FFI-RAPPORT

20/01050

Emerging technology trends for defence and security

Harald Andås

Emerging technology trends for defence and security

Harald Andås

Norwegian Defence Research Establishment (FFI) 7 April 2020

Keywords
Teknologisk utvikling
Langtidsplanlegging
Forsvar
Sikkerhet

FFI report
20/01050

Project number
1521

Electronic ISBN
978-82-464-3263-2

Approvers
Torgeir Mørkved, *Research Manager*
Hanne Bjørk, *Research Director*

The document is electronically approved and therefore has no handwritten signature.

Summary

This review is the first of a series of studies from a new research programme at the Norwegian Defence Research Establishment (FFI) tasked with identifying emerging technology trends and analysing their potential impact on Norwegian military operations. Keeping abreast of rapidly evolving technologies can help decision-makers to avoid strategic surprises and provide a better foundation for long-term defence planning. The project, 'Technological Trends and Consequences for Norwegian Military Operations (or TEKNO), will provide such advice by closely monitoring and analysing emerging military and civilian technology developments, seeking to identify disruptive technologies that are likely to influence future military operations, paying particular attention to the ways these emerging technologies interact and the operational context in which they are employed.

As a natural first step, this effort to assess technological trends is performed as a study of available unclassified literature, an approach deemed most advantageous given the primary goal of identifying a large set of overarching technological trends, and for which a substantial body of recently released literature and well-sourced studies already exist. Hence, the priorities and discourse of such work will closely follow and rely on the choices made by these primary sources.

The current report provides an overview of seventeen technology trends organised according to the period of anticipated main disruptive influence of the technology on military and security operations. Some comments are made on each list item in order to relate specific trends and technologies to defence and security, and a selection of these trends are explored further and commented separately. The report concludes with a discussion of the importance of civil-military cooperation and the challenges entailed with convergence.

The results discussed in this report will form the basis for further research and reports at later stages in this study series.

Sammendrag

Denne gjennomgangen er den første av en serie studier i et nytt forskningsprosjekt ved Forsvarets forskningsinstitutt (FFI) som har til oppgave å identifisere teknologitrender og analysere deres potensielle innvirkning på norske militære operasjoner. Det å holde seg oppdatert på teknologi i rask utvikling kan hjelpe beslutningstakere med å unngå strategiske overraskelser og gi et forbedret grunnlag for langsiktig forsvarsplanlegging. Prosjektet "Teknologiske trender og konsekvenser for militære operasjoner" (TEKNO) skal gi slike råd gjennom å studere og analysere militær og sivil teknologiutvikling og forsøke å identifisere banebrytende (disruptive) teknologier som med høy sannsynlighet vil påvirke framtidige militære operasjoner. Spesiell oppmerksomhet vil rettes mot de ulike måtene disse nye teknologiene samvirker på og hvordan de påvirker den operasjonelle konteksten.

Som et naturlig første skritt i arbeidet med å vurdere teknologiske trender har vi utført en studie av tilgjengelig ugradert litteratur. Denne tilnærmingen ble ansett som den mest fordelaktige, gitt at det primære målet har vært å identifisere overordnede teknologiske trender. Flere relativt nylig utgitte studier og annen relevant litteratur har blitt gjennomgått. Diskursen og prioriteringene i dette arbeidet vil derfor være preget av valgene som ble tatt i disse primære kildene.

Denne rapporten gir en oversikt over sytten identifiserte teknologitrender organisert etter tidspunktet for forventet disruptiv innflytelse på operasjoner i forsvars- og sikkerhetssektoren. Det gis noen kommentarer til hver av trendene som relaterer dem og de aktuelle teknologiene spesifikt til forsvar og sikkerhet, og et utvalg av disse trendene blir ytterligere kommentert separat. Rapporten avsluttes med en diskusjon om viktigheten av sivilt-militært samarbeid og utfordringene med konvergens.

Resultatene diskutert i denne rapporten vil danne grunnlaget for videre forskning og rapporter i prosjektet.

Contents

1 Introduction

The rate of technological change has intensified over the past several decades, driven in part by globalisation trends that have enabled the rapid dissemination of knowledge, substantial advances in digital technology that streamline design, modelling and production processes, and an ever-expanding commercial sector driving innovation forward [1]. Just as in previous centuries, many technologies developed for the civilian market also have clear military applications, ranging from artificial intelligence, autonomous systems, biotechnology, and quantum computing. Hence, in the context of warfare, technology will continue to play its essential part as new and emerging technological breakthroughs have the potential to change the conduct of warfare and the outcomes of battles.

This report is the first of a series of studies from a new research program at the Norwegian Defence Research Establishment (FFI) tasked with identifying emerging technology trends and analysing their potential impact on Norwegian military operations. Keeping abreast of rapidly evolving technologies can help decision-makers avoid strategic surprises and provide a better foundation for long-term defence planning. This report provides an overview of seventeen technology trends organised according to the period of anticipated main disruptive influence of the technology on military and security operations. Some comments are made on each list item in order to relate specific trends and technologies to defence and security. The results discussed in this report will form the basis for further research and reports at later stages in this study series.

One of these stages will involve investigations on how potential adversaries approach these trends and developments, and will look at both state and non-state actors in order to achieve a comprehensive understanding of future threats. The study series will also examine how our allies approach the technology trends, their technology development priorities, emerging operational concepts and other issues of relevance in order to better prepare for future joint operations. By doing so, the series will gain broader understanding of how technological development affects future military operations. The final stage aims at joining the results of the preceding effort and assesses consequences, including particular aspects of relevance for Norwegian military forces.

In addition to providing necessary definitions and clarifications, the current report briefly explains the chosen methodology and the source material used to identify the different technology trends, and then lists the seventeen identified trends. Some of these trends are explored further in Chapter 3. The report concludes with a discussion of the importance of civil-military cooperation and the challenges entailed with convergence.

1.1 Why trend studies?

Technology has always influenced the way conflicts are waged, and technological innovations have in turn altered strategic and political relationships away from the battlefield as well. Some

technological advances have had an obvious and immediate impact, such as the longbow, firearms, aircraft and nuclear weapons. The consequences of other inventions – ranging from microprocessors to the telegraph to something as simple and influential as the advent of paper to convey written orders to military commanders – have altered the strategic landscape in important, yet more subtle ways. In some cases, military tactics and doctrines have lagged behind the technological innovations, sometimes leading to tactical defeat due to a failure effectively to integrate new capabilities. Early adopters, on the other hand, can often gain an edge over slower, less agile adversaries. Although not necessarily the decisive factor in the outcome of a military conflict, technology nevertheless remains a crucial component of the modern security and defence landscape.

Similar to past centuries, technological innovation creates new opportunities as well as new threats. In some sense, defence innovation resembles a treadmill – the lack of persistent forward motion means that one is, in effect, falling behind rather than simply standing still. Moreover, it is demanding next to the impossible to identify and adapt relevant new technologies without a constant awareness of both civilian and military technological trends. This represents a considerable challenge, since the constituting technologies will be ranging widely in maturity from nascent to those on the cusp of becoming operational capabilities.

Within this context, it should be noted that the primary goal of forecasting is not to predict future trends accurately, but to provide actionable insights in the present. One futurist has argued that any useful idea about the future should appear ridiculous from today's point of view, and that the future considered most likely is probably the least likely to transpire. Accordingly, if the content of a technology foresight study seems reasonable then it likely has not looked far enough into the future. In other words, technology forecasts will be wrong – but they should aim to be wrong in useful ways.

Building on FFI's well-established role of providing long-term defence planning analysis for Norway, the project 'Technological Trends and Consequences for the Norwegian Military Operations' (or TEKNO) will provide advice on scientific and technical developments affecting defence planning requirements by closely monitoring and analysing emerging military and civilian technology trends. By attempting to anticipate medium and long-term developments, the TEKNO project seeks to identify disruptive technologies that are likely to influence future military operations, paying particular attention to the ways these emerging technologies interact and the operational context in which they are employed. The institutional knowledge repository at FFI on topics such as long-term planning, trends analysis and wargaming will be an important reference. This is particularly relevant given FFI's involvement in similar efforts within a NATO context, which remains a highly relevant model for forecasting.

1.2 Definitions and clarifications

This report understands technology as science or knowledge put into practical use to solve problems or to invent useful tools[1], particularly those having the potential to change the conduct of warfare and the outcomes of battles. Further, it is concerned with *technological trends*, understood as clusters of technology areas that all seem to point towards specific applications, developments, impacts and significant effects on the defence and security realm. In order to identify these trends, the terms *emerging*, *converging* and *disruptive* are applied[2].

Emerging technologies are technologies with low maturity or technology readiness level (TRL), currently in development. Thus, such technologies have yet to become widely in use within the defence and security realm. As a rule of thumb, the technologies discussed in the medium and long-term framework of this report are believed to be at an early stage with low levels of TRL.

Employing an emerging technology has the possibility of causing *converging* and/or disruptive effects on the battlefield. Technology convergence involves merging of existing technologies in order to create new and better possibilities and allows development and maturation. The resulting solutions will dramatically improve a given role in a component, a subsystem or within an entire system. The effects of converging technologies will rapidly boost the technological development cycle.

Disruptive technologies in the context of defence and security are technological developments that change the conduct of conflict and the rules of engagement. Such disruptive effects will have significance within a limited[3] time frame and force the planning process to adapt and change long-term goals for concepts, strategy and planning.

Armoured combat vehicles (‘tanks’) could serve as a case in point. The concept emerged in the early twentieth century, but saw little progress until the First World War when convergence in technologies (engine, gear, tracks, and armour) allowed a construction that had some impact on the battlefield. Developments in the interwar period produced considerable improvements on the platform level. However, only the convergence of platforms and effective command and control (C2) capacity offered by distributed radio frequency (RF) communications, combined with organisational and doctrinal adaptations, allowed the disruptive effect demonstrated by the German offensive in May 1940.

1.3 Methodology

To identify technological trends, several methodologies and approaches are available. This includes, but is not limited to scenario building, horizon scanning, in-depth analysis of ongoing research, as well as predictions that are more rudimentary based upon limited sources and expert

[1] Cf. discussion in reference [2].
[2] The following definitions are adapted from [3].
[3] Limited is a relative term; the full manifestation of the disruptive potential could take a generation to permeate all planning aspects.

opinions. A natural first step towards providing a structure that will allow a ‘usefully wrong’ analysis is often to gain a broad overview of the most interesting trends relevant for defence and security. Hence, the current effort to assess technological trends is performed as a study of available unclassified literature, an approach deemed most advantageous given the primary goal of identifying a large set of overarching technological trends, and for which a substantial body of recently released literature and well-sourced studies already exists.

In this report, we have chosen primarily to rely on work by the NATO Science & Technology Board (STO), the European Defence Agency (EDA), the Office of the Deputy Assistant Secretary of the Army (DASA R&T) and the consultant firm Gartner, partly selected because of its accessibility. For NATO STO this includes aspects of the unclassified work in Technology Panels, while for EDA it partly takes account of work in the Capability Technology Areas (CapTechs). Hence, the priorities and discourse closely follow and rely on the choices made by these primary sources.

Performing a meta-study of this kind has several advantages. It provides a good overview of the field, is economical and efficient since much source material already is published, and draws on the ‘wisdom of the crowd’ phenomenon (group predictions provide greater accuracy than single studies/perspectives). However, there are also drawbacks, since it is only as accurate as the sources upon which each sub-study relies. In addition, it is more difficult to interpret and to check the reliability of individual claims and predictions because the source material is several layers removed from the final product.

NATO STO has the task of actively keeping track of potentially disruptive emerging technology trends, in this context defined as science and technology developments that are likely to influence the future operating environment and shape warfighting capabilities. Periodic snapshots, in which similar science and technology trends are grouped together, are published as NATO STO Tech Trends Reports [4], which provide a current, but not exhaustive, synthesis of technology trends identified, by expert panels and groups of the NATO STO. Continuously updated Technology Watch Cards, highlighting science and technology progress of interest and presenting opportunities and challenges arising from the technology, form the basis of this process. The trends are presented in the order of when they seem most likely to deliver their most disruptive effect in military operations within timeframes corresponding to those used by NATO defence planners: short (6 years), medium (6-20 years), and long (> 20years) term.

Likewise, in an effort to recognise the most promising, relevant and powerful emerging technologies with significant effects on defence and society , EDA has identified several enabling technology areas [5-6] with potential application across the broadest range of possible future military tasks. These key technology trends are deemed vital to the European military capability development and requirements up until 2035 and beyond, i.e. chiefly in the medium term, as new technologies will have the potential to shape military strategies and tactics and thus drive the development of defence innovations. However, some major technologies were not included in detail in the unclassified summary [5], mainly related to manned platforms and weapon systems. Consequently, these fields are also excluded from the present study, which not in any way should be regarded as a comprehensive listing of relevant trends.

Unsurprisingly, there is a considerable overlap between the identified technology trends in the two approaches. Wherever possible, the presentation in this report attempts to merge the two approaches to portray a unified assessment. Otherwise, the relevant technology areas from the EDA studies are considered according to the overall approach of the NATO study.

Moreover, results from a recent synthesis of technology trend studies [2] for the US Army (DASA R&T) are added to the above findings. This report combines 52 open-source forecasts of science and technology development published by various actors, identifying common themes across multiple studies. These were analysed using natural language processing (NLP) techniques, yielding a set of ten predominant science and technology trends that emerge as likely to generate disruptive changes, influencing future operating environment and shaping warfighting capabilities in the long term (30 years).

This has been supplemented by business advisor and consultant Gartner's latest analysis [7] of strategic technology trends with broad impact on IT-industry and the potential to drive significant disruption for business innovation and digital transformation, typically within the short to near medium term perspective. The investigated technologies are expected to go through significant changes, reaching a level of maturity that crosses a critical tipping point within this period.

The approaches of these *primary sources* [2, 4-6, 7] are fused into the list of emerging technology trends relevant for the future of defence and security presented below[4]. In order to relate specific trends and technologies to defence and security, each trend is supplemented with a list containing key enabling technologies as well as prospective applications. An effort is made to group the presented technology areas as to reflect the period of anticipated main disruptive influence of the technology on military and security operations in line with the NATO study approach and philosophy.

This, of course, does not mean that the described technology trends will not have effects also in the other time frames. The use of additive manufacturing technology, for example, will likely have its primary disruptive impact by providing on-demand repair parts production already in the short term, but will allow development of new lightweight designs for military equipment in the longer term. Hence, for the listed applications and key enabling technologies, an effort is made to indicate explicitly whenever the timeline for the most disruptive effect for the relevant item is expected to diverge from that of the main trend.

In addition to these external sources, the report also looks to a recent study by the Norwegian Defence Research Establishment (FFI) [8], which identified some technology aspects with particular relevance to the development of Norwegian armed forces. Identified technology trends with particular relevance for these aspects are among those receiving further elucidation and discussion in Chapter 3 (with the exemption of autonomous systems, which are believed to

[4] The NATO planning timeframes are slightly different from the Norwegian approach, which operates with periods of 4, 12 and 20 years. In the trend list of Chapter 2, it is therefore attempted to modify considerations and conclusions as to adapt to this phasing, implying that some of the listed prospective applications for the mid and long term will be stretch goals in the Norwegian context.

be well covered in other analyses). This also applies to all trends with disruptive potential in the long term since they are deemed to have a significant impact on a broad spectrum of warfare capabilities. Moreover, several of the constituting technology aspects likely will influence defence and security operations also in earlier phases of their development.

