cameras-electronics-self-driving-cars	Biotechnology		
Soft robot integrates bacteria	https://robotics.sciencemag.org/content/4/31/eaax0765 https://www.ucdavis.edu/news/robot-arm-tastes-engineered-bacteria https://www.youtube.com/watch?v=jKL4U5fKJSU https://newatlas.com/robot-arm-taste-test-water/60331/	Biotechnology		
Novel super-resolution imaging technique	https://www.eurekalert.org/pub_releases/2019-07/cu-nim070819.php https://www.nature.com/articles/s41557-019-0288-8	Biotechnology		
Engineering bacteria for fuel	https://pubs.rsc.org/en/content/articlelanding/2019/EE/C9EE01214A#!divAbstract https://www.sciencedaily.com/releases/2019/07/190726094651.htm https://www.innovationtoronto.com/2019/07/bypassing-solar-cells-to-produce-butanol-with-microorganisms-carbon-dioxide-and-solar-energy/ https://techxplore.com/news/2019-07-solar-energy-biofuel-cells.html	Biotechnology		
Bio-structure facilitates cell growth	https://phys.org/news/2020-02-scientists-chemical-gardens-bone-substitute.html https://pubs.rsc.org/en/content/articlelanding/2020/BM/C9BM01010F#!divAbstract	Biotechnology		
Bio-inspired dry double-sided tape	https://www.nature.com/articles/s41586-019-1710-5 http://news.mit.edu/2019/double-sided-tape-tissues-could-replace-surgical-sutures-1030 https://www.bbc.com/news/health-50235451	Biotechnology		
Blocking laser attacks on aircraft	https://www.acs.org/content/acs/en/pressroom/newsreleases/2019/april/liquid-crystals-could-help-deflect-laser-pointer-attacks-on-aircraft.html https://www.sciencedaily.com/releases/2019/03/190331192543.htm https://www.siliconrepublic.com/machines/liquid-crystals-laser-attacks-passenger-jets	Technologies for the delivery of novel effect		

Title	Source(s)	Technology relevance	cluster	of
Nausea inducing lights	https://www.popularmechanics.com/military/navy-ships/a26134880/the-russian-navy-is-fitting-ships-with-barf-inducing-lights/ https://futurism.com/the-byte/russian-weapon-navy-hallucinate https://mysteriousuniverse.org/2019/02/russian-warships-have-new-weapon-that-causes-hallucinations/	Technologies for the delivery of novel effect		
Wattozz wireless energy weapon	http://en.azeridefence.com/wattozz-gun-made-in-turkey-will-put-an-end-to-the-monopoly-of-usas-taser-gun/ http://www.hurriyetdailynews.com/turkish-firm-debuts-non-lethal-weapon-in-south-africa-143817 https://www.dailysabah.com/defense/2019/01/10/turkish-defense-company-to-export-domestically-developed-arms-to-balkans https://www.hitechcentury.com/wattozz-wireless-electroshock-gun-now-available-malaysia/ http://www.milscint.com/en/wattozz-wireless-electroshock-gun-from-albayraklar-savunma/ https://futurism.com/the-byte/nonlethal-weapon-tasers	Technologies for the delivery of novel effect		
Hypersonic intercontinental weapon	https://techxplore.com/news/2019-12-russian-weapon.html https://apnews.com/597e7f2b20b21af959e4c6983b255c37 https://www.independent.co.uk/news/world/europe/russia-nuclear-missile-weapon-putin-hypersonic-speed-sound-a9262006.html	Technologies for the delivery of novel effect		
Electron beams to detect warheads	https://smdsymposium.org/ https://breakingdefense.com/2018/08/detect-nukes-in-flight-with-electron-beam-technology/	Technologies for the delivery of novel effect		
Hypersonic weapons development	http://usa.chinadaily.com.cn/a/201808/06/WS5b6787b4a3100d951b8c8ae6.html https://www.investors.com/news/hypersonic-weapons-china-starry-sky-2-waverider-lockheed-raytheon-boeing/	Technologies for the delivery of novel effect		
Russian combat lasers	http://tass.com/defense/1034344 https://futurism.com/russias-latest-weapon-laser-cannon/ https://www.globalsecurity.org/military/world/russia/vlk.htm https://gizmodo.com/russia-shows-off-new-laser-weapon-after-u-s-threatens-1830874116 https://defence-blog.com/army/russian-claims-new-peresvet-combat-laser-system-already-service.html	Technologies for the delivery of novel effect		

Title	Source(s)	Technology relevance	cluster	of
	http://tass.com/defense/1014121 https://www.youtube.com/watch?v=BOLcL0C1kzQ&feature=youtu.be			
Record in laser energy power	https://www.llnl.gov/news/nif-sets-new-laser-energy-record http://iopscience.iop.org/article/10.1088/1741-4326/aac69e/pdf https://phys.org/news/2018-07-national-ignition-facility-laser-energy.html	Technologies for the delivery of novel effect		
Electron gun	https://www6.slac.stanford.edu/news/2019-05-30-slac-fires-electron-gun-lcls-ii-x-ray-laser-upgrade.aspx https://phys.org/news/2019-05-slac-electron-gun-lcls-ii-x-ray.html	Technologies for the delivery of novel effect		
Light gas gun for hypersonic flight	https://arc.aiaa.org/doi/pdf/10.2514/6.2018-5382 https://techxplore.com/news/2019-10-hypersonic-spotlights-future-flight.html	Technologies for the delivery of novel effect		
Underwater acoustic cloak	https://acousticalsociety.org/wp-content/uploads/2018/04/thursda.pdf https://phys.org/news/2018-05-cloaking-devicesit-star-trek-anymore.html	Technologies for the delivery of novel effect		
Material with no reflection	https://www.nature.com/articles/s41563-018-0252-9 https://www.eurekalert.org/pub_releases/2018-12/asrc-rda122818.php	Technologies for the delivery of novel effect		
Computer-mediated deception	https://sml.stanford.edu/ml/2019/02/ho-chb-context.pdf https://newatlas.com/online-polygraph-truth-lies-detector-text-communication/58916/	Technologies for the delivery of novel effect		
Modified cable allows remote hacking	https://www.vice.com/en_us/article/evj4qw/these-iphone-lightning-cables-will-hack-your-computer https://futurism.com/the-byte/evil-charging-cable-infect-computer-virus https://mg.lol/blog/omg-cable/	Technologies for the delivery of novel effect		
Quantum radar for counter-stealth	https://www.livescience.com/62362-quantum-radar-detect-stealth-planes.html	Technologies for the delivery of novel effect		

Title	Source(s)	Technology relevance	cluster	of
Secure terahertz communications	https://www.nature.com/articles/s41586-018-0609-x https://phys.org/news/2018-10-exposes-vulnerabilities-terahertz-links.html https://spectrum.ieee.org/tech-talk/telecom/security/experiment-shows-terahertz-frequencies-are-vulnerable-to-hacking	Advanced energy and power systems		
Flexible miniature energy harvester	https://www.titech.ac.jp/english/news/2019/043410.html https://spectrum.ieee.org/nanoclast/energy/renewables/a-mems-vibration-energy-harvester-for-the-iot	Advanced energy and power systems		
Modern power grids dispatch strategy	https://ieeexplore.ieee.org/document/8731710 https://techxplore.com/news/2019-10-approach-modern-power-grids-efficiency.html	Advanced energy and power systems		
Wireless chargers in every shape	https://dl.acm.org/citation.cfm?doid=3301777.3287068 http://www.asahi.com/ajw/articles/AJ201901210051.html https://www.takuyasatani.com/projects/a-cuttable-2-d-wireless-power-transfer-sheet	Advanced energy and power systems		
Submarine batteries	https://www.defensenews.com/industry/techwatch/2018/11/16/new-battery-can-double-the-operational-time-of-submarines-says-south-korea/ http://www.samsungsdi.com/ https://energymetalnews.com/2018/11/07/home-developed-lithium-ion-batteries-ready-for-new-3000-ton-subs/	Advanced energy and power systems		
Using diamonds for batteries	https://lakediamond.ch/explore https://www.wired.com/story/drones-batteries-lasers-diamonds-lakediamond/ https://actu.epfl.ch/news/tech-transfer-using-diamonds-to-recharge-civilian-/	Advanced energy and power systems		
Energy generation using space	https://www.siliconrepublic.com/machines/radical-device-electricity-coldness-of-the-universe https://aip.scitation.org/doi/10.1063/1.5089783	Advanced energy and power systems		
Electrical engine for V/STOL aircrafts	https://www.safran-electrical-power.com/media/safran-unveils-electric-motor-its-engineous-range-designed-future-hybrid-and-electric-aircraft-20181016 https://www.flightglobal.com/news/articles/nbaa-safran-shows-off-electric-power-technology-452744/	Advanced energy and power systems		