1.4 Probability assessments and caveats

Predicting, describing or forecasting future developments may include some form of probability appraisals. Such assessments can act as guidance towards recognising and estimating likely developments. Some of the trends presented in this document depend on technologies currently at a very low TRL, yet their disruption potential is believed to be massive. Quantum computing could serve as an example of a technology of this kind. Dis-counting these trends thus involves high levels of risk, although the specific influence of the involved technologies is very hard to stipulate.

Attempting to gauge technological trends beyond the short-term future also involves additional aspects of uncertainty. Assessments both in terms of timing, i.e. when technologies reach a maturity level that could provide disruptive effects for defence and security, and of the possible emergence of technologies not identified in trend studies, i.e. the now notorious 'black swans' [9,10], are key. As indicated by the description of the primary sources above, the timing issue is mainly resolved by expert group assessment. The current review has no ambition to investigate the latter aspect, but this may be reconsidered in later stages of this study series.

Moreover, trend reports often use different definitions on what constitutes an emerging 'trend' (or even a technology), making it difficult to create a coherent picture and adhere to a strict classification. There are underpinning technologies like the aforementioned quantum computing, and there are broader conceptual areas like artificial intelligence (AI). A quantum computer, with immense computational power, could mimic intelligence by sorting through huge amounts of sensor data stored in a cloud and constitute the centre of autonomy in a vehicle. This could be regarded as multiple trends – quantum technology, AI, sensor fusion, big data analytics, cloud computing and autonomy - but could also be seen as aspects of one particular trend; autonomy.

The use of a coherent classification scheme, such as a technology taxonomy, would remedy this situation somewhat, especially when combined with clustering techniques to identify trends. However, the effort necessary for a consistent application across available sources would be prohibitive in the context of this brief survey. Fortunately, variations of such clustering (using both computers and human experts) have already been performed to some degree as part of the methodology of the primary sources (cf. Section 1.3 above) giving what appears to be reasonably consistent results when aiming at recognising overarching themes at a general level. In such a setting, trend categorisation by citing examples of constituent technologies should provide an adequate line of approach. With this in mind, each of the trends presented below has been issued with a listing of enabling technologies (although not within the framework of a well-defined taxonomy).

When looking into the future, it gradually becomes more difficult to separate enabling technologies from overarching concepts. In the short term, however, most of the underlying technology needed in order to make a concept work is well known, and one therefore simply looks at identifying missing pieces. These mechanisms are effectively demonstrated by the current review regarding the trends that are believed to support disruption in the long term. They mainly constitute broad themes, close to basic science and with low TRLs, such as quantum technologies, artificial intelligence or electromagnetic dominance. The constituting technology areas, such as machine learning, have a wide field of potential applications. Conversely, for short-term trends, the enabling technologies are quite mature and already in various stages of implementation, cf. additive manufacturing and unmanned aerial vehicles.

Of other caveats, it should be noted that some of the sources from the main studies now date a few years back, so a few enabling technology areas for short-term trends could need revision or supplementation. This may apply to the use of distributed ledgers (for example blockchain) in information security, for which alternative approaches are emerging.

Previous efforts to forecast future technological developments have met with varying degrees of success. The pitfalls of such forecasting – including cognitive biases such as overreacting to new information or emphasising technological innovation at the expense of organisational or doctrinal factors – are well known but still difficult to avoid completely even when researchers are cognisant of them[5]. Despite the uncertainties involved when attempting to predict future technologies, the trends presented below provide value as they give an overview of relevant technological research and development, as well as supplies a listing of potential applications. This supports the study purpose of offering a summary of technology trends, which in various degrees can create disruptive effects for defence and security in the short, medium and long term.

2 Technology Trends

2.1 Technology Trends for Disruption in Short Term

2.1.1 Additive Manufacturing[6]

Portable additive manufacturing and printing of components and supplies bears the promise to enhance logistical and operational agility of armed forces (such as self-sustainment when limited logistic support) and reduce maintenance of military platforms. A surge in production capacity of spare parts and equipment components in greater numbers with restructuring of

[5] Cf. the more thorough discussion in [10].
[6] In addition to the primary sources, this section draws on material from references [11-14].

supply chains is expected in the near term. Moreover, hybrid manufacturing by combining additive and subtractive manufacturing processes within the same machine could have great potential. Ultimately, military logistics will likely become more streamlined, as equipment and supplies will be printed directly at their point of use. However, it will probably not change the need to transport fuel, food, and water in large amounts to deployed troops. Thus, the overall effect on logistics operations may be a reduction in supply requirements by up to 20 percent.

It is also highly likely that terrorists and criminal organisations will print (from plans that are stolen, reverse-engineered, or traded illegally) weapons, sensors, and other equipment using raw materials that are difficult to track on the open market. Current and short-term applications mainly include printing of low-volume complex and/or obsolescent parts relevant for sustainment, such as field spare part production or repairs and replacement units for of high volume serial production (e.g. casts).

Prospective developments include	
Battlefield production	Printing repair parts on the battlefield or in space
	Printing large parts/structures directly in location thus circumventing transport vehicle size limitations (long-term)
Efficient production	Standardisation of production processes, certification of parts, virtual warehouses, legal (IP) aspects
	Efficient Obsolescence Management (OM) for defence
Advanced manufacturing	Embedding additively manufactured electronics directly in/on parts (mid-term).
	Use of additive manufacturing and advanced manufacturing techniques to enable; (mid-term) – New lightweight designs for aircraft, armour – Light weight ballistic protection – Packaging and cooling of electronic components – Manufacturing of energetic materials etc.
	On-demand manufacturing of customised prostheses, pharmaceuticals and other medical equipment (e.g. blood) to support medical operations (long-term) – Multi-Material Printing (combining materials, medical applications (prosthetics, organs) – 4D Printing (additive manufacturing of shape changing objects)

Enabling technologies

- 3D/4D printing processes
  - Material Extrusion based Additive Manufacturing (EAM)
    - Fused Filament Fabrication (FFF/FDM)
    - Liquid Deposition Modelling (LDM)
  - Powder Bed Fusion
    - Selective Laser Sintering / Melting (SLS, SLM)
    - Direct Metal Laser Sintering (DMLS)
    - Electron Beam Melting (EBM)
  - Directed Energy Deposition
    - Laser Metal Deposition (LMD)
    - Arc Metal Deposition
  - Sheet Lamination
    - Selective Deposition Lamination (SDL)
    - Ultrasonic Additive Manufacturing
  - Hybrid Manufacturing
- Materials development (properties)

2.1.2 Everywhere Computing[7]

Everywhere (or ubiquitous) computing is about connecting devices to each other and the ability for forces to benefit from distributed data structures and cloud computing services, incorporating devices connected to the 'Internet of Things' (IoT). It implies computing power made available 'anytime and everywhere´; letting users interact with (in principle) any type of computing device, ranging from relatively simple embedded devices (such as health monitoring sensors), input/output devices (speakers, screens), traditional computing devices (smartphones, laptops) to complex embedded platforms (autonomous vehicles). The paradigm could also support defence-related applications, such as integrated soldier systems or a distributed (coalition) modelling and simulation environment, by applying IoT technologies and concepts to the military domain — the Internet of Military Things (IoMT).

Novel mechanisms for distributed trust and authentication are a prerequisite for many aspects of this development. Distributed ledger (blockchain) technologies are currently popular candidates for such devices, but promising alternatives are under investigation.

[7] In addition to the primary sources, this section, as well as the corresponding elucidation in Section 3.1, draws on material from references [13, 15-20].

Prospective applications and developments include	
Sensor processing	Advanced processing at the sensor (lower bandwidth requirements, faster sensor to shooter times, more reliable data transfer).
	Distributed data structures (maintain ownership and control of own data, while sharing within a coalition).
Edge computing	Empowered Edge/IoT with permanently available, flexible cloud-based eco-system to provide on-demand accessible and convenient 'Modelling & Simulation as a Service' (customised AI-applications, IaaS/PaaS/SaaS, cf. Section 3.1).
	Enabling real-time decision support / live training (LVC) at all levels of command.

Enabling technologies

- Cloud/fog/edge computing
- 5G
- 6G (mid-term, 2030)
- Novel mechanisms for distributed trust and authentication
- Distributed Ledger (blockchain)
  (relevant for several aspects of combat information systems (CIS); information security, authentication, data integrity and resilient communications, cyber defence) (mid-term)
- Software Defined Networking/Cognitive Radio solutions
- Live, Virtual and Constructive Simulation (LVC)
- Network functions virtualisation — NFV

2.1.3 Predictive Analytics and Big Data[8]

Predictive Analytics is the process of generating understanding and providing insight for inference or forecasts of future states from data characterised by volume, velocity, variety and veracity (data quality). The term 'Big Data' generally refers to very large and complex data sets that are beyond the capacity of commonly used database management tools to adequately capture, manage, and process. Predictive Analytics uses machine learning techniques and a variety of (inductive) statistical methods and nonlinear system identification (regressions,

[8] In addition to the primary sources, this section, as well as the corresponding elucidation in Section 3.2, draws on material from references [13, 15, 20-22].

nonlinear relationships) on such large data sets to reveal relationships and dependencies, or to predict trends and exploit behaviour patterns.

These methods have gained importance of late, due to refinements in machine learning and considerably improved capacity for data processing and data management. This development is expected to continue. *Augmented analytics* using computerised machine learning algorithms will likely transform how analytics content is developed, consumed and shared (data preparation, data management, process management, process mining, auto-generated models). Modelling and simulation can contribute to and strengthen augmented analysis by adding models and simulations for prediction.

The proliferation of social media and the associated data generation has become, and likely will remain for some time, a testbed for analytics methods. Furthermore, the capacities (functions like GPS, video, audio) of associated mobile computing devices may be expected to transform traditional command, control communications computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities. In the defence and security context, this may include population surveillance, popular sentiment analysis, knowledge and information sharing, as well as strategic communications.

Prospective applications and developments include	
Analysis and awareness	Ascertaining situational awareness, patterns of life and anomaly detection
	Faster and more accurate intelligence, surveillance and reconnaissance capabilities with multiple intelligence source analysis
	Analysis of social behaviour on the internet (social media) merged with content extraction from multiple text documents
	Security risk assessment from a deep analysis of searches, personal contacts, locations and personal and social network behaviour
	A combination of social media data with traditional sensor data can provide a richer ISR picture (e.g. geo-tagging of pictures)
Security and defence	Real time cyber defence event detection and response
	Integrated System/Munition Health Management (smart management, optimization of defence capability life cycle costs)
	Social media provide significant opportunities to forces for flexible, redundant and scalable communications at strategic, operational and tactical levels
	Social media support doctrines that employ deception, diplomatic ‘warfare’ and influence operations

Enabling technologies

- Augmented analytics exploiting Big Data
  - Machine learning (with particular relevance to fields such as *Machine translation*, *Speech recognition / Natural language processing* and *Social network filtering*)
    - Deep learning
      - Artificial neural networks
      - Belief networks
    - Markov Decision Processes (reinforcement learning)
  - Data mining
- Context-Oriented Programming
- Modelling & Simulation

2.1.4 Unmanned Air Vehicles[9]

A variety of unmanned systems is already in use with military operations in all domains. They have become a regular feature of conflicts and their proliferation is expected to continue in all areas. Unmanned air vehicles (UAV), in particular remotely controlled drones, are in many ways mature technology with several products available in the market, and illustrative of the huge potential of unmanned systems. The use of remote-controlled unmanned systems is only a first step. Future unmanned systems will see higher degrees of autonomy, depending on the mission, adapting to the development of customised AI techniques (cf. also Section 2.2.1).

UAVs are already extensively employed for intelligence, surveillance, target acquisition and reconnaissance (ISTAR) missions, and contributions to this capability will likely remain the focus of UAV technology in the near term. An increasing level of automation and collaboration is predicted to result in better efficiency, making it uncomplicated for a single operator to control multiple UAVs. The use of unmanned vehicles as part of the solution to secure communications in military operations, i.e. as nodes in self-configuring, robust local (but not necessarily small) communications networks, is also anticipated.

The military value of UAVs that are armed, or otherwise can assist in strike missions against various targets, has been proven. Notwithstanding, vehicles optimised for tasks in non-permissive airspace, i.e. aerial combat against other aircraft or strike against defended targets, are still far from becoming operational. Extensive research and development is still required to increase the maturity of key technologies.

[9] In addition to the input from primary sources, this section draws on material from reference [13].

Prospective developments include	
Intelligence	Continued development of long-endurance, wide-area ISR capability
	Micro-UAVs, incl. micro / nano unmanned aerial systems (MUAS/NUAS), for information superiority in urban warfare as they are able to increase the situational awareness
Enhanced warfare	UAV role under expansion to logistics support (cargo transport) and Combat Search And Rescue (CSAR)
	Various UAV systems creating (flexible) deployable nodes for communication networks (cf. also Section 2.2.7)
	Full autonomy of unmanned systems for military use can be expected, in the near term, for simpler tasks only ([combat] logistics, long-range decoys, CSAR)

Enabling technologies

- Sense & Avoid Systems are crucial building blocks to promote the reliability of UAVs and to demonstrate their airworthiness (prerequisite to air traffic insertion of UAVs, ensuring safe operation in case of emergency)
- Lightweight hyperspectral sensors
- Complex aerodynamics related to micro-UAVs require powerful on-board computers, small and lightweight sensors and power sources, hence rely on advanced materials
- Guidance, Navigation and Control (GNC) (esp. GNSS-independent)
  - Machine Learning

2.2 Technology Trends for Disruption in Medium Term

2.2.1 Autonomous Systems with Manned-Unmanned Teaming[10]

Continued standardisation and enhancement of remotely operated or autonomous systems capabilities – with automation and/or autonomy as key elements – will continue into the medium term (integration of military remotely piloted aircraft systems (RPAS) in airspace, medical assistance to injured personnel in the field and/or provide casualty evacuation (CASEVAC) under fire). The use of such robotic and autonomous systems (RAS) in military operations will expand as they gain mobility, dexterity, and increasing degrees of (artificial) intelligence (cf. Section 3.5), allowing autonomous system control, automated information fusion and anomaly detection. This development will likely make them effective partners on

[10] In addition to the input from primary sources, this section draws on material from references [11, 13, 15-16].

future battlefields. Hence, the role of the soldier in combat will be re-evaluated as these systems proliferate and new operational concepts emerge. In this process, it will be essential to consider political, cultural and sociological regulatory issues, as well as potential ethical and legal implications and safety constraints. At the same time, adversaries will use robotic systems in ways that will be challenging ethically and tactically.

Prospective applications and developments include	
Intelligence	As for UAVs (Section 2.1.4); continued development of ISR capability
Enhanced warfare	Manned/unmanned teaming, adaptive cooperation between man and autonomous system – Enhancing operational capabilities like demining, reconnaissance, transportation, area control etc. through improved integration of UxVs – Includes controlling several unmanned vehicles at the same time
	Autonomous mine countermeasure (MCM) systems (USV/AUV)
	Unmanned logistics/delivery systems and engineering vehicles to reduce the force protection demands of manned supply convoys
	Multiple physical [robots] and virtual systems, such as virtual private assistants (VPA,) in air, land, cyber or maritime (also subsurface) domains to overwhelm adversary defences (swarming), including teaming with manned assets (long–term)

Enabling technologies

- Robotics and autonomous systems/entities — RAS.
  - Man-machine/machine-machine communication and integration (incl. trusted autonomy)
  - Verification/validation/evaluation (safety) procedures
  - Sensors and Control Systems (for robotics)
  - Multi-Robots Systems / Swarm robotics (MRS)
- Artificial Intelligence (AI) technologies for situational awareness and decision making (cf. Section 2.3.1)
  - Machine Learning exploiting Big Data
  - Knowledge representation/ engineering
  - Guidance, Navigation and Control (GNC) technologies (cross cutting domain) are key enablers aimed at improving decision-making algorithms for the coordination and interoperability of RAS / MRS
  - Virtual Personal Assistants (VPA)
- Underwater Communications Networks

2.2.2 Advanced / 'Smart' Materials[11]

Advanced materials have unique and outstanding properties compared to the more 'traditional' materials found directly in nature, such as metals, which have been in use for millennia. Advanced materials typically consist of a combination of materials, such a strong carbon fibres in a polymer, or small particles embedded in a continuous phase (which could be polymers, ceramics, metals). New production methods, such as additive manufacturing, open up for new materials or geometries/structures with novel properties or combinations of properties. Nanotechnology in part provides the basis for such new material development.

Such materials are useful in a wide range of domains and hostile environments where risks and damages can be reduced: clothing, building materials, vehicles, roads and bridges, and countless other objects. The defence sector will be able to benefit from advanced materials to produce systems with lower weight, body armour with improved protection, more cost-effective vehicles and shelters, batteries that are more robust and renewable energy systems.

Prospective applications and developments include	
New products	New materials for (new) design platforms as well as platform mid-life upgrades, lifetime extensions and reduced maintenance schedules that will allow
	– Flexible display coatings – Environmentally compliant coatings – Surfaces/coatings for anti-icing and anti–erosion – Camouflage – Structural Design / Health monitoring – Protective designs (including C-IED) – High strength body or platform armour – Energy harvesting and storage
Advanced properties	Materials (such as graphene) with extreme mechanical, thermal and electrical properties strength, elasticity, lightweight, temperature resistance, unique electrical/electromagnetic properties) will significantly contribute to all of the above, as well as high frequency electronics and sensors
	Advanced textiles for soldier systems and lighter land systems resistant to hostile environments (e.g. CBRN agents, humidity, salt water, radiation, icing, high temperatures). Integrated sensors will reduce the burden of extra wiring, and may be used for energy harvesting and personnel health monitoring
	Low-observable / (dynamic) stealth materials for covert reconnaissance and strike missions (long-term)
	Self-repairing, self-destructive and programmable smart materials to facilitate the assembly, security, resilience and structural health monitoring of infrastructure (long-term)

[11] In addition to the input from primary sources, this section draws on material from references [13, 16, 23-24].

Enabling technologies

- Nanomaterials
- Metamaterials
- Metallic foams
- Ceramic composites
- Graphene
  - Composites
  - Semiconductors
  - Coatings
- Plasmonics (enabling highly sensitive sensors)
- Smart textiles
  - E-textiles / Wearables
  - Fibretronics
- Triboelectric Nano-Generators (TENG)
- Architected materials (enabled by additive manufacturing)
- Design, manufacturing, joining and repair processes
  - Added layer manufacturing
  - On-site process verification
  - Bolt free repair/bonding

2.2.3 Synthetic Environments and Mixed Reality[12]

Mixed Reality denotes the fusion of real and virtual worlds through immersive technologies to produce new environments and visualisations where physical and digital objects coexist and interact in real time. Well-known concepts such as Augmented Reality (AR) and Virtual Reality (VR) are subsets of Mixed Reality. Currently, applications mostly focus on gaming and educational visualisations. However, it is likely that VR and AR will become standard technologies across a range of industries. Rapid progress has been made in technology that renders high fidelity, fully animated models of specific people. With these avatars, information warfare and the control of strategic narratives are likely to become significantly more complicated.

[12] In addition to the input from primary sources, this section draws on material from references [15-16, 25].

Prospective applications and developments include	
Visualisation, simulation and training	Head or body-worn virtual displays (e.g. heads up/helmet displays as currently used in aviation), will find uses in dismounted soldier systems
	Immersive visualisation of rapidly generated accurate 3D representations of physical environment (terrain + buildings + infrastructure) to assist planning and mission rehearsal (use of geo-referenced data and data gathered by unmanned micro-vehicles)
	Advances in computer technology and analytics will see current realistic mixed reality training environment set-ups used also in the battlefield
	Cost-effective and flexible training solutions with seamless interoperability based on live, virtual and constructive simulation environment (long-term) – Decision making support through exploring/analysing possible courses of action – Immersive simulations with improved human–machine interfaces to facilitate seamless manned–unmanned teaming
Other applications	Digital Avatars for Information Warfare
	Digital Twins for Logistics/Asset management

Enabling technologies

- Power efficiency of micro-displays.
- Optical fabrication techniques for free-form optical surfaces
- Human–machine interfaces
  - Visual displays, voice synthesis, wireless motion tracking
- Computer processing and networking (incl. 5G)
- Augmented analytics
- Modelling & simulation
  - Live, Virtual and Constructive Simulation (LVC)
  - High-fidelity synthetic environments

2.2.4 Sensors Are Everywhere[13]

Everywhere sensing refers to the detection and tracking of objects or phenomena from a distance by processing data acquired from a multitude of high tech, low tech, active and passive sensors. The continued advance of technology for underwater sensor networks will ensure that also the subsurface realm is included in this development. This sensor proliferation is occurring because reducing costs and sensor sizes are allowing their incorporation into a wide range of cheap every-day objects and, in combination with pervasive computational resources to fuse sensor data (cf. Section 2.1.2), will lead to an ability to sense at significantly greater ranges and with richer context than is currently possible. A new network paradigm, replacing current traditional IP network technology, may be needed to overcome the challenge of finding and accessing the vast amount of information generated by this expansion. In the context of health monitoring, it will have an effect on interoperability, safety and life cycle cost related issues, like the sharing of munition stockpiles.

Prospective applications and developments include	
Situational awareness	Sustaining a comprehensive situational picture through data fusion (of social data, environmental sensor data and radar data through a network of sensors embedded in the environment (IoT)
	Enhanced effectiveness of conventional high-resolution camera (visual) surveillance with ubiquitous computing and augmented analytics (cf. sections 2.1.2 and 2.1.3)
	Integration of sensors and effectors with the individual soldier to generate radical improvement in situational and environmental awareness, ISTAR and communication capabilities (long-term)
Monitoring and detection	Monitoring and maintaining resilience of headquarters through damage and intrusion monitoring using acoustic/seismic sensor systems and facial and physiological recognition sensors
	Systems/soldier health monitoring and life cycle management with embedded sensors in munitions, textiles and humans
	Smart dust sensor devices (millimetre-sized), for vibration, temperature or chemicals detection and with integrated communication capacity
Target acquisition	Classification and identification of small targets at long ranges with active optronics and hyperspectral sensors
	Advanced computational techniques for sensor data fusion enabling passive over the horizon (OTH) radar will lead to significantly greater sensing ranges against stealthy targets (long-term)

[13] In addition to the input from primary sources, this section draws on material from references [12-13, 16].

Enabling technologies

- Defence Internet of Things/Internet of Military Things / NEC 2.0
- Information Centric Networking (ICN)
- Augmented analytics
- Microelectronics / Microfabrication (incl. packaging)
- Micro-Electro-Mechanical Systems (MEMS)
- High-Resolution Hyperspectral Imaging/Camera (wideband)
- Active Electronic Scanned Arrays (AESA)
- (Active) optoelectronics
- Passive / Passive OTH radar
- Distributed underwater sensor networks
- Molecular/nano-scale sensors for ('smart') textiles and materials

2.2.5 Field-ready Rapid Gene Sequencing Technology[14]

Highly portable and field-ready rapid gene sequencing technology, with widely deployable and low use-cost sequencing instruments, is needed as part of a real-time response to perceived bio-threats. Real-time data of an outbreak could reveal key indicators of an emerging epidemic including the intentional spread of pathogens.

Current biological field detection methods rely on customised reagents targeting only a limited set of agents. Next generation sequencing (NGS) promises to target any agent ('wide-spectrum' method), but will require advanced supporting expertise such as bioinformatics. This bioinformatics analysis could be performed by other laboratories than those doing the genetic field sequencing. The use of NGS for biological threat preparedness in the defence context can be wider than just biodefence (general water and food quality control, sanitary medical purposes, forensics etc.).

[14] In addition to the input from primary sources, this section draws on material from reference [11].

Prospective applications and developments include	
Sequencing methods	Robust sample preparation and sequencing methods/protocols for complex field samples
Information management	Secure real-time exchange capabilities and platforms for sharing of data and information from the field
	Shared database with reference data as a necessary common resource for typing and identification of B-agents
	End user-friendly interface for field sequencing

Enabling technologies

- Next generation sequencing (NGS) / High-Throughput DNA Sequencing (HTS)

2.2.6 Synthetic Biology[15]

Humanity has manipulated the genetic code of plants and animals through selective breeding and hybridisation for millennia. Truly synthetic biology, where information on life itself can be manipulated much like computer code, will give rise to engineered living organisms (bio-hybrid systems) that can detect toxins, create biofuels from industrial waste, and deliver medicine through symbiosis with human hosts. At the same time, synthetic biology represents profound risks, including engineered biological weapons and invasive synthetic organisms that could destroy natural ecosystems. Systems and data that were once localised and contained to university or government laboratories, and therefore only accessible to those directly involved in related research, may be rendered vulnerable as digitisation and automation processes promote expansion of biotechnology expertise and use beyond traditional practitioners.

Likewise, the rise of 'biohacking' also increases the chances of such proliferation of expertise.

The development of gene editing techniques such as CRISPR, has enabled advances in genetic engineering that challenge the border between therapy and, most likely in the longer term, more troubling visions of genetically-engineered 'super-soldiers'. Currently, there is no global framework, neither legal nor ethical, making regulation of the research area challenging.

[15] In addition to the input from primary sources, this section draws on material from references [12-13, 16].

Prospective applications and developments include	
Synthetic microbes for production	Production of consumables; – organic fuels, plastics, lubricants – drugs, pharmaceuticals – energetic materials
	Production of bio-weapons (toxins, disease agents) and countermeasures
	Production of new (illicit) designer psychoactive substances
	Production of bio-sensors, -detectors, -computers (long-term)
Other applications	Rapid and efficient biometric and genetic analysis (of DNA or other genetic material) to improve border security.
	Genetically engineered microbes that detect and treat disease automatically (long term)
	Integrated genetically engineered microbes enabling photosynthesis-generated powering of electronics (long-term)

Enabling technologies

- DNA Synthesis and Sequencing
  - Gene sequence editing methods (e.g. CRISPR)
  - Gene drives / gene remediation tools
- Standardized DNA sequences ('BioBricks") for bioengineering
- Epigenetic Change Technologies
- Modelling and Simulation
  - Biochemical reactions and bio-systems interactions
  - Synthetic biology programming languages
  - DNA engineering
- Manipulation (laboratory) tools and techniques

2.2.7 Satellites and Pseudo-satellites[16]

Recent progress in low-cost commercial space flight, miniaturisation, materials, and space propulsion suggest that space will be an important focus of technological innovation as demonstrated by the development of new small (micro- and nano-) satellite technology. With

[16] In addition to the input from primary sources, this section, as well as the corresponding elucidation in Section 3.3, draws on material from references [12, 26-28].

the number of space-faring nations increasing, dependence on space-based tele-communications, global positioning, weather forecasting, and defence functions (mainly intelligence and C2) will likely make space a new domain for international competition, and potential conflict.

With the potential cost reduction for space assets connected to this development, even small states, private companies or even individuals have, or may soon obtain, access to data with quality and resolution that was previously reserved for major powers. Thus, space may rapidly become a congested and contested environment (‘battlefield’).

Pseudo-satellites or atmospheric satellites are a common designation of aircraft that operate in the atmosphere at high altitudes (around 20 km) for extended periods. Such systems have the potential to offer some services conventionally provided by a traditional satellite orbiting in space at considerably reduced costs, specifically related to launch and any required orbit alterations, and with a maintenance option.

Prospective developments include	
Resilient satellite networks	Sustaining a resilient network of military, civilian and commercial satellites or other communications nodes (incl. ‘pseudo-satellites’ and small satellites) for ISTAR purposes (responsive space capability)
	New launch technologies to ensure access to space
	Reprogrammable mission parameters
‘New space’ satellite constellations	Small satellite constellations / mega-constellations
	Highly effective rocket propulsion system for frequent small satellite orbit alterations
	High Altitude Long Endurance (HALE) UAVs and other systems creating deployable nodes for communication networks, in face of denied access to space
	Use of mission-specific clusters of small satellites (long-term)

Enabling technologies

- Cloud/fog/edge computing
- Microelectronics / Microfabrication (incl. packaging)
- Small satellite systems with dedicated functionality
  (e.g. Automatic Identification System (AIS), Communications link)
- (Re-)usable Launch Vehicles
  (launch components, cf. SpaceX, Rocket Lab, Virgin Orbit, Nammo)
- Small, effective rocket engines / thrusters
- Software Defined Satellites, cf. also Section 2.3.3
- Free Space Optical (FSO) communication
- Autonomous Space Vehicles (robotics, machine learning)
- Physical hardening, mobility and cybersecurity for space-based assets
  - Resilient Space Systems (material science, robotics (for repairs))
- HALE UAV, Airships/Balloons ('Pseudo-satellites")

2.2.8 Energy Generation and Storage[17]

Renewable energy sources such as solar and wind are rapidly approaching cost-parity with fossil fuels. The potential for domestic energy production and enhanced security of energy supply connected to this development will ultimately transform the world's strategic energy environment. With the gradual adoption of these energy sources, new frictions will emerge over access to rare materials used in batteries, solar cells, and other prerequisites for this energy revolution.

Digitalisation processes and 'smart grid' technologies will profoundly transform the operation of electricity networks. IoT sensors and advanced data analytics (cf. Section 2.1.3) will enable necessary sophisticated control and asset management with increased automation of network operation to adapt to the grater complexity due to diversified and fluctuating (renewable) sources. Integration challenges aside, a grid incorporating such sources is inherently more distributed and secure. Deployed forces will have to adapt to this development when incorporating their own power generation and storage capacities with available host networks. The logistics burden could be substantially relieved by improved battery design and efficiency, reducing or eliminating diesel generator fuel needs.

Stand-alone energy generation solutions ('islands') with possible relevance for military operations, including new nuclear reactor designs, have made progress in later years, promising to make this power source safer, cheaper and more readily available. Among them is the small

[17] In addition to the input from primary sources, this section draws on material from references [29-32].

modular reactor, or SMR, a slimmed-down version of conventional fission systems that typically produces in the tens of megawatts of power. Suitable fusion-based reactors still seem out of practical reach. Yet, unconventional approaches currently deemed unviable, such as the potential exploitation of low energy nuclear reactions, could become truly upsetting.