Title	Source(s)	Technology relevance	cluster	of
3D-printed supercapacitor electrode	https://www.safran-electrical-power.com/media/safran-unveils-electric-motor-its-engineus-range-designed-future-hybrid-and-electric-aircraft-20181016 https://www.flightglobal.com/news/articles/nbaa-safran-shows-off-electric-power-technology-452744/	Advanced energy and power systems		
Solar cells that works with rain	https://pubs.acs.org/doi/abs/10.1021/acsnano.8b00416 https://thinkprogress.org/breakthrough-solar-panel-can-harvest-power-from-raindrops-day-or-night-3a2ce74f9060/	Advanced energy and power systems		
Silicon wafers in batteries	https://www.cpexecutive.com/post/silicon-wafer-innovation-hailed-as-battery-breakthrough/ https://www.upsbatterycenter.com/blog/silicon-joule-lead-battery-surge/#prettyPhoto	Advanced energy and power systems		
New catalyst for hydrogen fuel cells	http://www.chinanews.com/gn/2019/01-31/8744430.shtml https://www.nature.com/articles/s41586-018-0869-5 https://fuelcellsworld.com/news/scientists-find-way-to-help-fuel-cells-work-better-stay-clean-in-the-cold/	Advanced energy and power systems		
Versatile organic transistors	https://www.nature.com/articles/s41563-019-0407-0 https://phys.org/news/2019-03-transistor-purposes.html	Advanced energy and power systems		
New electrolyte improves supercapacitors	https://www.nature.com/articles/s41563-019-0449-6 http://news.mit.edu/2019/new-electrolyte-supercapacitor-0812 https://www.nanowerk.com/nanotechnology-news2/newsid=53379.php	Advanced energy and power systems		
Electrical current sensing	https://www.purdue.edu/newsroom/releases/2019/Q4/sensing-technology-could-improve-machine-learning-precision-for-manufacturing,-electric-vehicles,-smart-homes.html https://youtu.be/1iuZNYcedZc https://techxplore.com/news/2019-12-technology-machine-precision-electric-vehicles.html	Advanced energy and power systems		
Heatshield for spacecraft	https://www.sciencedirect.com/science/article/pii/S0094576518303850#! https://www.eurekalert.org/pub_releases/2018-08/uom-psd080918.php https://www.manchester.ac.uk/discover/news/phd-student-develops-spinning-heat-shield-for-future-spacecraft/	Satellites and space-based technologies and assets		

Title	Source(s)	Technology relevance	cluster	of
Nuclear space propulsion system	https://www.rt.com/news/442521-nuclear-propulsion-system-russia/ https://sputniknews.com/russia/201810291069304609-russia-nuclear-propulsion-spacecraft-key-element-tests/ https://www.nextbigfuture.com/2018/11/russia-claiming-reusable-nuclear-rocket-progress.html	Satellites and space-based technologies and assets		
Steam propelled spacecraft	https://today.ucf.edu/steam-powered-asteroid-hoppers-developed-ucf-collaboration/ https://futurism.com/the-byte/steam-powered-spacecraft	Satellites and space-based technologies and assets		
Strong alloy for rocket propulsion	https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190001243.pdf https://3dprintingindustry.com/news/nasa-develops-new-copper-alloy-for-3d-printing-rocket-components-151593/ https://3dprint.com/238775/three-dimensional-printing-grcop-42-nasa-unveils-special-rocket-engine-alloy/	Satellites and space-based technologies and assets		
3D-printed launch vehicles	https://www.businesswire.com/news/home/20190405005073/en/Relativity-Contracts-Telesat-Provide-Launch-Services-Telesat%E2%80%99s https://spacenews.com/relativity-signs-contract-with-telesat-for-launching-leo-constellation/ https://3dprintingindustry.com/news/relativity-space-completely-3d-printed-rocket-to-send-telesat-satellites-into-leo-152913/ https://www.technologyreview.com/the-download/613273/a-space-startup-that-3d-prints-its-rockets-just-got-its-first-customer/	Satellites and space-based technologies and assets		
Static stratospheric balloons	https://www.technologyreview.com/s/612417/darpa-is-testing-stratospheric-balloons-that-ride-the-wind-so-they-never-have-to-come-down/ https://www.nextbigfuture.com/2018/11/darpa-lidar-can-see-the-wind-from-8-6-miles-for-stratospheric-balloon-positioning.html	Satellites and space-based technologies and assets		
3D printing small rocket thrusters	https://3dprint.com/227288/agile-space-production-3d-prints-thrusters/ https://www.nextbigfuture.com/2018/10/agile-space-working-on-3d-printing-small-rocket-thrusters.html	Satellites and space-based technologies and assets		
Frequency lasers systems in space	https://phys.org/news/2018-05-frequency-stable-laser-space.html	Satellites and space-based technologies and assets		