Prospective applications and developments include	
Generation and storage	Improved (renewable) energy generation and storage (electrical, electrochemical, mechanical and thermal), integrated with automated surveillance systems, to maximise engagement time of deployed forces and decrease their logistics footprint in-theatre
	Small and mobile nuclear (fission) power plants for ground operations (bases)
Increased efficiency	AI-assisted systems for efficient engine and power grid distribution
	Novel and improved efficiency propulsion to increase endurance and reduce fuel costs and deployment times (such as hypersonics)

Enabling technologies

- Energy Generation:
  - Solar cell efficiency (multi-layer devices, synthetic photosynthesis)
  - Other harvesting: wind, geothermal heat, tidal
  - very Small Modular Reactor — vSMR
  - Low Energy Nuclear Reactions — LENR (long-term)
- Energy Storage:
  - Batteries (solid-state cells, structural batteries).
  - Supercapacitors — SC
  - Solar fuels
    - catalytic membranes
    - biofuels (synthetic or natural organisms)
- Energy Distribution Grids
  - Smart (AI-assisted) power grids
  - Microgrids
  - DC/AC power converters

2.2.9 Hypersonic Vehicles[18]

The term ‘hypersonic vehicle’ is a common designation for aeroplanes, missiles or spacecraft which can move within the atmosphere at speeds beyond Mach 5, allowing a distance of 1,000 km to be covered in less than 10 minutes, and with prospective global reach with ranges in the order of 10 000 km.

Hypersonic technologies have the potential strongly to affect the conduct of future military operations. Various hypersonic flight vehicle concepts, such as the hypersonic glide vehicle or cruise missile, enable new or more advanced military capabilities. However, conventional ballistic (non-air breathing) technologies (as a low-risk measure) likely will be preferred for deployment in the short term. The high speeds of hypersonic vehicles allow for swift regional or global strikes against time critical targets from standoff distances, keeping the launching platform out of highly contested areas protected by modern Anti-Access / Areal Denial (A2/AD) systems. The speed of hypersonic penetrating systems makes kinetic intercept by any opposition extremely difficult.

Prospective applications and developments include	
Long-range strike	Hypersonic missiles will allow for rapid strike against time critical targets (‘time to target’ < 1 hour) from standoff distances with very low probability of intercept
	Conventional ballistic (non-air breathing) hypersonic missile technology development as risk mitigation for early deployment (short term)
Other missions	Hypersonic flight option for re-usable space transport vehicles
	Long range ISR by a hypersonic unmanned air vehicle a further possibility (more flexible than reconnaissance satellites and with a potential option for weapon delivery) (long-term)
	Rapid reaction interceptor against time sensitive aerial targets (long-term)

[18] In addition to the input from primary sources, this section, as well as the corresponding elucidation in Section 3.4, draws on material from references [11, 33-36].

Enabling technologies

- Supersonic Combustion Ramjet (‘scramjet’)
- Many scientific and technological aspects are unique to hypersonic flight and there are challenges in materials, design, heat management and guidance systems
- Novel and improved efficiency propulsion (to increase endurance/performance and reduce fuel costs)
  - Hydrocarbon vs. hydrogen fuel
  - Rotating Detonation Engine (RDE)

2.3 Technology Trends for Disruption in Long Term

2.3.1 Artificial Intelligence[19]

Artificial Intelligence (AI) refers to the ability of machines to match human problem solving, or at least mimic cognitive functions associated with the human mind, in terms of learning, reasoning, planning and acting in a complex cyber-physical environment, thus allowing autonomous robot or vehicle control, automated information fusion and anomaly detection and intelligent tutoring. Thus, the term AI in this setting is primarily concerned with the ability of a machine to perform an ‘intelligent action’.

An overall outcome of the ascent of AI and related technologies with relevance for military doctrines and operational concepts, such as Machine Learning, could be a ‘splitting up´ of the established OODA-loop (cf. Section 3.5). The prominence of speed and automation provided by machine intelligence would be pivotal for tasks requiring more immediate responses, like cyber threats or various counter-measures, associated with one part, and there might not be enough time for human review of the solutions provided by the system. Human decision makers then could primarily handle the other, in general slower, phase, focusing on higher-level analysis.

Predictive uses of AI systems could become critical, since such applications may change how planners and decision makers understand the potential outcomes of specific courses of action. Automated intelligence assessments will thus spur a drive towards (semi-)automated decisions.

[19] In addition to the input from primary sources, this section, as well as the corresponding elucidation in Section 3.5, draws on material from references [11, 13, 15-16, 37-39].

Prospective applications and developments include	
Decision-making support	Support tools to strengthen command and control at all levels, including – Predictive algorithms to anticipate threats/trends through analysis of big data (operational analysis, training/doctrine development, support to operations) – Computer generated forces (with realistic behaviour models) – Intelligence gathering and processing to establish a Common Operational Picture and provide situational awareness
	Support to activities such as strategic communication (STRATCOM), logistics planning, airspace management and analysis of lessons learned
Cyber defence	Intent Based Network Security (immune/self-adapting computer systems, malware reverse engineering) (near-term)
	Resilient autonomous networks and information systems configured, maintained, and protected by autonomous agents
Autonomous robotics	Advanced robotic capabilities for navigation within dull dangerous, dirty or heavy, hot, and hazardous situations, providing fully autonomous EOD in urban area
	Machine Learning (ML) enabled 'swarm' intelligence supporting (multi-)agent / robotic systems, making them truly effective partners on the battlefield
Electronic warfare	Advanced speech processing and synthesis technology allows realistic simulation of friendly and enemy personnel over communications links and broadcast media
	Adaptive techniques will outmode current intelligence cycles in areas like electronic warfare
'Human' perception	Neuromorphic computing will deliver deep learning with energy-efficiency, volume efficiency, speed-efficiency, and scalability affecting advanced large-scale data analysis and computer vision. Performance may rival human perception at very low power, enabling embedded sensor processing for 'visual' scene recognition, target discrimination etc.

Enabling technologies

- Predictive analytics exploiting Big Data
  - Machine Learning (with particular relevance to fields such as *Machine vision, Speech recognition / Natural language processing* and *Bioinformatics*)
    - Deep learning
      - Artificial neural networks
      - GAN — Generative Adversarial Networks
    - Markov Decision Processes (reinforcement learning)
  - Data mining / Knowledge Discovery
- (Multi-)agent systems
- Knowledge representation/ engineering
  - Ontologies
  - Belief networks /Fuzzy logic
- Robotics and autonomous systems/entities — RAS
- Neuromorphic computing in
  - Machine vision systems
  - Machine auditory processing systems
  - Autonomous robotics

2.3.2 Quantum Technologies and Quantum Computing[20]

Quantum Technology is an emerging field of physics and engineering turning the, admittedly sometimes strange, properties of light and matter revealed by quantum theory into practical applications -- such as the now much touted quantum computing. Quantum theory has fundamentally changed our understanding of the universe, showing that physical systems can exist in complex state configurations (superposition) and thus be deeply connected without any direct interactions (entanglement).

In later years, there has been a growing appreciation of the potential to use previously unexploited quantum effects in the development of customised systems and materials, with new devices that will actively manipulate and control quantum states of matter by taking advantage of the superposition and entanglement properties. The new generation of quantum technologies can be sorted into three broad classes: quantum communications, quantum sensing and metrology, and quantum computing. In all the classes, quantum technology will enable significant capability enhancements already by the mid-term, while grow to be truly revolutionary in the long term.

[20] In addition to the input from primary sources, this section, as well as the corresponding elucidation in Section 3.6, draws on material from references [12, 16, 40-44].

Quantum Communications

Quantum secure communications attempt to guarantee secure data transmission across information networks, such as the Internet, where the anticipated arrival of quantum computers has brought about the replacement of conventional asymmetric encryption methods (including key exchange) with quantum resistant algorithms. In an alternative approach, inherent properties of quantum systems are used to create optical quantum key distribution (QKD), where any attempt to intercept the key will result in the key's destruction.

Quantum Sensing and Metrology

Superposition states are inherently very sensitive to the environment. As a result, quantum sensing has the potential to provide unprecedented precision, sensitivity and accuracy of measurements of quantities such as acceleration and rotation, or electromagnetic and gravitational fields. Its applications include navigation in GPS-deprived environments, covert sensing or meticulous topographical mappings (of for example the seabed).

Quantum Computing

Quantum computing uses properties of subatomic particles like superposition and entanglement to represent and manipulate data. Based on 'quantum bits' or *qubits*, a quantum computer acts as a massive parallel device with an exponentially large number of computations taking place simultaneously. Quantum computing is expected to revolutionise multiple other technical domains, such as modelling & simulation, materials science (structure and properties), pharmaceutical research (drug discovery and design) and cryptography and communications security, and will have significant uses in computing fields such as big data analytics, optimisation and machine learning.

Prospective applications and developments include	
Quantum secure communications	Conventional asymmetric encryption methods will become vulnerable and gradually replaced by quantum secure communications systems exploiting – Quantum resilient algorithms (mid-term) – Photonics-based quantum random numbers generators (mid-term) – Secure key distribution systems with anti-tampering properties (fibre optic or line of sight connection; or via satellites)
INS for GPS-deprived environments	Small (cold-atom) precision clocks (mid-term)
	Chip-scale quantum inertial navigation systems (INS)
Quantum solid state / interferometric sensors	Through-the-wall / underground (tunnel) detection (mid-term)
	Improved RF spectrum analysers for electronic warfare (mid-term)
	Non-destructive testing/inspection of metals
	Gravimetric and magnetometric survey maps supporting geo-referencing
	Magnetometry enabling (short-range) submarine detection
Quantum imaging devices	Low-Probability of Detection (LPD) ultra-high-resolution (3D) imagery
	Low probability of detection range-finding (mid-term)
	Jamming resilient quantum radar for detecting, identifying and resolving stealth targets
QCaaS	Quantum Computing as a Service, cf. current cloud-based services (‘XaaS’)
Quantum simulators (dedicated architecture)	Materials science (structure, properties).
	Pharmaceutical research (drug discovery and design)

Enabling technologies

- Quantum secure/resilient communications
  - Quantum key distribution (QKD)
  - Quantum resistant algorithms
  - Quantum Random Number Generators – QRNG
  - Entanglement repeaters (processor, optronics interface)
- Solid-state quantum sensors
  - Gravimeters
  - EM Spectrum Analyser
- Quantum interferometer devices (cold atomic / molecular)
  - Gravimeters
  - Magnetometers
- Quantum imaging devices
  - Single photon counting (SPC) detector array
  - Entangled microwave photon sources
  - Quantum radar
- Quantum Computing
  - Computer design / architecture
  - Qubits / qudits (dubits)
- Quantum Computer Programming
  - Quantum (error correction) algorithms
  - Hybrid quantum-classical algorithms
  - Fault-tolerant protocols
  - Programming languages

2.3.3 Electromagnetic Dominance[21]

Electromagnetic Dominance refers to the ability to use more of the electromagnetic (EM) spectrum, to share the spectrum more efficiently, to protect own forces' use of the spectrum and to deny enemy use. Thematically, it ranges from materials technology for signature control through wireless communications and electronic warfare to directed energy weapons. The quest for EM dominance is becoming more contested and competitive due to commercial investment in advanced radiofrequency technology. Related advances in passive radar will likely make air superiority difficult to achieve.

[21] In addition to the input from primary sources, this section, as well as the corresponding elucidation in Section 3.7, draws on material from references [11-12, 16, 45-50].

Prospective applications and developments include	
Wireless communication and sensing	High performance, low power, robust wireless communication and sensing:
	Radars, EW and communication systems, with the exception of antennas and amplifiers, completely implemented with microwave photonics
	Completely software-defined configuration of multiband multifunctional radar and EW systems
	Multifunctional RF systems with larger operational frequency bandwidths for multiple-platforms compatible operations
	Increased network capacity and network adaptability (also space)
Electronic warfare (EW) systems	Electronic warfare (EW) systems and electromagnetic spectrum management to achieve tactical and operational effects against both civilian and high-grade military electronic systems:
	Algorithms and techniques for radar detection, tracking and identification of challenging targets (e.g. digital beam forming, radar interferometry)
	Passive radar (PCL) increases detection capability against stealth targets
Electronic protective measures and countermeasures	Electronic protective measures and countermeasures (EPM / ECM) to improve resilience of friendly systems to adversary ECM and sensor systems, along with reversionary modes and redundant systems:
	Fleets of longer-range multi-spectral (EM) decoys to emulate specific asset signatures and manoeuvres as integrated part of defensive aids suites (DAS) (mid-term)
	Passive radar (PCL) reduces the vulnerability against electronic countermeasures
	Jamming resilient quantum radar for detecting, identifying and resolving stealth targets
Directed Energy Weapons	Directed energy to counter adversary swarms of UAVs or mass firings (saturation), providing improved magazine depth and flexibility of effects:
	Close-in Laser Weapon System for point defence (mid-term)
	Countermeasures against EO/IR sensors (such as night vision goggles, cameras) with laser broadband source (Femto-second / QCL / ICL)
	Disruption of electrical systems at a distance (guided microwaves)

High-speed secure communications	Enabled transfer of increasingly huge datasets and automated analysis in real time with e.g. Free-Space Optical (FSO) laser communication
Smart coating of materials and metamaterials	Increases survivability of platforms through (radar) signature control and reduction (mid-term).

Enabling technologies

- Electrically powered lasers (high yield)
  - Solid-state
  - Multiple fibre
  - Diode-pumped alkali (DPAL)
  - Free-electron (FEL)
- Femto-second laser
- Quantum cascade laser (QCL)
- Interband cascade laser (ICL)
- High Power Microwave sources
- (Integrated) Microwave Photonics
- Microwave Monolithic Integrated Circuits (MMIC)
- Multiple-Input Multiple-Output (MIMO) Radar / Radio
- Software Defined Radio / Radar
- Quantum radar
- Passive radar (PCL)
- (multi-)Robotics and autonomous systems/entities — RAS/MRS
- Advanced Materials, cf. also Section 2.2.2

2.3.4 Soldier Enhancement Systems[22]

Soldier Enhancement refers to the augmentation of individual human abilities using artificial means such as robotic exoskeletons, smart textiles, drugs, and seamless man-machine interfaces. Advances in material, computer and human sciences (bioengineering, nano-technology and genomics), as well as convergence between these fields, are set to significantly enhance human capabilities and optimise overall soldier performance and effectiveness. Consequently, effective forces could consist of smaller groups, with possible implications for affordability. Regenerative medicine and associated breakthroughs could transform battlefield medicine, improving battlefield survivability and allowing troops to recover from injuries faster. Networked augmentations, such as exoskeletons and prosthetics, will likely be an appealing target for

[22] In addition to the input from primary sources, this section, as well as the corresponding elucidation in Section 3.8, draws on material from references [16, 23, 51-54].

hackers. It should be expected that adversaries might be similarly enhanced. The moral and ethical aspects of these issues must be addressed.

Prospective applications and developments include	
Personal soldier (protective) systems	Smart textiles providing adaptive camouflage, lightweight armour, CBRN protection, energy harvesting and storing, personnel health monitoring etc.
	Smart textiles that actively protect against water, oil, fire, IR-radiation, bacteria, insects and infections
	Embedded diagnostic systems (equipment health monitoring) that enable after-storage or possibly real- time fault and functionality control of personal protection equipment and collective protection units
	Human state/health monitoring with biomedical wearables in real-time to near real-time will allow individual and team performance (cognitive and physical) to be optimised (mid-term)
	Optimised nutrition and nutritional (time released) additives will increase physical capacity, improve effectiveness and enhance context awareness in decision making
Exoskeletons	(Relatively) widespread availability of powered exoskeletons (and prosthetics) to increase the physical strength, protection and mobility of deployed combat and logistics personnel, cf. – ONYX – TALOS – Tactical Assault Light Operator Suit
Pharmaceuticals and genetic engineering	Improving the resilience of individual soldiers to CBRN threats and other injuries in the field
	Genetic alterations to enhance human cognition
Integrated sensors and effectors	Radical improvement in situational and environmental awareness of the individual soldier, cf. also Section 2.2.4, (hyper-enabled operators)
	Haptic suits (wearable devices providing haptic feedback to the soldier)
Personalised and regenerative medicine	AI-based diagnostic tools
	Pharmacogenomics
	In vivo cell-reprogramming
Neuroelectronics devices	Improved mechanisms for the interface between neural structures/brain and electronics hardware:
	Neurochip-based biosensors
	Bionic implants
	Cybernetic augmentation to enhance human cognition
Nanobots	Increasing human resistance to damages, pathogens and toxins

Enabling technologies

- Bioengineering
  - Neuroenginering
    - Neuroelectronics
  - Brain–machine interface (BMI)
    - Transcranial Direct Current Stimulation (tDCS)
    - Transcranial Magnetic Stimulation (TMS)
  - Genetic engineering
- Pharmaceutics
- Genomics / Pharmacogenomics
- Artificial intelligence
  - Augmented analytics
  - Machine learning
    - Speech recognition / Natural language processing
    - Machine vision
- Human–machine interfaces
  - Visual displays
  - Augmented Reality
- Advanced materials (cf. also Section 2.2.2)
  - Nanomaterials and devices
  - Ceramic composites
  - Graphene
    - Semiconductors
    - Composites
- Smart textiles
  - E-textiles
  - Fibretronics
- Body-centric wireless networks (BCWN)
- Exoskeletons
  - Control architectures
  - Power systems

3 Elucidations of selected technology trends

In a recent study [8], the Norwegian Defence Research Establishment (FFI) has identified technology aspects with particular relevance to the development of Norwegian armed forces. Technology trends with particular relevance for these aspects are among those receiving further elucidation and discussion below (with the exemption of autonomous systems, which are believed to be well covered in other analyses). This also applies to all trends with disruptive potential in the long term since they are deemed to have a significant impact on a broad spectrum of warfare capabilities. Moreover, several of the constituting technology aspects likely will influence defence and security operations also in earlier phases of their development.

The discussion will form the basis for further research in later stages of this study series, as the elucidated trends are expected to influence future military operations profoundly, paying particular attention to the ways these emerging technologies interact and the operational context in which they are employed.

3.1 Everywhere Computing

Current cloud computing models delivers computing capabilities as a service using the internet. Software as a service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is typically accessed using a thin client, (web browser). It has become the common delivery model for most leading enterprise business applications in the centrally hosted cloud paradigm, such as office software or Geographic Information Systems (GIS), and SaaS is considered an integral part of cloud computing, along with Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

Edge Computing is the designation for a distributed computing paradigm that can be regarded as a complementary approach, modifying a centralised cloud data centre model with aspects of more distributed processing. Computation is performed largely or completely on distributed device nodes, pushing applications, data collection and computing power (services) away from centralised points. This places information processing and exchange closer to the origin of the information, primarily in order to reduce network traffic (volume) and latency. Further motivational factors include cost of data transmission into the data centre cloud, data retention policies, etc. Computation offloading for real-time applications, such as facial recognition, has been demonstrated.

Thus, an *edge* will be any location in a network where computing and related infrastructure, platform, software and services are offered which is closer to the user than the data centre cloud. Edge computing does not need contact with any centralised cloud, although it may interact with one. Its target is any application or general functionality needing to be close to the interaction of distributed systems technology with the physical world. Data coming in from this world through various sensors can be seen as constituting the basis for actions, based on computational analytics at the edge, to change the physical state through various mechanisms, taking

advantage of the proximity of the edge to the physical items of interest. This makes edge computing of particular relevance to fields where the need to supply distributed or local capabilities to embedded devices has become important (industries such as retail, e.g. Amazon), thus adapting the SaaS model to the requirements made by the IoT. Likewise, continuous growth of edge endpoints and the associated need to move large amounts of data from or to the edge will make 5G an important communication technology for everywhere computing.

The concept is also of relevance for defence and security. Of particular interest may be options of distributed simulation for decision support and training. NATO STO has proposed a combination of concepts, inspired by the as-a-service model of cloud and edge computing and designated 'Modelling & Simulation as a Service' (MSaaS), for a convenient and permanently available simulation environment to a large number of users. This will provide faster and more flexible availability of M&S, allowing reduced or no local footprint (computing power, storage, energy, cooling etc.) with service accessible through net browsers. A distributed data structure will allow for diverse services using national, coalition and mission specific clouds, i.e. coalition data sharing but with national control, providing a simulation environment with seamless interoperability between live, virtual and constructive simulations across coalition partners. The environment would sustain training and decision support, including immersive simulation with augmented/mixed reality (cf. also Section 2.2.3), and facilitate scenario planning with integrated scenario development tools. Ultimately, it could enable analysis of options and forecast of possible outcomes in real-time in the battlefield. Individuals and teams should have access to training anytime anywhere.

The paradigm could also supports other defence related applications, like integrated soldier systems, by applying IoT technologies and concepts to the military domain — the Internet of Military Things (IoMT) — to potentially work as a relatively simple and inexpensive sensor/C2 platform for the soldier BMS, including protective/health management systems.

3.2 Predictive Analytics and Big Data

These methods are not new *per se*, but have come to prominence over recent years due to refinements, particularly in machine learning, and considerably improved capacity for data processing and data management. This development is expected to continue. *Augmented analytics* using computerised machine learning algorithms will likely transform how analytics content is developed, consumed and shared (data preparation, data management, process management, process mining, auto-generated models). Modelling and simulation can contribute to and strengthen augmented analysis by adding models and simulations for prediction.

Predictive Analytics and Big Data techniques will thus constitute key elements of a 'revolutionary complex' when focused on fostering new capabilities that allow for enhanced perception (sensing/collecting data) and processing (data analysis/synthesis) to improve situational awareness, incorporating the general development of AI, virtual/augmented reality and enhanced (remote) sensing capability as complementary technology areas. Predictive analytics tools and techniques are therefore essential to a wide range of general tasks and

processes with relevance also for defence and security, such as risk analysis and adaptive (defence) planning, predictive logistics / optimisation, decision support as well as forensics / criminal investigations. The full impact of augmented analytics is anticipated to allow generalists such as officers (not specialised in data science) to perform advanced data analyses as part of a planning process.

The 'Internet of Things' (IoT) designates the technological trend where an increasing number of everyday objects are equipped with networked sensors, such as smart-phones, personal wearables, vehicles and domestic products, already numbered by the billions. Big data and IoT thus are complementary tools that readily match up, as data can be extracted from IoT devices and analysed to provide a mapping of device interconnectivity. Access to data generated through a proliferating network of sensors thus embedded in the environment to detect adversarial activities can provide considerable intelligence capability for defence and security using predictive analytics. Sophisticated facial recognition technologies could be combined with an improved ability to aggregate and analyse images, video, text and other content to establish patterns of movement, behaviours, and networks, to generate insights into what is happening in real-time, and ultimately foresee what might happen next. Similarly, IT Opera-tions Analytics (ITOA) applies big data principles with the concepts of machine intelligence to predict and potentially avoid issues in organisational IT systems, which makes the concept relevant for cyber defence (automated cyber response).

The IoT will pose a severe challenge for IT security, as both governments and private sector organisations currently rely on closed systems. Having 'everything connected to everything else' could lead to unpredictable effects of a potentially serious nature since it will be impossible to control complex global supply chains where components may come readily-assembled from anywhere in the world.

In the relative near term, central efforts within this field will deal with adapting and developing these tools to keep up with the expanding data volume. Undoubtedly, this effort will take place against a backdrop of increasing concerns regarding public (as well as private) access to and use of personal data, possibly within an increasingly restrictive legislative framework.

3.3 Satellites and Pseudo-satellites

The satellite market, and space applications in general, has been revitalised and trans-formed over the past decade through injection of new small (micro- and nano-) satellite[23] technology and considerable commercial investments, mainly focusing on communi-cations and earth observation capabilities. The transformation has been fostered by miniaturisation of payloads, plug-and-play technology and increasingly cost-effective satellite launches. SpaceX has become the principal commercial launch provider of this 'new space'. The current technology trends towards increased levels of automation, collaborative networking, artificial intelligence for decision support, and distributed

[23] The terms 'microsatellite' or 'microsat', and 'nanosat', are usually applied to artificial satellites with a wet mass between 10 and 100 kg, or between 1 and 10 kg, respectively.

supercomputing power will undoubtedly further increase efficiency and advance new uses for satellite technology.

The drive towards smaller satellites is motivated by the need to reduce mass and volume in order to reduce the cost for launch. As this miniaturisation almost inevitably reduces the performance of sensors, expansible apertures can be used, or satellites can be flown in constellations forming a synthetic aperture. The latter puts high demands on accurate positioning and communication between the satellites and requires synchronized movements of the satellites in the constellation. Moreover, maintaining very low earth orbits by performing orbit alterations enhances sensor resolution and enables higher communications bandwidth even for small satellites. Highly effective rocket engines and thrusters for frequent orbit adjustments are crucial for such capabilities.

Nonetheless, such small satellites could be fitted with a multitude of sensors and communication systems. Besides visual sensors, passive radars are available. Active radars could be feasible with reduced duty-cycles due to power limitations. It thus seems conceivable that very advanced small spacecraft could be procured and tailored to support advanced payloads for applications such as:

- Secure telecommunication
- AIS Ship tracking with Marine Search and Rescue (SAR)
- ADS-B Aircraft flight tracking, Next Generation Air Transportation System
- Arctic Satellite Navigation Augmentation System (GPS)
- Earth Observation; Visual and Hyperspectral
- Communication and Electronic intelligence (COMINT/ELINT).

Because of the potential reduced cost for space assets associated with this development, small states, private companies or even individuals have, or may soon obtain, access to data with quality and resolution that was previously reserved for major powers, with possible security implications for sensitive information[24]. Moreover, such actors may well obtain the capability to use small satellites to de-orbit or alter the orbit of other satellites, or even attack them.

In a defence setting, it should be possible to use constellations of small satellites for ISTAR to establish and maintain situational awareness, where a Maritime Domain Awareness (MDA) capability may be most relevant, or make up part of the C4-infrastructure. In this context, it should be noted that the geo-location of Norway is optimal for polar and near polar retrograde orbits providing good coverage of northern regions, as well as the existence of very favourable communications infrastructure.

[24] *Planet* is a commercial provider of earth observation data (imagery) based on a constellation of (currently around 200) nano-satellites [27]. Mega-constellations of thousands are conceivable in the future.

Pseudo-satellites or atmospheric satellites are a common designation of aircraft that operate in the atmosphere at high altitudes (around 20 km and above) for extended periods. Such systems have the potential to offer services conventionally provided by a traditional satellite orbiting in space at considerably reduced costs [28], specifically related to launch and any required orbit alterations. For defence and security purposes, it is also important to increase resilience of communications network and add flexibility (pseudo-satellites are, in an ideal world, available 'on demand' and can receive maintenance). Currently, the use of High Altitude Long Endurance (HALE) UAV (like Global Hawk) appears as the most significant solution for this area, although the potential for cost reductions still is not realised for these systems. Commercial actors are also experimenting with alternative concepts based on balloons or airships (for example Google's Project Loon). Such concepts have the advantage of allowing considerably longer operational time on station. However, all pseudo-satellite alternatives have severe challenges when operating in the High North.

3.4 Hypersonic Vehicles

Hypersonic technologies have the potential to affect the conduct of future military operations profoundly. Various hypersonic flight vehicle concepts, such as the hypersonic glide vehicle or cruise missile, enable new or more advanced military capabilities, most prominently the rapid mid- to long-distance standoff delivery of weapons. Higher speeds would allow for swift regional or global strikes against time critical targets from standoff distances, keeping the launching platform out of highly contested areas protected by modern A2/AD systems. Moreover, a powered hypersonic vehicle for ISR missions, possibly weaponised for reconnaissance-strike action, is also conceivable in a somewhat longer perspective.

The speed of hypersonic penetrating systems makes kinetic intercept by any opposition extremely difficult. Because of the potentially short flight times and thus limited warning, as well as uncertainties regarding possible use of nuclear warheads, a novel kind of 'terror balance' could result from this development. It should be noted that the extreme strains of hypersonic flight poses severe challenges to the structure and components of such vehicles, constituting a vulnerability. However, this might be a temporary limitation mostly relevant in early stages of development. Furthermore, any required target acquisition and vehicle guidance the terminal phase, is very challenging. In this context, there is also a question of the level of autonomy for such weapons, i.e. the need for or feasibility of a man-in-the-loop.

Supersonic combustion ramjet ('scramjet') powered vehicles, in which combustion takes place in supersonic airflow throughout the entire engine, will likely be a technology of particular interest since these vehicles permit and demand operations in the lower atmosphere due to the necessary oxygen supply for the engine. This would allow for the development of a hypersonic interceptor concept, with some hundred kilometres of range, to be used against time sensitive aerial targets (also for ballistic missile defence), and which would additionally have the potential to counter adversary missile and hypersonic vehicle threats.

Hypersonic vehicle design and development is extremely challenging because of many technological aspects (such as kinetic heating, aerodynamics, supersonic combustion, force loading, flight controls, (advanced) structural materials, instrumentation etc.) that are unique to hypersonic flight and are, after decades of hypersonic flight research, yet insufficiently studied to make the transition to a truly operational hypersonic system. The most challenging issues of hypersonic flight require several technical solutions considered to be at the edge or still beyond current state of the art. More recent advances, such as a possible adaptation of the evolving Rotating Detonation Engine (RDE) concept to hypersonics (which would eliminate the need for an initial boost phase), possibly suggest an accelerated development.

It is, however, reasonable to assume that obtaining mature operational hypersonic systems will take time, with an initial capability about a decade away. Conventional ballistic (non-air breathing) technologies likely will be preferred (as a low-risk measure) for deployment (gap filler) in the short term[25]. Continued investment in hypersonic test campaigns, with a stepwise development strategy due to the wide range of unresolved technical issues, will likely still be the way ahead (although at an enhanced pace). On this note, it is observed that hypersonics has now become a primary concern for U.S. military R&D (cf. DoD FY 2020 budget) [55].