Title	Source(s)	Technology cluster of relevance
Earth-space quantum communication	https://iopscience.iop.org/article/10.1088/2058-9565/aaefd4/meta https://phys.org/news/2018-12-satellite-global-quantum.htm https://www.picoquant.com/applications/category/quantum-optics/quantum-communication	Satellites and space-based technologies and assets
New CubeSat micropropulsion system	https://www.purdue.edu/newsroom/releases/2019/Q3/new-safer,-inexpensive-way-to-propel-small-satellites.html https://techxplore.com/news/2019-07-safer-inexpensive-propel-small-satellites.html http://www.ppps2019.org/assets/AbstractBook-20190524.pdf (paper abstract)	Satellites and space-based technologies and assets
Rockoons for rocket launch	https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/16747/Rockoons-Set-to-Rock-Rocket-Launching-Access.aspx https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/16747/Rockoons-Set-to-Rock-Rocket-Launching-Access.aspx https://www.leoaerospace.com/launch-system https://techcrunch.com/2019/10/02/leo-aerospace-provides-bespoke-rocket-launches-from-a-hot-air-balloon/ https://www.syfy.com/syfywire/hot-air-balloons-future-satellite-rocket-launches	Satellites and space-based technologies and assets
Russian space laser cannon	https://sputniknews.com/science/201806101065288031-laser-cannon-space-debris/	Satellites and space-based technologies and assets
New type of space flight fuel source	https://momentus.space/ https://techcrunch.com/2018/07/21/propelling-deep-space-flight-with-a-new-fuel-source-momentus-prepares-for-liftoff/	Satellites and space-based technologies and assets
Free space optical communication	https://doi.org/10.1364/OPTICA.5.001338 https://phys.org/news/2018-10-clouds.html	Satellites and space-based technologies and assets
First satellite extension service	https://www.theverge.com/2020/2/26/21154426/commercial-satellites-docking-space-northrop-grumman-intelsat https://www.forbes.com/sites/jonathanocallaghan/2020/02/27/historic-accomplishment-as-two-private-spacecraft-dock-in-space-for-the-first-time-in-history/#130e0ae2223a https://www.newscientist.com/article/2235591-first-private-space-rescue-mission-sees-two-satellites-latch-together/ https://www.nasaspaceflight.com/2020/02/northrop-grumman-history-mission-extension-vehicle-docks-satellite/	Satellites and space-based technologies and assets

Title	Source(s)	Technology relevance	cluster	of
	https://www.techtimes.com/articles/245597/20191007/northrop-to-launch-first-of-its-kind-satellite-refuelling-spacecraft-on-oct-9.htm			
Engineering metals' electronic surface	http://dx.doi.org/10.1002/adom.201870066 https://www.sciencedaily.com/releases/2018/10/181009175649.htm	Novel and advanced materials and manufacturing		
Improved carbon nanotubes	https://arstechnica.com/science/2018/05/forget-carbon-fiber-we-can-now-make-carbon-nanotube-fibers/#p3 https://www.ncbi.nlm.nih.gov/pubmed/29760522 http://news.tsinghua.edu.cn/publish/thunews/9670/2011/20110111130923452515411/20110111130923452515411_.html	Novel and advanced materials and manufacturing		
Material with no reflection	https://www.nature.com/articles/s41586-018-0367-9 https://phys.org/news/2018-08-artificial-material-negative-refraction.html	Novel and advanced materials and manufacturing		
Electricity generating materials	https://www.nature.com/articles/s41563-018-0268-1 https://www.eurekalert.org/pub_releases/2019-01/vt-med011819.php https://www.nanomotion.com/piezo-ceramic-motor-technology/piezoelectric-effect/	Novel and advanced materials and manufacturing		
Radiation resistant alloy	https://advances.sciencemag.org/content/5/3/eaav2002 https://www.eurekalert.org/pub_releases/2019-03/danl-nra030519.php	Novel and advanced materials and manufacturing		
Composite Metal Foam (CMF) armour	https://news.ncsu.edu/2019/06/metal-foam-stops-50-caliber/ https://www.sciencedirect.com/science/article/pii/S0263822319312607	Novel and advanced materials and manufacturing		
Ultra-incompressible hard metal	https://www.nature.com/articles/s41467-019-10995-3 https://phys.org/news/2019-07-extremely-hard-metallically-material-high-tech.html	Novel and advanced materials and manufacturing		
Mass production of graphene	https://phys.org/news/2018-04-team-cost-effective-technique-mass-production.html	Novel and advanced materials and manufacturing		
Mouldable graphene oxide dough	https://www.nature.com/articles/s41467-019-08389-6 https://news.northwestern.edu/stories/2019/01/go-dough-makes-graphene-easy-to-shape-and-mold/	Novel and advanced materials and manufacturing		

Title	Source(s)	Technology cluster of relevance
New graphene creation technique	https://www.nature.com/articles/s41586-020-1938-0 https://www.sciencemag.org/news/2020/01/electricity-turns-garbage-graphene https://www.sciencedaily.com/releases/2020/01/200127134751.htm https://newatlas.com/materials/high-value-flash-graphene-cheap-trash/ https://www.theengineer.co.uk/flash-graphene-rice-tour/ https://physicsworld.com/a/making-graphene-in-a-flash/ https://bigthink.com/technology-innovation/flash-graphene	Novel and advanced materials and manufacturing
Multi-purpose superior alloys	http://www.mynewsdesk.com/uk/chalmers/pressreleases/ground-breaking-discoveries-could-create-superior-alloys-with-many-applications-2546991?utm_source=rss&utm_medium=rss&utm_campaign=Subscription&utm_content=pressrelease https://www.scitecheuropa.eu/create-superior-alloys/87441/	Novel and advanced materials and manufacturing
Key-and-lock self-healing polymers	http://science.sciencemag.org/content/362/6411/220 https://www.sciencedaily.com/releases/2018/10/181011143135.htm https://newsstand.clemson.edu/mediarelations/clemson-university-breakthrough-in-self-healing-materials-detailed-in-journal-science/?utm_source=homepage	Novel and advanced materials and manufacturing
Fast discovery of new nanomaterials	https://www.pnas.org/content/116/1/40 https://phys.org/news/2018-12-megalibrary-approach-rapid-discovery-materials.html	Novel and advanced materials and manufacturing
Metallic fabrics	https://onlinelibrary.wiley.com/doi/full/10.1002/adfm.201804798 https://phys.org/news/2019-01-smart-fabrics-metal-deposition-technique.html	Novel and advanced materials and manufacturing
New materials with desired properties	https://www.nature.com/articles/s41586-018-0850-3 https://www.sheffield.ac.uk/materials/news/meta-crystals-1.824841	Novel and advanced materials and manufacturing
Brain computer interfaces for UAVs	https://www.defenseone.com/technology/2018/09/its-now-possible-telepathically-communicate-drone-swarm/151068/ https://futurism.com/jets-pilots-mind-control-darpa/ https://mysteriousuniverse.org/2018/09/darpa-achieves-telepathic-control-of-drone-swarms/	Human-machine interfaces

Title	Source(s)	Technology relevance	cluster	of
Improved prosthetic hands and wrists	https://ieeexplore.ieee.org/document/8360946/ https://techxplore.com/news/2018-05-tech-prosthetic-easier-patients.html	Human-machine interfaces		
Artificial skin that can morph	https://www.nanowerk.com/nanotechnology-news2/newsid=53654.php https://onlinelibrary.wiley.com/doi/full/10.1002/admt.201900260	Human-machine interfaces		
Gel-free and cheap EEG electrode	https://pubs.acs.org/doi/10.1021/acs.nanolett.9b02019 https://www.nanowerk.com/nanotechnology-news2/newsid=53620.php	Human-machine interfaces		
A new actuator improves haptic feedback	https://www.nanowerk.com/nanotechnology-news2/newsid=53685.php https://www.liebertpub.com/doi/10.1089/soro.2019.0013	Human-machine interfaces		
Big data neurotechnology	https://www.sciencedirect.com/science/article/pii/S1053811919309528?via%3DiHub#! https://www.sciencedirect.com/science/article/pii/S1053811919306366?via%3DiHub https://www.army.mil/article/232275/army_develops_big_data_approach_to_neuroscience https://sharpbrains.com/blog/2020/02/05/u-s-army-develops-novel-way-to-analyze-brain-imaging-data-and-shape-emerging-neurotechnology/	Human-machine interfaces		
Brain-linked artificial retinas	https://dx.doi.org/doi:10.1002/adfm.201800275 https://www.nanowerk.com/spotlight/spotid=49959.php	Human-machine interfaces		
Closed-network human body communications	https://www.nature.com/articles/s41598-018-38303-x https://newatlas.com/prototype-watch-body-hackers/58855/	Human-machine interfaces		
Brain to AI speech device	https://www.universityofcalifornia.edu/news/synthetic-speech-generated-brain-recordings https://www.nature.com/articles/d41586-019-01328-x https://www.nationalgeographic.com/science/2019/04/new-computer-brain-interface-translates-activity-into-speech/ https://www.nbcnews.com/mach/science/scientists-turn-brain-signals-speech-help-ai-ncna998551https://www.cnbc.com/2019/04/25/california-scientists-found-a-way-to-translate-thoughts-into-speech.html	Human-machine interfaces		