3.5 Artificial Intelligence

Artificial Intelligence (AI) refers to the ability of machines to match human problem solving, or at least mimic cognitive functions associated with the human mind, in terms of learning, reasoning, planning and acting in a complex cyber-physical environment, thus allowing autonomous robot or vehicle control, automated information fusion and anomaly detection and intelligent tutoring. Hence, the term AI does not necessarily refer to a general artificial intelligence, often referred to as *strong AI* and frequently associated with notions such as ‘the Singularity’ or machine consciousness, but more to the ability of a machine to perform ‘intelligent action’. Such *weak AI* does not attempt to perform the full range of human cognitive abilities, but is primarily concerned with the use of software to study or accomplish specific problem solving or reasoning tasks. It is this latter understanding of AI that is mainly of interest here.

The AI research field over time has split into separate subfields, often with limited interaction, based on technical issues such as particular goals (like ‘robotics’) or the use of particular tools such as generative models and artificial neural networks.

Machine Learning (ML) is one of these subfields that has come to prominence in recent years and provides much of the backdrop for the perceived relevance of artificial intelligence methods for defence and security. ML investigates algorithms and statistical models that computer

[25] Actually, the Russian hypersonic air-launched ballistic missile Kh-47M2 *Kinzhal* already seems to be deployed and operational to some extent. It is expected that a hypersonic glide vehicle, and possibly a cruise missile, will become operational in the next decade (also for Chinese and U.S. systems).

systems use to perform a specific task effectively without using explicit instructions, relying on patterns and inference to build a mathematical model based on sample data.

Deep learning refers to a broad class of machine learning methods mainly based on artificial neural networks, a model inspired by information processing and structure (distributed communication nodes) of biological systems, with multiple (‘deep’) layers to extract higher level features from available data sources. Deep learning algorithms are used in a wide variety of applications: computer vision, speech recognition, natural language processing, drug design, bioinformatics and other topics where it is infeasible to develop an algorithm of specific instructions for performing the task. These systems have proven successful at correctly recognising and classifying a wide variety of input data, but are at present sensitive (and vulnerable) to training procedures and data sets.

Neuromorphic computing or engineering is a somewhat complementary approach. Its goal is to design artificial neural systems, based on very large scale integration (VLSI) electronic circuitry and associated software, to mimic neuro-biological structures present in the nervous system, with potential applications in fields such as machine perception, motor control, or multisensory integration. Under-standing how the overall neuromorphic architecture creates desirable computations and affects representation of information is central to this line of study. A key objective is to reduce power consumption by replacing resource intensive convolutions and back-propagation training methods of traditional neural networks with biologically inspired neuron functions and feed-forward training methodologies.

An overall outcome of the ascent of AI and related technologies with relevance for military doctrines and operational concepts could be a ‘splitting up’ of the established OODA-loop. Two ‘new’, although interdependent, cycles would appear; OO (Observe, Orient) and DA (Decide, Act).

The prominence of speed and automation provided by machine intelligence would be pivotal for tasks requiring more immediate responses, such as cyber threats or various counter-measures, associated with the first part. Big data streams would be fed directly into complex computerised models that are not constructed by humans but developed with machine learning techniques. When real-time decision-making is required in order to move faster than the opponent does, there might not be enough time for human review of the solutions provided by the system. Automated intelligence assessments will thus spur a drive towards (semi-)automated decisions.

Human decision makers then, conceivably, would primarily handle the latter, in general slower, phase, focusing on higher-level analysis. Predictive uses of AI systems could become critical, since such applications may change how planners and decision makers understand the potential outcomes of specific courses of action. If such predictive systems become sufficiently accurate and trusted, the vision of autonomous entities fighting other autonomous entities might become reality.

3.6 Quantum Technologies and Quantum Computing

Quantum Technology is an emerging field of physics and engineering turning the, admittedly sometimes strange, properties of light and matter revealed by quantum theory into practical applications -- such as the now much touted quantum computing. Quantum theory has fundamentally changed our understanding of the universe, showing that physical systems can exist in complex state configurations (superposition) and thus be deeply connected without any direct interactions (entanglement).

Until quite recently, quantum science has been a primarily academic pursuit. Nonetheless, practical technologies such as atomic clocks, lasers and semi-conductor devices (for example transistors) have also materialised, without which modern computers and the Internet would be impossible. In later years, there has been a growing appreciation of the potential to use previously unexploited quantum effects in the development of customised systems and materials for even more transformative products and applications in a ‘second quantum revolution’ with large-scale impact on modern society, including defence and security [40-41]. The combined capabilities of all forms of quantum technology could create an entirely new technological infrastructure, much as the semiconductor revolution starting in the 1960s. The new devices will actively manipulate and control quantum states of matter by taking advantage of the superposition and entanglement properties. These attributes, originally viewed as features begging for a more complete theory, have become accepted as the essential mechanisms by which quantum technology operates.

The new generation of quantum technologies can be sorted into three broad classes: quantum communications, quantum sensing and metrology, and quantum computing. In all the classes, quantum technology will enable significant capability enhancements already by the mid-term, while grow to be truly revolutionary in the long term.

3.6.1 Quantum Communications

Quantum communication attempts to guarantee secure data transmission across information networks, such as the Internet, and long-term security of information by using quantum properties for communication protocols. Quantum secure communications methods are expected to be quantum safe in the advent of a quantum computing systems that could break conventional asymmetric encryption methods.

It is anticipated that quantum computers effectively will be able to compute solutions to many problems that would take traditional computers thousands of years. Such mathematical problems are currently forming the basis of most asymmetric encryption, leaving the field vulnerable, although quantum computer cannot easily solve every problem of this type. As such, many cryptographic primitives therefor still will be secure. However, the perceived high risk associated with functioning quantum computers has induced the replacement of conventional asymmetric encryption methods (including key exchange) by quantum resistant algorithms.

Procedures of this kind are currently being standardised [43], with essential results being expected also in the short term.

In an alternative approach, inherent physical properties of quantum systems are used to create quantum secure communications based on optical quantum key distribution (QKD) hardware. These systems use entangled light in a way that reveals any attempt at intercepting a transmission of the encryption key. Whenever the transmission is compromised, the key is abandoned and another sent until both parties are sure it is unobserved, after which they can securely communicate over ordinary channels.

Laser-based QKD systems using fibre optic transmission are commercially available, but with limited range and low bandwidth (tens or hundreds of kilobits per second). Consequently, they are currently only suited for specific cases, such as highly critical links between major infra-structure components, rather than field deployments. Entanglement repeaters acting as trusted nodes are needed for global reach, but still need years of research to achieve maturity. Satellite-based quantum key distribution networks could be an interim solution or fall-back option, and could ultimately lay the groundwork for a future quantum Internet, incorporating IoT, with all transactions protected by quantum cryptography.

3.6.2 Quantum Sensing and Metrology

Superposition states are inherently very sensitive to the environment and are therefore suitable for making very accurate sensors, notably with coherent combinations enabled by entanglement distribution (quantum repeaters). As a result, quantum sensing has the potential to provide unprecedented precision, sensitivity and accuracy of measurements of quantities such as acceleration and rotation, or electromagnetic and gravitational fields. Its applications include navigation in GPS-deprived environments, covert sensing or meticulous topographical mappings (for example of the seabed).

Quantum metrology employs quantum mechanical features such as the quantum Hall effect to perform very precise measurements of fundamental quantities; time, frequency, voltage, current and resistance. (Superconducting) *solid-state quantum sensors* can measure very small magnetic fields, with applications in bio-sensing and non-destructive testing / inspection of metals. *Quantum imaging devices* use entangled light for higher resolution images orders of magnitude better than current state-of-the-art. *Atomic and molecular interferometer devices* measure acceleration and rotation very precisely for inertial navigation. Significant progress in this field over the past years has resulted in a redefinition of the SI unit system in 2018.

3.6.3 Quantum Computing

Quantum computing uses properties of subatomic particles like superposition and entanglement to represent and manipulate data. Based on ‘quantum bits’ or *qubits*, which are devices that can store and process quantum data (as opposed to binary data) with links that transfer information

between the qubits, a quantum computer acts as a massive parallel device with an exponentially large number of computations taking place simultaneously. This increased capacity is possible since groups of qubits can be in entangled states, thereby providing a larger state space in which to process information. Quantum computers are predicted to calculate problems that are intractable using even the fastest and largest conventional supercomputers. Several algorithms that take advantage of this power already exist, of which 'Shor's Algorithm' for factorising large numbers into primes (important for the secure data transmissions of today, cf. Quantum Communications), is the most renowned.

Quantum computing is expected to revolutionise multiple other technical domains, such as modelling & simulation, materials science (structure and properties), pharmaceutical research (drug discovery and design) and cryptography/cyber defence, with significant uses in computing fields such as big data analytics, optimisation and machine learning.

Research efforts over the last two decades, with significant efforts also from well-established IT companies, have demonstrated the basic principles of quantum computing based on solid-state systems and on atomic or optical systems. The most advanced are based on trapped ions (IonQ) and superconducting circuits (IBM, Google, Rigetti, Intel, D-Wave) with architectures using logic gates analogous to those found in conventional computers, where small prototypes have already run basic algorithms and protocols. Currently, their sizes are limited to around 50 qubits for the research-based efforts[26], but a smaller 20 qubits version has been made available publicly in the cloud by IBM Q for experimentation and program development. This should be compared to the hundreds of billions of 'classical' bits available in a traditional device.

As quantum computers are impaired by loss of quantum coherence (decoherence) due to interactions of qubits with the outside environment, their operation will fall apart. Given the current rates of decoherence and other errors, contemporary quantum computers[27] are unlikely to return correct answers except for programs with brief execution times, and are thus unable to support large-scale computations. Further advances in quantum computer design and architecture, fault-tolerant protocols, algorithms supporting error correction to enable qubit stability and new fabrication technologies are required to address these challenges. A definite breakthrough is probably several years away and a universal quantum computer might not be seen for several decades.

Thus, realising a quantum computing capability demands that hardware efforts should be complemented by the development of quantum software to obtain optimised algorithms able to solve problems of interest. An obviously mitigating approach involves the use of hybrid quantum-classical algorithms, which run only the most performance-critical sections of a program on a quantum computer and is adjusted to the specificities of the given hardware device, with the bulk of the program running on a more robust classical computer. Recent efforts are beginning to demonstrate systems that might have practical applications and may constitute the basis for a realistic programme prepared to provide within limited time, which

[26] D-Wave claims 2048 qubits in their latest adiabatic quantum computer, D-Wave 2000Q.
[27] Often referred to as NISQ — Noisy Intermediate-Scale Quantum

might not be much more than a decade, fully programmable quantum computers sophisti-cated enough to crack encrypted messages.

3.7 Electromagnetic Dominance

Electromagnetic Dominance refers to the ability to use more of the electromagnetic (EM) spectrum, to share the spectrum more efficiently, to protect own forces' use of the spectrum and to deny enemy use. Thematically, it ranges from materials technology for signature control through wireless communications and electronic warfare to directed energy weapons. The quest for EM dominance is becoming more contested and competitive due to commercial investment in advanced radiofrequency technology. Related advances in passive radar will likely make air superiority difficult to achieve.

3.7.1 Microwave Photonics

The use of optical devices and techniques to generate, manipulate, transport, and measure high-speed radiofrequency signals with a wavelength between one millimetre and one meter, is known as *microwave photonics* (MWP). Enhanced processing bandwidth obtained from up-converting the radiofrequencies to the optical frequencies, availability of low loss optical fibres as transport medium, and flexibility in tailoring the radiofrequency response have been key drivers in the early development of the technology, permitting functionality in microwave systems, comparable to RF circuits, that are complex or even not directly possible in the radiofrequency domain. The parallel development of photonic integration technologies has allowed a dramatic footprint reduction of the resulting fairly complex *integrated microwave photonics* systems, significantly altering the capabilities of MWP systems to achieve higher performance with reduced power consumption. This includes modulation bandwidth, spectral resolution and noise performance, enabling the integration of all the key components (light sources, modulators and detectors) of MWP systems into a single complex processor chip with multi-functionality and re-configurability similar to electronic devices. These recent synergies of integration, advanced functionalities, and high performance have been key highlights of the field.

MWP technology is suited for applications such as generation of very stable multi-band radiofrequency (RF) sources up to millimetre frequencies with low phase noise, precise wideband RF signal detection and digitisation, wideband beam steering of RF signals in phased array antennas, tuneable RF filters and stable clock and signal distribution in networks.

The development of integrated MWP technologies has been driven by communications-related applications such as radio-over-fibre systems (eased connection to remote antennas). This is expected to continue with new concepts such as 5G systems and the internet of things (reconfigurable antennas). Likewise, integrated MWP is expected to play a key role for next generation (cognitive) radio systems with massive multiple-input multiple-output (MIMO), increasing network capacity and network adaptability. Photonic-based wideband radar as well as MIMO radar are other emerging applications, the flexibility and re-configurability of MWP

technology allowing for future complete software-defined configuration of radar and EW systems.

3.7.2 Passive Radar

Passive radar systems (also referred to as passive coherent location, PCL) refer to a class of radar systems that detect and track objects by processing reflections from external non-cooperative sources of illumination (Illuminator of Opportunities, IO) in the environment, such as DVB-T/S, FM radio, UMTS, DAB, GSM and similar, to implement the radar functionality (target detection and tracking). The lack of a proper radar transmitter greatly simplifies the system design. In addition, the use of IOs reduces the vulnerability of the system against electronic countermeasures (ECM) and increases the detection capabilities of the radar with respect to stealth targets, specifically designed to defeat monostatic systems.

Modern ubiquitous and affordable computing power has led to a resurgence of interest in passive radar technology, allowing system designers to apply digital signal processing techniques to exploit a variety of broadcast signals and to use cross-correlation techniques to achieve sufficient signal processing gain to detect targets and estimate their range and Doppler shift. Making use of multistatic / multiband configurations of passive radar can significantly enhance the tracking capabilities. Moreover, recent developments in passive radar imaging via ISAR processing can be exploited for non-cooperative target recognition and may enable automatic target recognition capability in future systems. Extended OTH range PLC may become available by taking advantage of forward scattering. Due to radar cross-section magnification in the forward scattering region, the target ranges could be increased up to 1000 km. As usual with new developments, it will be essential to explore the potential of PCL technology by finding effective attack vectors against PCL radars and develop corresponding protective measures to maintain the integrity of own stealth capability.

3.7.3 Quantum Radar

Advances in quantum technology have had a considerable impact on the development of sensing devices that exploit quantum phenomena in order to increase their sensitivity, cf. sections 2.3.2 and 3.1.6. Quantum illumination offers the prospect of enhanced target detection capabilities by exploiting the existing correlation between emitted photons bounced back by an illuminated object and their entangled partners kept inside the illumination source. Progress in optomechanics and the development of efficient microwave-optical converters permit the application of this concept also to the microwave regime, thus the concept of *quantum radar*. If successfully developed, it will allow the radar system to pick out its own signal even when swamped by other sources. This permits it to detect stealth aircraft, filter out deliberate jamming attempts, and operate in areas of high background noise. Although stealth technologies will still be just as effective at reflecting the original signal away from the receivers of quantum radars, the system should still be able to separate out the remaining signal by taking advantage of the correlations provided by the radar source. This concept is currently rather immature. However, basic principles have been demonstrated [48].