Title	Source(s)	Technology relevance	cluster	of
	https://www.nytimes.com/2019/04/24/health/artificial-speech-brain-injury.html https://www.newscientist.com/article/2200683-mind-reading-device-uses-ai-to-turn-brainwaves-into-audible-speech/ https://www.bbc.com/news/health-48037592 https://www.theguardian.com/science/2019/apr/24/scientists-create-decoder-to-turn-brain-activity-into-speech-parkinsons-als-throat-cancer https://www.sciencealert.com/a-new-kind-of-brain-decoder-turns-neural-activity-for-speaking-directly-into-speech https://www.technologyreview.com/s/613421/scientists-have-found-a-way-to-decode-brain-signals-into-speech/			
Sensor that creates experience of pain	https://www.liebertpub.com/doi/10.1089/soro.2018.0049 https://www.dgist.ac.kr/_prog/bbs/?mode=V&site_dvs_cd=en&menu_dvs_cd=060202&code=060104&no=4489ffbfa283ca4713ea7e7c50413d7f https://www.eurekalert.org/pub_releases/2019-08/dgi-pes082919.php	Human-machine interfaces		
Carbon fibre artificial muscles	http://dx.doi.org/10.1088/1361-665X/aab52b https://phys.org/news/2018-04-strong-carbon-fiber-artificial-muscles.html	Human-machine interfaces		
On-chip quantum emitters	https://www.nature.com/articles/s41565-018-0275-z https://www.eurekalert.org/pub_releases/2018-10/siot-rs102618.php	Quantum technologies		
Technique for detecting quanta	http://science.sciencemag.org/content/363/6431/1072 https://www.tudelft.nl/en/2019/tnw/listening-to-quantum-radio/ https://interestingengineering.com/new-quantum-radio-can-detect-universes-weakest-quantum-signals https://www.slashgear.com/new-quantum-circuit-lets-researchers-listen-to-weakest-radio-signals-11569390/ https://sciscomedia.co.uk/quantum-radio/ https://www.techexplorist.com/listening-quantum-radio/21458/	Quantum technologies		
Nano-sized photon emitting device	https://www.eurekalert.org/pub_releases/2019-04/uoc-nia042319.php https://www.osapublishing.org/optica/abstract.cfm?uri=optica-6-4-524 https://www.nanowerk.com/what_are_quantum_dots.php	Quantum technologies		

Title	Source(s)	Technology relevance	cluster	of
Quantum computing using light	http://optics.org/news/10/7/33 https://www.utwente.nl/en/news/!/2019/6/319975/boosting-light-based-computing https://www.laserfocusworld.com/optics/article/16566918/new-dutch-silicon-nitride-photonics-company-quix-aims-at-quantum-computing	Quantum technologies		
Quantum teleportation	https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.123.070505 https://phys.org/news/2019-08-complex-quantum-teleportation.html https://www.popularmechanics.com/technology/a28798458/quantum-teleportation/	Quantum technologies		
Material for quantum computing	https://science.sciencemag.org/content/365/6454/684 https://www.eurekalert.org/pub_releases/2019-08/nios-nsm080919.php	Quantum technologies		
Next generation quantum bits	https://science.sciencemag.org/content/366/6470/1225.editor-summary https://spectrum.ieee.org/tech-talk/computing/hardware/scalable-qubits-quantum-computer-news-silicon-wafer	Quantum technologies		
Particle helps prevent cyber intrusions	https://phys.org/news/2018-04-scientists-uncover-cyber-intrusions.html	Quantum technologies		
Large-scale 3D photonic chips	https://hardware.slashdot.org/story/18/05/14/2213253/chinese-scientists-develop-photonic-quantum-analog-computing-chip?utm_source=rss1.0mainlinkanon&utm_medium=feed http://advances.sciencemag.org/content/4/5/eaat3174.full	Quantum technologies		
Molecular 3D printing for electronics	https://www.theengineer.co.uk/3d-printing-quantum-leap/ https://onlinelibrary.wiley.com/doi/full/10.1002/adma.201800159?hootPostID=5d9a79dd84d53f4c99045ebb8ee53498 https://www.electronicweekly.com/news/research-news/nottingham-prints-molecular-3d-memory-2018-06/	Quantum technologies		
New way of measuring quantum states	https://www.theengineer.co.uk/3d-printing-quantum-leap/ https://onlinelibrary.wiley.com/doi/full/10.1002/adma.201800159?hootPostID=5d9a79dd84d53f4c99045ebb8ee53498 https://www.electronicweekly.com/news/research-news/nottingham-prints-molecular-3d-memory-2018-06/	Quantum technologies		

Title	Source(s)	Technology relevance	cluster	of
Quantum secret-sharing	https://link.springer.com/article/10.1140%2Fepjd%2Fe2018-90055-5 https://phys.org/news/2018-07-high-fidelity-quantum-secret-eavesdropping.html https://www.sciencedaily.com/releases/2018/07/180711105712.htm	Quantum technologies		
3D atomic-scale quantum device	https://www.nature.com/articles/s41565-018-0338-1 https://phys.org/news/2019-01-quantum-scientists-world-first-d-atomic-scale.html	Quantum technologies		
Security of quantum communication	https://link.springer.com/article/10.1140/epjd/e2018-90563-2 https://www.eurekalert.org/pub_releases/2019-01/s-qhm012819.php	Quantum technologies		
New way of hacking quantum cryptography	https://arxiv.org/abs/1902.10423 https://www.technologyreview.com/s/613079/theres-a-new-way-to-break-quantum-cryptography/	Quantum technologies		
Thinner magnetic information storage	http://science.sciencemag.org/content/early/2018/05/02/science.aar4851 https://www.nanowerk.com/nanotechnology-news/newsid=50128.php	Computing, data storage, and telecommunications		
Improved data storage possibilities	https://link.springer.com/article/10.1140%2Fepjb%2Fe2018-90006-0 https://www.nanowerk.com/nanotechnology-news/newsid=50472.php https://www.sciencedaily.com/releases/2018/06/180619122443.htm	Computing, data storage, and telecommunications		
Optical data storage	https://www.osapublishing.org/oe/abstract.cfm?uri=oe-26-9-12266 https://phys.org/news/2018-06-next-generation-storage.html	Computing, data storage, and telecommunications		
High-performance computing	http://conferences.computer.org/sc/2018/pdfs/SC2018-2xTiczKsrPOZuWFsgCODpF/7edQMM6Q1UsHbmonm04wYE/QSOkcYFTXgDd3JQPYX4Nd.pdf https://www.sciencedaily.com/releases/2018/11/181112191723.htm https://www.businesstelegraph.co.uk/new-framework-pushes-the-limits-of-high-performance-computing/	Computing, data storage, and telecommunications		

Title	Source(s)	Technology cluster of relevance
Photonic chips with smaller components	https://journals.aps.org/prx/abstract/10.1103/PhysRevX.9.021032 http://news.mit.edu/2019/ai-chip-light-computing-faster-0605 https://www.computing.co.uk/ctg/news/3076958/photonic-chip-mit-optical-neural-networks https://www.eenewseurope.com/news/photronics-based-ai-chips-break-all-energy-efficiency-benchmarks	Computing, data storage, and telecommunications
Nanoscale spintronic semiconductor	https://aip.scitation.org/doi/10.1063/1.5088227 ; https://www.eurekalert.org/pub_releases/2019-03/uot-nhr030519.php https://phys.org/news/2019-03-ferromagnetic-nanoparticle-ultrahigh-speed-spintronics.html	Computing, data storage, and telecommunications
Creation of magnetic quasi-particles	https://journals.aps.org/prb/abstract/10.1103/PhysRevB.98.104402 https://www.nature.com/articles/s41565-018-0255-3 https://onlinelibrary.wiley.com/doi/full/10.1002/adma.201805461 https://phys.org/news/2019-01-fast-tiny-magnetic-bits.html	Computing, data storage, and telecommunications
6G standard data transceiver	https://ieeexplore.ieee.org/document/8758316 https://techxplore.com/news/2019-07-electrical-team-5g-wireless-transceiver.html https://www.sciencedaily.com/releases/2019/07/190716073729.htm	Computing, data storage, and telecommunications
Hard drive enables more data storage	https://www-users.york.ac.uk/~rfl500/research/heat-assisted-magnetic-recording/ https://blog.seagate.com/craftsman-ship/hamr-next-leap-forward-now/ https://arstechnica.com/information-technology/2012/03/hamr-time-seagate-demos-terabyte-per-inch-hard-disk-technology/ https://arstechnica.com/gadgets/2020/02/hamr-dont-hurt-em-laser-assisted-hard-drives-are-coming-in-2020/	Computing, data storage, and telecommunications
Thinnest ever optical waveguide	https://www.nature.com/articles/s41565-019-0519-6 https://www.eurekalert.org/pub_releases/2019-08/uoc-tow080919.php	Computing, data storage, and telecommunications
Computer processing without heat waste	https://www.nature.com/articles/s41467-018-07597-w https://phys.org/news/2018-12-supercomputers.html	Computing, data storage, and telecommunications

Title	Source(s)	Technology cluster of relevance
Stable one atom information storage	https://www.nature.com/articles/s41467-018-06337-4 https://phys.org/news/2018-09-scientists-mechanism-storage-atom.html	Computing, data storage, and telecommunications
Rewritable memory	https://www.nature.com/articles/s41467-018-05171-y https://www.nanowerk.com/nanotechnology-news2/newsid=50736.php	Computing, data storage, and telecommunications
New type of algorithm	https://www.seas.harvard.edu/content/breakthrough-algorithm-exponentially-faster-than-any-previous-one https://techxplore.com/news/2018-06-breakthrough-algorithm-exponentially-faster-previous.html http://proceedings.mlr.press/v80/rosenfeld18a/rosenfeld18a.pdf	Computing, data storage, and telecommunications
Molecular 3D printing for electronics	https://www.theengineer.co.uk/3d-printing-quantum-leap/ https://onlinelibrary.wiley.com/doi/full/10.1002/adma.201800159?hottPostID=5d9a79dd84d53f4c99045ebb8ee53498 https://www.electronicweekly.com/news/research-news/nottingham-prints-molecular-3d-memory-2018-06/	Computing, data storage, and telecommunications
Chinese quantum radar	https://www.scmp.com/news/china/diplomacy-defence/article/2151086/chinas-latest-quantum-radar-wont-just-track-stealth https://www.popsci.com/china-quantum-radar-detects-stealth-planes-missiles?dom=rss-default&src=syn	Sensor and radar technologies
First proof-of-concept quantum radar	https://arxiv.org/abs/1908.03058 https://futurism.com/the-byte/working-quantum-radar-device https://www.technologyreview.com/s/614160/quantum-radar-has-been-demonstrated-for-the-first-time/	Sensor and radar technologies
Sensor capable of small-scale detection	http://iopscience.iop.org/article/10.1088/1367-2630/aabb8d/meta https://spectrum.ieee.org/nanocast/semiconductors/nanotechnology/a-quantum-drum-brings-quantum-mechanics-to-the-macroscopic	Sensor and radar technologies
Lidar and smart engineering	https://techcrunch.com/2018/04/12/luminar-puts-its-lidar-tech-into-production-through-acquisitions-and-smart-engineering/	Sensor and radar technologies

Title	Source(s)	Technology cluster of relevance
Data-gathering robot for rescue teams	https://www.oru.se/english/news/smokebot--a-robot-serving-rescue-units/ https://newatlas.com/smokebot-fire-rescue-robot/55103/ https://phys.org/news/2018-06-smokebot-robot.html	Sensor and radar technologies
Compliant capacitive acoustics sensor	https://ieeexplore.ieee.org/document/8367789/ https://www.nanowerk.com/nanotechnology-news/newsid=50524.php	Sensor and radar technologies
Diamond nanocrystal magnetic sensor	https://www.sciencedaily.com/releases/2018/09/180910142415.htm http://advances.sciencemag.org/content/4/9/eaat6574 http://news.berkeley.edu/2018/09/10/diamond-dust-enables-low-cost-high-efficiency-magnetic-field-detection/	Sensor and radar technologies
Mobile photonic sensor	https://www.nature.com/articles/s41377-018-0063-4 https://www.eurekalert.org/pub_releases/2018-09/wuis-eo091218.php https://www.eurekalert.org/multimedia/pub/180420.php	Sensor and radar technologies
Microsensors with increased sensitivity	http://advances.sciencemag.org/content/4/7/eaat4436 https://phys.org/news/2018-07-kirigami-inspired-technique-nanoscale.html	Sensor and radar technologies
Graphene-based biosensors	https://arxiv.org/abs/1808.05557 https://arxiv.org/ftp/arxiv/papers/1808/1808.05557.pdf	Sensor and radar technologies
More sensitive ultrasound sensors	https://www.nature.com/articles/s41467-018-08038-4 https://www.uq.edu.au/news/article/2019/01/ultra-ultrasound-revolutionise-technology https://www.itnews.com.au/news/uq-unveils-ultra-ultrasound-sensor-precise-enough-to-hear-a-cell-breathe-517896	Sensor and radar technologies
Real-time 3D sensor technology	https://www.fraunhofer.de/en/press/research-news/2019/march/sophisticated-3d-measurement-technology-permits-gesture-based-human-machine-interaction-in-real-time.html https://phys.org/news/2019-03-sophisticated-d-technology-gesture-based-human-machine.html	Sensor and radar technologies
Printable and wearable sensor system	https://onlinelibrary.wiley.com/doi/full/10.1002/adma.201804285 https://www.nanowerk.com/nanotechnology_articles/newsid=52647.php	Sensor and radar technologies

Title	Source(s)	Technology relevance	cluster	of
Improved laser-based sensor	https://www.osa.org/en-us/about_os/newsroom/news_releases/2019/sensor_detects_buried_os_laser_congress/ https://www.eurekalert.org/pub_releases/2019-09/tos-nvs091319.php	Sensor and radar technologies		
Bioacoustic identity recognition	https://ieeexplore.ieee.org/document/8859636 https://spectrum.ieee.org/the-human-os/telecom/security/the-bioacoustic-signatures-of-our-bodies-can-reveal-our-identities	Sensor and radar technologies		

Looking towards 2040, the global innovation and technology landscape is expected to evolve significantly, driving change in the character of warfare as well as in the capabilities, concepts and doctrines employed by actors on the battlefield. As such, there is a need to understand the technological changes and explore their potential influence and impact on the future battlefield so as to formulate policies and investment decisions that are as future-proof as possible.

Providing an assessment of the risks, challenges and opportunities relating to new and emerging technologies that are most expected to shape the future battlefield between now and 2040, this study outlines the implications stemming from consideration of individual technologies, while also offering a cross-cutting analysis of their interactions with broader political, social, economic, and environmental trends. In doing so, the study highlights a need for the EU institutions and Member States to pursue a broad range of capability development initiatives in a coherent and coordinated manner, ensure the development of an agile regulatory and organisational environment, and guide investments in technologies most relevant to the European context.

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.



ISBN 978-92-846-8399-4 | doi: 10.2861/620590 | QA-05-21-220-EN-N