3.7.4 Directed Energy Weapons

Directed-energy weapons, incorporating lasers and microwave weapons, damage or incapacitate their targets with highly focused energy. Conceivable targets for laser weapons include (ballistic) missiles, hypersonic weapons, (unmanned) vehicles and mortar rounds. When fielding these systems, initial focus will be on obtaining tactically relevant effects against common threats as well as cutting-edge point defence capabilities[28]. In addition, non-lethal applications, such as crowd control or the disabling of machinery and sensor systems, are of considerable interest. For the latter application, short-pulsed laser providing white-light broadband electromagnetic radiation could be used for very effective dazzling of electro-optical devices. Likewise, progress in quantum and interband cascade lasers could provide the basis for next-generation infrared countermeasure (IRCM) systems to reduce the vulnerability to heat-seeking missiles. Also high power microwave devices, such as the Active Denial System, will remain relevant for non-lethal uses.

While the power issue will persist for some time for laser devices, as systems currently under development based on practical electrically driven lasers tend to be in the mid-power (100 kW) range, maturity has reached levels indicating that the practical impact of directed energy technology, such as its intended use and integration in existing combat systems, must be seriously addressed.

3.8 Soldier Enhancement Systems

Soldier Enhancement refers to the augmentation of individual human abilities using artificial means such as robotic exoskeletons, smart textiles, drugs, and seamless man-machine interfaces. Advances in material, computer and human sciences (bioengineering, nano-technology and genomics), as well as convergence between these fields, are set to significantly enhance human capabilities and optimise overall soldier performance and effectiveness. Effective forces could therefore consist of smaller groups, with possible implications for affordability. Regenerative medicine and associated breakthroughs could transform battlefield medicine, improving battlefield survivability and allowing troops to recover from injuries faster. Networked augmentations, such as exoskeletons and prosthetics, will likely be an appealing target for hackers. It should be expected that adversaries might be similarly enhanced. The moral and ethical aspects of these issues must be considered.

3.8.1 Exoskeletons

Powered exoskeletons tailored for defence and security applications, such as the now concluded or abandoned American TALOS, HULC and XOS 2 programmes, still face significant technical challenges. A main concern relates to power supply for extended use without tethering to immobile power sources. Work in the field currently seems primarily to rely on development in the commercial sector. Despite this, one can expect that exoskeletons will become standard

[28] U.S. Navy signals intention to replace close-in weapon systems of the surface fleet with HELIOS (High Energy Laser with Integrated Optical-dazzler and Surveillance) [49].

issue for military forces in the long term, at least when it comes to logistics tasks and heavy maintenance duties. It is also possible they could enhance the performance of front-line forces by enabling soldiers to increase mobility and carry significantly greater loads or weapons.

3.8.2 Operator Support Measures

Concepts such as the *Hyper-Enabled Operator* [51] focus more on soldier support in the cognitive domain, i.e. how immersive technologies can affect and benefit human perception. For one part, it envisions pushing information to the tactical edge, i.e. the individual soldiers or their unit, by a robust communication and optimised data throughput, cloud-supported edge computing and augmented reality projected on a heads-up display for soldier helmets. Further technologies of interest include tailorable (individual) optimised human-machine interfaces and protocols, adaptable and flexible sensors for human performance and environmental monitoring; biometric and forensic tools, scalable near range communications (wireless area) networks, heuristic / probabilistic techniques and predictive analytical models to speed and enhance decision-making (analytics based cognitive decision support).

Other advances pertaining to the individually enhanced soldier relate to organic aspects including optimised nutrition, time-released nutritional supplements, or performance enhancing drugs such as nootropics. Modafinil, a drug for treating wakefulness disorders such as narcolepsy, has found use in operations by some armed forces and may be worth investigating for use in enhancing alertness if proven safe. Genetic engineering and manipulation techniques could be used to improve individual environmental tolerance, resilience and prophylaxis, as well as personalised therapies in case of illness or injury, taking advantage of the completely characterised soldier genome.

Knowledge of human genomics, modelling and analytics, and bioengineering standards constitute the fundaments of regenerative medicine. The basic idea is to deliver desired corrective treatment, designed to fit with the diseased individual's physiology, to damaged tissues using engineered genetic material or stem cells. Preventive therapies are also anticipated. A major challenge is to deliver the treatment precisely to the affected tissues. Emerging techniques for in vivo cell reprogramming based on electric charge-induced 'nano-channels´ could remedy this and allow initial treatment for some injuries to begin already on the battlefield.

Bionic implants improve or correct the function of organs or other body parts, mimicking the functions and appearances of natural equivalents. Cochlear and some retinal implants are currently available. In the longer run, visual implants that enable users to see infrared light could enable soldiers to see in the dark. Moreover, tiny robotic devices at the nanoscale ('nanobots") could improve human resistance to damage, pathogens and toxins.

In addition, enhanced or extended sensing capability beyond typical human performance parameters could be very useful in the defence context. Neurostimulation methods, such as transcranial direct current stimulation (tDCS) or magnetic stimulation (TMS), are of particular

interest, but require extended research to be developed into useful and safe tools. These methods are also of relevance for implementing brain-machine interfaces.

3.8.3 Smart Textiles

Advances in fields such as nanotechnology, organic conducting polymers (flexible/plastic electronics), metals, ceramic semiconductors, body-centric (wireless) networking concepts, computer modelling and novel textile construction methods are enabling a range of textile–based technologies with the ability to sense and react to their surroundings. This includes monitoring biometric data, such as heart rate, and environmental factors such as temperature, as well as producing real time feedback in the form of electrical stimuli, haptic feedback or changes in colour. Moreover, adapted energy storage technologies, from flexible batteries to graphene supercapacitors, are supporting developments in these fields leading to the potential for capabilities not traditionally associated with textiles. Such *Smart Textiles* (cf. also Section 2.2.2) combine aspects of textile technology with advanced materials and novel integration approaches, permitting garments to act as sensors and actuators. Smart Textiles may also integrate other material forms (bulk materials, membranes, films and combinations of these materials) as well as embedded sensor components, combining to provide for a range of integrated capabilities. Amongst these are *Soldier Protection* (environmental and antimicrobial monitoring and protection), *Physiological Health Monitoring* (wearable biomedical systems), *Energy Harvesting and Storage* (photovoltaic fibres, hybrid batteries or supercapacitors for energy harvesting and storage) as well as *Sensing and Communications* (compact packaging of electronics and sensors integrated in a textile platform).

3.8.4 Neuroelectronics

Neuroelectronics involves the coupling of electronics with neural tissue, from individual neurons to larger neural networks. It aims at designing and developing biocompatible electronic devices that allow efficient interaction with neural networks and the brain; i.e. combining nerve cells and microchips. Neuroprosthetics and possibly biological (neuro-morphic) computers are among the ambitious applications for such chips. This field is multidisciplinary, and requires integration of materials science (biocompatible devices, nanoelectronic synaptic devices), electronics engineering (integration aspects) and neuroscience.

Neuroelectronics components that can effectively implement brain-like algorithms and interface directly with living tissue are offering possibilities for new technological capabilities that could have significant impact on both civilian and military applications, i.e. offering new treatment methods for neurological diseases and long-term treatment for battlefield trauma, including paralysis, loss of limbs (improved mobility) and potentially even brain injury. These advances would also improve mechanisms for human neurological interface with external electronics for enhanced control of human-machine systems, such as artificial limbs and capable exoskeletons. They could even enable cybernetic augmentations. Biosensors for assessing toxic or pharmaceutical / chemical substances based on nerve cells are among other exciting possibilities.

4 Preliminary conclusions and further work

An important aspect of technology development is convergence. In the context of this survey, convergence refers to the synergistic combination of two or more technology trends, each of which in its own development may be progressing at a considerable rate, thus reinforcing each other to expand the applicability of their specific technologies and change military operations. The trends discussed in this report will enable such convergence in technology to a varying degree. The broader conception of convergence, understood as a confluence between technology development and societal aspects involving people and processes with fundamental consequences for the future operational environment of armed forces, is not discussed here but will be investigated in follow-up work.

Additive manufacturing is a technology that first emerged in the 80's but just recently has obtained maturity levels bringing it on the verge of causing real disruption, cf. presentation in Section 2.1.1. A major issue hampering development in this field has been intellectual property rights and patent management. However, the field also needed development in other areas, ranging from increased computational power for developing 3D-models, internet, cheaper 3D-scanning equipment, software development for CAD, material development and reduced cost of production materials. Additive manufacturing is thus an instructive example of the importance of convergence in technology.

Likewise, as has been argued above, artificial intelligence (AI) is a trend enabling and boosting further development within many technology fields, significantly those involving various degrees of automated intelligence assessments[29]. Advancements in AI can greatly benefit areas such as predictive analytics, autonomous systems or the quest for electromagnetic dominance in all time frames. Moreover, AI-technology will provide a bridging function between other technologies, widening their area of applicability. Much the same applies to topics such as autonomous systems, sensors and quantum technologies. Advancements here could end up greatly increasing the speed at which other areas develop, with major potential for innovation and radical change in interaction. To illustrate, autonomous swarms of unmanned systems, provided with new sensor technology and artificial intelligence (machine learning) support for guidance and analysis of large amounts of data, could grant an actor vastly superior real-time situational awareness in a future operating environment.

Identifying various technology areas with potential for disruptive convergence is always going to be unpredictable and somewhat arbitrary, although the given AI-example appears rather evident based on the above discussions. Other technology fields emerging as likely candidates for convergence in this work are bioengineering, including synthetic biology and human performance enhancement, advanced material sciences and additive manufacturing processes, as well as robotics.

[29] These aspects are discussed further in e.g. [55].

The increasing convergence between the fields of biosecurity and cybersecurity is, obviously, still uncharted territory. One instructive case, exposing inherent vulnerabilities, involves the use of active implantable medical devices (IMDs) which can connect wirelessly to external appliances, an issue that relates to unmanned systems in general. Moreover, systems and data that were once localised and contained to university or government laboratories, and therefore only accessible to those directly involved in related research, may be rendered vulnerable as digitisation and automation processes promote expansion of biotechnology expertise and use beyond traditional practitioners.

Developments of this kind will potentially add value to a number of defence activities, from performance optimisations and cost reductions to completely new operational concepts. When looking at technological trends in a 20-year perspective, one must therefore assume both that novel technologies will emerge in the process, as well as the appearance of new convergence phenomena, which allow applications that were previously unimagined. In a security and defence context such disruptive effects and converging applications represents both opportunity and a threat.

Convergence can allow new technologies to fill multiple requirements at once and reduce the time it takes to achieve desirable effects, acting as a force-multiplier that increases operative output and relative firepower of forces. If a state is able to identify and exploit convergence phenomena at an early stage, it can end up achieving a comparative advantage. Consequently, ignoring technological trends is not an option, as this can inadvertently lead to critical vulnerabilities for national security. By staying on top of trends, actors are able to pursue technologies that can lead to convergence and cause disruption, simultaneously reducing the likelihood of potential adversaries realising the benefits.

Although government research centres and the defence industry will likely remain important players investing in research and development relevant for defence and security, an increasing share of this activity will take place outside such organisations. Public universities, civilian research institutes and private companies conduct much of the R&D undertaken within the technology fields discussed here, with investments mainly driven by the commercial market, and thus not necessarily coincidental with the security needs of the society [5, 57]. State participation will therefore have to remain a crucial factor in the development of technology for defence purposes. For national governments, this entails that access to emerging technology, which could bring about disruption in the security realm, warrants a thorough understanding of actors in the civilian sector. In order for them to harvest technology that can provide necessary capacities and capabilities, proper incentive mechanisms must be found and relevant systems and processes supporting close cooperation established.

Moreover, to facilitate cooperation, defence actors must make sure the civilian companies and research institutes have a thorough understanding of military requirements. They must also broaden their horizon when looking for new capabilities, and be ready to exploit promising opportunities from emerging technology that have not yet reached sufficient maturity to enable requirements definitions. In some rare cases, it will be possible to adapt technology created for civilian sector directly for defence purposes, although predominantly it will serve as a

foundation for further development. Companies and research institutes should be given the opportunity to approach the defence sector and provide new solutions and technology beyond established requirements. Arenas of innovation and experimentation forums facilitating cooperation between warfighter and developer is a much-employed arrangement meant to foster such activity in order to achieve disruptive effects.

Conversely, the able use of drone technology by the Islamic State and similar non-state actors illustrate a type of future threats with potentially unpleasant and dangerous outcomes that are significantly derived from dual-use commercial (COTS) technologies [58]. Dual-use science and technology thus opens the door to unexpected nefarious weapons or exploitations and ought to be effectively monitored to identify risks and develop counters, begging the question of how to establish functioning control mechanisms.

The technology trends discussed in this report will surely have impact on the future of warfare. Several of the discussed technologies will permit enhanced situational awareness of decision-makers. Other consequences of the technological development in the longer term are pointing in another direction, such as increased engagement range, precision, speed and faster decision cycles. Further research on technology trends should attempt to explore these consequences and identify actionable areas in order to support long-term planning and enable development of future military capabilities and operational concepts, a process that is challenging in many ways. Several, if not most, current capabilities are defined with existing technologies, systems and operational concepts in mind. Hence, it cannot be expected that future technologies map to present-day capabilities in a direct, linear way. Capabilities are also redefined at irregular intervals, so such a mapping will be expected to change over time anyway. Similarly, it is necessary to investigate the other aspects of the convergence phenomenon, those involving personnel and processes (or in more military terms – doctrine and organisation), conceivably using a DOTMPLFI[30]-perspective.

It should nevertheless be feasible to find a framework to portray a future with prospective systems based on emerging technologies and assess the consequences for Norwegian military operations. This quest would aspire to discover surfacing operational concepts and other issues of relevance in order to be better prepared for a future operational environment, using an overarching narrative in ways that will capture the imagination. By doing so, this study series will aim at gaining a broader understanding of how technological development influences future military operations.

[30] Doctrine, Organisation, Training, Materiel, Personnel, Leadership, Facilities and Interoperability

References

[1] *Global Trends: Paradox of Progress* (NIC 2017-001, Office of the Director of National Intelligence, January 2017), viewed 25 February 2020, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf

[2] *Emerging Science and Technology Trends: 2017-2047 — A Synthesis of Leading Forecasts* (Office of the Deputy Assistant Secretary of the Army for Research and Technology – DASA R&T, November 2017)

[3] *Assessment of Possible Disruptive Technologies for Defence and Security* (AC/323(SAS-062)TP/258, NATO Research & Technology Organisation, 2010), NATO UNCLASSIFIED

[4] *STO Tech Trends Report 2017* (AC/323-D(2017)0006 (INV), NATO Science Technology Board, 2017), Public Release

[5] *Exploring Europe's capability requirements for 2035 and beyond — Insights from the 2018 update of the long-term strand of the Capability Development Plan* (EDA/Rand Europe, Marta Kepe, James Black, Jack Melling and Jess Plumridge, June 2018)

[6] *A journey into the future* (European Defence Matters, Issue 14, 2017)

[7] *Top 10 Strategic Technology Trends for 2019* (G00374252 Gartner, Inc., David Cearley and Brian Burke, October 2018)

[8] *Hvordan styrke forsvaret av Norge? — Et innspill til ny langtidsplan (2021–2024)* (FFI-RAPPORT 19/00328, Espen Skjelland & al., 2019) (in Norwegian)

[9] *The Black Swan* (NY: Random House, Nassim Nicholas Taleb, 2010)

[10] *Å forske på Forsvaret i fremtiden — muligheter, begrensninger og kognitive fallgruver* (FFI-RAPPORT 16/01810, Alexander W. Beadle, 2016) (in Norwegian)

[11] *Forecasting Change in Military Technology, 2020-2040* (Washington, DC: Brookings Institution, Michael O'Hanlon, 2018)

[12] *Defence Future Technologies – What we see on the horizon* (armasuisse Science and Technology, Quentin Ladetto, 2017)

[13] *Future technology trends in security* (Ministry of Defence – Defence and Security Accelerator, 2018)

[14] *Europe to explore 3D printing applications for military and defense* (3Ders.org, 2016), viewed 10 March 2019, http://www.3ders.org/articles/20161222-europe-to-explore-3d-printing-applications-for-military-and-defense.html

[15] *Top 10 Strategic Technology Trends for 2018* (G00327329 Gartner, Inc., David Cearley, Brian Burke, Samantha Searle and Mike Walker, October 2017)

[16] *Defence Future Technologies – Emerging Technology Trends 2015* (Federal Department of Defence, Civil Protection and Sport DDPS - armasuisse Science and Technology, Quentin Ladetto, 2015)

[17] *Modelling and Simulation as a Service (MSaaS) Rapid deployment of interoperable and credible simulation environments One Pager* (MSG-136 RTG, NATO Modelling and Simulation Group (MSG), 2015), Public Release

[18] *Decision Support and Planning Support with Modelling and Simulation in the Battlefield Technology Watch Card* (NATO Modelling and Simulation Group (NMSG), 2015), Public Release
[19] *Integrated Live Virtual and Constructive (LVC) Simulation in a Distributed Networked Environment Technology Watch Card* (NATO Modelling and Simulation Group (NMSG), 2015), Public Release
[20] *Provision and Discovery of Modelling and Simulation Tools and Services in the Cloud Technology Watch Card* (NATO Modelling and Simulation Group (NMSG), 2015), Public Release
[21] *EDA BIDADEMS Study Final Report* (EDA / SVGC Limited, 2017)
[22] *Big Data, Synthetic Biology and Space Planes Are the Weapons of the Future* (Defense One, Patrick Tucker, 2014), viewed 10 March 2019, http://bit.ly/2mu285s
[23] *Smart Textiles Technology Watch Card* (NATO STO Sensors & Electronics Technology (SET) Panel, 2013), Public Release
[24] *Graphene Technology Watch Card* (NATO STO Applied Vehicle Technology (AVT) Panel / NATO STO Sensors & Electronics Technology (SET) Panel, 2016), Public Release
[25] *Mixed Reality System to Revolutionize Defense Training* (iHLS, 2016), viewed 10 March 2019, http://ihls.com/2016/12/mixed-reality-system-revolutionize-defense-training/
[26] *Analysis of Small Space Assets Supporting Air Defense Applications and Survey of Enabling Technologies* (Bruhnspace Report P7-1-13-RP-003, Bruhnspace AB, 2013)
[27] *Very Small Satellites, Very Big Deal* (Army AL&T Magazine, Michael Bold, January - March 2018)
[28] *Drone technology achieves new heights at Yuma Proving Ground* (Army.mil, Mark Schauer, 2019) viewed 10 January 2020, https://www.army.mil/article/217347/unmanned_aircraft_stays_aloft_for_nearly_26_days_above_us_army_yuma_proving_ground
[29] *Task Force on Energy Systems for Forward/Remote Operating Bases Final Report* (Department of Defense – Defense Science Board (DSB), 2016)
[30] *Study on The Use of Mobile Nuclear Power Plants for Ground Operations* (U.S. Army Deputy Chief of Staff - G 4, Juan A. Vitali, Joseph G. Lamothe, Charles J. Toomey Jr., Virgil O. Peoples and Kerry A. Mccabe, 2018)
[31] *Revisiting the cold case of cold fusion* (Nature vol. 570, Curtis P. Berlinguette & al., 2019)
[32] *Energy Transition Outlook 2019* (DNV GL, 2019), viewed 25 March 2020, https://eto.dnvgl.com/2019/index.html
[33] *Hypersonic Vehicles — Game Changers for Future Warfare?* (Joint Air Power Competence Centre (JAPCC), Hans-Ludwig Besser, Dennis Göge, Michael Huggins, Alan Shaffer and Dirk Zimper, 2017), viewed 22 February 2019, https://www.japcc.org/hypersonic-vehicles/

[34] *Russia's 'Invincible' Weapons: An Update* (Changing Character of War Centre, Pembroke College / University of Oxford, Julian Cooper, 2019)
[35] *Hypersonic Vehicles Technology Watch Card* (NATO STO Applied Vehicle Technology (AVT) Panel, 2015), Public Release
[36] *Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control* (United Nations Office for Disarmament Affairs, United Nations, 2019)
[37] *Artificial Intelligence and The Future of Defense: Strategic Implications for Small- and Medium-sized Force Providers* (The Hague Centre for Strategic Studies (HCSS), Stephan De Spiegeleire, Matthijs Maas and Tim Sweijs, 2017)
[38] *Towards spike-based machine intelligence with neuromorphic computing* (Nature vol. 575, Kaushik Roy, Akhilesh Jaiswal and Priyadarshini Panda, 2019)
[39] *IBM's brain-inspired chip TrueNorth changes how computers 'think,' but experts question its purpose* (TechRepublic, Hope Reese, 2016), viewed 10 March 2019, https://www.techrepublic.com/article/ibms-brain-inspired-chip-truenorth-changes-how-computers-think-but-experts-question-its-purpose/
[40] *Quantum Technologies Flagship Final Report* (EC High-Level Steering Committee, 2017)
[41] *The US National Quantum Initiative* (Quantum Sci. Technol. vol 4, Michael G Raymer and Christopher Monroe, 2019)
[42] *Before The Quantum Revolution* (Nature vol. 574, Michael Brooks, 2019)
[43] *Post-Quantum Cryptography* (National Institute of Standards and Technology, 2017), viewed 29 January 2020, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[44] *Satellite-relayed intercontinental quantum network* (Phys. Rev. Lett. vol. 120, Sheng-Kai Liao & al., 2018)
[45] *Microwave Photonics Technology Watch Card* (NATO STO Sensors & Electronics Technology (SET) Panel, 2014), Public Release
[46] *Passive Radar NCTR Technology Watch Card* (NATO STO Sensors & Electronics Technology (SET) Panel, 2015), Public Release
[47] *Quantum Radar Technology Watch Card* (NATO STO Sensors & Electronics Technology (SET) Panel, 2013), Public Release

[48] *Quantum radar has been demonstrated for the first time* (MIT Technology Review, Emerging Technology from the arXiv, 2020), viewed 14 February 2020, https://www.technologyreview.com/s/614160/quantum-radar-has-been-demonstrated-for-the-first-time/
[49] *Key Themes from the 2019 Directed Energy Summit* (Booz Allen Hamilton Inc., 2019), viewed 14 October 2019, https://www.boozallen.com/d/insight/blog/key-themes-from-2019-directed-energy-summit.html
[50] *Femtosecond Laser Applications for Defence and Security Technology Watch Card* (NATO STO Sensors & Electronics Technology (SET) Panel, 2013), Public Release

[51] *The Hyper-Enabled Operator* (Small Wars Journal, Alex MacCalman, Jeff Grubb, Joe Register and Mike McGuire, 2019), viewed 6 November 2019, https://smallwarsjournal.com/jrnl/art/hyper-enabled-operator

[52] *'Hyper-Enabled Operator' Concept Inches Closer to Reality* (National DEFENSE, Yasmin Tadjdeh, 2019), viewed 6 November 2019, https://www.nationaldefensemagazine.org/Articles/2019/5/3/Hyper-Enabled%20Operator%20Concept%20Inches%20Closer%20to%20Reality

[53] *SOCOM's Iron Man Suit - A Worthy Moonshot* (National DEFENSE, Stew Magnuson, 2019), viewed 6 November 2019, https://www.nationaldefensemagazine.org/articles/2019/5/20/editors-notes-socoms-iron-man-suit---a-worthy-moonshot

[54] *Neuroelectronics Technology Watch Card* (NATO STO Information Systems Technology (IST) Panel, 2016), Public Release

[55] *Proceedings and Debates of The 116th Congress* (Congressional Record, vol. 165 p. H10812, 2019), viewed 10 March 2020, https://www.govinfo.gov/content/pkg/CREC-2019-12-17/pdf/CREC-2019-12-17-house-bk2.pdf

[56] *AI, Robots and Swarms: Issues, Questions and Recommended Studies* (Alexandria: CNA Corp., Andrew Ilachinski, 2017)

[57] *Technological trends and their impact on defence planning* (FFI-RAPPORT 20/00228, Norwegian Defence Research Establishment (FFI), 2019)

Islamic State's Weaponised Drones (Conflict Armament Research, 2016), viewed 11 March 2020, https://www.conflictarm.com/perspectives/islamic-states-weaponised-drones/

List of Acronyms

A2/AD	Anti-Access / Areal Denial
ADS-B	Automatic Dependent Surveillance/Broadcast
AESA	Active Electronically Scanned Array
AI	Artificial Intelligence
AIS	Automatic Identification System
AR	Augmented Reality
AUV	Autonomous Underwater Vehicle
BCWN	Body-Centric Wireless Networks
BMI	Brain–Machine Interface
BMS	Battlefield Management System
C2	Command and Control
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance
CAD	Computer-Aided Design
CASEVAC	Casualty Evacuation
CBRN	Chemical, Biological, Radiological and Nuclear
C-IED	Counter Improvised Explosive Device
CIS	Combat Information Systems
COMINT	Communication Intelligence
COTS	Commercial-Off-The-Shelf
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CSAR	Combat Search And Rescue
DAB	Digital Audio Broadcasting
DAS	Defensive Aid Suites
DASA	Office of the Deputy Assistant Secretary of the Army
DC/AC	Direct Current to Alternating Current
DNA	Deoxyribonucleic Acid
DMLS	Direct Metal Laser Sintering
DVB-T/S	Digital Video Broadcasting – Terrestrial / Satellite
DOTMPLFI	Doctrine, Organisation, Training, Materiel, Personnel, Leadership, Facilities, Interoperability
DPAL	Diode-Pumped Alkali Laser
EAM	Extrusion based Additive Manufacturing
EBM	Electron Beam Melting
ECM	Electronic countermeasures
EDA	European Defence Agency

ELINT	Electronic Intelligence
EM	Electromagnetic
EO	Electro-Optic
EOD	Explosive Ordnance Disposal
EPM	Electronic Protective Measures
EW	Electronic Warfare
FDM	Fused Deposition Modelling
FEL	Free-Electron Laser
FFI / NDRE	Forsvarets forskningsinstitiutt / Norwegian Defence Research Establishment
FFF	Fused Filament Fabrication
FSO	Free Space Optical communication
GAN	Generative Adversarial Networks
GIS	Geographic Information Systems
GNC	Guidance, Navigation and Control
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HALE	High Altitude Long Endurance
HTS	High-Throughput DNA Sequencing
HULC	Human Universal Load Carrier
IaaS	Infrastructure as a Service
ICL	Interband Cascade Laser
ICN	Information Centric Networking
Io(M)T	Internet of (Military) Things
IMD	Implantable Medical Device
INS	Inertial navigation systems
IO	Illuminator of Opportunities
IP	Internet Protocol
IR	Infrared
IRCM	Infrared Countermeasures
ISAR	Inverse Synthetic Aperture Radar
ISR	Intelligence, Surveillance, Reconnaissance
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
LMD	Laser Metal Deposition
LDM	Liquid Deposition Modelling
LENR	Low Energy Nuclear Reactions
LPD	Low Probability of Detection
LVC	Live, Virtual and Constructive Simulation
MCM	Mine Countermeasures

MDA	Maritime Domain Awareness
MEMS	Micro-Electro-Mechanical Systems
MIMO	Multiple-Input Multiple-Output
ML	Machine Learning
MMIC	Microwave Monolithic Integrated Circuits
MRS	Multi-Robots Systems
MSaaS	Modelling & Simulation as a Service
MUAS	Micro Unmanned Aerial Systems
MWP	Microwave Photonics
NGS	Next Generation Sequencing
NEC	Network-Enabled Capability
NFV	Network Functions Virtualisation
NISQ	Noisy Intermediate-Scale Quantum
NLP	Natural Language Processing
NUAS	Nano Unmanned Aerial Systems
OODA	Observe, Orient, Decide, Act
OM	Obsolescence Management
OTH	Over-The-Horizon
PCL	Passive Coherent Location
QCaaS	Quantum Computing as a Service
QCL	Quantum Cascade Laser
QKD	Quantum Key Distribution
QRNG	Quantum Radom Number Generator
R&D	Research and Development
PaaS	Platform as a Service
PCL	Passive Coherent Location
RAS	Robotic and Autonomous Systems
RDE	Rotating Detonation Engine
RF	Radio Frequency
RPAS	Remotely Piloted Aircraft Systems
SaaS	Software as a Service
SAR	Search-And-Rescue
SC	Supercapacitors
SDL	Selective Deposition Lamination
SI	International System of Units
SLS / SLM	Selective Laser Sintering / Melting
SMR	Small Modular Reactor
SPC	Single Photon Counting
STO	NATO Science & Technology Board

STRATCOM	Strategic Communication
TALOS	Tactical Assault Light Operator Suit
tDCS	transcranial Direct Current Stimulation
TMS	Transcranial Magnetic Stimulation
TEKNO	Technological Trends and Consequences for the Norwegian Armed Forces
TENG	Triboelectric Nano-Generators
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
UMTS	Universal Mobile Telecommunications System
USV	Unmanned Surface Vehicle
UxV	Unmanned x Vehicle
VLSI	Very Large-Scale Integration
VPA	Virtual Personal Assistant
VR	Virtual Reality
XaaS	X as a Service

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

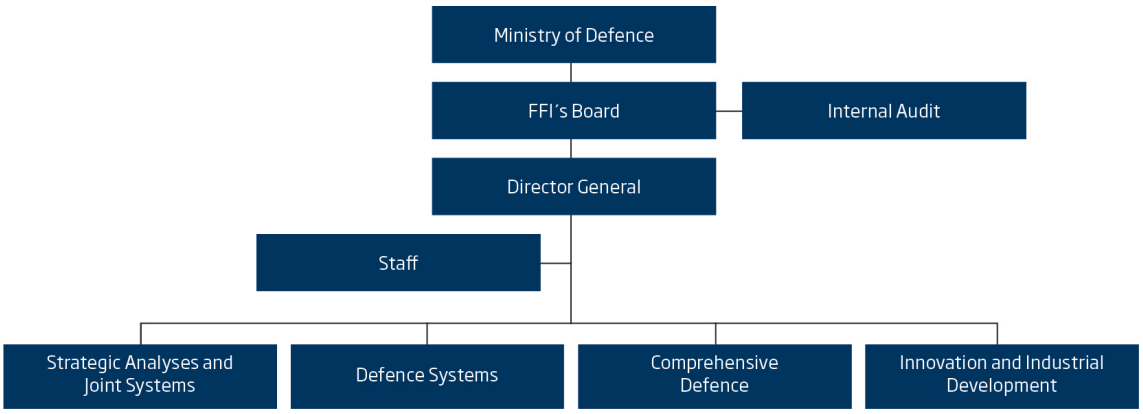
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt