Science & Technology Trends 2020-2040

Exploring the S&T Edge

NATO Science & Technology Organization

DISCLAIMER

The research and analysis underlying this report and its conclusions were conducted by the NATO S&T Organization (STO) drawing upon the support of the Alliance's defence S&T community, NATO Allied Command Transformation (ACT) and the NATO Communications and Information Agency (NCIA). This report does not represent the official opinion or position of NATO or individual governments, but provides considered advice to NATO and Nations' leadership on significant S&T issues.

D.F. Reding
J. Eaton

NATO Science & Technology Organization
Office of the Chief Scientist
NATO Headquarters
B-1110 Brussels
Belgium
http:\www.sto.nato.int

First published, March 2020

Foreword

As the world changes, so does our Alliance. NATO adapts. We continue to work together as a community of like-minded nations, seeking to develop military capabilities fit for the geostrategic challenges of today and the future. As such, NATO nations must remain at the forefront of innovation, S&T based or otherwise while facing challenges from all strategic directions and across all operational domains. To do so requires an appreciation of the potential future security environment, especially the military and security challenges presented by emerging or disruptive S&T. Drawing upon the intellectual strength and knowledge advantage of the Alliance, ***Science & Technology Trends: 2020-2040*** provides just such an assessment. The informed insights and information provided will help guide NATO at all levels and the Alliance as we prepare to evolve and adapt to the future security environment and the challenges ahead.

Science & Technology Trends: 2020-2040 provides an assessment of the impact of S&T advances over the next 20 years on the Alliance. This assessment is based on a review of selected national and international S&T foresight and futures studies; multi-national workshops; and, technology watch activities conducted by the Science & Technology Organization. I gratefully acknowledge, the collaboration and support provided by Alliance and Partner defence R&D communities, the NATO international staff, Allied Command Transformation (ACT), and the NATO Communication and Information Agency (NCIA).

Air Chief Marshal Sir Stuart Peach
Chairman of the Military Committee

Dr. Bryan Wells
NATO Chief Scientist

ToC

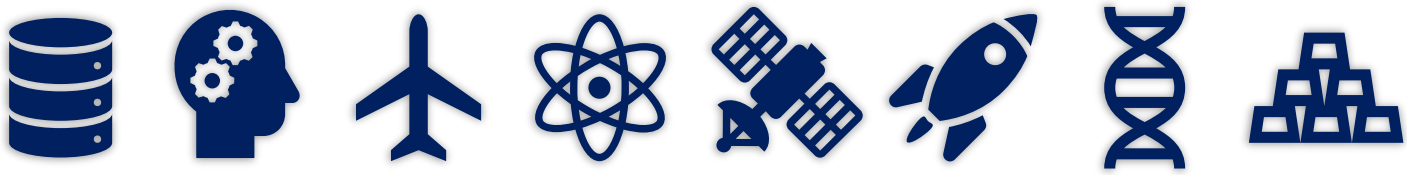


Table of Contents

Executive Summary

Science & Technology Trends: 2020-2040 provides an assessment of emerging or disruptive Science & Technologies (S&T) and their potential impact on NATO military operations, defence capabilities, and political decision space. This assessment draws upon the collective insights of the NATO Science & Technology Organization (STO), its collaborative network of over 6000 active scientists, analysts, researchers, and engineers, and associated research facilities. These insights have been combined with an extensive review of the open-source S&T futures literature and selected national research programs.

The report aims to assist current and future military and civilian decision-makers in understanding emerging and disruptive technologies (EDTs). In particular, it focuses on:

- *Why* EDTs are important to future Alliance activities;
- *How* they are expected to develop over time; and,
- *What* this will mean to the Alliance from an operational, organisational or enterprise perspective?

Ultimately, this assessment is intended to provide focus to Alliance S&T efforts and will: (1) at senior level provides an overview of the threats and opportunities presented by EDTs; (2) at a staff level, assist in guiding the design of future military concepts and capabilities; and, (3) overall, aid policymakers in preparing Alliance forces and the NATO enterprise for mission success in the future security environment.

Over the next 20 years, four overarching characteristics can be expected to define many key advanced military technologies:

- **Intelligent**: Exploit integrated AI, knowledge-focused analytic capabilities, and symbiotic AI-human intelligence to provide disruptive applications across the technological spectrum;
- **Interconnected**: Exploit the network of virtual and physical domains, including networks of sensors, organisations, individuals and autonomous agents, linked via new encryption methods and distributed ledger technologies;
- **Distributed**: Employ decentralised and ubiquitous large-scale sensing, storage, and computation to achieve new disruptive military effects; and,
- **Digital**: Digitally blend human, physical and information domains to support novel disruptive effects.

Technologies with these characteristics are bound to increase the Alliance's operational and organisational effectiveness through: the development of a *knowledge and decision advantage*; leveraging of

emergent *trusted data sources*; increased effectiveness of *mesh* capabilities across all operational domains and instruments of power; and, adapting to a future security environment replete with *cheap, distributed and globally available* technologies.
Eight highly interrelated S&T areas were considered to be major strategic disruptors over the next 20-years. The first seven EDTs were approved by Defence Ministers in October 2019, while an eighth (Materials) was added as an area for future consideration and development by the STO. These S&T areas are either currently in nascent stages of development or are undergoing rapid revolutionary development. The EDTs are:

Data *Artificial Intelligence (AI)* *Autonomy* *Space* *Hypersonics*
Quantum *Biotechnology* *Materials*

Technological development in *Data*, *AI*, *Autonomy*, *Space* and *Hypersonics* are seen to be predominately disruptive in nature, as developments in these areas build upon long histories of supporting technological development. As such, significant or revolutionary disruption of military capabilities is either already on-going or will have a significant impact over the next 5-10 years. New developments in *Quantum*, *Biotechnology* and *Materials* are assessed as being emergent, requiring significantly more time (10 - 20 years) before their disruptive natures are fully felt on military capabilities.

Disruptive effects will most likely occur through combinations of EDTs and the complex interactions between them. The following synergies and inter-dependencies are projected to be highly influential for the development of future military capabilities:

- **Data-AI-Autonomy**: The synergistic combination of Autonomy, Big Data and AI using intelligent, widely distributed, and cheap sensors alongside autonomous entities (physical or virtual) will leverage new technologies and methods to yield a potential military strategic and operational decision advantage.

- **Data-AI-Biotechnology**: AI, in-concert with Big Data, will contribute to the design of new drugs, purposeful genetic modifications, direct manipulation of biochemical reactions, and living sensors.

- **Data-AI-Materials**: AI, in-concert with Big Data, will contribute to the design of new materials with unique physical properties. In particular, this will support further developments in the use of 2-D materials and novel designs.

- **Data-Quantum**: Over a 15 - 20-year horizon, quantum technologies will increase C4ISR data collection, processing and exploitation capabilities, through significantly increased sensor capabilities, secure communications, and computing.

- **Space-Quantum**: Space-based quantum sensors, facilitated by Quantum Key Distribution communication, will lead to an entirely different class of sensors suitable for deployment on satellites. Increasingly commercial, smaller, lower power, more sensitive and more distributed space-based sensor networks enabled by quantum sensors will be an essential aspect of the future military ISR architecture in 20 years.

- **Space-Hypersonics-Materials**: Development of exotic materials, novel designs, miniaturisation, energy storage, manufacturing methods and propulsion will be necessary to fully exploit space and hypersonic environments by reducing costs, increasing reliability, improving performance and facilitating the production of inexpensive task-tailored on-demand systems.

Alliance forces and a NATO enterprise enabled by EDTs will expand the Alliance's ability to operate in rapidly evolving operational environments, such as space, cyber (including the information sphere) and urban areas. However, NATO will be challenged to ensure legal, policy, economic and organisational constraints are properly considered early on in the development of these technologies.

1. Introduction

Prediction

"Prediction is very difficult, especially if it's about the future." - *Nils Bohr* [1]

1.1 Context

NATO, as an alliance of like-minded countries, strives for peace, security, and stability across the Euro-Atlantic area. It continues to provide the essential framework for defence and security collaboration across the operational spectrum, be it collective defence, crisis management or cooperative security. But today's NATO faces a dangerous, unpredictable, and fluid security environment, with existential challenges and threats from all strategic directions including state and non-state actors; near-peer military forces; cyber threats; space; terrorism; hybrid warfare; and, information operations.

NATO is the most successful alliance in history, preserving peace and stability around the world for an unprecedented seven decades. This success is built upon the military and political framework that NATO provides for consultation, collaboration, coordination, interoperability, effective deterrence and, ultimately, united action. A key enabler of this accomplishment has been the NATO S&T community (the original NATO *innovation engine*), which has provided NATO with the intellectual and technological edge needed to ensure Alliance success across the operational and diplomatic spectrum.

Building an alliance capable of reacting to current and future needs over a broad range of potential operations requires a delicate balance between the needs of today and those of decades to come. Getting it right begins with a clear understanding of the S&T landscape, especially the enabling and destabilising role of emerging or disruptive technology (EDT). If NATO is to maintain the intellectual, technological, scientific and innovation edge [2] that it has enjoyed over the preceding 70 years, it will need to fully understand these developments, their potential use and the operational and strategic implications. Further, it will need to creatively engage the entire alliance to adapt to the associated threats and opportunities, leveraging the unmatched financial and intellectual capital available.

The Science and Technology Office (STO), plays a decisive role in supporting *innovation*; providing deep *insights* into alliance challenges; ensuring the *integration* of Alliance capabilities; and making available an *interconnected* network of science and knowledge workers capable of providing evidence-based *advice* to NATO, as well as alliance members and partners (Figure 1.1). At its core, the role of NATO's S&T community is to [3]:

> *"... maintain NATO's scientific and technological advantage by generating, sharing and utilising advanced scientific knowledge, technological developments and innovation to support*

the alliance's core tasks."

The impact S&T has had on the defence capabilities of the alliance and nations as a whole has been profound [4, 5]. Over the past 70 years, NATO has effectively employed a *strategy of technology* [6, 7], leveraging a decision and S&T advantage to significant intellectual, political, economic and military effect. However, in recent years, this intellectual and technological edge has been degraded due to many strategic, economic, social and technical challenges. The concerns about losing this technological edge are very real [4, 8].

Figure 1.1: *Five Objectives of the NATO Science & Technology Organization (STO).*

As noted by NATO Secretary General, Jens Stoltenberg [9]:

> *"NATO's technological edge has always been an essential enabler of its ability to deter and defend against potential adversaries. Our future security will depend on our ability to understand, adopt and implement technologies such as Artificial Intelligence, autonomy, and hypersonic systems. In October 2019, Defence Ministers approved an Emerging and Disruptive Technologies (EDT) roadmap to help structure NATO's work across key technology areas, and enable Allies to consider these technologies' implications for deterrence and defence, capability development, legal and ethical norms, and arms control aspects."*

1.2 Purpose

Science & Technology Trends (2020-2040) provides context for the work that will underpin the development of the EDT roadmap. The core objective is to increase the level of understanding within the Alliance of the potential for S&T developments to enhance or threaten Alliance military operations. As such, the report is an aide to decision-makers in considering:

- Why emerging and disruptive technologies (EDTs) will be important to future Alliance activities;
- How these EDTs may develop over time; and,
- What developments and potential consequences are expected for the alliance in the short, medium and long term.

Anticipating the future security environment better than potential adversaries is one way in which the alliance has maintained a competitive advantage. S&T foresight is a critical aspect of this preparation. It does not attempt to predict the future in detail (a difficult task at best, and impossible at worst), instead it seeks to provide a context for anticipating the potential development and impact of technology on future Alliance operations.

Analyses of technology trends and the associated process of technology watch are critical steps to identify new militarily important technologies and communicate the potential impact of these technologies on NATO and national leadership. Those technologies so identified hold the promise to enable the development of disruptive military capabilities for both Alliance (BLUE) and potential adversarial (RED) forces. To explore the implications of these changes the report provides an assessment of S&T trends (emerging and/or disruptive technologies) projected to impact NATO operations, capability development

and core functions over the next 20 years. These S&T areas are broad, have significant overlaps and are expected to:

- Mature over a 20 year period;
- Be transformative or revolutionary in nature; and,
- Be emergent or create generational shifts in S&T development.

The NATO Science and Technology Office (STO) has the responsibility to provide these assessments for NATO. As stated in the STO charter (2012) [3]:

> *"To fulfil its mission, the STO will ... provide advice to NATO and Nations' leadership on significant S&T issues, including the identification of emerging technologies, and the assessment of their impact on defence and security."*

1.3 Approach

This report aims to reach a wide audience, both inside and outside of NATO and its partners. We do so to stimulate a frank and open discussion as to potential opportunities and risks presented by technological developments over the next 20 years. As such, the report is based strictly on:

- Technology trends discussed in the open literature;
- A global perspective on technological progress;
- Logical reasoning informed by S&T expertise; and,

Candidate S&T trends, as well as disruptive and emerging technologies, were identified using the following considerations:

- Are likely to be realised in a non-cost prohibitive manner within the next 20 years;
- Will present a significant challenge to Alliance forces (e.g. survivability, defence, C4ISR, etc.); and,
- Will significantly impact Alliance capability or planning decisions (i.e. decision making, counter-measures, etc.)

Science & Technology Trends: 2020-2040 supersedes the *STO Technology Trends (2017)* report [10], but draws upon its foundations, insights and lessons learned. Further, the report exploits a broad range of open-source reports, internal assessments and futures studies to develop a comprehensive understanding of the future technology landscape. These sources include:

- Existing NATO S&T trend and future security environment studies, discussions and assessments;
- Technology watch activities conducted by the S&T Organisation, including existing Technology Watch Cards (TWC) (current as of Feb 2019) and Von Karmon Horizon Scans (vKHS);
- Meta-analyses and reviews of open source technology watch and futures research articles/reports, from defence, security and industry sources;
- NATO-sponsored EDT workshops and innovation system engagements; and,
- Alliance and partner EDT studies and research programs.

Taken together, and in consultation with NATO staffs, a picture of the future technological landscape was developed and a sub-set of S&T areas selected. This subset highlighted the S&T areas most likely to disrupt NATO and Alliance nations and was later consolidated with an EDT taxonomy and roadmap approved by Defence Ministers in October 2019. An additional EDT (Novel Materials and Agile Manufacturing) was added for this report. Each EDT is further broken down into capability and technology focus areas, highlighting specific areas that will require development and research. Appendix I discusses this decomposition in further detail.

In reading this report, several caveats should be kept in mind:

1. The prediction of S&T trends is a difficult task, although there is some evidence that such studies have been successful at anticipating S&T development within broad time horizons [11];

2. Technologies rarely evolve in a simple linear fashion, and complex synergies between EDTs are often as crucial as the EDTs themselves;

3. The list of EDTs provides *a* grouping of related technologies capable of technological disruption. The development of sub-technologies may be very different than the aggregate. Further, such a grouping is not unique, and one finds many such taxonomies in the literature. All such clusters, or taxonomies, are simplifications; however, this particular clustering of technologies has proven useful for our purposes; and,

4. Technology has historically driven the changing nature of human conflict, but not conflict itself [12]. In this context *"technology is neither good nor bad; nor is it neutral"* (Krazberg's First Law of Technology [13]). New technologies will inevitably be used in conflict, and it is necessary to understand how that might occur. This understanding provides a necessary first step to support technology-policy decisions, potential capability development and prepare defensive countermeasures. As such, *discussion of the impact of S&T on future NATO operations or vignettes (e.g. the Conjecture Cards presented in the appendices) should not be taken as an indication of current or future NATO S&T research efforts*.

1.4 Overview

Within the following chapters, an analysis is presented of identified, and militarily relevant S&T trends which may impact NATO capability development and operational challenges over the upcoming 20 years (2020-2040). The approach and key data sources used to conduct this assessment are described in Appendix I.

The assessment is presented in three parts:

1. An overview is provided of the general nature of S&T development. This synopsis includes a primer on S&T attention and readiness. Specific EDT areas are identified that are expected to significantly impact NATO over the period 2020-2040 (Chapter 2). These EDTs are presented separately, broadly considering the state and rate of development as well as the military implications. This overview is followed by consideration of critical potential synergies between EDTs, as it is in the overlap between these developments that significant disruptions will occur;

2. The broad strategic context and drivers are outlined that will impact defence S&T development (Chapter 3); and,

3. Separate appendices provide a more detailed exploration of each EDT, drawing heavily upon STO research and technology watch activities. This section also includes *Conjecture Cards*, short vignettes that describe the potential future application of these technologies. Earlier versions of these cards were used during workshops [14] conducted to support this analysis, and they are added to help contextualise the potential impact of these technologies.

An extensive list of useful references is provided in the bibliography at the end of this document. These are also used throughout the body of the text where appropriate. When using the Adobe PDF version of the report, *clicking* on a numbered reference will take the reader to the relevant entry in the bibliography. If desired and available, *clicking* on the provided URL (i.e. web-link) will provide an option for the reader to open the source reference directly for further study and exploration of the topic.

2. Science & Technology Trends

Anticipation
"I skate to where the puck is going to be, not where it has been." - *Wayne Gretzky* [15]

2.1 S&T Development

How can NATO explore, develop and exploit the best, cutting-edge technology able to deliver disruptive military effects for the Alliance? What do we mean by *emerging* or *disruptive* S&T. What are these emerging or disruptive technologies or scientific insights? What do they mean for an agile and innovative Alliance? To answer these questions, this chapter provides a summary of the modern technology landscape.

For purposes of this report, we narrowly define technologies as:

- **Emerging**: Those technologies or scientific discoveries that are expected to reach maturity in the period 2020-2040; and, are not widely in use currently or whose effects on Alliance defence, security and enterprise functions are not entirely clear.
- **Disruptive**: Those technologies or scientific discoveries that are expected to have a major, or perhaps revolutionary, effect on NATO defence, security or enterprise functions in the period 2020-2040.
- **Convergent**: A combination of technologies that are combined in a novel manner to create a disruptive effect.

Not all technologies or scientific discoveries are emergent or disruptive, nor is disruption driven solely by technology [4]. Further, not all emerging technologies will be disruptive; not all disruptive technologies are emergent; and, not all convergent technologies are driven by emerging ones. For this report, we focus on those technologies assessed as most likely to be disruptive over a twenty-year time-frame, including those that have moved beyond the initial exploration phase but have not yet become widely exploited. Understanding the natural pattern of EDT development is a necessary prerequisite in understanding and assessing their potential effects on NATO and the Alliance.

2.1.1 S&T Context

The *seventh generation military revolution* [16] is being driven (once again) by rapid changes in the technological landscape. Human organised conflict (war in its most extreme case) is, in a Clausewitzian

sense, a fundamental clash of wills between large social groups (e.g. states, pseudo-states, communities, societies, etc.). During such conflict, whether with peer competitors or asymmetric threats, technology is an *edge* [17] to be exploited. As democratised technology becomes even more central to human existence, so too will it gain an outsized role in shaping conflict. As noted by General Sir Richard Barrons [18], former commander of Joint Forces Command (UK):

> *"The same wide span of Fourth Industrial Revolution technology (data, processing, connectivity, AI, robotics, bio-sciences, autonomy and so forth) that is changing how we live, work and play will now transform the way war is waged - in a process spanning at least a generation ... Military transformation will largely be about the rapid adoption and adaptation of civil-sector-derived technology and methods in disruptive military applications ... The future of military success will now be owned by those who conceive, design, build and operate combinations of information-based technologies to deliver new combat power."*

Within a broad strategic and geopolitical context (see Chapter 3) the nature of conflict is seen to be changing, with general agreement that the transforming technological environment is a significant factor [19, 20, 21, 22, 23, 24, 25]. This changing nature of conflict manifests itself in *hybrid war* [26, 27], *hyper-war* [28], *memetic warfare* [29] or *next-generation conflict* [30]. In each, disruptive technologies are merged with existing technologies and military capabilities to create new ways and means of engaging in conflict.

The common factors that link these Fourth Industrial Revolution technologies are that they are all in some way shape or form *intelligent*, *interconnected*, *distributed* and *digital* (I2D2) in nature. More specifically, and building on [31, 32, 33], we note that the future S&T landscape will be characterised (and at the same time driven) by the following:

- **Intelligent**: Integrated and integral artificial intelligence, analytics and decision capabilities across the technological spectrum.
  - **Autonomy**: Artificial intelligence-enabled autonomous systems capable of some level of autonomous decision making. Such autonomous systems may be robotic, platform based or (digital) agent-based.
  - **Humanistic Intelligence**: The seamless integration of psycho-social-techno systems supporting enhanced human-machine teaming and synergistic behaviours.
  - **Knowledge Analytics**: Advanced analytical methods (including AI) exploring large data sets and advanced mathematics to provide insights, knowledge and advice hitherto impractical.
- **Interconnected**: Exploitation of the network (or mesh) of overlapping real and virtual domains, including sensors, organisations, institutions, individuals, autonomous agents and processes.
  - **Trusted Communications**: The use of technologies such as distributed ledger technologies (e.g. blockchain), quantum key distribution (QKD), post-quantum cryptography and AI cyber-agents to ensure trusted interactions and information exchange.
  - **Synergistic Systems**: The development of mixed (physical or virtual) complex systems-of-systems allowing for the creation of novel ecosystems (e.g. smart cities).
- **Distributed**: Decentralised and ubiquitous large scale sensing, storage, computation, decision making, research and development.
  - **Edge Computing**: Embedding of storage, computation and analytics/AI into agents and objects close to information sources.
  - **Ubiquitous Sensing**: Embedding of low (or lower cost) sensors to create large sensor networks across the human-physical-information domains.

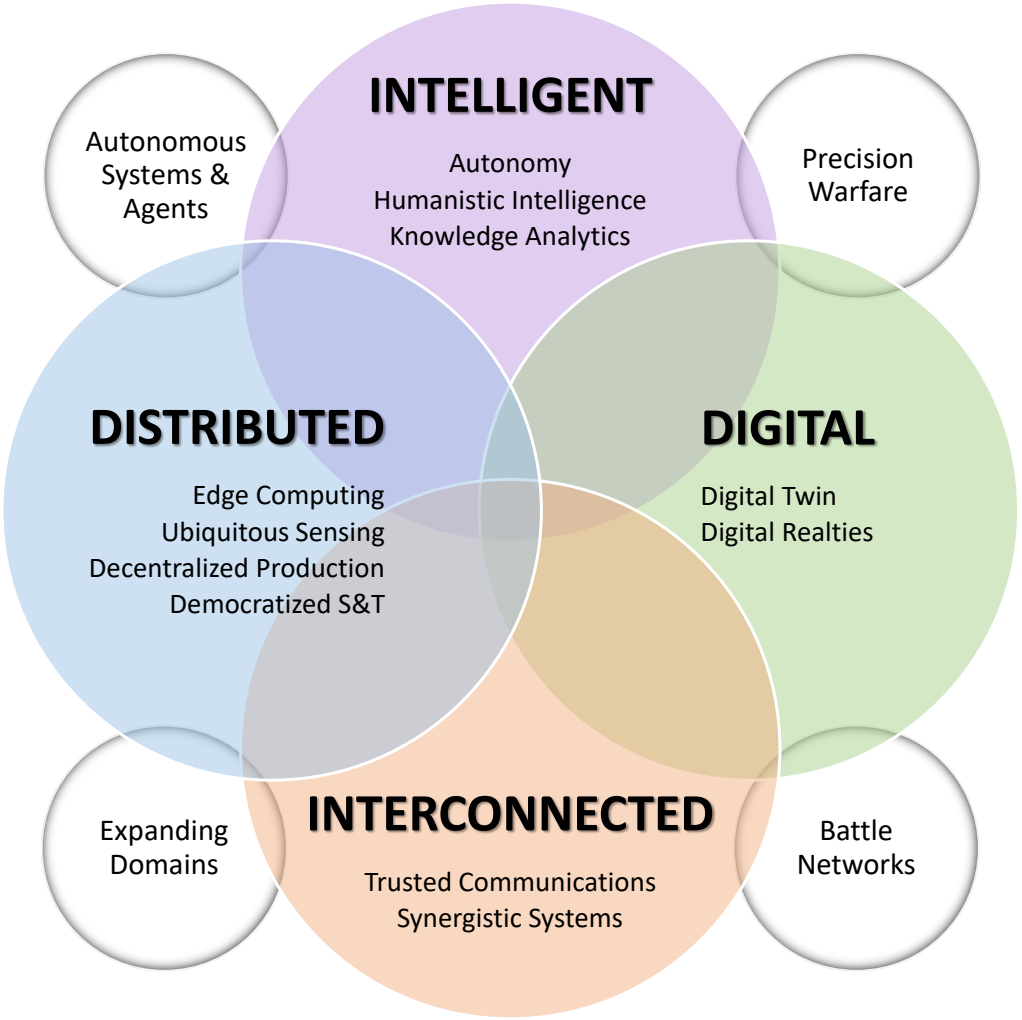


Figure 2.1: *Intelligent-Interconnected-Distributed-Digital (I2D2) with associated military trends.*

  - **Decentralised Production**: Exploitation of AI-assisted design, novel materials, and (mixed material) 3D/4D printing technologies, to support just-in-time local digital manufacturing and production.
  - **Democratised S&T**: Reducing costs of design and production, increasing computational capabilities and the broad availability of S&T information will increase innovation and the generation of novel science.

- **Digital**: Blending of the human, physical and information domains to create new physiological, psychological, social and cultural realities.
  - **Digital Twin**: A digital simulacrum of physical, biological or information entities digitally linked (often in near real-time) to the original, supporting predictive analytics, experimentation and assessment.
  - **Synthetic Realities**: The creation of new perceived cognitive or physical realities based on the integration of psycho-socio-technical systems. Such realities may be augmented, virtual, social or cultural in nature.

New EDTs do not arrive fully formed, nor are they divorced from the military operational environment in which their use is contemplated. Effort, experimentation and innovation are needed to turn these EDTs into actionable military capabilities, and these, in turn, will force changes to Alliance forces and force

structure. Each of the four identified technology characteristics combine to drive a specific military trend (Figure 2.1) [34]:

- **Intelligent + Distributed ⇒ Autonomous Systems and Agents**: Intelligent and, increasingly autonomous systems, are already supplanting and exceeding the capabilities of human forces. Autonomous systems to date have been quite limited, employing fixed rule-sets and various levels of direct human-control. The increased use of AI will enable autonomous systems capable of significantly more sophisticated decision making, self-directed activity and, at the same time, increasingly complex human-machine teaming. Such increased used of intelligent agents will dramatically expand into our synthetic realities, including cyber, battle networks [34, 35, 36] and digital social networks. Autonomous agents will provide rapid analysis, advice and courses-of-action for strategic-operational-tactical planning, allowing for increased OODA (Observe-Orient-Decide-Act) loop effectiveness and bringing an entirely different perspective on old problems unconstrained by old strategies. Such intelligent battle networks have the potential to increase decision speeds to levels that will require new methods of human-machine interaction and visualisation. The resulting competition between battle networks will generate increased evolutionary pressures on algorithms, each seeking an edge or combination of effects that will lead to a decisive victory. Similarly, autonomous vehicles so enabled will increase their effectiveness across the conflict spectrum, creating large mesh sensor and strike networks.

- **Interconnected + Digital ⇒ Battle Networks** : Evolving agile and adaptive mesh C4ISR networks will create deep operational dependencies underlying military action. Such evolving battle networks will increasingly become targets in and of themselves and subject to effects based conflict. This increased reliance on seamless and ubiquitous connectivity will increase the value in targeting such networks (military or civilian) in disinformation, cyber or physical manner. Such attacks may be implemented long before the conflict itself is initiated, and could strike indirectly at logistic, personnel, information, financial or other supporting elements of modern operational and strategic networks.

- **Interconnected + Distributed ⇒ Expanding Domains**: As the operational environment expands to include space, cyber and the broader information sphere, the need to think, plan and operate in a widely dispersed, interconnected and multi-domain manner will become even more critical. The growing numbers and wide distribution of multi-domain sensors, multi-domain missions, and the rising processing capabilities increasingly embedded at the edges of the networks, will present new demands for dominance, counter-domain capabilities, protection, counter-measures, counter-counter-measures and other secondary functions. The increase exploitation of new domains will inevitably lead to the search for *domain superiority*, with attendant costs and capability demands.

- **Intelligent + Digital ⇒ Precision Warfare**: Increased digitisation across C4ISR capabilities, along with miniaturisation, edge processing and falling costs, have been the underpinning technological developments enabling increasingly intelligent, interconnect and distributed systems. In aggregate, this has dramatically increased the development of precision strike and effects orient capabilities. Swarming and the use of lower-cost cheap precision weaponry has and will continue to put large high-value capabilities at risk, while increased digitalisation opens up new and hitherto unanticipated vulnerabilities. New sensors (e.g. quantum technology-enabled), increased reliance on synthetic realities (virtual, social, mixed, twinned, etc.) will present risks and opportunities. The use of more and more sophisticated analytical tools, leveraging the increased volumes of digital data, will lead to the development of new operational capabilities (e.g. novel hypersonic weapon designs developed using increasingly higher-fidelity computational fluid dynamics models and embedded sensors).

AI will change the landscape of warfare, while the availability of digital data will allow distributed and interconnected (autonomous) systems to analyse, adapt and respond. These changes will, in turn, potentially support better decision-making through predictive analytics [37]. All of this will take place in

a context of synergistic and symbiotic systems-of-systems, including sensors, societies, and organisations. In this way, EDTs will continue to change the ways and means of conflict for at least a generation, but at the same time will need to integrate and operate alongside existing systems.

2.1.2 Synergy

To maintain a military-technological edge and to prevail in future operations, NATO forces must continually evolve, adapt, and innovate in order to be credible, networked, aware, agile, and resilient [24]. Such adaptation is most rapid and disruptive where EDTs work to enable one another or where the human, information or physical domains overlap [38]. Several such critical synergistic connections are identified later in this report.

In addition to interconnections between EDTs, it should be noted that many of the issues driving and limiting the effective development of new capabilities are non-technical. Murray [39, 40] notes that:

> *"What matters in the technological adaptation as well as technological innovation is how well new and improved technologies are incorporated into effective and intelligent concepts of fighting: it is not the technological sophistication that matters, rather it is the larger framework."*

For active development of EDTs into Alliance capabilities, the implications of culture, concepts, risk-tolerance, organisational structure, policies, treaties, human capital and ethics must be fully appreciated. These factors will need to evolve as much as the technology if EDTs are to be fully developed into new operational capabilities.

2.2 Assessment

To understand the state and rate of EDT development, it is necessary to consider several perspectives on each EDT: **(1)** the potential military impact; **(2)** the level of *attention* or *hype* around a particular technology or scientific area; **(3)** the current technology readiness level; **(4)** the time horizon in which the science or technology is expected to be fully mature; **(5)** the relevance to NATO operational capabilities; and, **(6)** the S&T domains relevant for enabling research.

Such an assessment is problematic as each EDT encompasses many different core aspects, each potentially at a different stage of development. As a result, for this report, each EDT is broken into several areas identified for focused development, or (emerging and disruptive) *technology focus areas*.

2.2.1 Impact

Assessing the potential impact of emerging or disruptive technologies is not a straightforward process. To do so successfully requires consideration of the threat environment (current and future), legal & policy constraints, political factors, investment decisions, as well as estimating the potential for organizational uptake (i.e. entrepreneurial drive and risk tolerance) [41]. These estimates are further compounded if the road to disruption involves complex combinations of such technologies (i.e. synergies) or requires new concepts to be developed.

For purposes of this report we follow [41], defining *Impact* in a somewhat subjective and imprecise manner as (Table 2.1):

Table 2.1: *EDT Impact.*

Scale	**Performance**: speed, range, accuracy, lethality, survivability, affordability, availability, dependability or other defining capability characteristic
Moderate	10 - 50 %
High	50 - 100 %
Revolutionary	Greater than 100%, or conducting activities or tasks hitherto deemed impractical or impossible

Assessments are based on a variety of sources, including a review of previous trends assessments [20, 24, 33, 41, 42, 43, 44, 45], workshop results [14] as well as STO technology watch activities and reports (e.g. [46]).

2.2.2 Attention

Technological development is distinctly cyclic on many levels. The most well-known of these cycles is the *Gartner Hype Cycle* [31] (Figure 2.2), itself based on Howard Fosdick's work on the sociology of technology adoption [47, 48].

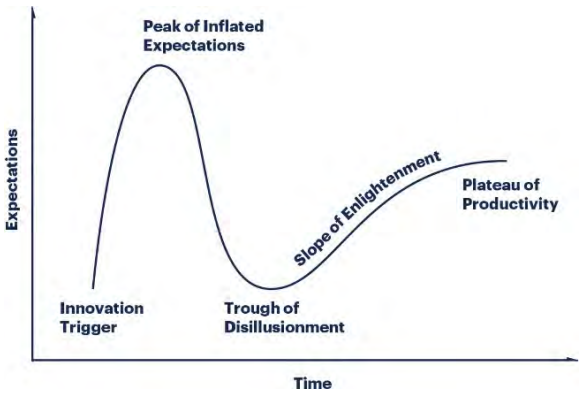


Figure 2.2: *The Gartner Hype Cycle.*

Technologies do not always progress from beginning to the end of such a cycle; indeed most technologies *fail*. Many avenues of science or technological discovery never breakthrough to ignite innovation, or they disappear from public consciousness after initial enthusiasm as unproductive avenues of development, or they may appear later on as new convergent developments reinvigorating an old idea. Finally, even successful technologies may reappear as novel ideas create innovation triggers and old technologies becomes so integrated into production systems that the original connection is lost on all but the most technically minded. Such an evolutionary process built on *heroic failures* [49] or *creative errors* is essential to scientific and technological progress, as lessons and ideas that arise will often lead to entirely new areas for exploration, innovation and development.

During a hype cycle, a successful trending technology will (arguably) ultimately go through five key phases: [50, 51]:

- **Innovation Trigger**: After a long period of supporting research, a potential new technology breakthrough starts to show promise. This initial innovation trigger builds upon early experimentation, results in proof-of-concept stories and media interest is triggered. This spark yields growing publicity and internet search activity. At this stage, no viable product exists, and commercial viability remains unproven.

- **Peak of Inflated Expectations**: Early publicity produces many success stories — often accompanied by scores of failures. Interest (e.g. as measured by web searches) is at an all-time peak. Some innovative companies take action; many do not.

- **Trough of Disillusionment**: The limitations of the technology become clear, and some implementation efforts fail to produce useful results. As a result, general interest falls, and negative stories become more frequent, although these may be overly pessimistic. Eventually, some developers and producers move onto other areas or fail outright. A bifurcation occurs at this point, where investment and continued developments occur only if continued progress can be shown through the refinement of the underlying technology, development of a better understanding of where this technology is most applicable or a convergence of other technologies or demand. If this does not happen, the technology will eventually be deemed *unproductive* and disappear entirely from consideration, or return to the *start gate* to await further developments, technological convergence or changing circumstances.

- **Slope of Enlightenment**: With a better understanding of what is practical and where it can be best applied, the potential begin to crystallise and become more widely understood and appreciated. Next-generation products occur, and positive attention begins to increase with more and more successful trials and pilot products. Some companies remain cautious.

- **Plateau of Productivity**: Mainstream adoption occurs. With a better understanding of value, applicability and limitations, the technology has found its market. Issues and new ideas may still arise, potentially kicking off a new cycle. Otherwise, the technology becomes so well integrated into the technological landscape that its use becomes common-place until it is supplanted by a new technological advance.

Balancing out the highs of *inflated expectations* and the lows of the *trough of disillusionment* is a critical task in making investment and long term capability decisions. The Gartner Hype Cycle is useful for this purpose. Nevertheless, while the approach is well known, there are noted flaws in its use as an assessment and decision tool [47, 52, 53]. In particular, the exact placement of technology on such a curve is problematic, as is the focus on hype rather than a measurable quantity such as attention. Therefore, generalising from [48], we will simplify the assessment and describe the state of technological attention and understanding in broad categories only. These categories are: **Trigger**: New technology or scientific discovery; **Expectation**: Increasing publicity and discussion; **Disillusionment**; Exploring limitations; **Enlightenment**; Understanding utility; and, **Productivity**; Mature Application.

This report assesses *technological attention* through a review of Gartner technology assessments [31], other technology futures analyses already mentioned, STO technology watch activities, and an analysis of web search activity drawn from Google Trends [54] (see Appendix I.6).

2.2.3 Technological Maturity

In general successful S&T proceeds along a developmental path captured in the use of a *technology readiness levels (TRL)*, originally developed by NASA [55, 56], with each step being a potential *off-ramp* or *pause* for that particular technology (see Table 2.2). These levels provide a useful *shorthand* for interpreting technology maturity level and, as such, are widely used within industry and government.

Table 2.2: *Technology Readiness Levels.*

TRL 9	Actual system proven through successful mission operations.
TRL 8	Actual system completed and qualified through test and demonstration.
TRL 7	System prototype demonstration in a space environment.
TRL 6	System/subsystem model or prototype demonstration in a relevant environment.
TRL 5	Component and/or breadboard validation in relevant environment.
TRL 4	Component and/or breadboard validation in laboratory environment.
TRL 3	Analytical and experimental critical function and/or characteristic proof-of-concept.
TRL 2	Technology concept and/or application formulated.
TRL 1	Basic principles observed and reported.

Technologies, or the underlying sciences, may be unsuccessful in generating new operational capabilities or pause at any point along the path to TRL 9+ due to several factors, including interconnectedness or dependencies on other technologies, costs, ethics, policies or fundamental physical, information or human limits. However, unsuccessful developments are critical within S&T to inform and ultimately give rise to new approaches and technologies that may themselves be more successful in moving from basic principles to operational capabilities.

We assess the current TRL levels primarily through assessments made within the STO Technology watch activities, related futures assessments and reference to several available TRL calculators [57]. It should be noted that emerging technologies are usually in the range of TRL 1 through 5 [58].

2.2.4 Capability

For NATO, EDTs are primarily of interest through their influence on current and future Alliance defence capabilities. To better connect EDTs to their military impact, each EDT is evaluated for its potential effect on NATO operational capabilities. NATO's operational capability taxonomy ([59] provides a structured list of capabilities and sub-capabilities. An assessment is presented for the first level of the operational taxonomy only: Prepare, Project, Engage, C3, Sustain, Protect, and Inform. This assessment is presented

later in this chapter for each EDT, and in Appendices A - H. The evaluation employs a 3-point scale describing low, medium or high impact on the performance of the associated operational capability (Table 2.3). Such a subjective assessment provides a preliminary appraisal of potential disruptive effects.

Table 2.3: *EDT Impact on NATO Capabilities.*

Relevance: The impact of this EDT on current and future operational capability is expected to be ...	
Low	Limited and secondary in nature.
Medium	Moderate overall, or of significant relevance to a limited subset only.
High	Significant or revolutionary impact.

2.2.5 S&T Domains

Defence Science is broadly broken into three large domains, encompassing research in the human (including biological), information and physical S&T domains [60, 61]. Linking EDTs to these three major areas of scientific inquiry helps to ensure a holistic approach to research, development and operationalisation of an EDT. This assessment is provided later in this chapter and in Appendices A - H. The evaluation employs a 3-point scale describing low, medium or high alignment or relevance (Table 2.4) of this research area to NATO in the development of the EDT.

Table 2.4: *EDT Connection to S&T Domains.*

Relevance: The relevance of EDT research in this S&T domain to NATO ...	
Low	Limited and secondary in nature.
Medium	Moderate overall, or of significant relevance to a limited subset only.
High	Significant relevance.

2.3 Disruptive Technologies

2.3.1 Data: Big Data and Advanced Analytics (BDAA)

(Big) Data and Advanced Analytics (BDAA)

Big Data describes data that presents significant volume, velocity, variety, veracity and visualisation challenges. Increased digitalisation, a proliferation of new sensors, new communication modes, the internet-of-things and virtualisation of socio-cognitive spaces (e.g. social media) have contributed significantly to the development of Big Data. *Advanced (Data) Analytics* describes advanced analytical methods for making sense of and visualising large volumes of information. These techniques span a wide range of methods drawn from research areas across the data and decision sciences, including artificial intelligence, optimisation, modelling & simulation (M&S), human factors engineering and operational research.

Figure 2.3: *Big Data and Advanced Analytics.*

Since the beginning of the 1960s, our world has become increasingly digital and virtual. For the next 20 years, this trend is expected to accelerate and to have a fundamentally disruptive effect on Alliance operations and capabilities. Data sets of a magnitude that are difficult to handle logistically (a definition that it must be noted changes yearly) due to increasing *volume*, *velocity*, *variety*, *veracity* and *visualisation* issues will present significant technical, organisational and interoperability challenges. Distributed sensors, autonomy, new communication technologies (e.g. 5G), increased use of space, virtual socio-cognitive spaces, digital twins and the development of new and

expanded analytical methods will increase our ability to *understand* the human, physical and information spaces around us. BDAA is the enabling technology for all EDTs and will be central to their exploitation for enhanced military capabilities. AI, in particular, requires high-quality training data to develop new algorithms and applications.

For NATO BDAA will enable increased operational efficiency, reduced costs, improved logistics, real-time monitoring of assets and predictive assessments of campaign plans. At the same time, it will generate significantly greater situational awareness at strategic, operational, tactical and enterprise levels. These applications will lead to a deeper and broader application of predictive analytics to support enhanced decision making at all levels. It has the potential to create a knowledge and *decision advantage*, which will be a significant strategic disruptor across NATO's spectrum of capabilities. There is the potential to significantly impact NATO's kinetic and non-kinetic targeting effectiveness through the use of cheap widely distributed sensors (as part of the internet-of-things (IoT)), linked by new communication protocols (such as 5G), building on analyses and dissemination of critical information in real-time. Potential peer or near-peer adversaries will seek a similar technical edge, while asymmetric threat actors will exploit increasingly open and available sources of data for targeted effect or disruption.

Industry is investing heavily in BDAA and will continue to lead in the overall development and application. The effectiveness of this investment underlies the current knowledge economy. Nevertheless, the unique needs of NATO military forces will require the development of methods and standards for inter-operability, sharing, collection, modelling & simulation, analysis, classification, curation, communication and data management. Finally, it is not a given that more data and advanced algorithms will ultimately produce better decisions. Understanding the complex socio-cognitive-technical context around decision making and the proper role and integration of BDAA in this context will be essential to developing a NATO decision advantage.

Appendix A provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.5: *Big Data and Advanced Analytics (BDAA) 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Data	Advanced Analytics	Revolutionary	Expectation	4	2025
.	Communications	High	Enlightenment	6	2030
	Advanced Decision Making	Revolutionary	Disillusionment	6	2025
	Sensors	High	Expectation	4	2030

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.3.2 Artificial Intelligence (AI)

Artificial Intelligence

Artificial Intelligence (AI) refers to the ability of machines to perform tasks that normally require human intelligence – for example, recognising patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems [62].

The availability of big data has driven both the development of and the need for AI. Starting in the mid-1950s, AI has moved through three primary development cycles. As a result, AI (e.g. expert systems and machine learning) algorithms are already deeply embedded in modern technology. However, in 2012 there was a significant leap forward in their application to practical problems, driven by improvements in underlying algorithms (deep learning) and the wide availability of sizeable publicly available training sets.

In concert with BDAA, AI has the potential for revolutionary impact on NATO operations and capabilities. AI is the fulcrum around which big data will be turned into actionable knowledge and,

ultimately, a NATO decision advantage. Integration of AI into combat models & simulation, enterprise systems, decision support systems, cyber defence systems and autonomous vehicles will allow for rapid and more effective human-machine decision making. Use of AI on sensors to pre-process information and provide adaptive use of frequencies (e.g. cognitive radar) and bandwidth will paradoxically lead to a decrease in communication traffic. AI will also have a significant effect on the conduct of NATO S&T efforts as meta-analyses of existing research will expose new discoveries, identify promising research areas and provide improved S&T tools to support further research.

Figure 2.4: *Artificial Intelligence.*

In the commercial world, AI is a priority R&D area, with many nations making significant investments. Business is the primary driving force behind AI, although research is often based on widely available open-source tools and publicly available data [63, 64]. The brittle nature of most existing applications and the need for explainable AI are just two serious technical challenges that remain to be overcome. Complex problems associated with human-AI teaming and psycho-socio-technical issues will also need to be considered, but hold the promise of revolutionary applications. Notwithstanding these limitations, by 2030, it is estimated that the contribution of AI to the global economy will be $15.7 trillion (USD) [65].

The development of Artificial General Intelligence (AGI, i.e. human-level generalised intelligent behaviour), presents a significant (and potentially impossible) technical challenge, in-spite of over 60 years of AI research. It is considered unlikely that AI systems will meet this level of cognitive ability within the next 20 years.

Policy, legal, and interoperability challenges will be serious challenges for NATO. Ensuring AI advice is trusted, ethical and consistent with national rules-of-engagement (ROE) will require AI approaches with a strong emphasis on *explainability*, *trust* and human-AI *collaboration*. Further, it will be necessary, especially in the context of Alliance operations, to define processes and standards for verification, validation and accreditation (VV&A) of such AI systems.

Figure 2.5: *Artificial Intelligence in the Real World (CREDIT: DARPA).*

Appendix B provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.6: *Artificial Intelligence: 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Artificial Intelligence	Advanced algorithms	Revolutionary	Expectations	4	2030
	Applied AI	Revolutionary	Expectation	6	2030
	Human-Machine Symbiosis	High	Trigger	4	2035

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.3.3 Autonomy

Autonomy

Autonomy is the ability of a system to respond to uncertain situations by independently composing and selecting among different courses of action in order to accomplish goals based on knowledge and a contextual understanding of the world, itself, and the situation. Autonomy is characterised by degrees of self-directed behaviour (levels of autonomy) ranging from fully manual to fully autonomous [66, 67, 68]. *Robotics* is the study of designing and building autonomous systems spanning all levels of autonomy (including full human control). *Unmanned Vehicles* may be remotely controlled by a person or may act autonomously depending on the mission. Applications include access to *unreachable* areas, persistent surveillance, long-endurance, robots in support of soldiers, cheaper capabilities, and automated logistics deliveries.

The history of autonomous systems in defence is a long one going back to at least 1898 with Nikola Tesla's demonstration of a wireless remotely operated unmanned boat [69]. However, there has been a significant push over the last 20 years to use system autonomy across a wide variety of physical and virtual environments. The success of these efforts is seen in the increased use of platform autonomy (UxVs), with ISTAR (intelligence, surveillance, targeting and reconnaissance) and precision strike platforms being increasingly common in operations. The ultimate objective has always been to unite the human and autonomous system (at whatever level of independent operation) into a formidable team, allowing the automated system to take on *dull*, *dirty*, *dangerous* and *dear* tasks (the four D's of robotization) [70]. The underlying motivation is to decrease costs, reduce manning, improve operational effectiveness and reduce casualties.

Figure 2.6: *Autonomous Systems (CREDIT: CMRE).*

Approaches to autonomy may range from fully-autonomous to semi-autonomous or even unmanned systems. Specific levels of autonomy are a function of sensors, mission type, communication links, on-board processing and legal/policy constraints. The drive for more and more semi-autonomous and fully autonomous systems in operations will dramatically expand future NATO capabilities into an environment where every soldier acts as a company, every ship as a task group and every aircraft as a squadron.

Autonomous systems development is primarily driven by operational needs such as high-altitude-long-endurance (HALE), increasing levels of integrated AI, and human-machine factors (i.e. how to make the overall human-machine team/system more effective while retaining necessary human oversight and decision making). In particular, legal, policy and interoperability considerations will challenge the use of autonomous systems across the kill-chain. Nevertheless, given the operational advantages to both NATO and potential adversaries, there is little doubt that the use of autonomous systems will significantly enhance, threaten and enable operational capabilities over the next 20 years.

Appendix C provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.7: *Autonomy 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Autonomy	Autonomous Systems	Revolutionary	Expectation	6	2025
	Human-Machine Teaming	Revolutionary	Trigger	4	2030
	Autonomous Behaviour	High	Expectation	4	2030
	Countermeasures	High	Disillusionment	5	2025

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.3.4 Space Technologies (ST)

Space Technologies
Space is generally considered to begin 90 - 100 km (the Karman line [71]) above sea-level. *Space Technologies* exploit or must contend with the unique operational environment of space, which includes: freedom of action, global field of view, speed, freedom of access; a near-vacuum; micro-gravity; isolation; and, extreme environments (temperature, vibration, sound and pressure).

Figure 2.7: *The Alliance from Space.*

Humankind has been making effective use of space for over 60 years. However, two interrelated and interacting trends have emerged that are driving an explosion in the exploitation of space and space-based assets. First, the global commercial space industry has taken a leading role not just in the development of satellites, but increasingly in sensors, communications and launch. This trend has led to dramatic decreases in launch costs, new options for the deployment of space-based assets, and the near real-time commercial availability of high-quality space-derived information (EO/IR, SAR and ELINT). Second, new technologies and manufacturing methods have changed the nature, availability and costs of using space [e.g. 3-D printing [72]]. Such technologies included new propulsion options such as advanced electric propulsion systems, on-board AI, advanced robotics, on-orbit remote servicing of satellites, system miniaturisation (enabling smaller and cheaper satellites), improved and novel sensors, 3D-printing, improved power storage and efficiency, and next generation encryption technologies. As a result, space is becoming increasingly commercial, congested, contested and competitive [73, 74].

Use of space for C4ISR, navigation and defence is central to many of NATO's existing capabilities, and ultimately it is the foundation upon which NATO has built a technological edge. This use of space and space-derived data will only increase over the next 20 years, enabling increasingly capable and ubiquitous C4ISR capabilities. Combined with BDAA and AI, this has the potential to significantly improve situational awareness at all levels, support near real-time assessments of operational effectiveness and increase targeting success. However, as more and more Alliance capabilities come to rely on these assets, the risks from ASAT (anti-satellite) or robotic parasitic systems will become more acute. Increasingly congested orbits, increased use of large constellations of smallsats and increasing levels of space debris will impact the effectiveness and reliability of space-based systems [75].

Many nations have significantly increased their presence in and access to space. Nevertheless, commercial developments and the increased use of space derived data are expected to dominate events over the next 20 years. Increasingly powerful smallsats and large scale constellations/swarming will facilitate increased used of space while posing significant policy and legal issues. These legal and policy challenges include conflicts between commercial, academic and military use; governance of the global (space) commons; and, the potential for the increased militarization of space.

Appendix E provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.8: *Space (Systems) 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Space	Platforms	Moderate	Expectation	6	2025
	Operations	Moderate	Expectation	5	2030
	Sensors	High	Trigger	3	2035

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.3.5 Hypersonic (Weapon Systems) (HWS)

Hypersonics (HWS)

(Advanced) Hypersonic Weapons Systems (missiles, vehicles, etc.) operate at speeds greater than Mach 5 (6125 kph). In such a regime, dissociation of air becomes significant, and rising heat loads pose an extreme threat to the vehicle. Hypersonic flight phases occur during re-entry from space into the atmosphere or during propelled/sustained atmospheric flight by rocket, scramjet or combined cycle propulsion. This class of weapon system includes air-launched strike missiles (HCM), manoeuvring re-entry glide vehicles (HGV), ground-sea *ship killers*, and post-stealth strike aircraft. Systems of this nature may rely primarily on kinetic effects alone or may include supplemental warheads (nuclear or non-nuclear). Countermeasures against individual, salvoed or swarms of hypersonic systems are particularly challenging due to their speed and manoeuvrability. [45].

Research on hypersonic systems goes back 70 years to the start of the space age. Still, recent developments and testing have increased the likelihood of operational hypersonic weapons being developed and deployed within the next ten years. There are four types of hypersonic systems typically discussed: (manoeuvring) hypersonic glide vehicles (HGV); air-breathing hypersonic cruise missiles (HCM); Hypersonic rail guns [76]; and, hypersonic crewed aircraft. The primary focus of this EDT will be on missile systems (HGV and HCM).

New materials and propulsion methods have enabled recent developments in hypersonic research and have greatly increased the likelihood of their wide operational use [77]. China, Russia, US, UK, France, India, Japan and Australia all have openly acknowledged research and testing of hypersonic systems [78]. These systems are particularly strategically disruptive given the reduced reaction times available for ITWAA (Integrated Tactical Warning/Attack Assessment), the difficulty in developing countermeasures, and the threat they pose too high valued targets individually or en masse [45].

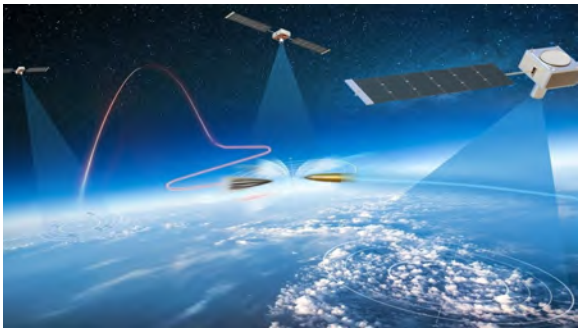


Figure 2.8: *Hypersonic Glide Vehicle (HGV) Defence (CREDIT:Northrup-Grumman).*

For NATO hypersonic capabilities would provide increased effectiveness (lethality and response) against priority ground and naval targets. Due to the high speeds involved, they may also dispense with warheads, relying entirely on mass and kinetic energy, thus simplifying weapon design. Such speeds will increase the odds of a successful strike and reduce the risks of interception. U.S. systems are expected to fielded by 2025, with hypersonic drones following by 2035 [79, 80]. Both China and Russia have demonstrated advanced supersonic programs [81, 82] and limited fielding of hypersonic weapons.

More worryingly, these advantages are available for a peer or near-peer adversary with hypersonic weapons. Given the high costs associated with developing hypersonic systems, it is unlikely that they will be available in this period to asymmetric antagonists.

Hypersonic weapons present considerable challenges to strategies and technologies for defensive countermeasures. This challenge is particularly acute due to the speeds involved and the possibility of large swarms. Countermeasures, employing soft kill approaches (e.g. jamming, deception, etc.) may be useful to some extent. Nevertheless, directed energy weapons (high energy lasers or particle beam) or space-based interceptors provide the best overall hope of a hard kill. These systems will need to be refined and be made operational, within the appropriate policy and legal constraints, if effective defensive countermeasures are to be deployed over the next ten years.

Appendix F provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.9: *Hypersonic (Systems) 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Hypersonics	Platforms and Propulsion	High	Trigger	5	2025
	Countermeasures	High	Trigger	3	2030

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.4 Emergent Technologies

2.4.1 Quantum (Technologies) (QT)

Quantum Technologies (QT)

Next-generation *quantum technologies* exploit quantum physics and associated phenomena at the atomic and sub-atomic scale; in particular quantum entanglement and superposition. These effects support significant technological advancements primarily in cryptography; computation; precision navigation and timing; sensing and imaging; communications; and, materials.

Quantum mechanics counts its origins from the beginning of the last century and is generally used to describe the behaviour of matter at the atomic scale (less than $10nm$). Quantum phenomena underlie much of modern technology including the transistor, nuclear energy, electron microscopes, superconductivity, photoelectric detectors, medical imaging (functional magnetic resonance and positron emission imaging), lasers and solid-state devices. Over the last ten years, quantum phenomena, in particular, superposition and entanglement, have been used to develop novel emergent technologies. These *next-generation developments* include: ultra-sensitive sensors; incredibly accurate clocks; *unbreakable* encryption and communications; and, quantum computing [46, 83, 84, 85, 86, 87, 88].

Although new quantum technologies have the potential for revolutionary impact on NATO operations, most (but not all) are in early stages of development, and significant technical challenges lie ahead before operational systems will be developed. The use of ultra-sensitive gravimetric, magnetic or acoustic sensors will significantly increase the effectiveness of underwater warfare capabilities, potentially rendering the oceans transparent [90]. Quantum radar [91, 92, 92] has the potential to make stealth technologies obsolete, provide more accurate target identification, and allow covert detection and surveillance. Accurate clocks will enable the development of (precision) positioning, navigation and timing (PNT) systems for use in GPS denied or inaccessible areas (e.g. under-ice). Unbreakable quantum key encryption will support substantially more robust and secure communication. Quantum computing, potentially the most disruptive quantum technology of all, has the potential to render previously untenable classical computational tasks in areas such as optimisation, BDAA, AI, and modelling & simulation viable. This computational edge has the potential to increase the decision making and operational effectiveness of NATO forces significantly, as well as render current encryption techniques and encrypted data *crack-able* for the first time.

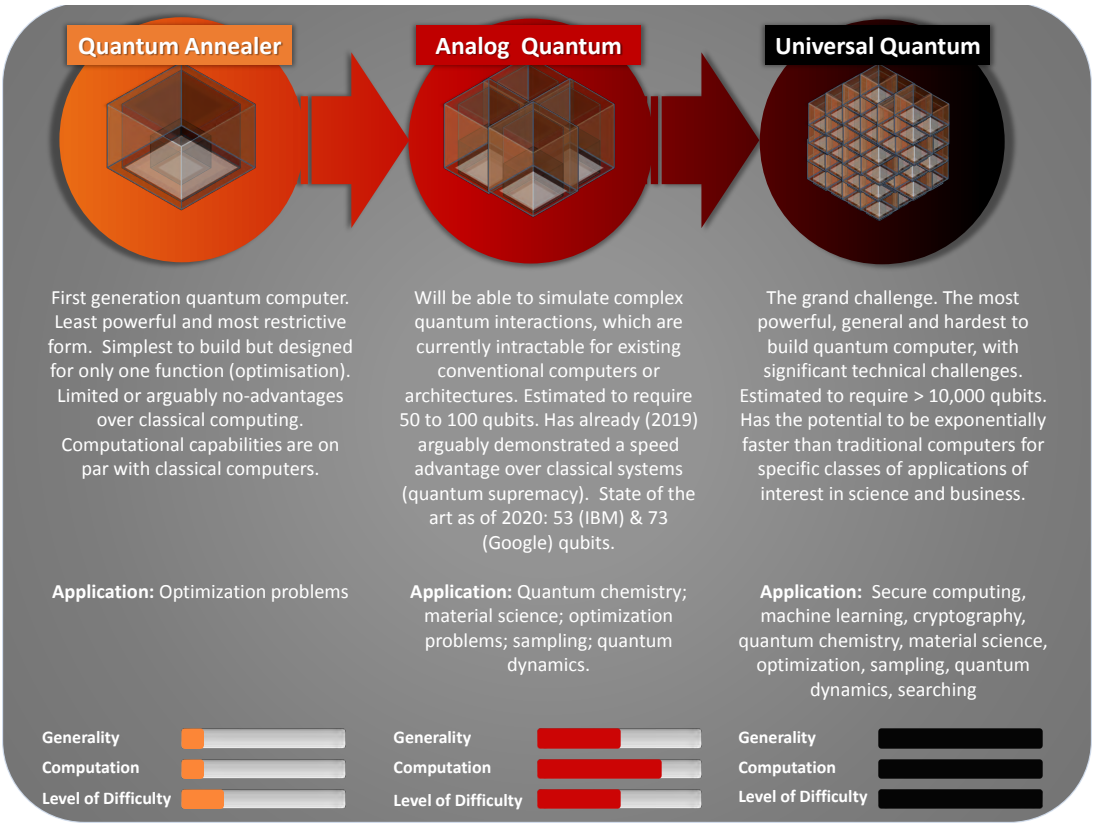


Figure 2.9: *3-Types of Quantum Computers (CREDIT:Adapted from [89]).*

Interoperability considerations will be critical for the successful implementation of some quantum enabled capabilities. Standardisation around quantum encryption and communications protocols will be a more immediate concern. PNT, sensors and computing will present fewer interoperability challenges as these will be tightly integrated into operational capabilities, but this may also lead to significant disparities in operational performance between alliance members.

Of all the EDTs Quantum technologies are perhaps the most nascent and variable in development, with substantial national and commercial investments being made. In particular, the operational viability of new sensors that have been demonstrated at the laboratory level is a significant area of continued research [93]. This development is generally agreed to be at a very much lower level of technical readiness [94, 95] than other quantum technologies. PNT and QKD are much closer to being fielded operationally.

Quantum computing (or quantum information science) (Figure 2.9) has enjoyed considerable visibility in the media and has undergone significant commercial development. Nevertheless, the development of *widely* available general quantum computing (i.e. capable of significantly exceeding the theoretical limits of classical computing (i.e. *quantum supremacy*)) is at least 15-20 years away. However, business application outside of a research environment is envisaged as 5 - 10 years away [96, 97]. To achieve this goal requires surmounting some significant theoretical and engineering challenges (particularly around error correction), which may ultimately render such systems impractical over this period [98]. However, for NATO, research into non-classical quantum optimised algorithms (e.g. quantum neural networks for AI) suitable for Alliance defence and security problems is a cost-effective development strategy in the short term [99, 100].

Appendix D provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.10: *Quantum 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Quantum	Communication	High	Trigger	5	2030
	Information Science	Revolutionary	Trigger	4	2035
	Precision Navigation	High	Disillusionment	6	2025
	Sensors	Moderate	Trigger	3	2040

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.4.2 Bio-(& Human Enhancement) Technologies (BHET)

Bio & Human Enhancement Technologies (BHET)

Biotechnologies use organisms, tissues, cells or molecular components derived from living things, to act on living things; or, act by intervening in the workings of cells or the molecular components of cells, including their genetic material [101]. *Human Enhancement Technologies* (**HET**) are biomedical interventions that improve human form or functioning in excess of what is necessary to restore or sustain health.

Figure 2.10: *Biotechnology.*

Manipulation of our biological environment and human enhancement goes back to the earliest days of humankind when our ancestors employed skins, stones and agriculture to create an evolutionary advantage. However, bio- and human-enhancement technologies (BHET) are expected to be available over the next 20 years that change our very definition of what it means to be a soldier, sailor or aviator. These technologies span the spectrum of biological sciences: Genetic manipulation (e.g. CRISPR) to develop novel pathogens or medical countermeasures; Manufacturing methods exploiting biological processes; Human enhancement via integrated robotics (e.g. exoskeletons or replacement parts); Neural interfaces; Enhanced vision; Socio-technical symbiosis with AI and autonomous systems; Pharmacological approaches to cognitive and physical enhancement; Increased virtualisation of the socio-cognitive environment supporting the development of new social, information and organisational structures; and, New bio-sensors and bio-informatics, which will increase our understanding of socio-cognitive, physiological, economic and neurological behaviours to improve operational performance and resilience, as well as increase the effectiveness of non-kinetic targeting.

Disruptive BHET research areas of potential interest to NATO are: **Bioinformatics and Biosensors**: The collection, classification, storage, retrieval and analysis of biological and biochemical data. **Human Augmentation**: The use of genetic modifications, pharmacological agents, electro-mechanical devices, or neurological interfaces to increase human physiological and neurological performance beyond normal limits. **Medical Countermeasures and Technologies**: The development of new diagnostics, therapeutics and vaccines (employing bioinformatics, genetic engineering and biosensors) to support predictive diagnostics, CBRN threat identification and treatments. **Synthetic Biology**: The deliberate design, engineering and creation of novel synthetic or modified biological components or systems.

These changes will and already are presenting significant societal, legal and policy issues.

Appendix G provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.11: *Biotechnologies and Human Enhancement 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Biotechnologies	Bioinformatics	Moderate	Expectation	6	2025
	Human Augmentation	High	Expectation	5	2030
	Medical Countermeasures	High	Trigger	4	2030
	Synthetic Biology	High	Trigger	6	2025

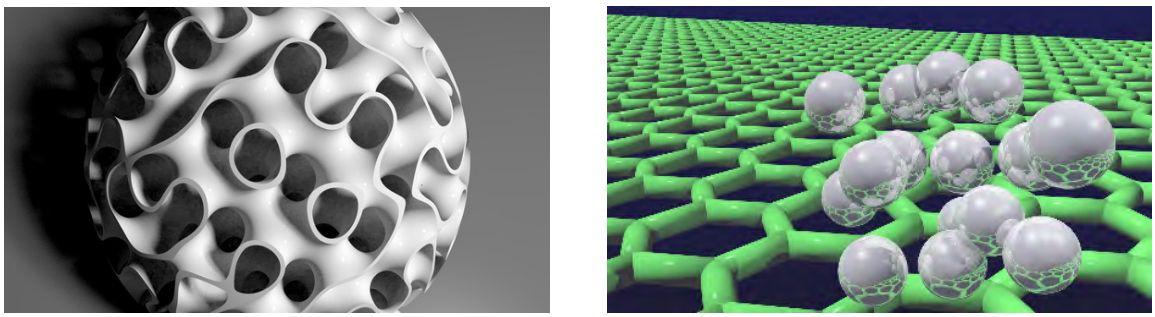
Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.4.3 (Novel) Materials and Manufacturing (NMM)

Novel Materials and Manufacturing (NMM)

Advanced (novel) materials are artificial materials with unique and novel properties. Advanced materials may be manufactured using techniques drawn from nanotechnology or synthetic biology. Development may include coatings with extreme heat resistance, high strength body or platform armour, stealth coatings, energy harvesting & storage, superconductivity, advanced sensors & decontamination, bulk production of food, fuel and building materials. Research into graphene, other novel 2-D materials, and topological materials are an area of high potential and growing interest. *Additive Manufacturing*, which is often used as a synonym for *3-D printing* [102], is the process of creating an almost arbitrary 3D solid object from a digital model through layered addition of materials. Additive Manufacturing can be used for: rapid prototyping; in situ production & repair of deployed military equipment; and production of precision, custom or unique parts.

Developments in novel materials and manufacturing will demonstrate both disruptive and emergent aspects over the next 20 years. While aspects of this EDT, such as agile manufacturing (e.g. 3D/4D printing), are assessed to be highly disruptive in areas of capability development, acquisition and logistics, the underlying technologies are already well in place and continue to be developed, expanded and used at a brisk pace by industry. However, at the cutting edge of research are the development and exploitation of new materials (e.g. graphene first discovered in 2004 and other 2-D materials); new material properties [103]; production of hitherto *impossible* designs; new manufacturing methods (e.g. biotechnology-based [104]); nano-scale manipulation of materials; mixed materials printing; and, the use of AI and BDAA to find new materials. These research areas are driven by a desire to discover or exploit new and unique physical properties (e.g. superconductivity), as well as cheaper, stronger, lighter, more durable, or higher capability materials (e.g. energy).



(a) *Topological Materials [103].* ***(b)*** *2-D Materials*

Figure 2.11: *Novel Materials.*

Appendix H provides a more comprehensive review of this EDT. The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table 2.12: *(Novel) Materials 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Materials	Novel Materials	High	Trigger	2	2040
	Additive Manufacturing	Moderate	Enlightenment	7	2025
	Energy Storage	Moderate	Trigger	5	2030

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

2.5 Convergence, Inter-Dependencies and Synergies

EDTs rarely create an impact in isolation. Instead, they are most disruptive at the boundaries of the physical, information or human domains or where these EDTs overlap or converge. These synergies, along with serendipity and explicit inter-dependencies between the following EDT groups are projected to be especially important in the development of future capabilities. It is impossible to fully characterise all combinations of these EDTs, but six are deemed to be potentially the most disruptive.

2.5.1 Data-AI-Autonomy

The synergistic combination of autonomy, BDAA and AI is expected to have the largest disruptive effect on the Alliance and its military capabilities over the next ten years. Increased use of intelligent, widely distributed, ubiquitous, cheap, interconnected sensors and autonomous entities (physical or virtual) will lead to volumes of data that are virtually impossible to analyse by current methodologies and approaches. Interrelated technologies and methods will underlay solutions to these problems. Such technologies include 5G (and similar communication technologies), cognitive EM management, the-internet-of-things (IoT), the AI-of-things (AIoT) [105], better battery technologies and even 3-D printing. Such changes, coupled with supporting space, bio- and quantum technological developments, have the potential to create a NATO strategic and operational decision advantage, leading to the need for new cyber and memetic warfare concepts and capabilities [29, 106].

Figure 2.12: *Sense Making.*

2.5.2 Data-Quantum

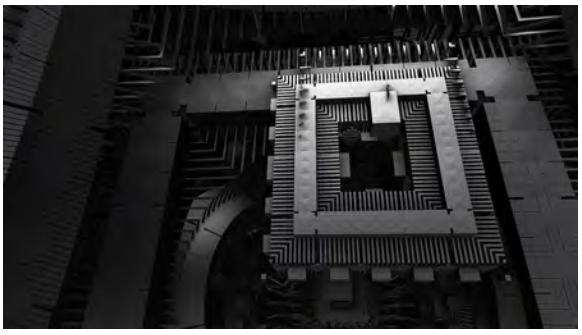


Figure 2.13: *Deeper Insights.*

Over a 15 - 20 year horizon, quantum technologies will greatly increase C4ISR data collection, processing and exploitation capabilities, through greatly increased sensor capabilities, secure communications, and computing. In particular, quantum computing may greatly increase modelling & simulation speed and fidelity for predictive analytics, and enable a quantum approach to deep learning neural networks for greatly enhanced AI and data analytics. This increased computational and simulation capability will also significantly impact the conduct of Alliance S&T through a meta-analysis of existing science and the simulation of quantum dominated systems. This capability will, in turn, lead to the discovery of new fundamental and applied science, novel designs, purpose-built genes

or organisms, as well as identification of novel material, chemical and biological properties. All of these have the potential to generate disruptive effects beyond 2040.

2.5.3 Space-Hypersonics-Materials

Space and hypersonics present challenging operational domains. The development of exotic materials, novel designs, miniaturisation, energy storage, manufacturing methods and propulsion will be necessary if space and hypersonic systems are to exploit the inherent advantages and opportunities of these domains fully. Space and hypersonic systems share many of the same environmental challenges. The development of new cheap, strong and exceptionally heat resistant materials will be essential to develop practical and affordable systems. The increased use of 3D/4D printing will also be critical as the printing of essential parts (e.g. engines) will help to reduce costs and increase reliability.

Figure 2.14: *Near Real Time Global Reach.*

2.5.4 Space-Quantum

Figure 2.15: *Trusted Global Communications.*

Space-based quantum sensors, facilitated by QKD communication, will lead to entirely different classes of sensors suitable for deployment on satellites. Currently, power limitations and sensor sensitivity significantly impact satellite design and operation. Smaller, lower power, more sensitive and more distributed space-based sensor networks enabled by next-generation quantum technologies will be an essential aspect of NATO's future ISR architecture in 20 years.

The development of large-scale satellite-relayed QKD quantum communication (QC) networks [107], will be essential if the Alliance is to maintain a fully secured global communication network. Satellite-to-Earth QC has already been demonstrated for ranges over 5000km. China, in particular, is developing a number of very ambitious demonstration projects. Technological developments over the next 5 - 10 years are expected to greatly expand these early experiments and provide the technological framework for robust commercial capabilities.

2.5.5 Data-AI-Biotechnologies

AI and biotechnology are developing at an exponential rate, driven by greatly reduced costs, increased speeds and rising commercial interest [65]. For example, the original human genome project took ten months and cost $3 billion USD (in 2001). Today, it takes less than one hour and costs about $1000 (USD) to decipher a human genome [65].

AI, in-concert with BDAA and biotechnology, will have an outsized impact on the world's economy and health. Such a combination of EDTs will greatly contribute to the design and discovery of new drugs, purposeful genetic modifications, di-

Figure 2.16: *Bio-Engineering.*

rect manipulation of biochemical reactions, development of optimised biological agents, living sensors, development of new CBRN counter-measures and identification (through meta-analysis) of new research areas. The use of AI to optimise the design of new biological agents molecule-by-molecule or cell-by-cell will greatly expand our ability to tailor-make new pharmaceuticals (e.g. [108]) as well as create new means of manufacturing for sensing. Such disruption will not be confined to the bio-sciences but will be mirrored across all areas of S&T development.

2.5.6 Data-AI-Materials

Figure 2.17: *New Materials and Products.*

AI, in-concert with BDAA, will contribute to the design of new materials, the identification and design of unique physical properties (e.g. [109, 110]), direct manipulation of chemical reactions, creation of novel designs and identification (through meta-analysis) of new research areas. In particular, this will support further developments in the development of 2-D materials. This disruption will be mirrored across all areas of S&T development.

AI and BDAA, in combination with 3D/4D printing or bio-manufacturing, will push production towards the edge (i.e. the user) and greatly facilitate the development of reliable, tailored, mixed material manufactured products.

2.6 Countering EDT Threats

RED forces are themselves complex and adaptive. It is misleading to consider RED force development of EDTs as being a simple mirror of BLUE force development. Potential asymmetric and peer/near-peer competitors will take differing exploitation paths and may potentially target novel applications in the physical, human or information domains.

Nevertheless, for every military capability, there are eventually counter-measures and counter-countermeasures. As such, even where there are strict national, legal and ethical limits to the deployment of such capabilities, Alliance nations must conduct appropriate S&T in these areas to develop such countermeasures. As an example, this has been and will continue to be the case for CBRN threats, where (medical) countermeasures have been developed and in some cases have yielded significant benefits in the fight against virulent diseases such as Ebola [111, 112, 113].

Development of countermeasures for each advantage an EDT may provide will also need to be considered within the NATO capability development process. As technology is increasingly globalised and democratised the life-span of a technological advantage may become increasingly short. Therefore, operational success will come to those best able to effectively integrate EDTs within enterprise and operational functions, as well as those who continue to push the technological edge.

2.7 Summary

It is essential for the Alliance and the nations to understand the potential impact, current level of hype, readiness, operational applicability and synergies associated with each EDT. As noted by Possony and Pournelle [6] there is little choice but to adapt to this environment as:

> *"The primary fact about technology in the twentieth century is that it has a momentum of its own. Although the technological stream can, to some extent, be directed, it is impossible to dam it; the stream flows on endlessly. This leaves only three choices. You may swim with the stream, exploiting every aspect of technology to its fullest; you may attempt to crawl out on the bank and watch the rest of the world go past, or you can attempt to swim*

against the stream and "put the genie back in the bottle"... The research itself does not create technology but is merely one of technology's major prerequisites, and technology by itself cannot guarantee national survival."

EDTs are poised to have a significant effect (positive and negative) on the Alliance over the next 20 years. However, productive employment of these new technologies will pose severe challenges and raise fundamental questions of ethics and legality. Expanded use of AI, BDAA and autonomy will provide greater access to critical operationally relevant data and knowledge, but at the risk of the *fog of more*. Information itself will increasingly become a warfighting domain and a commodity. In parallel, the use of automated and potentially autonomous systems in operations in which humans are not directly involved in the decision cycle, will become more widespread and increase the pace of strategic competition.

Despite these potential leaps in innovation, the evolving battlespace will continue to feature a mix of old legacy systems and new weapon systems. This mix may challenge the Alliance's ability to fight together. Technological gaps will pose connectivity, communications, doctrinal, legal and interoperability challenges. Capability and capacity mismatches, as well as capacity shortfalls, are to be expected as nations come to terms with the implications of these new technologies.

Technological advances coupled with demographic changes will place a premium on the development of the right human capital capable of leading and operating across all domains, including strategic, operational and tactical levels, and across multiple terrains.

While it is likely that the Alliance will maintain a degree of technological advantage in some EDT areas, EDTs (in particular AI, Big Data, biotechnology, hypersonic) will likely become cheaper and more accessible to hostile actors. The Alliance's dependence on advanced technology could increasingly become a liability if care is not taken on how they are integrated and in the development of counter-measures. Allies must be prepared to operate in a practical (credible, aware, networked, agile and resilient) manner. EDTs will need to be aligned with NATO military functions (prepare, project, protect, engage, sustain, C3 and inform) and development must be focused on achieving desired military effects (assure, contain, deter, defeat, defend, deny, stabilise and transform). It is essential that we understand the nature of these new technologies, analyse their implications for defence and security, explore the opportunities they offer, push the boundaries of what is possible, and ensure that we are ready to mitigate their risks. NATO is by its international and collaborative nature well placed to consider these issues.

The development of an EDT is rarely, if ever, constant in speed or unerring in its path towards practical application, either in the military or civilian spheres. How the underlying science and resulting technologies will develop, what complex interactions they will have with one another, and ultimately what military capabilities they will enable or engender is fundamentally uncertain either in result or timeline. Nevertheless, much as the former US President and NATO's first Supreme Allied Commander Europe (SACEUR) Dwight D. Eisenhower said *"Plans are worthless, but planning is everything"* [114], the *process* of forecasting S&T trends prepares NATO for the associated opportunities and risks presented by these technologies.

3. Contextual Trends

Initial Conditions

"Le présent accouche, dit-on, de l'avenir." - *Voltaire* [115]

3.1 Introduction

S&T developments do not take place in a vacuum, as they are driven by technological, individual, economic, societal and organisational needs and trends. In turn, these S&T developments drive events that fundamentally change societies/individuals and force the evolution of organisations and governments. Understanding the forces that generate these developments is an essential first step in assessing future technological and scientific disruption.

This section presents a brief contextual overview for of key global and strategic forces that are driving technological progress. It draws on a number of future studies including [20, 24, 33, 44, 116, 117, 118, 119, 120, 121, 122].

3.2 Innovation and Investment

Driven by these global trends, specific technological advances, breakthroughs, applications and ultimately, military capabilities may be generated through multiple innovation paths (Figure 3.1). Such paths may include the novel use of old technologies; application of new technologies to old problems; the application of modern science to develop novel techniques and technical tools engendering new science and ultimately new technologies; and, the creative convergence and integration of old and new technologies.

For NATO, the path from S&T idea to military capability is tied to a continuous process of assessment, concept development and experimentation. This process is an essential framework for evaluating the potential military value of EDTs

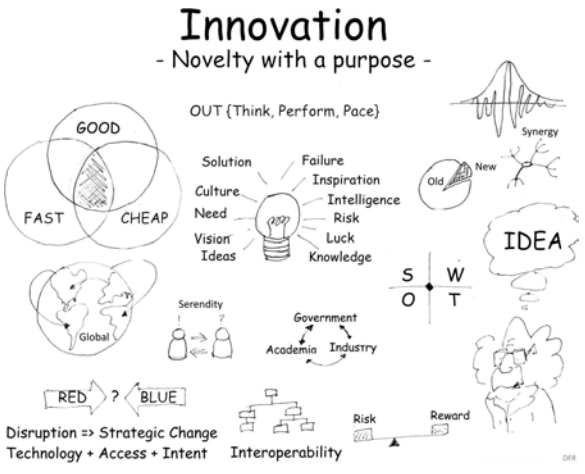


Figure 3.1: *Innovation.*

and ensuring appropriate operational concepts exist for uptake into operational capabilities. Alliance collaboration facilitates these activities through coordinated investment and assessment. Differing national S&T funding levels, acquisition programs, operational priorities and time horizons are challenges to this collaboration. Nonetheless, bringing to bear the intellectual and financial resources available across the Alliance provides a robust framework for assessing and developing new EDT based capabilities. Despite existing monopolies, new technologies which offer a cost-effective alternative to current approaches tend to be eventually adopted widely and quickly. With this investment comes the increased availability of technology for military capabilities.

High levels of investment generally drive rapid technological development and reflect their success (real or potential) in the marketplace or on the battlefield. Innovative countries leverage this investment through intense R&D efforts, development of high-value and value-added industries, and the nurturing of a highly skilled, productive and educated workforce. Figure 3.2 presents a ranking of the top 60 innovative countries for 2020 [123]. As expected, Alliance countries consistently rank highly for innovation. What is perhaps more surprising is to note that in 2020 the U.S. has fallen from first place in 2013 to ninth place, while China has risen to fifteenth place from twenty-first place in 2017.

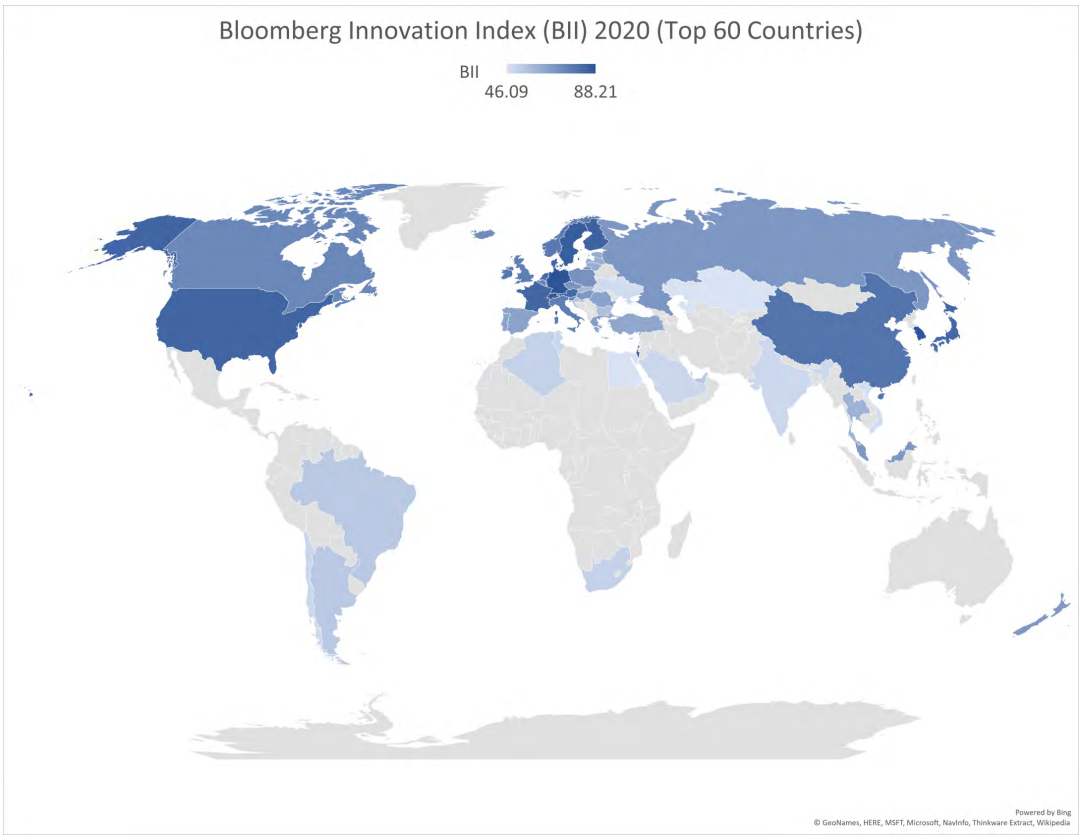
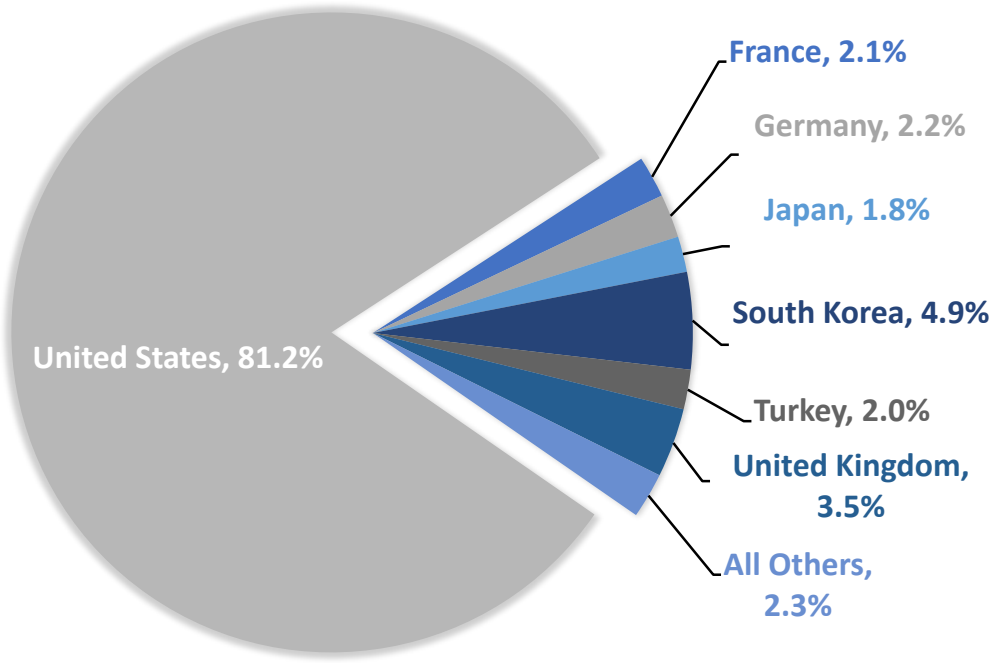


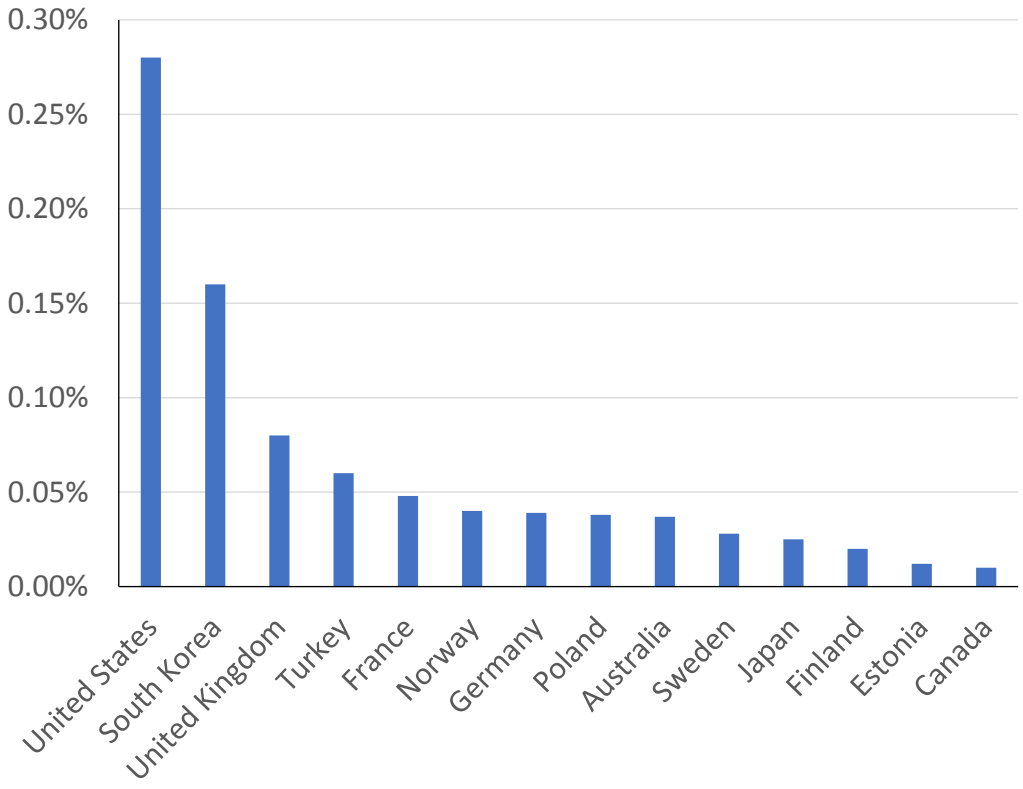
Figure 3.2: *Bloomberg Innovation Index - Top 60 Countries (2020) - Scale 0 (Poor) - 100 (Excellent) (SOURCE: [124]).*

Investment in defence S&T remains substantial (see Figure 3.3) as it is often seen as a key mechanism for shaping the national innovation agenda [125]. However, over the last 20 years, the drivers for S&T development have resided more and more outside the Defence and Security community, with commercial and societal needs providing the impetus for new capabilities (e.g. [126]). Technology uptake within a society impacts the development of EDTs, as well as creating potential vulnerabilities in both military and civilian spheres.

Underlying science (TRL 1-3) for such commercial successes still overwhelmingly comes from government funding and research activities, which are better placed to absorb the risks associated with such developments [41]. The level of such investments and those from industry are a vital factor in determining the long term rate of technological and capability development.



(a) Share of Total OECD Government Defence R&D Funding, by Country, 2017 (in purchasing power parity terms).



(b) OECD Countries with the Highest Levels of Government Defence R&D Funding as a Share of GDP, 2017.

Figure 3.3: *Government Defense R&D Funding (SOURCE: OECD, RDS Database) [127].*

As noted by [32] and [128] there are growing investments in AI, quantum computing and information, commercial space, synthetic biology, cloud computing, cybersecurity and (big data) analytics. These investments are key drivers of new military capabilities [18, 23]. For example, global investment in AI research is set to exceed $1 trillion by 2030, driven in no small measure by Chinese investment and a stated goal to become the world's leader in AI by 2030 [129]. The US and the EU have also pledged billions of dollars & euros to support AI research with more than $2 billion dollars set aside for defence-related AI research.

Global investment in S&T has changed substantially over the last few decades [130]. For example, in the 1960s, the USA share of global research and development was 69%. By 2016 this share had fallen to 28% with Chinese investment rising substantially as a function of purchasing power and as a percentage of Gross Domestic Product (GDP) (see Figure 3.4).

On a less positive note, the Organisation for Economic Co-operation and Development (OECD) [132] observes that:

> *"The share of government in total funding of R&D decreased by four percentage points (from 31% to 27%) in the OECD area between 2009 and 2016 ... But current trends in public research and development (R&D) spending may not be commensurate with the similar ambition and challenges delineated in mission-oriented policies. Since 2010, government R&D expenditures in the OECD as a whole and almost all Group of Seven countries have stagnated or decreased, not only in absolute amounts and relative to gross domestic product but also as a share of total government expenditure."*

At the same time that government funding has been decreasing some research suggests that technological innovation is slowing down [133, 134, 134, 135]. Others, such as Microsoft's Bill Gates disagree strongly [136]. Both perspectives may be correct given the ambiguity in defining *innovation* and the long lead times between national investments, scientific discovery and practical application.

Innovation (i.e. novelty for a purpose) should not necessarily be conflated with *emerging* nor is *disruption* necessarily *game-changing technology* [137]. Other aspects of the innovation ecosystem are equally important, such as access, design, motivation, costs, intent, culture and societal expectations. Further, advances in mathematics, engineering and human factors are not necessarily technological but may be highly disruptive and innovative. Serendipity and synergy often play a critical role in bringing together ideas, people and technology to create *disruption*. Low cost, widely available technologies used in creative ways, employing creative designs, or addressing problems in a manner that facilitates easy adoption can be highly disruptive (e.g. the Apple iPhone [138]). In seeking military innovation, it is essential to distinguish between *innovation* and *disruption* and to appreciate the critical nature of these additional factors, which range across all aspects of DOTMLPFI [Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability].

3.3 Strategic Drivers

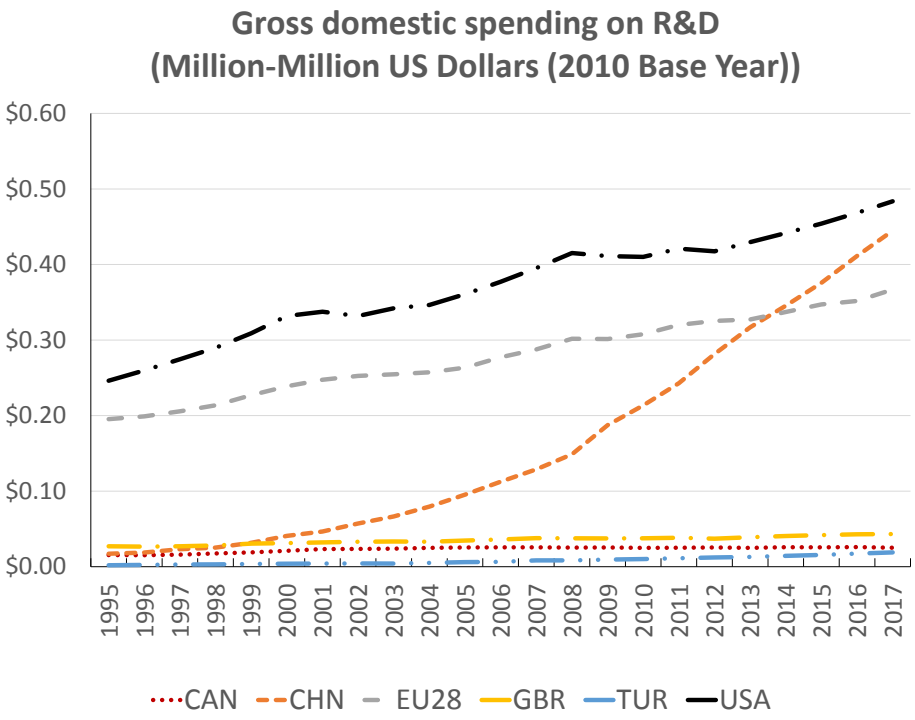
The following key strategic drivers will likely affect technology trends over the next 20 years. This section offers some thoughts and assumptions regarding these drivers.

3.3.1 The Operational Environment (Space & Info-sphere, Arctic, Urban)

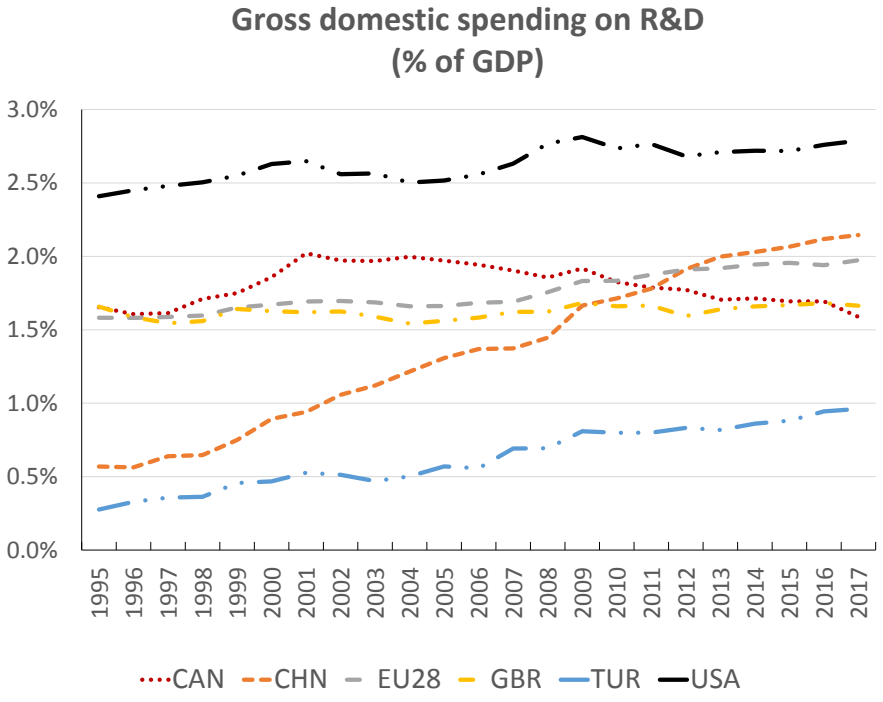
The range of potential NATO operations is expanding and evolving as the geopolitical, military, economic, social, climatic and technological landscapes change [139]. Space, the info-sphere, the arctic and urban domains are particular areas of rapid evolution.

The Space Domain

Space has been a *human* domain for over 60 years, and essential militarily for at least that long. However, commercialisation, new propulsion options, novel materials, miniaturisation of sensors and electronics, and agile manufacturing have issued in a new era of rapid development. These have significantly reduced the cost of space access and increase the availability of space derived information. As a result, space



(a) *Gross domestic spending on R&D (2010 USD).*



(b) *Gross domestic spending on R&D (% of GDP), 2017.*

Figure 3.4: *Total R&D Funding By Select Countries (Canada, China, European Union, Great Britian, Turkey, USA) (SOURCE: OECD, RDS Database [131]).*

is increasingly contested, congested, competitive and commercial. With growing Alliance and global reliance on space-based technologies, the *control of space could become a significant flash-point* [118]. The risk of militarisation is not insignificant. This risk includes the use of anti-satellite (ASAT) (hard or soft kill) weapons [140, 141, 142], which have the potential to *pollute* the near-earth environment, significantly increasing the risk of collision with space debris.

Figure 3.5: *Satellite Based Automatic Identification System (S-AIS) for Maritime Situational Awareness (CREDIT: MarineTraffic.com).*

Given these concerns, NATO has recently declared space as an operational domain, implicitly recognising that with the increased peaceful use of space and space-based technologies (e.g. communication and sensing) comes an increased risk of malicious actions in space. As noted by the NATO Secretary-General Jens Stoltenberg [143]:

> *"Satellites can be jammed, hacked or weaponised. Anti-satellite weapons could cripple communications and other services our societies rely on, such as air travel, weather forecast or banking. Space is also essential to the Alliance's deterrence and defence. Including the ability to navigate, to gather intelligence, and to detect missile launches. Around 2,000 satellites currently orbit the Earth. And around half of them are owned by NATO countries. NATO has no intention to put weapons in space. We are a defensive Alliance. And our approach will remain fully in line with international law. But making space an operational domain will help us ensure that all aspects are taken into account to ensure the success of our missions."*

Given the Alliance's reliance on space-based systems, NATO will need to increase its vigilance and resilience in this domain.

The Infosphere (Cyber, Electronic Warfare (EW), and the Electromagnetic (EM) Spectrum)

The information domain (including cyber, EW (Figure 3.6) and electromagnetic (EM) spectrum management) or info-sphere, is a unique operational environment. This domain is driven by the digitisation and virtualisation of individuals, organisations and societies [44]. Global access to social media and mobile communications have created new virtual communities and empowered individuals working within complex social networks unbound by geographic boundaries but increasingly defined by emergent virtual ones and associated *echo chambers*. Social and individual empowerment so engendered have become in many ways as important to the modern world as food, water or shelter. This empowerment is true across the globe and at all levels of economic development, driven by the deep-seated human need for social contact. Blended and virtual reality systems have blurred the distinction between physical and artificial realities. 5G and the internet-of-things (IoT) will also increasingly enable the use of the info-sphere.

Such empowerment is being challenged by nations, through national firewalls and social metrics to control, shape and constrain social discourse and individual expressions of discontent. At the same time, fringe communities and near peer-competitors have found a voice in the info-sphere with trolling, mob behaviour, and disinformation campaigns becoming increasingly sophisticated. The use of AI in this context to create competing narratives and *alternate facts* (e.g. deep fakes, chatbots, etc.) is not a question for the future but a reality today.

The information space is an evolving operational domain and one where others are increasingly active [145, 146, 147]. NATO operations in the info-sphere will require increasingly sophisticated approaches to cyber, EW and EM management. The info-sphere is *the* critical operational domain for hybrid warfare. Success in hybrid warfare will require winning the war in the info-sphere. This success will require the development of a competing Alliance narrative, trolling the increasingly deep and murky *data ocean*

Figure 3.6: *Electronic Warfare in Today's Military Environment [144].*

that such virtualisation and digitisation creates, and developing a *decision advantage* in terms of speed, accuracy and effect. The impact of EDTs in this area will be profound.

The Arctic

The Arctic has reemerged as an area of strategic importance to Alliance nations [148, 149, 150, 151], partners [152], and others with interests in polar climate change and resource development [153, 154]. Of more concern has been the resurgence of Russian military activity [155, 156, 157], as well as growing interest by non-arctic nations [153, 154, 158].

(a) *RCAF Twin Otter (440 Sqn): Ellesmere Island.*

(b) *HDMS Knud Rasmussen.*

Figure 3.7: *Austere Arctic Operations (CREDIT: DF Reding).*

Increased military and commercial activity in the Arctic, driven by the allure of resources, new shipping routes, tourism and changing climatic conditions suggests that NATO will need to expand its limited ability to operate across the Arctic. While many Alliance nations have considerable Arctic operational experience (e.g. Figure 3.7), this will present a challenge for the vast majority of NATO capabilities that were designed for more benign operational conditions. Operations over vast distances, where few satellites

regularly pass, will make GPS and communication coverage sparse. Weather conditions (both atmospheric and space) will degrade sensor, communication and vehicle performance. The freezing winters, swarming insects, permafrost, short summers, muskeg and highly variable weather conditions pose a further risk to human health and equipment not prepared to withstand such conditions. Technologies, including many of those considered in this report, will be challenged to operate successfully in the Arctic.

The Urban Theatre

Figure 3.8: *NATO Joint Military Operations in an Urban Environment: A Capstone Concept [159].*

Urban areas are expected to be a stage upon which NATO operations are increasingly conducted [44]. Estimates by the United Nations are that by 2050 68% of the world's population will live in urban areas [160]. As this develops, the number of mega-cities (i.e. those with populations greater than 10 million) will increase from 28 to 50 [161]. This increased urbanisation, driven by economic and climatic changes, will stress civil societies and present a challenge to military operations at any scale [162].

The engagement space of the future urban operational environment will be highly multi-dimensional and hybrid in nature, with strategic success depending on successful information, social, EM and cyber engagements. There will be an increased need to operate with minimal or no collateral damage in environments where the difference between combatants and non-combatants may be difficult to discern or change minute-to-minute. New technologies will be essential to ensure adequate situational awareness and (kinetic or non-kinetic) precision in these scenarios, with the internet-of-things providing millions of possible sensors and urban transportation systems increasing the complexity of operations [118]. But, buildings and underground systems inhibit sensor systems, and radio-frequency interference can severely degrade sensor and communications performance. Furthermore, military forces will need to work comprehensively alongside local governments, NGOs, OGDs and security forces. However, they may not be completely interoperable with multinational deployed military forces or even seek the same strategic objectives.

3.3.2 Culture, Ethics & Law

Culture, ethics and laws shape the integration of technology into society and ultimately define its effect and value. As a result, Alliance nations have differing constraints around the operational use of EDTs

and the capabilities they engender. These constraints ultimately impact development, interoperability and employment of EDTs as part of Alliance military capabilities. As noted by A. Kaspersen, the former Head Geopolitics and International Security at the World Economic forum [163]:

> *"Such is the speed, complexity and ubiquity of innovation today, we need a regulation process that looks ahead to how emerging technologies could conceivably be weaponised, without holding back the development of those technologies for beneficial ends. "Hard governance" of laws and regulations remain necessary, but we will also need to make more use of faster-moving "soft governance" mechanisms such as laboratory standards, testing and certification regimes, insurance policies and mechanisms like those set up by academics to make potentially dangerous research subject to approval and oversight. This will need to proactively anticipate and adapt to not only technological changes, but also macro-cultural ones, which are a lot harder to predict."*

NATO itself is well-positioned to ensure that such fundamental issues are addressed so that EDT derived military capabilities will be interoperable, used in a legally defined manner, and seamlessly integrated into Alliance operations.

As technology advances at an increasingly rapid pace, legal frameworks, social norms and regulations are lagging. Despite the global reach and implications of many technologies, there are few international regulatory agreements. As the centre of mass for technology development moves to the commercial realm, there are associated risks and opportunities, e.g. the increased use of *lawfare* [45] whereby strategic legal actions maybe taken to limit the use and exploitation of *contested* technologies. Contracts with industry may increase operational risks e.g. through the loss of the *right to repair*, with additional restrictions placed on system performance and maintenance documentation due to IP restrictions [165, 166, 167]. Alternatively, the development of *publicly available* data and *open source* tools, such as those employing the GNU General Public License, have been credited as a driver of innovation in artificial intelligence research [63, 64].

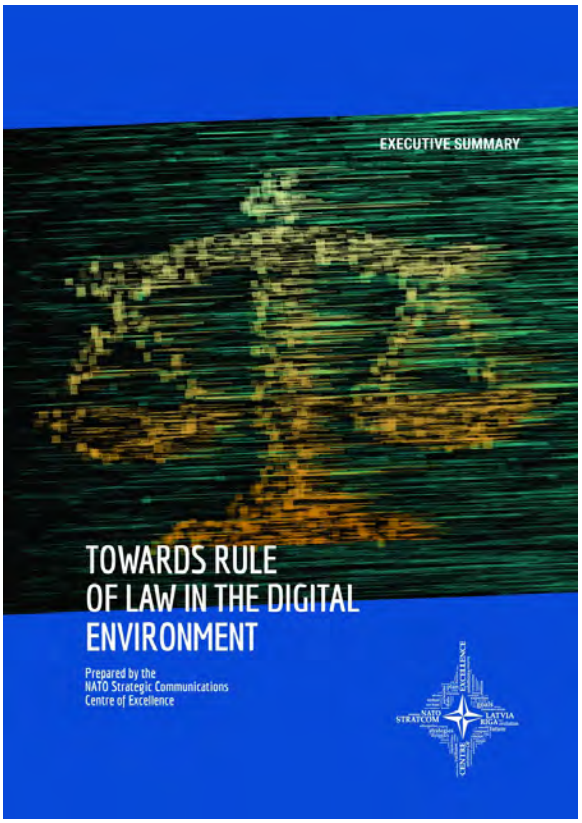


Figure 3.9: *Towards Rule of Law in the Digital Environment [164].*

Ethical and regulatory issues have surrounded the development of EDTs and have had a direct impact on the development of defence-related capabilities, in particular in the areas of autonomy, AI and big data (e.g. [68, 163, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177]). On the other hand, the democratisation of technology (i.e. reduced costs and increased access), raises the concern as to how much regulation is needed to safeguard society from high-tech rogue actors whose capabilities are only limited by their imagination. Chemical, Biological, Radiological and Nuclear technologies (CBRN) in particular have traditionally been highly regulated to prevent proliferation, but these regulations may be inadequate if anyone can set up a bio-engineering laboratory in a backyard or basement.

From a broad societal perspective, there is cultural resistance to integrating civilian capabilities into the military arsenal. For example, while non-lethal weapons may reduce casualties or collateral damage, even in high-intensity war-fighting scenarios, and increase operational effectiveness, they are seen by many as *not a military weapon* thereby slowing down their adoption and integration into the operational

toolkit. Similarly, the military use of current information and cyber capabilities has been slower than expected, likely due to cultural resistance in both civil and military societies.

The challenges of maintaining privacy in a digital and virtual world are profound. When it comes to ethics and confidentiality, there is no single global social norm regarding how personal data is used. In the West, populations are generally resistant to the use of their data by governments. Nevertheless, even in Alliance countries, privacy concerns may be overridden in the name of security [178]. Some societies or governments see value in using such data to reinforce social norms (e.g. [179]). Having uninhibited access to an entire population's worth of data gives a clear advantage for training AI and conducting advanced social analytics.

3.3.3 The Environment

Protecting and sustaining the environment is a critical concern when it comes to defence and security. As noted, environmental disruption can quickly lead to disruption of a society, or the use of toxic materials in weapons can render large areas unusable or hazardous. Long term stewardship of the environment (urban, space, maritime, land and air), including consideration of flora and fauna, is an important factor in weapon system design as well as training.

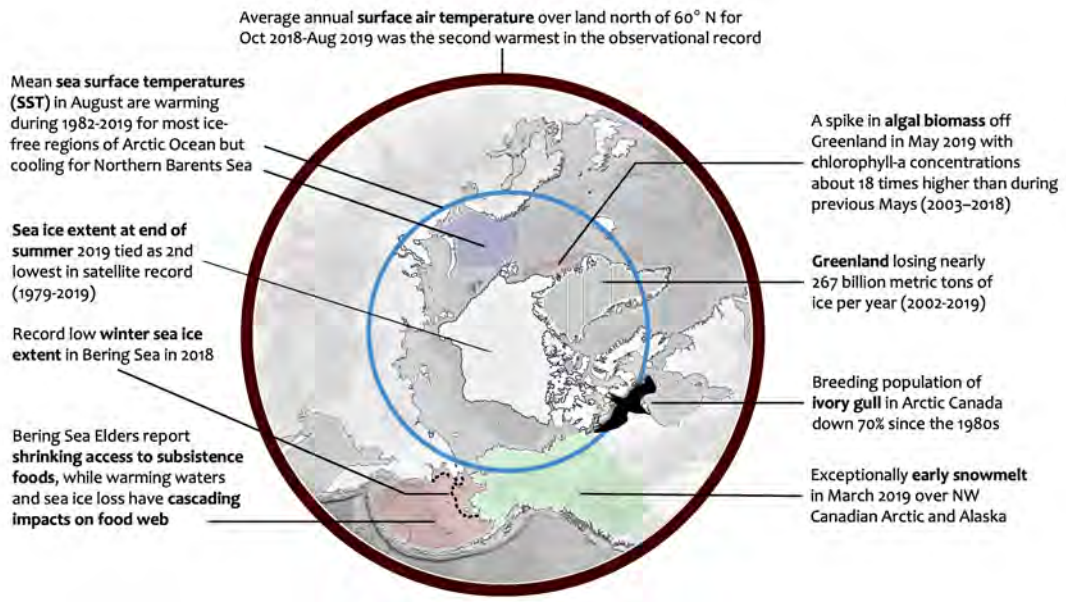


Figure 3.10: *The Changing Arctic Environment (CREDIT: NOAA [180]).*

Climate change will be a major disruptive force in the upcoming decades (e.g. Figure 3.10), with a number of future studies (e.g. [24, 41, 44, 116, 117, 118, 120, 128, 181] to name a few) highlighting the potential for climate change to drive future conflict. Increased shortages and control of food, lack of fresh water, reduced biodiversity, mineral and energy competition will all challenge global cohesion and power balances. Climate change and rising sea levels will threaten individuals and cities, leading to mass migrations and whole societies struggling to adapt. It is projected that by 2050 [182] more than 150 million people around the world currently living on land will be below the high-tide mark. The projected loss of entire islands, coastal areas and cities will challenge national boundaries and economies leading to further social, economic and military disruption.

3.3.4 Miscellaneous

Following [20, 24, 39, 44, 120, 121, 122, 183, 184, 184], we also note that several other strategic trends have the potential to impact future NATO capabilities or operations. These include:

- **The Changing Nature of Work**: Increased reliance on AI and Autonomy will redefine work;
- **Education**: Use of virtual realities, AI, big data etc. will enable personalised training;

- **Automated Logistics**: AI and Autonomy increasingly enable automated transportation and logistics;
- **Food and Water Technologies**: Application of novel materials and techniques, along with bio-engineering and biotechnologies may increase water and food supplies;
- **Human Capital**: An ageing global population, economic migration patterns and uneven developments within nations will challenge societies and recruitment efforts by military forces. Further, the ability of a society to exploit and absorb new technologies is limited by the availability of talented and skilled individuals able and willing to take on the challenge. Demographic shifts, job losses due to AI and autonomy, globalisation of talent and a growing skills mismatch may ultimately challenge the Alliance's ability to manage and absorb the disruption and exploit the opportunities presented by EDTs.
- **Changing Global Economic Framework**: Increased pressure on and decoupling of the international economic framework into protected technological silos (bifurcation) will hamper technological and economic development [185, 186]; and,
- **Infectious Diseases and Pandemics**: New diseases, reduced vaccination rates and growing resistance to countermeasures (e.g. antibiotics) will challenge global health & development and Alliance operations.

3.4 Defence and Security

The defence and security environment itself is changing [24] driven by the evolving nature of conflict and geopolitical factors. *Chaos*, *complexity* and *competition* [187] are said to be the defining characteristics of this future.

Two decades after the fall of the Berlin Wall, the potential for great power competition [188, 189] is greater than ever. As stated in the 2019 NATO London Summit Declaration:

> *"We, as an Alliance, are facing distinct threats and challenges emanating from all strategic directions. Russia's aggressive actions constitute a threat to Euro-Atlantic security; terrorism in all its forms and manifestations remains a persistent threat to us all. State and non-state actors challenge the rules-based international order. Instability beyond our borders is also contributing to irregular migration. We face cyber and hybrid threats... To stay secure, we must look to the future together. We are addressing the breadth and scale of new technologies to maintain our technological edge while preserving our values and norms... We have declared space an operational domain for NATO, recognising its importance in keeping us safe and tackling security challenges, while upholding international law. We are increasing our tools to respond to cyber-attacks, and strengthening our ability to prepare for, deter, and defend against hybrid tactics that seek to undermine our security and societies. We are stepping up NATO's role in human security. We recognise that China's growing influence and international policies present both opportunities and challenges that we need to address together as an Alliance."*

The NATO Secretary-General Jens Stoltenberg has also stated [190]:

> *"China's role and influence is another sign of increasing global power competition ... Its economic rise and technological prowess are powering global growth. This brings many opportunities, financially and politically. But China's rise also has implications for the global rules-based order and our security. We see this in the South China Sea, in cyberspace, and Chinese investments in critical infrastructure. So we need to understand better the challenges and opportunities China presents."*

Such geopolitical challenges are expected to grow over the next 20 years. These developments will present significant operational challenges to the Alliance, compounded by the increased democratisation of technology, as well as new technological threats from peer & near-peer competitors, terrorists, criminals and irregular forces.

Figure 3.11: *The NATO Secretary-General Jens Stoltenberg at the NATO Summit - London 2019.*

4. Conclusion

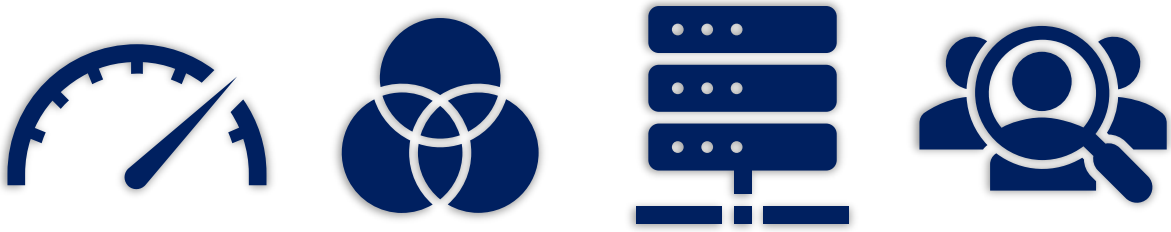
Understanding Trends

"We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run." - *Amara's law* [191].

Conflict is enduring, but the nature of that conflict continues to change, driven in no small measure by advances in technology, tools and scientific understanding. This evolution will be a vital feature of the future battlespace or zones of conflict, whether physical or virtual. These evolving multi-domain complex operational spaces will have significant implications for the development and future employment of the Alliance's instruments of power. If NATO is to develop a new *strategy of technology* it must do so in the context of evolving geographic, geopolitical and military domains, which in themselves are driven in no small part by technologies that are increasingly intelligent, interconnected, distributed and digital.

This report has considered how EDTs will disrupt, degrade and enable NATO military capabilities in the 2020-2040 timeframe. Such characteristics of modern technologies are drivers of the current evolution and revolution in data, AI, autonomy, space, quantum, hypersonics, biotechnologies and materials. Alone or in combination, they define the technological edge necessary for NATO's operational and organisational effectiveness. How quickly, in what order, and ultimately how successful these technologies will be, or what threats they will present, is yet to be determined. However, long term forecasts of military technologies provide a useful exercise while offering a guide to prioritising capability and technology investments. The techno-policy, legal and ethical challenges that they present NATO can not be overstated. Understanding *why* they present a problem or opportunity, *how* they are expected to manifest, and *what* this will mean to the Alliance is an excellent first step and will ensure NATO remains technologically prepared and operationally relevant.

Appendices



A. Data

Big Data - Impact

"So you should expect big data to have a big impact. And you can bet that it will help machines interact more usefully with our unstructured, changing, and sometimes downright confusing human ways. But if you're counting on it to make people much more predictable, you're expecting too much." - *Gregory Piatetsky-Shapiro* [192]

Definition

(Big) Data and Advanced Analytics (BDAA)

Big Data describes data that presents significant volume, velocity, variety, veracity and visualisation challenges. Increased digitalisation, a proliferation of new sensors, new communication modes, the internet-of-things and virtualisation of socio-cognitive spaces (e.g. social media) have contributed significantly to the development of Big Data. *Advanced (Data) Analytics* describes advanced analytical methods for making sense of and visualising large volumes of information. These techniques span a wide range of methods drawn from research areas across the data and decision sciences, including artificial intelligence, optimisation, modelling & simulation (M&S), human factors engineering and operational research.

Keywords

Big Data · Optimisation · Analytics · 5G · Operations Research ·Decision Science · Data Science · AI·Human Factors · Predictive Analytics · Business Analytics · Business Intelligence

Overview

BDAA (*Big Data and Advanced Analytics*) is a direct outgrowth of our increasingly digital and virtual world, and the subsequent need to make sense of the resulting information deluge. In particular, *analytics* is the process of generating understanding (e.g. through mathematical analysis and visualisation) and providing insights into current system states (*descriptive*) or future system states (*predictive*). The analyst is often faced with data having significant volume, velocity, variety, veracity or visualisation challenges. Vast amounts of data available throughout the future physical, human or information battle-spaces will

enable analytics to deliver insights and predictions, provide real-time decision support, and highlight early indicators of success and warnings of crises. Increased use of predictive analytics and M&S will enable decision-makers to exceed their cognitive limits while improving consideration, interdependencies, intransparencies and temporal dynamics [193, 194]. In the end this will allow decision-makers to better understand the potential impact of their decisions, and adjust plans accordingly (Figure A.1). Many aspects of BDAA are well developed and, while it is and will continue to be highly disruptive in nature, some have questioned whether it is truly an emergent technology at this time [195].

BDAA is understood to encompass four essential components: **(1)** collection (sensors); **(2)** communication; **(3)** analysis; and, **(4)** decision making. The 5V's (*volume, velocity, variety, veracity* and *visualisation*) describe the essential challenge of BDAA: how to make sense of large amounts of non-homogeneous data coming too fast, and of potentially dubious authenticity and accuracy. BDAA covers the human (social media, bioinformatics, etc.), physical (sensors) and information (cyber, analysis, etc.) domains.

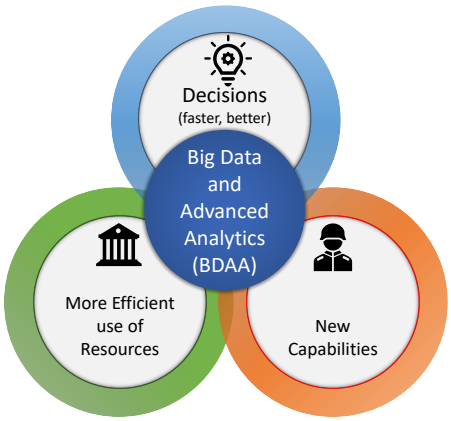


Figure A.1: *BDAA Goals.*

BDAA is a foundational technology and, as such, understanding its projected development is a critical step in understanding other EDTs. From a technology watch perspective, BDAA will be enabled by S&T developments in a variety of areas, which include: exploitation of human signatures; modelling and simulation for social media; modular multisensor fusion engines; provision and discovery of M&S tools and services in the cloud; visual analytics; decision support and planning support with M&S in the battlefield; virtual mission areas; distributed ledger technologies (e.g. blockchain); cognitive sensing; compressive sensing; computational imaging; deep learning; electric-and magnetic-field sensing; photonic integrated circuits; sensing sources data fusion; swarm centric systems; and, wideband telecommunications.

Sensors are a critical enabler of BDAA. Sensors provide the data in the physical domain, and increasingly in the human domain. *Ubiquitous sensing* or *sensors everywhere* will be significantly enabled by the growth of 5G communication and the internet-of-things (IoT). The concept of *sensors everywhere* refers to the ability to detect and track any object or phenomenon from a distance by processing data acquired from high tech, low tech, active and passive sensors. Effectively everything will be a sensor, and every sensor will be networked. Military applications will be wide-ranging, including the development of a multi-domain common operating picture, large scale underwater sensor mesh networks, exploitation and weaponising of social media, automated logistics planning, autonomous systems, and integrated soldier systems. While sensor technologies are expected to evolve to support greater precision and accuracy, the most disruptive development will be the combination of further miniaturisation, reduced costs, novel (3D/4D) manufacturing and the sheer volume and wide distribution of sensors in the military sphere. Advances in materials technology also promise future sensors at the molecular, nano or quantum scale.

Technological development of new sensor technologies will be rapid over the next 20 years. Such developments include:

- Smart textiles [196] imbued with molecular/nanoscale sensors providing real-time health and environment monitoring are expected to be widely available by 2030.

- Next-generation Over-the-horizon (OTH) [197, 198, 199, 200] and passive radar systems will provide wide-area air space surveillance, employing sophisticated data processing and multiple-input multiple-output (MIMO) technologies. Passive OTH radar is likely to be in a mature prototype state within 5-10 years, with fully fielded systems in place in the 10-15 year time-frame. Air target detection ranges could increase from 350km to 1500km.

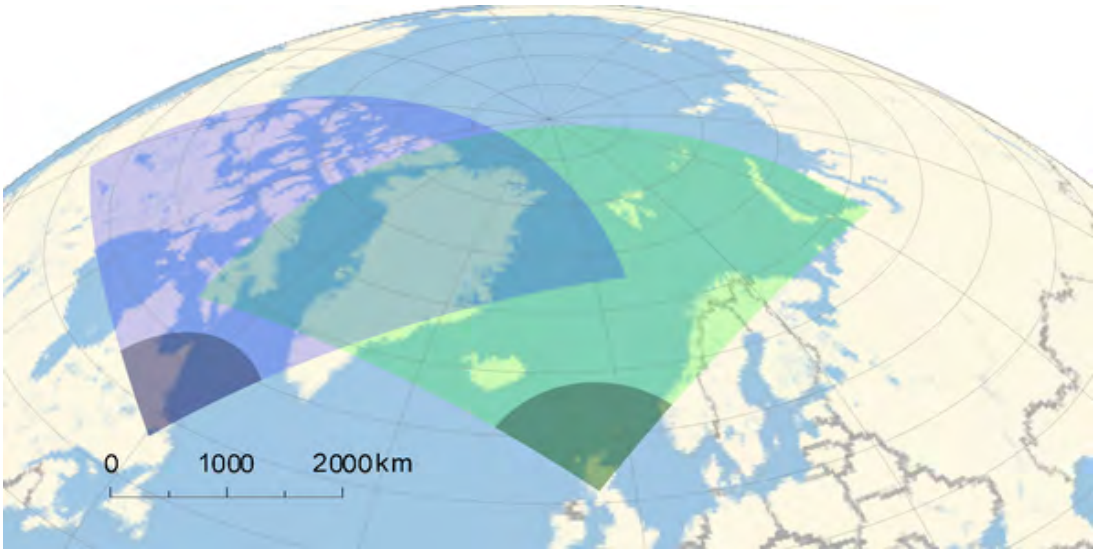


Figure A.2: *Hypothetical OTH Northern Radar Coverage.*

- Quantum sensing which, in the long term, will generate a revolution in sensing technology, enabling very high sensitivity sensors capable of long-range detection of aircraft, submarines or subterranean activities. This capability allows the development of smaller higher performance sensors to monitor weapon system health and performance.
- The use of digital twins (highly detailed virtual models of a specific weapon system [201]) will become increasingly commonplace over the next ten years, relying on extensive embedded sensor networks, including those tied to the human and information aspects of such systems.
- Computational imaging (CI) which holds great promise to revolutionise such EO/IR sensors, as well as providing significantly increased sensitivity. CI refers to image formation techniques that use digital computation to recover an image of the scene. Compressive sensing (CS), a CI subset, involves capturing a smaller number of specially designed measurements from the scene to recover the image or task-specific scene information computationally. CS has the potential to acquire an image with similar information content to a large format array while using smaller, cheaper, and lower bandwidth components. More significantly, data acquisition can be designed to capture task-specific and mission-relevant information guided by the scene content with more flexibility. CI has the potential to reduce system size, weight, power, and cost while enabling simultaneous target acquisition and situational awareness (multiplexed imager), perception range extension (Non-Line-of-Sight Imager, multispectral imaging), and multipurpose imagers.
- Microwave photonics, which is on the verge of delivering higher performance, lower power, more robust sensing and wireless communication on the battlefield.

The EM spectrum and associate communication modalities are at the centre of big data, enabling both sensors and communication. Control of the EM spectrum is a necessary prerequisite to information dominance. *Electromagnetic Dominance* is the ability to use more of the spectrum, to share the spectrum more efficiently, to protect one's own forces' use of the spectrum and to deny enemy use. The future will bring, among other things, faster, more reliable wireless/radio communications, electronic warfare resilience, secure streaming video and smaller deployed footprint. As a result, the EM spectrum is and will continue to be increasingly congested as military and commercial systems via for bandwidth. The use of AI to support cognitive sensors (e.g. cognitive radars) and communications, which adjust in an agile fashion to maximise collection and through-put, will become essential to avoid conflict in the congested (and perhaps contested) EM spectrum. This will be especially essential for operations in urban environments.

By 2025, decoys will have the capability to obscure visual and thermal and radar wavebands and be an integrated part of defensive aids suites. It should be technically possible to have fleets of robotic decoys for deception operations, but simple decoys aimed at mimicking the electromagnetic signature of headquarters of manoeuvre units are more likely to be developed in the short term. Electromagnetic field-based stealth systems and broadcast electronic decoys hold promise for the defensive capabilities of future electrically powered systems.

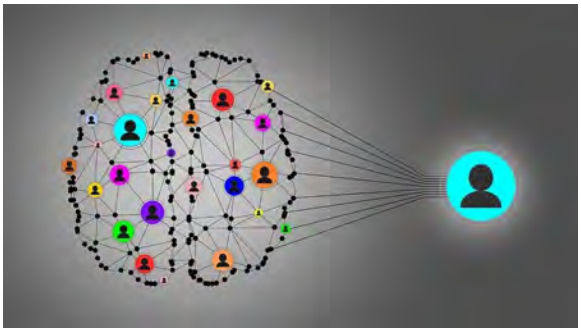


Figure A.3: *The Social Brain.*

Changing from the physical to the human domain, the increased virtualisation of social and individual interactions has contributed dramatically to the availability of social and personal data. One aspect of this virtualisation, *Social Media*, refers to the full range of internet-based and mobile communications where users participate in online shared exchanges and contribute user-related content or participate in online communities of mutual interest. Its applications in defence and security include population surveillance, sentiment analysis, knowledge and information sharing, low-cost means to stay in touch with families and strategic communications. Social media content continuously grows with ever-increasing rate but struggles to deal with issues of veracity and value. DARPA [202], in particular, continues to explore the implications of social media in such areas as linguistic cues; patterns of information flow; topic trend analysis; narrative structure analysis; sentiment detection and opinion mining; meme-tracking across communities; graph analytics/probabilistic reasoning; pattern detection; cultural narratives; inducing identities; modelling emergent communities; trust analytics; network dynamics modelling; automated content generation; bots in social media; and, crowd-sourcing. As social media reaches more corners of society, it increasingly enables significant and subtle influences on the expression of collective political and social power. The technology has already demonstrated the potential to alter the nature of political and social discourse leading to new, rapid and decisive mobilisation of populations at the right place and the right time to achieve political and social objectives. Similarly, data collection in the social sphere allows an unprecedented understanding of human social behaviour and group dynamics.

BDAA is being enabled in no small measure by *ubiquitous computing*, that is computing anywhere, anytime and on any device. Integrated with military mobile networks and mission cloud computing, ubiquitous computing has the potential to provide real-time decision support to the individual soldier at all times and all places. Such mesh networks of connected devices will allow BLUE forces to leverage and exploit distributed data structures and cloud computing services. It also encompasses software-driven functionality, with the ability to process incoming data at the sensor before transmission, and exploits advances in encryption that will enable assured information transfer across a network.

Figure A.4: *Global Data.*

Secure communication and data storage is essential in military operations. Databases are the traditional means to store and maintain structured and related data. More recently, distributed ledger technologies (e.g. blockchain) have emerged and been used as the distributed, transparent, and permanent data management technology underlying the Bitcoin cryptocurrency. The increased use of blockchain technologies (along with AI-enabled defensive cyber-bots/agents, quantum key distribution (QKD) and post-quantum encryption) will significantly increase the Alliance's ability to ensure trusted communications and data storage.

Analytics and advanced computational techniques for data processing and fusion, will improve

sensor ranges and provide richer contextual information than is currently possible. Artificial Intelligence, specifically machine learning, is a promising computational technique capable of processing large volumes of seemly disparate, disorganised, and ostensibly unrelated information. These predictive, correlative models are valuable tools for detecting intent and predicting possible future actions and events. The utility of these models and deep learning techniques will increase as methods for data-driven learning mature and as the underlying data grows almost without bounds.

Figure A.5: *Advanced Decision-making.*

Over the next 20-years, data volume will continue to grow, as the number of handheld and internet-connected devices grows exponentially, and the IoT becomes a reality. By 2021 global spending on IoT is expected to reach 1.4 trillion USD [203], and by 2030 500 billion items are expected to be interconnected [204]. The sheer volume of data that this will create is difficult to comprehend. The associated legal, policy and privacy considerations are decidedly non-trivial. To deal with this deluge, better tools for analysis (without the analyst) will need to emerge. Companies will grow increasingly data-driven and willing to apply analytics-derived insights to critical business operations. Intuitive decision-making will diminish somewhat as companies integrate analytics across the board. Organisations will struggle with data privacy, security and governance issues.

Visualisation techniques are critical enablers in assessing social media data supporting decision making. The civilian market is making extensive use of visual analytics methods for marketing purposes. This technology may be partly transferable to the defence and security domains.

A continuing trend away from centralised-only data silos is also noted. Smart devices will collaborate, while processing will increasingly be at the edge where the data was born and exists. Machine-learning algorithms will be able to adjudicate *peer-to-peer* communications and decisions in real-time.

Decision-makers will have access to sophisticated simulation models to support time-sensitive decision making. Access to models will also be available during training to improve realism. Low power flexible displays for soldiers will enhance information flow between the tactical and command levels and enhance situational awareness. Quantum encryption will allow encrypted communications between parties, instantly revealing eavesdropping.

Developments in BDAA S&T are driven by *massive* commercial investments, as well as the availability of publicly available training data sets and tools for algorithm development and testing [63, 64]. Many alliance nations have made significant BDAA investments in both civilian and military environments. NATO will, therefore, be able to leverage these investments, while extending, adapting and integrating them into NATO processes and operations. Continued investment in enabling capabilities, R&D collaboration and common standards and policies for data collection, curation and management will be necessary to ensure the successful integration of BDAA into the Alliance enterprise and operations. Potential legal, commercial and IP issues may provide additional challenges to the successful use of BDAA in a NATO context. Such challenges include introducing unanticipated vulnerabilities, limited configuration control and a lack of explainability.

MILITARY IMPLICATIONS

BLUE

Excelling at BDAA has the potential to create a NATO decision and knowledge advantage, grounded in the innovative collection, processing, exploitation, dissemination and fusion of immense and wide-ranging data sources and information products. Success in this area would support a more refined and comprehensive understanding of tactical, operational and strategic environments and courses of action. Areas most likely to be affected include:

1. **ISR**: The proliferation of advanced sensors and the increased use of autonomous systems will dramatically increase NATO's ability to detect, classify, recognise, identify and engage threats across physical and virtual operational domains. Adaptive solid-state power amplifiers and optimised waveforms will support simultaneous search and track capability for the interdiction of airborne targets, resulting in faster and more accurate ISR and exploitation of multiple intelligence source analysis. Passive radar reduces the vulnerability of systems to electronic countermeasures and increases the detection capabilities of stealth targets. Advanced processing at the sensor itself, will result in lower bandwidth requirements, faster sensor-to-shooter times and more reliable data transfer. Capabilities inherent in devices utilised to enable social media, such as video, audio, text, GPS, proximity detection, and others will transform traditional ISR capabilities. The addition of social network sensing to traditional sensor data fusion will enable: multimodal content filtering and summarization; data fusion for event detection; event tracking; analysis of social dynamics; and, anomaly determination.

2. **Situational Awareness**: Improved mapping of mission areas for planning & preparation and rehearsal environments will support operational planning and increased situational awareness (SA). This increased SA includes improved patterns of life, human terrain and anomaly detection. This awareness will be further enabled by enhanced low power display capabilities for soldier systems, embedded analytics (e.g. AI) and increased information flow between the tactical and command levels. Geo-tagged soldier system and social media data will also be used to generate increasingly accurate environmental information. Deep learning used in the deciphering of internet content has the potential to identify security-relevant information through social behaviour on the internet merged with content extraction from multiple text documents (even if specific intent is not explicitly referenced). Fusing social media data with more traditional sensor data provides a more vibrant and accurate human-terrain mapping and common operational picture [205, 206].

3. **Training and Readiness**: Virtual environments and bioinformatics will support improve training for operations. Physiological and psychological state monitoring will maximise overall human performance and readiness through increased health and safety monitoring and injury protection. Algorithmic optimisation of individual and team performance & readiness will also be possible.

4. **Enterprise Management**: NATO's basic business processes, policy development and strategic planning will all benefit from an increasingly sophisticated and evidence-based approach, including real-time monitoring of the impact of decisions and predictive assessments of options through advanced M&S.

5. **Logistics**: The increased integration of weapon system health monitoring sensors, real-time inventory monitoring and the use of *digital twins* will significantly increase the efficiency and effectiveness of the logistic system while reducing life-cycle costs. A greater understanding of the current status of munitions and their ability to achieve mission objectives will also be possible through *Integrated Munition Health Management* models enhancing relative safety, reliability and performance risks.

6. **Support to Operations**: Vast quantities of sensor data (ISR, logistics, bioinformatics, human terrain, etc.) will support a more comprehensive understanding and approach to the operational environment. Combined with AI, this will enable a more holistic approach to operational planning, courses of actions analysis and (kinetic and non-kinetic) targeting. Improved understanding and modelling of adversarial group behaviours will help enable the ability to generate courses of action that are disruptive to their goals and activities.

7. **S&T**: BDAA will have a significant impact on (defence) S&T through meta-analyses of existing scientific and technical knowledge. This meta-analysis, in turn, will lead to the creation of novel materials, development of new and better sensors, the discovery of new underlying science etc. which will directly impact the development of new NATO capabilities.

8. **Information Management**: Contextual programming will enable search engines to move beyond simple keyword searches by discerning the intent behind the search and offer more targeted information. This approach may be used to predict security risks from a deep analysis of personal contacts, social network behaviour, and location information.

RED

RED BDAA is expected to develop along the lines of those outlined for BLUE, where RED forces will seek to develop their decision advantage and get inside of the NATO OODA (Observe-Orient-Decide-Act) loop. Further:

- BDAA will increase the effectiveness and expansion of RED operations into non-traditional domains, enabling sophisticated targeting of individuals and social groups via and across the instruments of national power (*DIME*: diplomatic, information, military and economic).
- Increased NATO use of BDAA will introduce vulnerabilities in command decision making that may be exploited by sophisticated and non-sophisticated RED opponents. The focus of targeted cyber or information attacks will become more covert and explicitly designed to undermine BLUE decision making and destroy trust. Over-reliance on BDAA in decision making will increase the risk to and damage from cyber/information attacks.
- Increased globalisation and commodification of information and sensors means that potential adversaries will have access to much of the same data, commercial tools and encryption methods as BLUE.
- Proliferation of access to mobile computing solutions by adversaries is to be expected as these will be increasingly commercial in nature.
- Hybrid or memetic warfare employing social media deception, diplomatic *warfare* and influence operations undermine, delay or frustrate BLUE forces, nations and populations.
- The potential to locate camouflaged, stealthy, protected or submerged targets through the processing of large volumes of data from persistent active and passive sensors will have a significant tactical and operational impact on future Alliance operations. For example, the US nuclear triad could be highly destabilised [45].

Interoperability

Interoperability challenges are expected in the following areas:

- **Technical Obsolescence**: Rapid RED and BLUE BDAA technological evolution will require constant investment to maintain a technological edge and ensure operational resilience. This will challenge Alliance nations to maintain common technological and interoperable force, especially as the NATO enterprise, and operational commanders, come to rely on BDAA engendered near-real-time feedback, increased situational awareness and improved operational effectiveness.
- **Network Allocation**: The EM Spectrum is becoming more commercial, congested, contested and competitive globally from the commercial use of advanced radio-frequency technology. Alliance agreement on spectrum allocation and conflict will need to be undertaken.
- **Data**: Distributed data and verification structures will need to be developed to allow nations to maintain ownership and control of data while sharing within a coalition. Big data raises significant concerns about security, privacy and governance that will need to be addressed at an Alliance level. Development of policies on data collection, retention, exchange, curation, classification, bandwidth, taxonomies and privacy will be necessary.

- **Unique Standards**: NATO operational and enterprise environments have unique characteristics not shared by commercial and civil environments, including reduced risk tolerance and policy constraints. Legal issues may also become a concern as commercial interests seek to protect underlying intellectual property (IP) (e.g. explainable AI), thereby limiting *explainability* of recommended courses of action or assessments.
- **Standards**: National adoption of critical BDAA technologies (e.g. 5G) may create a significant digital divide due to differing threat perceptions and adoption of underlying technologies. A lack of standards and the development of incompatible or *untrustworthy* systems may limit NATO's ability to share C4ISR and other sensitive data.

S&T Development

BDAA research is highly interdisciplinary, with strong commercial and open-source underpinnings. Key areas of research and development are:

1. **Engineering Defence**: Counter-social-engineered and cyber agents (i.e. bots) to auto-identify, disrupt and investigate bot-mediate social and cyberattacks [202].
2. **Optimised Communications**: Novel technologies to optimise network resources, data throughput and (cognitive) spectrum management (including operations in a contested and congested environment with limited knowledge of other appliance, vehicles or sensors on the network) for distributed applications or sensing. The research will include exploration of new communication modes (e.g. 5G), mesh networks, post-quantum encryption methods and the increased used of cognitive (AI) methods.
3. **Analytics**: Novel mathematical, computational and human-factors approaches to the analysis of complex and complicated military socio-technical systems-of-systems (e.g. operational command), including fusion of noisy and uncertain data and operational decision making. This includes modelling and simulation of complex multi-scale physical, information and engineering systems. Development of data-driven discovery models [202] will be an essential aspect of this research as human engagement in the development of predictive models is a significant limiting factor. New distributed computational architectures (edge computing), as well as search and assessment technologies, will be necessary to discover, organise and present multi-domain content [202].
4. **Sensors**: New, distributed, low power and sensitive sensors capable of large scale mesh behaviour and self-organisation (ubiquitous sensing). This includes developments in analysis, fusion and assessment of signals from passive sources (e.g. bio-engineered), bio-social sensors, multisensor/multi-domain sources, and edge-computing.
5. **Trust**: Distributed ledger technologies, cyber-agents, improved visualisation and predictive analytics to support trusted information exchange and enhanced support to human decision making. This includes tools for identification and attribution of malicious social or cyber actors, as well as the development of RED-team cyber agents to assist cybersecurity operators in the determination of cyber-physical-human vulnerabilities.

The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

References

[32, 41, 44, 50, 192, 202, 207, 208, 209, 210]

Table A.1: *Big Data and Advanced Analytics (BDAA) 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Data	Advanced Analytics	Revolutionary	Expectation	4	2025
	Communications	High	Enlightenment	6	2030
	Advanced Decision Making	Revolutionary	Disillusionment	6	2025
	Sensors	High	Expectation	4	2030

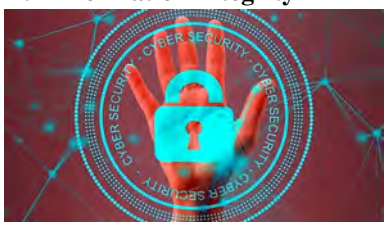
Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

Conjecture Card: Data

A.1 Real-Time Video Feeds

Access reliable real-time unhackable streaming video feeds from hand-held wireless devices.

A.2 Information Integrity



Assure the source and integrity information, networks and data to prevent insertion of distracting or false information by hackers.

A.3 Commercial Networks

Utilise state-of-the-art global always-on commercial networks for secure encrypted communication and data transfer.

A.4 Situational Awareness

Know the location and history of every single individual or item in a organisation or operation at any time, using digital twins and the IoT.

A.5 Trusted Systems

Trusted information exchange in zero trust environments, for example to exchange money or control check points.

A.6 Assured Connectivity

Store and retrieve strongly encrypted data/information across the network so it is always accessible and recoverable.

A.7 Courses of Action

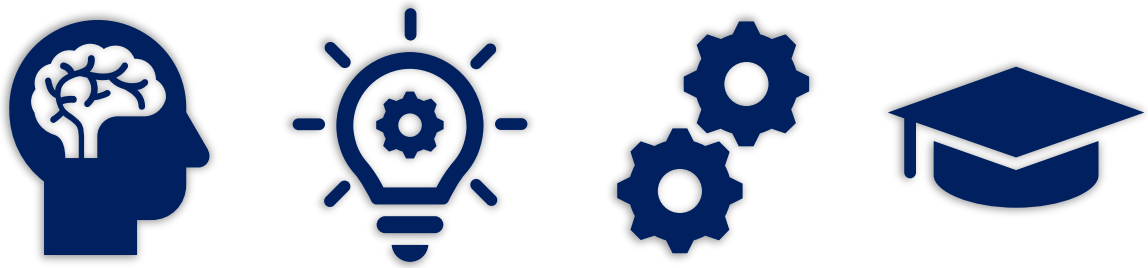
Simulate in near real-time billions of potential courses of action, identify optimal solutions, while adapting recommendations to real-time sensor information.

A.8 Global Intelligence

Conduct continuous global ISR and target acquisition in all operational domains, while fusing data into a single coherent rich intelligence system.

A.9 Algorithmic Advantage

Optimise enterprise functions, as well as providing predictive assessments in-real time to support enterprise decision making and capability development.



B. Artificial Intelligence

Artificial Intelligence
"By far the greatest danger of Artificial Intelligence is that people conclude too early that they understand it." - *Eliezer Yudkowsky* [211]

Definition

Artificial Intelligence
Artificial Intelligence (AI) refers to the ability of machines to perform tasks that normally require human intelligence – for example, recognising patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems [62].

Keywords

Artificial Intelligence · Machine Intelligence · Deep Learning · Neural Networks · Machine Learning · Expert Systems · Semantic Analysis · Supervised Learning · Unsupervised Learning · Reinforcement Learning · Clustering · Deep Fakes · Machine Vision · Chat-bot · Decision Trees · Data Science · Genetic Algorithm · Autonomy

Overview

Artificial Intelligence (AI) emulates aspects of human cognition such as perception, reasoning, planning, and learning. AI is able to autonomously perform tasks such as planning, understanding language, recognising objects and sounds, learning, and problem-solving. AI has been identified as the biggest technological challenge facing Alliance nations [45, 212], with some calling it the most important technology ever invented [213]. Over the next 20 years, AI is expected to play a significant disruptive force through its effects on:

- Exploitation of increased digitalisation and the resulting availability of (very) large data sets, including publically available data for system training and development;

- Widespread deployment and use in cyber-physical systems;
- Novel areas of application, driven by greater investment in and wider adoption of AI techniques;
- Decision making and optimal control (e.g. power systems, investment, etc.);
- Computation, such as advances in everywhere/edge computing, ubiquitous sensors, database design, developmental tools, cloud computing, new algorithmic approaches and using AI to bootstrap the development of AI; and,
- Development of advanced large data analysis tools and computer vision.

Since its beginnings in the mid-1950s, AI has moved through three development cycles (Figure B.1). The initial period focused on rules-based approaches (decision trees, Boolean and fuzzy logic), e.g. *expert systems* [214]. The second cycle focused on the development and application of statistical methods (i.e. supervised, unsupervised and reinforcement learning). Such *machine learning* methods have been highly successful and underlie everything from e-mail spam filtering to internet web searches. The third cycle of development focuses on the use of bio-inspired learning methods (neural networks, deep learning), with considerable success in the areas of sensing and perception [215].

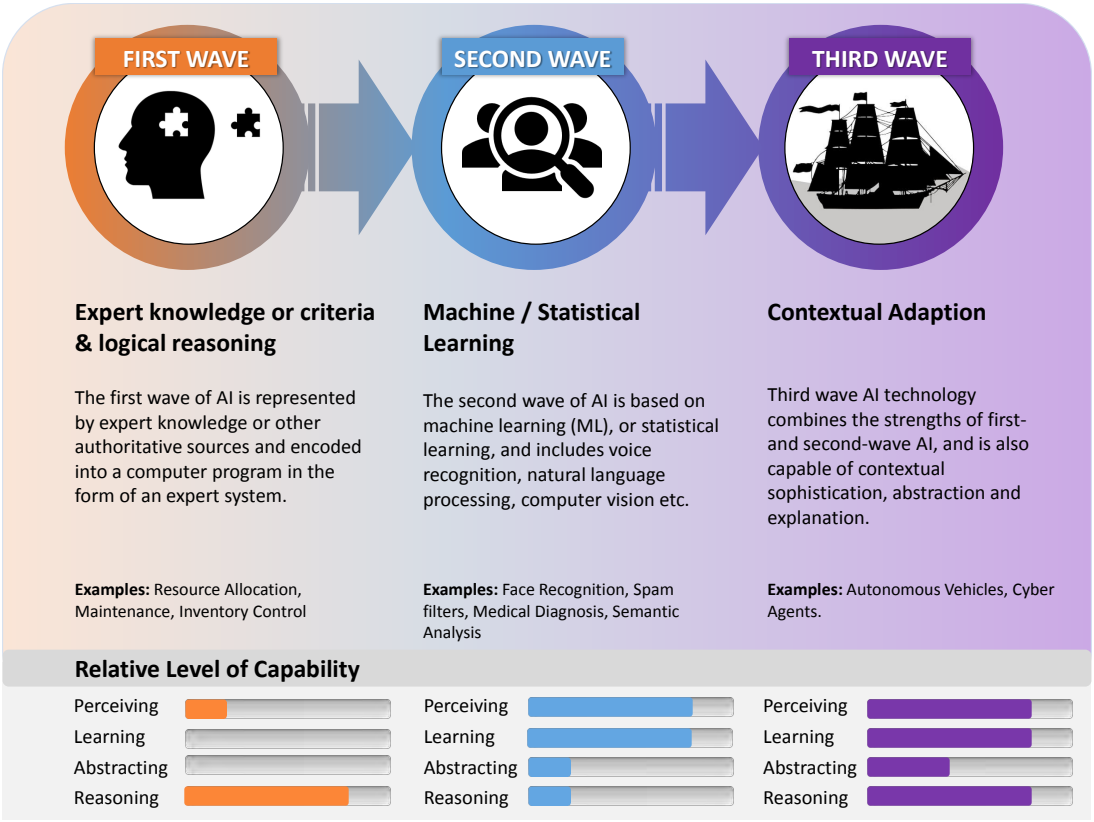


Figure B.1: *3 Cycles of AI (CREDIT: Adapted from [216]).*

While major strides are continuing to be made in deep-learning methods [118], new research areas are being developed, including *neuromorphic computing*, which attempts to more accurately emulate the neural structure and operation of the human brain [215], and *adversarial machine learning* which seeks to understand how to confuse AI systems [217, 218]. Another promising area is that of *probabilistic computing*, designed to deal with *uncertainty, ambiguity, and contradiction in the natural world.* [215]. Research in these areas includes new machine and deep learning methods focusing on the use of smaller training sets and explainability. Another major area of R&D will be the development of new machine and deep learning algorithms based on quantum information science and quantum computers. Continued R&D into new and more general-purpose algorithms will be critical in maintaining the current momentum behind AI research and moving AI beyond its current practical limitations.

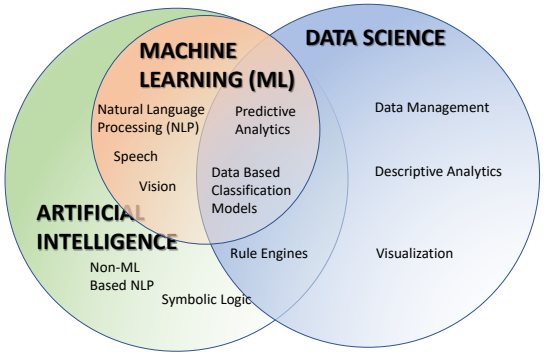


Figure B.2: *The Relationship Between AI, Machine Learning and Data Science (CREDIT: Adapted from [219]).*

R&D opportunities exist to substantially expand the analysis of large data sets, including those associated with sensor data processing, fusion and analysis. Indeed, the expected continued rapid explosion in digitised data will make the use of AI (and its derivatives) even more useful and a practical necessity for BDAA. To put this in context, in 2020 the world is expected to produce 44 trillion gigabytes of digital data, with an annual growth rate expected to be on the order of 60% [45], with over 500. Without AI, individuals and organisations will be challenged to turn this *data glut* into actionable knowledge.

This reliance on large quantities of data is both a strength and a weakness of AI. Data quality, in particular, is a critical issue, both for assessment and training. Reliance on large curated and filtered (training) datasets is an essential element of many AI algorithms and a significant contributor to the fragile nature of many AI application. Research is being conducted on the development of more adaptable and efficient machine learning algorithms that will require less labelled data and are capable of making inferences with sparse or contradictory data while making them easier to train, more resilient to unpredictable real-world conditions and generalizable to new environments [202]. In a similar vein, research is being conducted into the use of deceptive data and adversarial attack, whereby the injection of malicious data could be used to manipulate or provide an assessment of an AI system [202]. As AI systems become ubiquitous and underpin decision making in complex systems-of-systems, the need to develop appropriate countermeasures and algorithmic resilience will be essential.

Development of symbiotic AI (i.e. human-centric), whereby humans and cognitive machines work together as trusted partners in a complex-hybrid system, is a significant research challenge [202]. Fundamental R&D is necessary to improve the understanding of human speech, extraction of semantic information inherent in a wide variety of media and responding to non-verbal aspects of communication. Such capabilities will also allow a more natural interaction and partnership, but will also necessitate the integration of analogues to human perception in the physical (e.g. vision) and human domains (e.g. emotions), along with the development of *machine common-sense* (i.e. the embedding of *a priori* knowledge [202]. This will also necessitate the development of systems capable of asking questions, speculating, proposing multiple options, enhanced learning and explaining clearly the decision or deliberative process. As noted by DARPA [202]:

Figure B.3: *Symbiotic AI.*

> *"Enabling computing systems with such human-like intelligence is now of critical importance because the tempo of military operations in emerging domains exceeds that at which unaided humans can orient, understand, and act."*

Such human-machine symbiosis provides a more robust and potentially more effective construct leveraging the strengths of both human and machine.

The application of AI is considered a priority S&T investment area across the globe [31, 45]. Significant developments in the application of AI are primarily driven by industry. Still, advancement in the application and development of AI has been significantly enabled by the development and availability

of open-source tools and publically available data (e.g. Enron data set [220]). This does not mean that Alliance nations themselves are not also investing in AI. As noted in [221]:

> *"The Pentagon is figuring ways to harness artificial intelligence (AI) for advantages as far-flung as battlespace autonomy, intelligence analysis, record tracking, predictive maintenance and military medicine. AI is a key growth investment area for DoD, with nearly $1 billion allocated in the 2020 budget. The Defense Department's Joint Artificial Intelligence Center (JAIC) will see it's budget double to over $208 million, with significant increases likely in 2021 and beyond ... The military is currently seeking to integrate AI into weapon systems development, augment human operators with AI-driven robotic manoeuvre on the battlefield and enhance the precision of military fires."*

National capacity and proclivity to use AI are as important as research and development of AI methods (see Figures B.4 and B.5). As such, other nations are staking a claim in the AI gold rush. For example, Figures B.4 and B.5 highlights the range of preparedness by national governments to exploit AI and the current level of application or experimentation of AI within national industries. China, following the release in 2017, of its AI development plan [129] has also obviously moved quickly to expand the science of AI and explore its use. As noted by [45]:

> *"The growth in AI development is not limited to the United States. China has identified AI as a strategic priority. Last summer, China's State Council issued an ambitious policy blueprint calling for the nation to become "the world's primary AI innovation center" by 2030, by which time, it forecast, the country's AI industry could be worth $150 billion ... In the words of one analyst, "the digital revolution is going to be the biggest geopolitical revolution in human history [. . .] Every other twenty-first-century geopolitical trend will look piddling by comparison."*

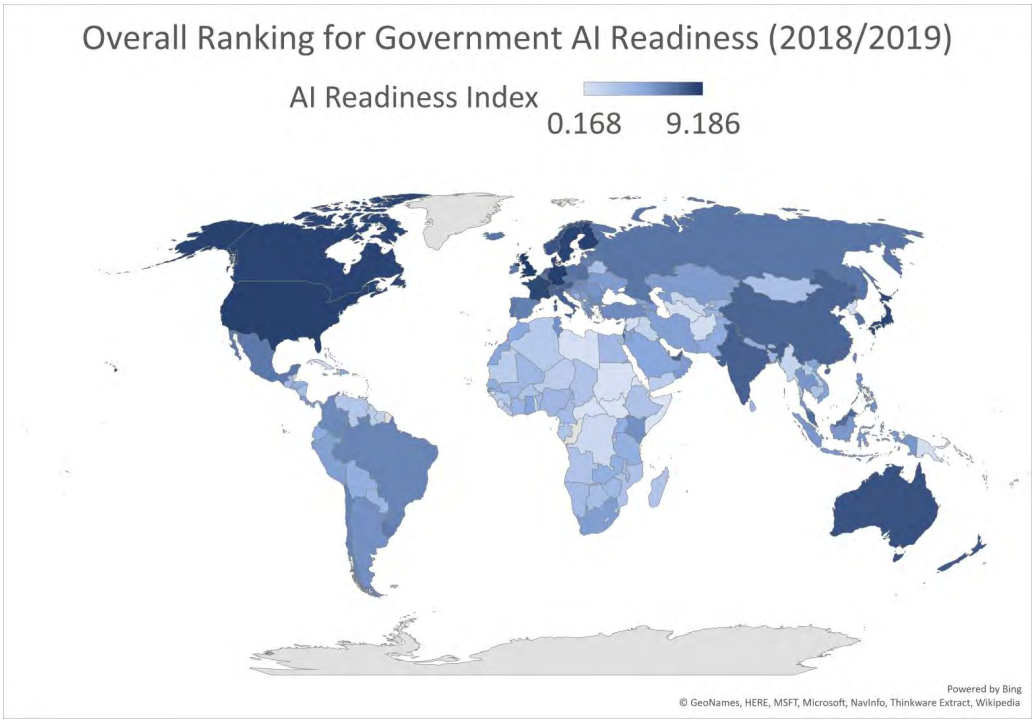


Figure B.4: *Overall Ranking for Government AI Readiness (2018/2019) (SCALE: 0 [Poor] - 10 [Excellent]) (SOURCE: [222])*

Nevertheless, the current state of AI is complicated. While there is considerable investor interest driving an explosion of practical AI applications, there are early indications that AI research is reaching a

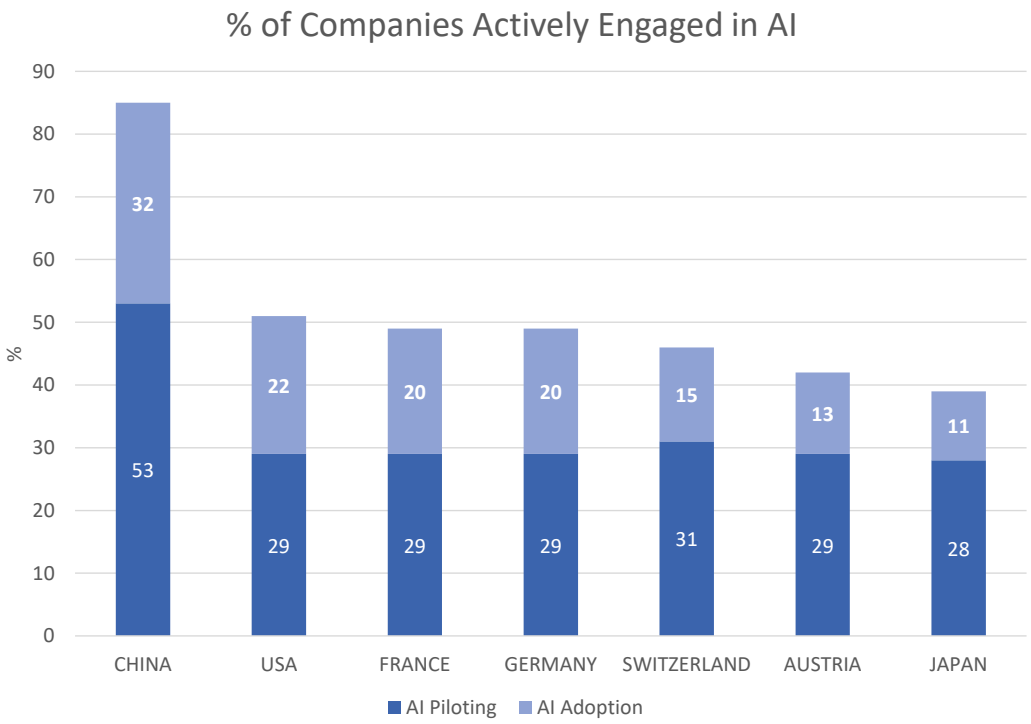


Figure B.5: *Percentage of Companies Actively Engaged in Piloting or Adoption of AI, by Selected Countries (SOURCE: [223])*

plateau. Concerns that AI is approaching another *AI winter* of slow growth and disappointment have been raised by several authors [224, 225]. The need for new algorithmic approaches and a better understanding of human-machine teaming has probably never been stronger [202, 226, 227]. In particular, the development of *Artificial General Intelligence* (AGI) (i.e. human-level generalised intelligent behaviour), is a significant technical challenge and remains a very difficult or perhaps even chimeric goal, in-spite of over 60 years of AI research. It is considered unlikely that AI systems will meet this level of cognitive ability within the next 20 years [228].

Finally, one area of fundamental AI disruption will be its use to augment science and increase the rate of innovation [213, 229, 230, 231, 232, 233, 234, 235]. The combination of human-AI reasoning will be a powerful combination in exploring new and exciting areas of research and innovation. Sir Issac Newton (1642-1727), the great English physicist, once said:

> *"I do not know what I may appear to the world; but to myself I seem to have been only like a boy playing on the seashore, and diverting myself in now and then finding a smoother pebble or a prettier shell than ordinary, whilst the great ocean of truth lay all undiscovered before me."*

AI & BDAA, as applied to science, has the potential to become humankind's digital *best friend* greatly expanding our ability to explore the scientific seashore and find even more interesting pebbles and shells. Schrodinger may have his cat, but Newton will have a dog.

Military Implications

BLUE

AI will significantly impact alliance military capabilities and forces. This impact will occur predominately through the use of embedded AI in other associated technologies such as virtual/augmented reality; quantum computing; autonomy, modelling & simulation, space; materials research; manufacturing &

logistics; and, big data analytics [236]. AI will have transformative effects on nuclear, aerospace, cyber, materials and bio-technologies. It has been stated that these effects will have a strategic impact on the same order as the introduction of nuclear weapons [237]. Further, over-reliance on AI systems will also introduce significant new vulnerabilities and usher in an adversarial AI arms-race.

Some areas of potential areas of impact over the next 20-years are expected in the following areas:

- **C4ISR**: War-fighting units will employ trusted AI-enabled autonomous systems capable of performing tasks that move beyond those that are deemed dull, dirty, dangerous or dear. Some of the areas for potential application are expected to be in the increased use of virtual assistants (analogous to *Google Home*, *Apple Siri*, or *Amazon Alexa*), AI-enabled decision support to war-games and AI recommended courses of action (COA). AI holds considerable promise for enhanced data fusion, as well as categorisation and effects based assessments (or targeting). For example, Intelligence analysts will be able to leverage trusted systems capable of tasking, collecting, processing, exploiting, disseminating (TCPED), and retrieving information across the entire spectrum of available sensors and relevant archival data. Additional areas of AI integration will include enhanced indications & warning, information and knowledge management tools, as well as decision aides enabling more rigorous and robust intelligence analyses. This will include establishing patterns of life, human terrain mapping, social network analysis, as well as decision support for targeting. Very high speed, very low power neuromorphic electronic components offer the possibility of autonomous systems and computer architectures that may rival human perception at very low power, enabling embedded sensor processing for scene recognition, target discrimination, and identification.

- **Weapons and Effects**: AI is seen to be of potential use in cross-cueing, trajectory planning, collision avoidance, swarming, weapon selection, battle damage assessment and effects coordination.

- **UxV**: Areas of potential AI impact in trajectory planning, collision avoidance/swarming, operator assistance (e.g. one operator controlling multiple-UxVs). Dynamic mission planning for autonomous systems (e.g. navigation, data collection, environmental characterisation and adaptive sensing). The integration of deep learning systems into mobile platforms will enhance robotic capabilities for navigation within dull, dangerous, dirty or dear situations. AI could enable fully autonomous explosive ordnance disposal in urban areas. Intelligent autonomy will enable capabilities such as long duration unmanned underwater vehicles.

- **Capability Planning**: AI will support the development of analytical solutions to assist in long term planning within NATO, including supporting complex decision-making that cuts across traditional internal boundaries; assisting assessments of complex factors and effects chains for decision-makers.

- **CBRN**: NATO requires a suite of enabling and integrated technologies that provides rapid detection, identification, and monitoring (DIM) of CBRN threats/hazards during any mission, in all operational environments, which informs on the course of action necessary to mitigate the threat/hazard. AI may support improve autonomy to perform detection, sensor integration and data fusion. AI is seen as a means of alleviating the burden of human involvement in determining the position of sensors and initiating data fusion and data interpretation. Use of AI will enhance command situational awareness and support through new abilities to self-organise and assume the optimal posture needed to achieve desired end-states. Ultimately, this will increase the knowledge of current and potential controlled agents incorporated in software suite in Stand-off platforms, increasing hazard management capability.

- **Medical**: Modern military forces require clinically relevant and empirically validated medical interventions and associated procedures. AI has the potential to assist in developing evidence-based clinical knowledge, evidence-based diagnostics and treatment best practices to reduce morbidity and mortality and maintain/recover essential functions in the face of hazards from across the mission spectrum. Further, AI will provide automated decision support and diagnostic support tools to assist medics in the field who are dealing with novel trauma situations.

- **Enterprise Management**: NATO requires more efficient and effective processes for enterprise resource management (investment and business planning, program performance and risk management, strategic transformation, and improvement initiatives, strategic readiness management, and strategic management practice) based on advanced analytics and evidence-based decision making. With respect to finance, AI can assist in cost analysis, assessment of economic impacts and drivers, and the provision of timely evidence-based decision support.

- **Logistics**: AI systems (especially when paired with digital twins) have the potential to minimise equipment downtime, minimise system failures, improve inventory and repairs management etc. Problems of these sorts are similar to those encountered in the commercial world and are therefore primed for early adoption by NATO.

- **Cyber & Info-space**: Intelligent (i.e. AI-enabled) autonomy extends beyond mobile platforms. For resilient autonomous networks and cyber-warfare, the system must detect, evaluate and respond well before humans would be capable of understanding the situation. Desktop applications will assess and interpret vast amounts of sensor and intelligence data. These systems and virtual agents will have the capacity to make independent decisions and act upon these decisions rapidly, while at the same time, work as part of a human-AI team. One would expect that networks and information systems will be configured, maintained, and protected by AI-enabled autonomous agents.

- **Training**: AI systems (especially when paired with virtual/augmented reality systems) have the potential to improve individual and customised training through real-time adaption to human behaviour and the generation of customised training environments or scenarios.

RED

The advantages outlined for NATO forces are equally applicable for near-peer or asymmetric RED forces. However, the reliance on AI will also increase the potential impact of cyber and information attacks. Further, with fewer ethical and legal bounds, RED may enable AI functions from beginning to end of the kill chain, in order to achieve a tactical decision advantage or as a response to a loss of communications. Additional RED aspects of future AI developments are:

- **Cyber**: AI systems are particularly vulnerable to cyber attacks, whereby small, deliberate changes may lead to erroneous recommendations or sub-optimal actions.

- **Information**: Advances in speech processing and synthesis technology are likely to allow the realistic simulation of friendly and enemy personnel over communications links and broadcast media (i.e. deep fakes). Combined with twitter-bots and other social media hacks, ever more effective AI (e.g. generative adversarial networks (GANs)) will greatly increase the scale and effectiveness of hybrid attacks, whether by near-peer or asymmetric threats [238].

- **Aberrant Behaviour**: Unanticipated behaviour in AI systems is simultaneously a strength (e.g. creating entirely new strategies [239] and at the same time a significant potential liability. Limitations imposed through legal, ethical and policy considerations may be more relaxed for peer or near-peer opponents. A RED weapon system unrestricted by the physical limitations of the human body, whose behaviour is often unpredictable and inexplicable, would potentially constitute a formidable adversary.

- **IEDs**: Increasingly intelligent, learning systems will enable new generations of improvised explosive devices, less susceptible to traditional countermeasures.

Interoperabilty

AI interoperability will be a serious challenge. As AI-enabled systems become increasingly common, the need to define interoperability, data and specialised communication standards will become acute. One

critical aspect is the need to define and conduct verification, validation and accreditation (VV&A) of AI enabled operational decision support AI systems for use in Alliance military operations. The Alliance will be challenged to do so by differing standards on verification, validation and accreditation (VV&A); differing rules on data management, taxonomies, and training sets; explainability concerns; man-machine teaming & symbiosis concepts; and differing levels of system and organisational *trust*. It will be necessary to build processes and policies that fundamentally recognise, as with any human part of the system, their potential fallibility.

As has been noted, AI explainability is an active and vital research area [202]. However, it must also be noted that commercial interests may push back on such a requirement given the possibility of exposing intellectual property and underlying algorithms [240]. Standardising this across the Alliance will present significant challenges.

S&T Development

AI faces a number of critical challenges or areas of research. Advances are necessary in the following areas:

- **Advanced Algorithms**: Improvements in the effectiveness and generalisation of AI. Continued research will be necessary in the areas of machine & deep learning, adversarial AI, as well as neuromorphic & probabilistic computing.
- **Human-Machine Symbiosis**: Advances in interfaces, human-centric AI, visualisation, explainability, and socio-technical implications (e.g. team dynamics);
- **AI Application**: AI is an underpinned technology supporting predictive, prescriptive and even cognitive data analytics. There is a need for processes to transform both structured data (e.g. machine learning techniques with varying levels of complexity, from regression to neural networks) and unstructured data (e.g. using deep learning and natural language processing) into insights and foresight for decision-makers. These tools may then be applied to critical defence and security challenges such as:
  - **Psycho-Socio-Technical**: The use of AI to enable human, social or complex system agents within M&S, supporting more realistic analysis and personalised training.
  - **Adaptation**: Adaptive techniques will out-mode current intelligence cycles in areas such as electronic warfare. The development of a new intelligence paradigm may be required.
  - **Cyber**: Development of AI agents for defensive cyber (e.g. bio-inspired equivalents of immune systems T-cells) and offensive cyber operations (e.g. penetrative and vulnerability seeking agents).
  - **Infospace**: Weaponising information through AI (e.g. deep fakes) and development of hybrid-warfare countermeasures (e.g. sustain trust and counter vulnerabilities).

The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table B.1: *Artificial Intelligence: 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Artificial Intelligence	Advanced algorithms	Revolutionary	Expectations	4	2030
	Applied AI	Revolutionary	Expectation	6	2030
	Human-Machine Symbiosis	High	Trigger	4	2035

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

References

[45, 105, 173, 212, 216, 219, 221, 224, 234, 235, 236, 241, 242, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252]

Conjecture Card: Artificial Intelligence

B.1 Detect/Generate Fake Media

Automatically detect or create fake media reports, video, audio and social media posts responsive to live situations or to communicate in real-time with targeted individuals or groups.

B.2 Virtual Command Advisor

Support and advise operational commanders in real-time with human-like reasoning and advice based on previous operations, leveraging comprehensive operational awareness.

B.3 Automated Communication

Equip individual soldiers to automatically, instantly identify and accurately translate languages, body language and human emotions anytime and anywhere.

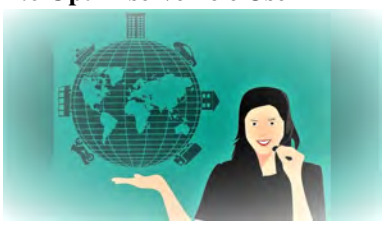
B.4 Spoof AI Systems

Covertly get in-side the OODA loop of adversary's AI systems to insert misleading data or information to impact their decision-making processes.

B.5 Deep Fakes

Modify and mimic adversarial communications, including those in real-time (video, audio, etc.) to destroy trust.

B.6 Optimise Vehicle Use



Optimally allocate and route vehicles (e.g. transport, medevac, ISR, tanks, APC, etc.) using real-time situational awareness of the operating environment.

B.7 Disruptive Behaviour

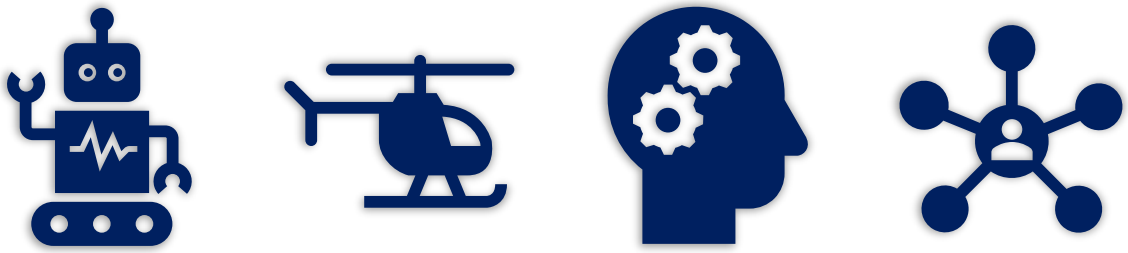
Accurately predict the behaviour of humans or groups from background data (e.g. social media, surveillance, biometric devices).

B.8 Precision Engagement

Acquire and engage targets in a crowded, cluttered or dynamic environment with highly localised-effects (kinetic or energy-based) and selective lethality.

B.9 Automated Targeting

Provide precision targeting advice, across the military, economic, information, and diplomatic spectrum to achieve a desired operational/strategic effect.



C. Autonomy

Autonomy
"Autonomous Systems raise challenging operational, strategic, and policy issues, the full scope of which cannot yet be seen. The nations and militaries that see the furthest into a dim and uncertain future to anticipate these challenges and prepare for them now will be best poised to succeed in the warfighting regime to come." - *Paul D. Scharre* [176]

Definition

Autonomy
Autonomy is the ability of a system to respond to uncertain situations by independently composing and selecting among different courses of action in order to accomplish goals based on knowledge and a contextual understanding of the world, itself, and the situation. Autonomy is characterised by degrees of self-directed behaviour (levels of autonomy) ranging from fully manual to fully autonomous [66, 67, 68]. *Robotics* is the study of designing and building autonomous systems spanning all levels of autonomy (including full human control). *Unmanned Vehicles* may be remotely controlled by a person or may act autonomously depending on the mission. Applications include allowing for access to unreachable areas, persistent surveillance, endurance, robots in support of soldiers, cheaper, automated logistics deliveries.

Keywords

Autonomous Vehicles · Automated · U(A/U/CA/x)AV · Man-Machine Interface · Autonomy · Human-(in/out/on)-the-loop · RAS (Robotics and Autonomous Systems) · Human-Machine Teaming

Overview

Robotics and Autonomous Systems (RAS) are a key enabler and beneficiary of developments in other EDT areas. From a technology watch perspective, developments of interest to NATO will be predominantly in the areas of: **(1) Autonomous Systems** (platforms, devices & agents): e.g. new platforms; propulsion; software agents; low power sensors; IoT devices; and, applications. Areas of particular

note are: autonomous hypersonic vehicles; bio-inspired micro and mini aerial vehicles; miniaturisation, small satellites (smallsats); hybrid-electric aero-propulsion systems; light-weight high-resolution hyper-spectral imaging technology for semi-persistent surveillance missions; RF sensor miniaturisation; plasmonics for decreasing IR detector size; rapid 3D environment modelling; and use of robotic decoys; **(2) Human-machine teaming**: human performance enhancements, human-machine collaboration and communication; **(3) Counter-measures**: high power radio frequency (HPRF) weapons; and, **(4) Autonomous Behaviour**: control, swarm centric systems and intelligent autonomy (i.e. increasingly advanced embedded AI).

Platform autonomy is one of the more important examples of militarily relevant robotics and autonomous systems (RAS) [176, 253]. Such *UxVs* are uncrewed vehicles for air (UAV, UCAV if combat capable), sea (underwater (UUV) and surface (USV)) and land/ground use (UGV). Since the launch of the first experimental, fully autonomous spacecraft (Deep Space 1) in 1998 [254], AI-enabled autonomous systems (especially smallsats) have catalysed novel technological developments in and use of space [255, 256]. UxVs may be remotely piloted or may act at varying levels of autonomy throughout a mission [66]. Research into UxVs cover a wide spectrum of enabling technologies including: stealth (signatures: infrared, acoustic); qualification & certification; structures & materials; propulsion; performance; stability & control; and, design.

Figure C.1: *Underwater Autonomous Vehicle.*

While UxVs have become increasingly common and essential capabilities for military operations [257, 258], the use of virtual software agents or *bots* are also being investigated for offensive and defensive action in information and cyberspace. Analogous to the immune system, the development of safe, secure and reliable autonomous software agents as part of a cyber-physical immune system [259] will provide a means to counter and characterise bot-nets & large scale malware attacks, along with other cyber events. Such counter cyber-adversary systems will also observe and monitor attacks in a covert fashion while minimising the impact on alliance network systems and infrastructure [202]. Adversarial agents support cyber operations at both the enterprise and internet-scale.

Of critical importance are resilient autonomous networks and cyber-warfare agents, where the system must detect, evaluate and respond well before an operator could understand and react. A good deal of important decision software must utilise autonomy to reduce the operator s cognitive load. These systems will assess and interpret vast amounts of sensor and intelligence data to produce actionable information and recommendations for the warfighter. They will have the capacity to make independent decisions and act upon these decisions rapidly, while at the same time, have the ability to work as part of a team which includes people. This level of intelligent autonomy will result in systems that work seamlessly with the warfighter, can enhance warfighter trust in the systems, and lead to an almost unlimited force multiplier and substantially increase the pace of operation.

Autonomous systems, whether unmanned platforms or agent-based, may execute defined missions with or without human interaction or supervision. The degree of autonomy of the unmanned system (UMS) depends on the agent's or vehicle's own abilities for sensing, analysing, communicating, planning, deciding and acting. These, in turn, are influenced by the complexity and constraints (e.g. legal, policy, etc.) of the mission. While unmanned systems are increasingly being used in military operations, for the near term full autonomy of unmanned systems will be practical only for more straightforward tasks. An example would be a remotely piloted or autonomous helicopter that is capable of fully independent operation for a portion of its flight in order to deliver supplies and ammunition to troops in the field or medivac casualties [260].

While fully autonomous systems may be a long term goal, in the short and medium-term, semi-autonomous systems will have more impact on operations. These systems will collaborate with the

warfighter who will retain control and ultimately, final decision-making authority while enhancing situational awareness, effective reach, and reducing the risk to personnel participating in the operation. The major challenge for such autonomy is the limitation of risk during operation. Mission complexity is a major driver for risk, and the resulting feasibility of risk limitation or mitigation may limit use.

Research into UxV stealth technologies relevant for smaller and low power systems, is also essential, originating from the need to limit or avoid the detection of BLUE systems by RED forces. Developments in this area aim to reduce vulnerability to detection methods (radar, infrared, sonar). Such signature requirements may also influence and drive novel platform designs. At the same time, new miniaturised, low power sensors are required to support embedded AI, situational awareness and generally increase ISR capabilities. Research in this area is also driven by commercial needs for autonomous vehicles, leading to increasingly more powerful and cheaper EO/IR, LIDAR and RADAR sensors.

Figure C.2: *Global Hawk.*

The application of RAS is the commercial world and for military operations is developing rapidly [253]. In a defence context ISR, logistics, cyber defence and targeting are all areas that have or are expected to be heavily impacted by the wide-spread use of autonomous systems (e.g. [261]). The growth and wide-spread adoption of low-cost persistent sensing (including multi-statics) combined with large scale autonomous collection & systems, will create *the-domain-of-things* in airspace/space [45], oceans [262], or in urban areas [202]. This includes distributed networks of heterogeneous or possibly multifunctional sensors and specialised sensor suites on multiple autonomously operating mobile platforms. The potential impact on situational awareness and operational effectiveness will be substantial.

Figure C.3: *Small Drone.*

To fully realise the benefits of autonomous vehicles, unstructured geospatial data and metadata will need to be of high quality, easily accessible, and readily available [208]. As such, increased use of autonomous systems to characterise virtual or physical environments helps to *bootstrap* increased effectiveness. There will be associated challenges on the fusion and categorisation of this information. The research will need to draw upon advanced statistics, combinatorial optimisation, statistical decision theory, and mathematical game theory. Robust, systematically evolving, and adaptive fusion engines for military multiple purpose applications will need to be modular, controllable, and embedded via interoperable interfaces.

For Alliance activities in the air and space domains, the use of autonomous systems will be an essential element of future operational success [66, 241]. This success will, however, be built on a continuing exploration of converging technologies as noted by [241]:

> *"Swarms of low-cost, autonomous air and space systems can provide adaptability, rapid upgradability, and the capacity to absorb losses that crewed systems cannot. By leveraging advances in artificial intelligence, low-cost sensors, and networked communications, low-end systems can restore the agility to attack adversary weaknesses in unexpected ways by exploiting numbers and complexity. ... Multidisciplinary efforts are needed to combine research across low-cost platforms, agile digital and additive manufacturing, modular component and material technologies, autonomous system algorithms, and risk-based certification. Methods are needed to control large numbers of autonomous systems coordinated with tradi-*

tional manned assets. Artificial intelligence advances are needed to achieve high levels of intelligence in small, embedded systems and execute complex missions with trust."

Mini, micro and nano UxVs are an emerging solution for a broad range of modern military missions, including urban and unconventional warfare, battle damage assessment, tactical (ISR) (e.g. [263, 264, 265]). Research in this areas aims to exploit bio-mimetic materials (e.g. artificial mussels), as well as propulsion and behaviour (e.g. [266, 267, 268]). The development of cheap swarms of micro-UxVs will be an essential element of future IoT ISR networks but arming such systems present significant operational, policy and ethical challenges [269].

In the land domain, the impact will be dramatic [176]:

"The increased use of RAS capabilities will fundamentally change the way the Army fights by increasing situational awareness, reducing the soldier's physical and cognitive workloads, improving sustainment, facilitating movement and manoeuvre, increasing reach and range and force protection. In turn, this will afford Joint Force commander's new opportunities and, potentially, replace soldiers in some of the most dangerous tasks in the battlespace. RAS technology will also provide a significant opportunity in the training and education of Army to improve learning and provide cost-effective and realistic training."

The US Army, in particular, has identified five land force RAS capability objectives [270]: to increase situational awareness; lighten soldiers' workloads; sustain the force; facilitate movement and manoeuvre; and, and protect the force. In addition to UGVs, development of new autonomous subterranean vehicles will be a requirement for land forces, especially those operating in an urban setting. Such vehicles will need to navigate networks of tunnels, sewers, caves and other urban subterranean environments [202].

For maritime operations, multiple capabilities are seen to be especially amenable to the use of autonomous systems: Mine Counter Measures (MCM), denied-area ISR, Anti-Submarine Warfare (ASW), environmental characterisation, the-ocean-of-things, SIGNIT/ELINT collection and operational deception [202, 271, 272, 273]. Ocean environments are particularly challenging, facing pressure, temperature, navigation and corrosion limitations, as well as long operational deployments. Long range underwater gliders are particularly well suited for this role.

Figure C.4: *Anti-Submarine Warfare (ASW) Continuous Trail Unmanned Vessel (ACTUV) (CREDIT: DARPA).*

The impact of autonomous systems will be felt not just on the battlefield but also within operational support. For example, logistics operations are an area where warehouse robotics are widely used in commercial applications, with obvious benefits for military operations [257]. The broader applications of robotics (e.g. exoskeletons) and autonomous systems within the logistics chain (e.g.aerial refuelling [274] or squad support vehicles [275, 276]) have the potential to increase operational availability, weapon system effectiveness (e.g. loitering munitions [277, 278]), improve effectiveness and efficiency of the logistics system and reduce casualties [279].

With the broad availability across physical and virtual domains comes significant human-machine teaming challenges. This challenge will occur across the spectrum of autonomous operations. Most of today's deployed military uncrewed systems are remotely operated by an operator who augments the system s guidance, situational assessment, and decision-making. These systems have demonstrated unquestioned value, playing vital roles such as Improvised Explosive Device (IED) interrogation, aerial surveillance, checkpoint inspection, and land or sea mine clearance. Although these systems help keep warfighters safe and improve ISR capabilities, current unmanned system technologies result in increased manpower needs and place an increased cognitive load on the warfighter [280, 281]. While some levels of autonomy have been introduced in recent unmanned systems, autonomous systems lack the intelligence

to actually reduce manning requirements, reduce warfighter cognitive load, or increase the pace of operations. Intelligent autonomy will enable capabilities that are not currently possible, such as long-duration unmanned underwater vehicles, where the vehicle must be able to work for months without human intervention or communication.

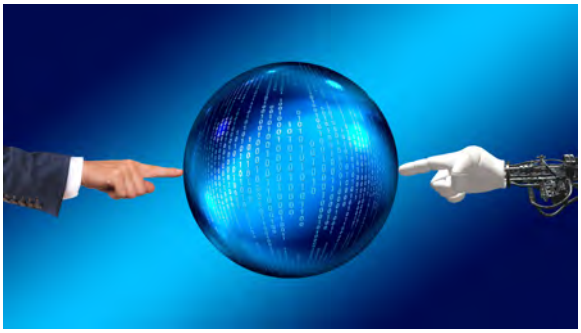


Figure C.5: *Human-Machine Teaming.*

Collaborative autonomy is a feature of widely autonomous systems acting as a social-technical team (eventually with distributed tasks) under the command of a warfighter. Systems of this nature will assess and interpret vast amounts of sensor and intelligence data to produce actionable information and recommendations for the warfighter. They will have the capacity to make independent decisions and act upon these decisions rapidly, while at the same time, work as part of a human team (with attendant social, collaboration and communication issues). This level of intelligent autonomy will result in systems that work seamlessly with the warfighter, are able to build warfighter trust, and act ultimately as a significant force multiplier. Research continues on the development of procedures to evaluate vehicle/operator/team system performance as a function of platform autonomy.

New modalities for human-machine communication are being developed [173] to fully exploit human-machine teaming, including non-invasive neurological & neuro-motor interfaces, virtual environments, biosensors, new visualisation approaches and controls. The technical limitations of human control must also be considered and mitigated as RAS systems are subject to well-known problems of automation bias, lack of situational awareness and moral buffering [169]. Finally, as we move towards the seamless integration of RAS the socio-technical implications, especially around team behaviour and collaboration, will need to be explored and better understood (e.g. [282]).

In the context of military sensor systems, a single large multisensor platform can be conceptually broken down into a *sensor team* comprising a limited number of platforms, where each platform possesses fewer or cheaper sensors than the single large platform. This concept can then be extended to a *swarm* whereby each platform is even smaller and possesses limited performance sensors; however, the loss in sensor performance at each platform can be compensated for by large numbers of cheap platforms in the swarm.

A swarming system is potentially low-cost and robust against the failure or destruction of the nodes in the swarm but comes with an increase in organisational complexity. Solving the self-synchronisation problem for moving platforms will pave the way to multisensor and networked drone swarming. Swarms can also display adaptability and intelligent autonomous behaviours through relatively simple local interactions and coordination. A swarm is dependent on a variety of technologies, such as sensor signal processing, data fusion, cognitive and intelligent control and learning. Swarms can be deployed for a range of intelligence, surveillance and reconnaissance (ISR) applications. The use of C-130 (Hercules) *flying aircraft carriers* [283] and *arsenal* vehicles (ships or aircraft [284]) to carry and deploy large numbers of UxVs into theatre is already being explored as a means of rapid swarm deployment. The use of large scale swarms of autonomous vehicles in urban areas, in particular, is seen to be a significant potential force multiplier [285].

Figure C.6: *Drone Swarm (CREDIT: DARPA).*

Small satellites are fast becoming viable platforms for effecting specific military missions, with cheap smallsats ideally suited for wide deployment. They can carry common or specialised payloads and can

operate individually, together in constellations, or autonomously in swarms for higher complexity missions. As such, swarms of smallsats provide a cost and potentially highly effective ISR and communication missions.

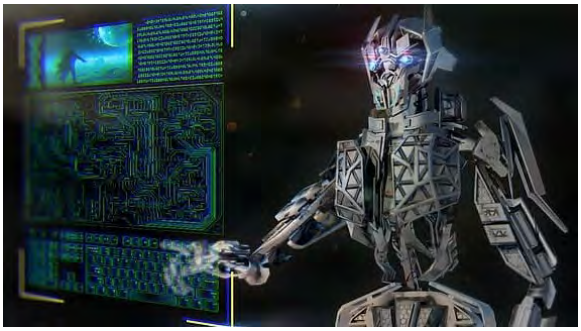


Figure C.7: *Machine Learning and Testing.*

As learning-enabled RAS becomes more widely deployed on the battlefield and in other uncertain environments, it will be necessary to develop innovative system designs, as well as new analysis, testing, and verification and validation (V&A) methods [202]. Success in this area will allow more rapid deployment of learning-enabled systems, as well as reducing operational risks.

As RAS (both physical and virtual) becomes more and more essential on the battlefield, the need to protect one's own forces becomes acute. Use of intercepting counter swarms [286], electronic countermeasures, lasers and other directed energy systems (e.g. high power radio frequency weapons) offer some options. Nevertheless, the broad range of autonomous systems, from large high altitude long-endurance (HALE) systems to nano-UAVs for surveillance or attack, presents many technical challenges for the development of effective countermeasures. With hundreds of millions of dollars being spent around the world on counter-UxV technologies, it should also be no surprise that counter-counter UxV technologies are also being developed [287].

RAS development is a high priority for many Alliance and partner nations [66, 176, 288, 289, 290]. Commercial interests are expected to create a proliferation of readily available and deployable systems (e.g. automated logistics & transportation). To put these developments into perspective, the global autonomous vehicle market is expected to reach $172.3B USD by 2024 [291]. Military investment in such technologies is growing as well with [290] noting that for 2020 the US defence budget adds $3.7 billion of new funding for unmanned/autonomous systems technologies and $927 million of related funding for AI. This will present both an opportunity and an interoperability risk for Alliance military application. Still, the successful development of fully autonomous systems is expected to be slower than anticipated, overlapping with technological developments in low-power sensors, propulsion and artificial intelligence. This may lead to a growing sense of disillusionment in their effectiveness. Nevertheless, successful integration of autonomous systems at lower levels (<4) of autonomy will provide a major driver of alliance capability development and future operational success.

Military Implications

BLUE

UAVs of different size and degrees of autonomy are already used for ISR and strike missions, taking advantage of long loitered times and flexible positioning near potential targets. The long-endurance type of UAVs is particularly important for surveillance when operations are conducted over a period of days. However, the increased use of small swarms of UxVs offers considerable advantages for ISR, as well as offensive and defensive operations.

Autonomous systems are expected to lead changes in:

1. **Force Structure**: UxV and autonomous software agents will replace humans in operational/tactical jobs environments that are deemed dull, dirty, dangerous or dear (e.g. CBRN, EOD, reconnaissance, etc.). Increased use of autonomous systems will, therefore, challenge the development of appropriate military skills, organisational/force structures and training.

2. **Effectiveness**: Employing a *warfighter as a system* concept will see next generation networks and advanced AI seamlessly integrating disparate techno-human systems into unified and focused capability (e.g. [292]), allowing every *soldier to act as a squad, every ship as a task group and*

every aircraft as a squadron. Agile manufacturing (e.g. 3D/4D mix-materials printing) will provide task tailored systems in theatre on demand.

3. **Counter-Measures**: The wider use of UxVs and swarming on the battlefield will require additional force protection assets with explicit counter-UxV capabilities. These will span the spectrum of hard and soft kill options, such as electronic countermeasures, cyber, kinetic kills, directed energy weapons, interceptor swarms, and deception. It will be necessary to defend critical assets from swarms, where each node in the swarm is highly manoeuvrable, adaptable and hard to detect. Counter-swarm techniques will need to engage each node very quickly and cost-effectively to defeat the swarm.

4. **Swarming**: UxV swarms will enable new sensing and attack paradigms for friendly forces (e.g. [293]). One approach is to use a swarm as an expendable asset, for example, to penetrate into defended areas through the saturation of defences or to protect BLUE critical assets through large numbers of sacrificial sentinels. Ultimately, it will cost more time, energy and money for RED to defend against a swarm than to overcome it.

5. **Logistics**: UxVs will transport passengers and cargo onto the battlefield, especially in the relatively small quantities that would apply in tactical situations. Current levels of technology may be sufficient to create remotely piloted or autonomous UxVs that are capable of delivering supplies and ammunition to troops in the field, under well-defined circumstances. Wider application within the logistics and transport system will reduce waste, increase operational availability and support warehousing operations.

6. **Situational awareness**: Improved ISR through widely dispersed, persistent, low-observable vehicles/sentinels employing a broad range of low-power sensors (EO/IR, radar, magnetics, etc.). Increased use is expected in evolving operational areas such as space, cyber and urban environments. Hand-carried micro-UAVs deployable by soldiers in urban environments will be available and widely used. UAVs of different size and degrees of autonomy are already used for ISR, taking advantage of the fact that UAVs can have long loiter times and can be positioned flexibly near potential targets. Long endurance UxVs are particularly important for surveillance when operations are conducted over days to years. Cyber agents will also increasingly be used to maintain situational awareness within virtual spaces (social or otherwise), and to aide in the identification of threats or vulnerabilities.

7. **Lethality**: Large numbers of low-cost systems and improved human-machine teaming, will greatly improve force projection. This will lead to the capability to gather constant and reliable information over vast geographical areas at a much greater level of detail than ever before. An armed UAV would provide air combat capability without exposing a pilot to risk. Ordnance could be carried by the UAV, or the UAV itself could be integrated into the aircraft in a manner similar to an air-launched cruise missile. UAVs can be used to attack high-value, sea or ground targets in military operations. Through a *loyal wingman* concept current air, land (e.g. [292]) or naval assets could act as a *shepherd* for several assigned UxVs, especially in an area denial or Anti-Access/Area Denial (A2AD) role.

8. **Manoeuvrability**: Increased tactical and operational agility, through increased presence, numbers (swarms) and reduced logistics needs. Automated systems will be able to rapidly exploit tactical opportunities consistent with operational direction.

9. **Survivability**: Reduction in combat casualties (due to smaller forces), more rapid medical care, and greater operational effectiveness. It is conceivable as well that UAVs will conduct future combat search and rescue missions, further increasing survivability.

10. **Sustainability**: A combination of agile manufacturing and autonomous systems may enable automated logistics support in dangerous or isolated operational environments. Reduced manning

may also substantially diminish costs, with commensurate changes required in training and military occupations.

11. **Urban Operations**: Micro-UAVs will increase situational awareness in complex urban areas. These vehicles are also applicable for regular or special operations in unconventional and/or asymmetric threat environments, providing ISR and target acquisition capabilities in complex and complicated operations. Such vehicles could provide real-time data, directly support command decision-making processes and would reduce the risk for the warfighter.

12. **Cyber**: Autonomous software agents will increasingly undertake cyber (offensive and defensive) operations.

RED

Peer or near competitors will leverage the same advantages, potentially cancelling out the organisational and operational value of Alliance autonomous forces. Their use in covert hybrid war operations could provide plausible deniability while achieving tactical, operational or strategic objectives. As costs to produce autonomous systems decrease, their use and employment by non-state actors will increase both in number and effectiveness. Current countermeasures do not scale or adapt well to the broad operational use of large numbers (swarms), small or cheap widely dispersed autonomous systems. Various approaches exist for countering Alliance autonomous systems, such as cyber-attacks (platforms or C2); electronic warfare; counter-swarms; or directed energy weapons. RED may also employ small-UAVs in targeted attacks against individuals [294] or as a means of increasing the effective disbursement of CBRNE materials [293]. Technologies supporting (limited) swarming are becoming widely available and are no longer beyond the technical capabilities of non-state actors (e.g. the 2019 attack on Saudi oil facilities by the Yemen-based Houthi movement [295, 296]).

Interoperabilty

Increased integration of autonomous systems within Alliance and partner nations are expected to be incremental, but by 2025 and beyond such system are expected to be omnipresent in Alliance operations.

Communication, control and operational integration issues will need to be addressed. These include alignment of ROEs, sharing of large volumes of data and standardising operating protocols (e.g. deconfliction, collaboration, mission planning, data fusion and swarming) across a wide range of physical and virtual operational environments. While such issues (especially effective control of large swarm) present considerable technical challenges [293] even for advanced nations, solutions are becoming more widely available to regular and irregular forces.

Figure C.8: *Interoperability Challenges.*

Drawing upon the current operational experience with UxVs, significant ethical and legal factors will need to considered as nations move towards increased levels of autonomy [174]. International collaboration addressing all aspects of DOTMLPF-I will be critical in avoiding the creation of a complicated, ineffective and chaotic future operational environment.

S&T Development

Research areas of note span the range of challenges in system designs, sensing, interfaces, countermeasures, human control and application. These include:

1. **Systems**: Next-generation low observable vehicles and systems; novel propulsion; space & hypersonic systems; low powered, less expensive and highly sensitive sensors; mesh optimised distributed

ISR collection; decoys; increased miniaturisation; new cyber-physical immune systems; offensive and defensive cyber; social bots; and, application in complex dynamic environments across the physical (air, sea, land, space), human (social) and information (cyber) domains.

2. **Human-Machine Teaming**: Improved human-machine teaming; optimised socio-technical integration; and, new interface and control designs (including microelectronics).

3. **Counter-Measures**: Directed energy weapons (DEW); EM countermeasures; decoys; cyber; intercept swarms; and, kinetic weapon defence for counter-UAV and counter-swarm engagement.

4. **Autonomous Behaviour**: Large scale swarming; increased embedded AI; precision navigation; and digital controls.

The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table C.1: *Autonomy 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Autonomy	Autonomous Systems	Revolutionary	Expectation	6	2025
	Human-Machine Teaming	Revolutionary	Trigger	4	2030
	Autonomous Behaviour	High	Expectation	4	2030
	Countermeasures	High	Disillusionment	5	2025

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

References

[44, 66, 67, 68, 68, 169, 171, 172, 173, 175, 176, 177, 255, 257, 257, 271, 288, 289, 297]

Conjecture Card: Autonomy

C.1 Access Inaccessible Areas

Access contaminated, high threat or inaccessible environments to identify risks and MEDEVAC casualties without, necessarily, requiring human supervision.

C.2 Repurpose Commercial Systems

Take control of or piggyback off commercial unmanned systems for own purposes.

.C.3 Replace the Soldiers

Complement human forces with human-like robots that have beyond human strength and information processing ability.

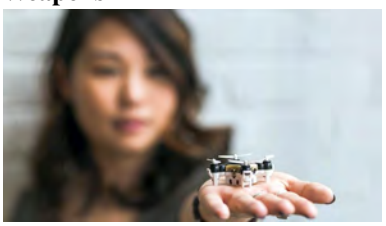
C.4 Cyber Immune System

Employ cyber agents capable of immune system like independent identification, monitoring and response to cyber-physical network attacks.

C.5 Sustainment

Summon unmanned refuelling or strategic logistics on demand, deployable in air, maritime or land environments.

C.6 Autonomous Lethal Weapons

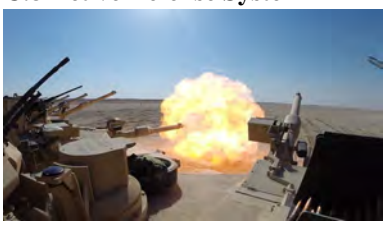


Automatically attack specific individuals, vehicles, objects or facilities with fly-sized or smaller systems.

C.7 Deploy a Swarm

Infiltrate or disrupt adversary actions or conduct surveillance using massive swarms (e.g. millions of nano-UAVs) at sea, on land or in the air.

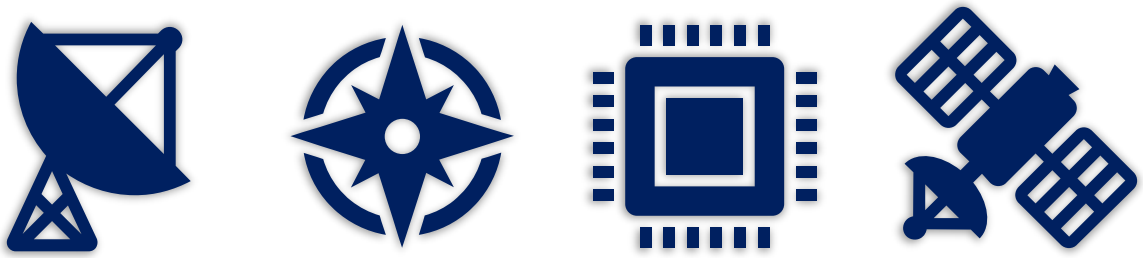
C.8 Active Defense System



Automatically defend unarmoured or lightly armoured vehicles or individuals from a variety of incoming threats via automatic countermeasures systems.

C.9 Driverless Transportation

Travel anywhere including urban areas (sea, air, littoral, near-space and ground) in unmanned vehicles ranging in size from personal transporters to strategic lift.



D. Quantum Technologies

Quantum Computing

"In less than ten years quantum computers will begin to outperform everyday computers, leading to breakthroughs in artificial intelligence, the discovery of new pharmaceuticals and beyond ... The very fast computing power given by quantum computers has the potential to disrupt traditional businesses and challenge our cyber-security. Businesses need to be ready for a quantum future because it's coming." - *Jeremy O'Brien, University of Bristol* [298]

"A lot of promises are made, and it's not always stressed that it's still in a kind of research phase ... Sometimes people think: Okay, it went fast with mobile phones, it went fast with this and that, so maybe in a few years I will have my own quantum computer on a mobile phone. I think this is simply not realistic. If we even have working quantum computers in the first stage, they will be in a computer centre like this one" - *Kristel Michielsen, Jűlich Supercomputing Center* [299]

Definition

Quantum Technologies (QT)

Next-generation *quantum technologies* exploit quantum physics and associated phenomena at the atomic and sub-atomic scale; in particular quantum entanglement and superposition. These effects support significant technological advancements primarily in cryptography; computation; precision navigation and timing; sensing and imaging; communications; and, materials.

Keywords

Quantum · Superposition · PNT · Entanglement · Photonics · Cryptography · Sensors · Radar · Imaging · Novel Materials · Positioning, Navigation and Timing (PNT) · Quantum simulation

Overview

Modern military systems are predicated upon the exploitation of classical, statistical, quantum and relativistic physics. In particular, the *first quantum revolution* laid the groundwork for transistors, computer chips, lasers, magnetic resonance imaging and modern communications technologies. However, while the

practical application of such physics has transformed the nature of contemporary society and the battlefield, over the last ten years advanced tools and a deeper understanding of such phenomena have provided technological opportunities hitherto undreamed. Thus, the second generation of quantum technologies are now emerging (Figure D.1), with the ability to produce and exploit more esoteric and subtle aspects of quantum phenomenology. The impact of this new technology, sometimes referred to as *the second quantum revolution* [300, 301], is expected to be profound and wide-ranging [83]. While the practical application of these second-generation quantum effects is currently being investigated, and in many cases actively employed, there is an increased acceptance that this is part of a more massive revolution potentially leading to a fourth industrial age created through the complex interplay of autonomy, advanced manufacturing, material science, energy storage and next-generation quantum effects [302].

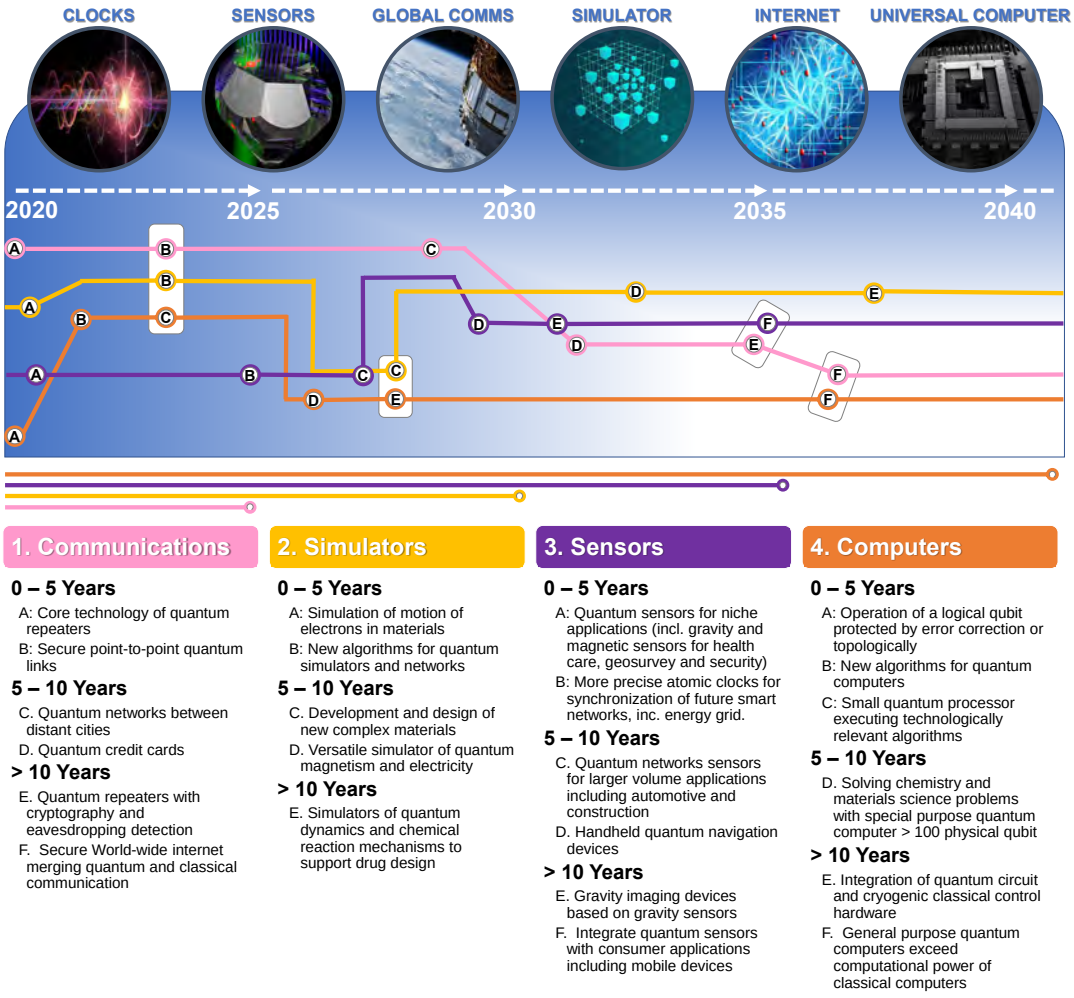


Figure D.1: *Quantum Technologies Timeline (CREDIT:Adapted from [83]).*

Next-generation quantum technologies (QT) are developing at a phenomenal rate, but defence and security applications are not progressing evenly amongst the four key lines of activity: (1) Communication; (2) Computing; (3) (Precision) Positioning, Navigation and Timing (PNT); and, (4) Sensing. Developments for quantum *computing* are primarily driven by commercial interests, while those in quantum *sensing, communications* and *PNT* are motivated by defence and security interests. National levels of investment are substantial and increasing [303], but the focus remains predominantly on commercial applications. Collaboration across nations will be instrumental in advancing the basic science, and in particular defence applications. As per [46], in the longer-term for QT, typically over 20 years from now, a step-change in quantum capabilities is expected when quantum devices can reliably exploit entanglement despite noise across a variety of time and distance scales and when the number of entangled logical qubits per device

increases.

Military Implications

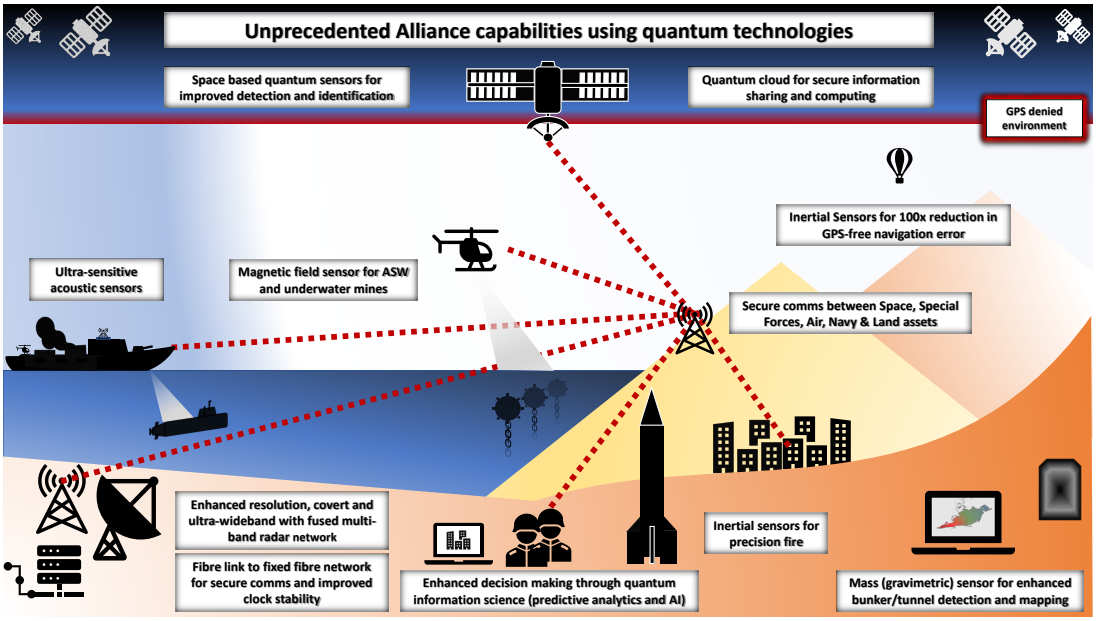


Figure D.2: *Alliance Quantum Capabilities (Adapted from US ARMY [304]).*

BLUE

NATO military capabilities enabled by next-generation quantum technologies are anticipated to offer unprecedented improvements in the following areas (Figure D.2):

1. **Computing**: Quantum computers are expected to provide orders of magnitude better computational capabilities, beyond the theoretical limit of classically designed computers for **specific** classes of analytical problems (e.g. optimisation and simulation). This computational leap will enable highly sophisticated approaches to encryption and decryption of codes, rendering current cryptographic methods obsolete. Sophisticated and rapid M&S will enable complex operational and organisational decision making, as well as new ways of developing hitherto undiscovered materials and biotechnologies, as well as next-generation AI (e.g. quantum neural networks for target and image identification problems).

2. **Sensing**: Quantum sensors will be many times more sensitive than current systems. This will support the development of counter-stealth and covert radars [92, 305]; magnetic, acoustic and gravity sensors with greatly increased ASW capabilities [90]; and, support the development of hitherto impractical low power high sensitivity airborne and spaced based sensors. Some example applications are for all-weather, day-night tactical (battlefield etc.) sensing (short-range, active/passive, covert, using EO/IR/THz/RF frequencies) for ISTAR, as well as strategic (long-range maritime, airspace, space) surveillance (active, RF). Quantum sensors are potentially more resistant to jamming.

3. **PNT**: Quantum effects support the development of very sensitive precision instruments for PNT. Such PNT technologies will enable operations in a GPS denied or difficult operational environment (e.g. long-duration submerged under-ice autonomous operations). In the short to medium term, rack-mounted units suitable for exploitation on larger mobile military systems (e.g. ships) will be available.

4. **Communication & Cryptography**: The development of *unbreakable* cryptography and the ability to decrypt encoded messages using current cryptographic methods will provide significant

challenges for current C4ISR systems.

RED

Within the 2020-2040 time-frame, the primary threat is from near-peer competitors, especially given the high level of mathematical sophistication and R&D investment required. The potential security implications due to the loss of useful encryption methods, the possible loss of air and underwater stealth, and a possible RED analytic/decision advantage enabled by quantum computing will challenge Alliance operations.

Interoperability

The use of next-generation quantum technologies will present significant interoperability challenges, primarily driven by differing rates of investment and, given the potentially dramatic improvements in sensing and communication capabilities, national security considerations.

S&T Development

Defence research areas of note are [46, 87]:

- **Sensing**: TRL for quantum sensing is still quite low; however, several of the enabling technologies are advancing quite rapidly and may be available in the mid-term to address NATO ISR challenges. Improved sensors may be used to build georeferenced maps of gravitational and magnetic anomalies around the world. Near-term targeted investments in QT gravity, magnetic and EW sensors could demonstrate new military capabilities for tunnel surveys, magnetic anomaly detection and electromagnetic sensing. In the mid-term better QT sensors will enable these capabilities to be deployed in more challenging military environments such as space. In the long-term, the use of entanglement distribution networks may make distributed sensors thousands of times more precise than is currently available.

- **Positioning, Navigation and Timing (PNT)**: There are two fundamentally different approaches to PNT: one involving the transmission and receipt of external signals, such as GPS, and the other relying on the self-contained sensing of motion, such as provided by inertial systems. Since the future security environment anticipates a highly contested electromagnetic environment (jamming and spoofing), NATO will need to be prepared to operate in a GPS denied environment. Investment in QT will enhance resilience to these emerging vulnerabilities. Quantum technologies are expected to support the combination of ultra-precise time measurements with ultra-precise acceleration and angular rotation measurements (each of which uses a different quantum technology), to provide ultra-precise inertial navigation (and timing), which will be needed as GPS, and other signal-dependent means become unavailable due to countermeasures (or inside structures). There are several competing concepts (solid-state nitrogen-vacancy, atom trapping in free space, cold atomic interferometry, etc.). Developing cold-atom QT will enable resilience to Global Navigation Satellite System (GNSS) denial through smaller QT clocks, and both gravity and magnetic sensing could be used to georeference using survey maps. It is expected that PNT will be first fielded through rack-mounted units (e.g. desktop computer size), suitable for exploitation on larger mobile military systems, e.g. ships. With continuous investments in the mid and long term, the systems are expected to reduce in size, weight, power and cost and ultimately provide navigation better than current GNSS performance, with greatly reduced reliance on external references.

- **Quantum Remote Sensing**: Quantum remote sensing, such as quantum radar [91, 92, 92] has the potential to make stealth technologies obsolete, provide more accurate target identification, and allow covert detection and surveillance. There are two known approaches to Quantum-enhanced remote sensing: either by using quantum interferometry or by using quantum illumination. Both rely on using entangled photons and retaining one half of an entangled photon pair while sending the

other out (in a known direction) to interact with the environment. These sensors will enable much more accurate and sensitive measurement and the use of much lower power, for applications such as the detection and tracking of small, stealthy targets. Developments will rely on several quantum engineering capabilities, such as the controlled generation of individual entangled photon pairs, the ability to retain one of each pair in isolation and to detect the returning photon for comparison with the idler.

- **Magnetic and Gravity Sensing**: Precise measurement of the magnetic field are used by maritime patrol aircraft for the localisation of submarines, using MAD (magnetic anomaly detection) sensors. Current sensors are not suitable for use on small UAVs, due to size-weight-power constraints, but emerging quantum technologies may provide a solution. There are also special applications of gravity sensing that could be enabled by quantum technology, for specialised surveillance applications such as underground structure detection (tunnels, bunkers) from an airborne platform.
- **Quantum Computing**: Quantum computing research is being driven predominately by commercial interests. While special-purpose *quantum computing devices* may be available in the mid-term, the development of a true general-purpose *universal quantum computer*, applicable to NATO problems, is likely a long way from being available. As per [46], experts estimated that such a quantum computer might be built within the next 15 to 50 years. In the medium term, the development of new quantum optimised algorithms and M&S for defence problems may be applied to special and limited BDAA problems.
- **Quantum Communications**: Quantum communication capability (for ultra-secure channels) is an important research area, but it is being driven in many cases by strong commercial and intelligence interests. Use of near-term QT may enable the detection of an eavesdropper on a communication channel. Further development of quantum key distribution (QKD) and quantum post-quantum encryption options will provide the Alliance with superior encryption capabilities. In the mid-term investment should focus on QT optical communications for anti-eavesdropping capabilities and as a defence against jamming to enable the Alliance to understand vulnerabilities and opportunities. In the long term, a global-reach quantum entanglement distribution system should be developed to support secure communications and other advanced QT applications.
- **Materials**: Quantum simulations, which accurately model quantum many-body systems, offer the promise of predicting material behaviours. This capability will allow the explicit design and creation of new materials with specific desirable physical properties such as ultra-hard armour, superconductivity, high-temperature tolerance, etc.

The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table D.1: *Quantum 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Quantum	Communication	High	Trigger	5	2030
	Information Science	Revolutionary	Trigger	4	2035
	Precision Navigation	High	Disillusionment	6	2025
	Sensors	Moderate	Trigger	3	2040

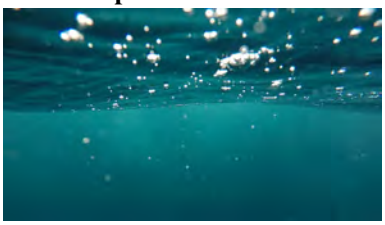
Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

References

[46, 83, 84, 85, 86, 87, 88, 91, 94, 96, 97, 99, 100, 306, 307, 308, 309, 310]

Conjecture Card: Quantum Technologies

D.1 Transparent Ocean



Obtain the position of any submarine, at any depth, everywhere on Earth, through ultra-sensitive magnetic, gravity or acoustic sensors.

D.2 Quantum Cryptography

Crack certain types of encryption in microseconds. Overcome cyber defences to disrupt or destroy others' computer systems.

D.3 Quantum Radar

Use air and space-based covert ultra-sensitive very low power radar systems to track and identify air targets at the extreme line-of-sight ranges.

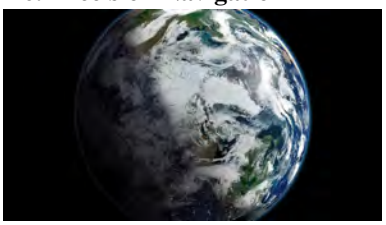
D.4 Computational Dominance

Utilise novel quantum algorithms (optimisation, neural networks, etc.) to provide a decision edge supporting military and enterprise operations and functions.

D.5 GPS Denied Environment

Operate for weeks at a time in a GPS denied environment with complete geospatial and temporal awareness, equivalent to that of today's GPS systems at sea, in the air or on land.

D6. Precision Navigation



Conduct under-ice precision navigation with unmanned underwater vehicles for months, without GPS updates, in the deep ocean and littoral areas.

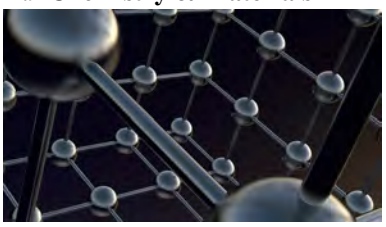
D.7 Quantum Illumination

Short-range very low power non-invasive imaging for security or biomedical applications.

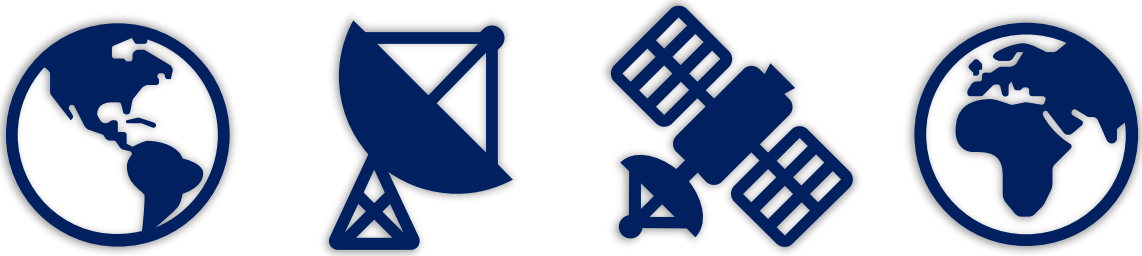
D.8 Quantum Communications

Communicate instantaneously at long range without being prone to eavesdropping.

D.9 Chemistry & Materials



Simulate the quantum structure and behaviour of new chemicals and materials to create new biochemicals and materials important for CBRN countermeasures.



E. Space Technologies

Space Technologies

"Space is extremely important for all civilian and military activities, for communications, for navigation, for the transmission of data, so of course, space and satellites are of great importance for all NATO Allies ... We will not weaponise space, we will not deploy weapons in space, but we make sure that the assets there are available in peace, crisis and conflict." - *NATO Secretary-General Jens Stoltenberg (2019)* [311].

Definition

Space Technologies

Space is generally considered to begin 90 - 100 km (the Karman line [71]) above sea-level. *Space Technologies* exploit or must contend with the unique operational environment of space, which includes: freedom of action, global field of view, speed, freedom of access; a near-vacuum; micro-gravity; isolation; and, extreme environments (temperature, vibration, sound and pressure).

Keywords

Space · Satellites · Micro-sat · Smallsat · Picosat · Nanosat · Propulsion · Launch vehicle · ITWAA · EO/IR Sensors · SAR Sensors · Geosynchronous - Geostationary - Polar - Sun-synchronous - LEO (low-earth) - MEO (medium-earth) - HEO (high-earth) - Molniya orbit · Thruster · Solar Sail · ISR · Imagery · National Technical Means · Missile Defence · ASAT (Anti-Satellite Weapon) · Kinetic kill · AIS · Earth Observation

Overview

Space is the ultimate *high-ground* (Figure E.1) and NATO is fundamentally dependent upon space capabilities to conduct missions responsively and efficiently. To do so requires national or commercial access to launch vehicles, platforms (satellites), sensors, C2 and constellations that are resilient to environmental or human-made threats. NATO has identified 5 core space capabilities [312] outlined in Table E.1.

S&T has a strong interest in space technologies and the use of space, but many aspects are beyond the scope of this report, as they fall outside of NATO's defined areas of concern. These include uses or

Table E.1: *NATO Space Capabilities and Usage.*

Space Capability	**NATO Use and Effects**
Position, Navigation, Time (PNT) & Velocity	Precision Strike Force Navigation Support to Personnel Recovery (PR)/Combat Search and Rescue (CSAR) Network Timing
Integrated Tactical Warning and Threat Assessment	Force Protection Attribution Missile Warning
Environmental Monitoring	Mission Planning Munitions Selection Weather Forecasting
Communications	Command and Control Unmanned Aerial Vehicle Ops Beyond-the-Horizon communications
Intelligence, Surveillance and Reconnaissance	Coverage of Operation Execution (in the operations centre) Battle Damage Assessment (BDA) Intelligence Targeting

technologies more align with the civilian sector or of uniquely national interest, including (heavy) launch, astronomy, planetary exploration, surveillance of space, and human performance. For this appendix space technology is understood to encompass three essential components:

1. **Platforms**: Including satellites, power, station keeping, propulsion, photonics, materials, and active/passive countermeasures;
2. **Sensors**: High-performance sensing; and,
3. **Operations**: Including space control, space situational awareness, space weather, autonomy, communications.

Figure E.1: *The Earth at Night.*

Specific tech watch activities related to space have been conducted by the STO around: sensors (compressive sensing, computational imaging, persistent infrared surveillance); materials (energy storage, 3D printing) and operations (system health management, 3D environmental modelling, ultra-short lasers, wide-band communications, robotics, and autonomy).

Operating predominately in low-Earth (LEO) and medium-Earth (MEO) orbits (Figure E.2), small satellites (smallsats) are delivering affordable science and services to academia, commerce and government and offer significant benefits to the warfighter. Active individual satellites and entire constellations can be deployed at greatly reduced costs in capability areas such as communications, extended ISR and geographical positioning. Smallsats are spacecraft which are less than 500 kg in mass and encompass several subcategories including [313]: (1) *minisatellites* (100 - 180 kg); (2) *microsatellites* (10 - 100 kg); (3) *nanosatellites* (1 - 10 kg); (4) *picosatellites* (0.01 - 1 kg); and, (5) *femtosatellites* (0.001 - 0.01 kg). A special category of modular smallsats (*cubesats*) have a standard size of $10cm \times 10cm \times 10cm$ per

constituent cube. These satellites are significantly cheaper than larger platforms, allow greater risk-taking and can be launched quickly at a lower cost. Moreover, smallsats enable the deployment of constellations or formations of space assets that can perform tasks with increased resolution, repeat cycle and higher performance across the constellation of satellites. Consequently, smallsats may enable military capabilities on-demand, tailored to specific operational needs. In the context of NATO, smallsats could support three of NATO's strategic capabilities: (1) strategic information dominance; (2) reliable, secure communication; and, (3) enhancement of situational awareness.

As a technological solution, smallsats have advanced significantly over the last decade from educational and experimental platforms to fully mission capable space assets. The miniaturisation of payloads and the entry of dedicated small satellite launch services to the market (e.g. Rocket Lab [72]) facilitated this development. In some instances, small satellites augment the capabilities of conventional larger spacecraft, such as off-loading less demanding tasks or supporting communication relays. Small satellites are also fast becoming viable platforms for effecting specific military missions. They can carry conventional or specialised payloads and can operate individually, together in constellations, or autonomously in swarms for higher complexity missions.

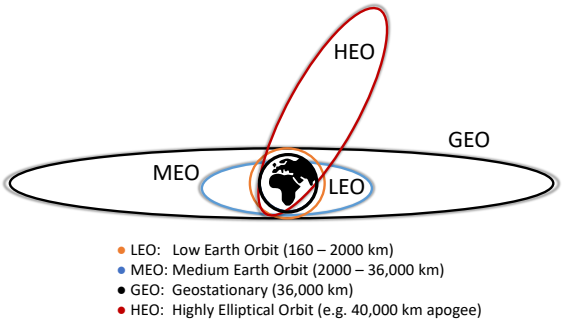


Figure E.2: *Orbit Types.*

Smallsat concepts and technology developments have focused on moving beyond the traditional space mission paradigm. These developments have had and will continue to require scientific, technological and engineering efforts in such areas as large (mesh) constellations; functional separation and control; increased robustness and resiliency through reduced complexity; mission studies to reduce revisit times at an affordable cost; rapid assembly, integration and verification studies to reduce time and cost to launch; rapid technology insertion through dedicated platforms to reduce risk of emerging technologies; innovative propulsion options; integration into space operations (figure E.3); and, responsive launch. Technologies to temporarily increase or remedy capacity loss are also of interest.

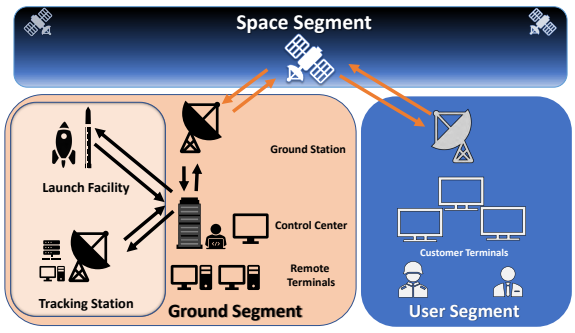


Figure E.3: *3 Segments of Space Operations (CREDIT: Adapted From [312]).*

Satellites are fully or semi-autonomous vehicles and as such benefit from continued research and development in autonomy related technologies such as stealth (signatures: infrared, visible, radar); qualification & certification; structures & materials; performance; stability & control; and design tools. In particular, increased responsiveness, improved power management and reduced communication bandwidth are being enabled through the development of more effective on-board processing, automated collection, multi-sensor data fusion and on-board target recognition. Increased use of robotics in space is also facilitating the refurbishment, refuelling and repair of satellites on-orbit [314]. While still nascent this technology will over the next ten years greatly reduce life-cycle costs and increase longevity. As noted in [315]

> *"The vision for on-orbit servicing and assembly is to create a robust and resilient space ecosystem that drives humanity toward a new era of space exploration, ultimately lowering the cost of access to space, and helping to build a better world."*

Communications and observation (i.e. C4ISR) have always been important motivators for the use of space. The development of specialised EO/IR sensors (electro-optic/infrared) notably to support missile defence, SAR (synthetic aperture radar), ELINT (e.g. Automated Identification System (AIS)) continues.

New sensor modalities are being explored, driven by improved sensor sensitivity, miniaturisation, the developing quantum sensor and communication revolution, and increased commercial satellite density. For example, radars operating at frequencies above 100GHz, (sub-Terahertz) can have very good range and angular resolution. Radars at these wavelengths are also sensitive to surface texture in a way which is closer to electro-optical systems than to conventional radars. The small wavelength also makes them very compact. Such sensors offer great potential for space-based imaging as space-borne systems are unaffected by atmospheric attenuation. Similarly, MIMO (Multiple Input Multiple Output) radars and Passive Coherent Radars (PCL), currently on its third development cycle [316], are well suited for space-based sensing and exploiting transmissions from commercial systems.

As part of the democratisation of S&T and commercialisation of space, access to these sensors and space derived data will increasingly be widely available as will sophisticated analysis tools [317]. This access will not be limited to lower quality imagery, but increasingly exploited data based on fused high-quality electronic intelligence (ELINT), Measurement and Signature Intelligence (MASINT), radar (synthetic aperture radar), and state of the art hyper-spectral & EO/IR imagery.

A wide variety of other space-related technologies will have a direct impact on future NATO space operations. Among the most critical, is an increased reliance on developing BDAA and AI technologies to mitigate the projected increase in space derived data. These technologies include the increased use of digital reality (virtual, mixed, etc.) to support space operations and training; high-data-rate space-to-ground/space-to-space optical communications [318]; improved cyber hardening to prevent unauthorised use or re-purposing of satellites or constellations; and, increased M&S support and analysis increasing resilience (e.g. debris, space weather) and space situational awareness.

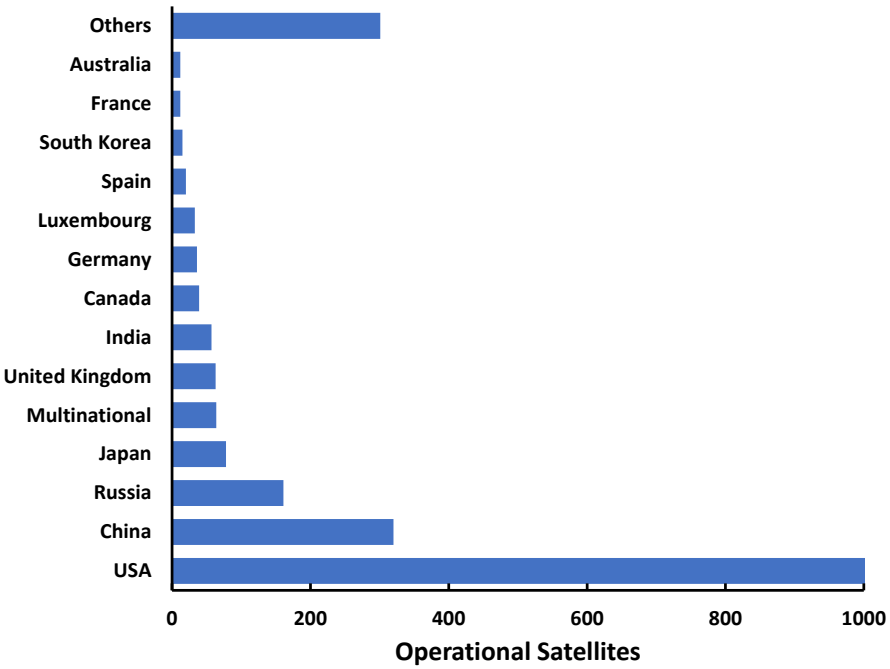
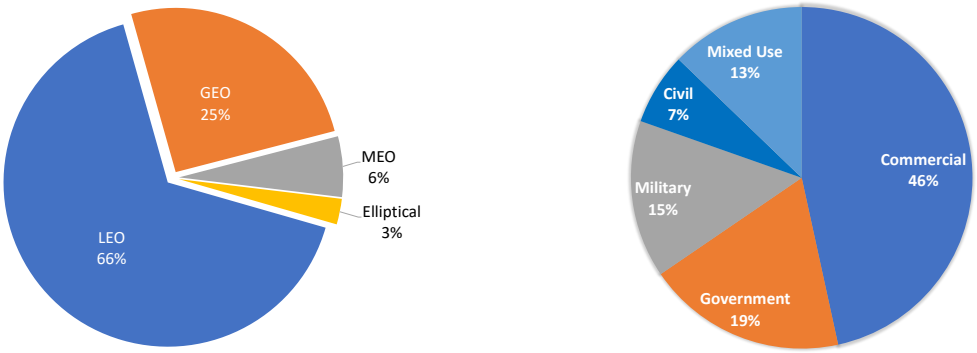


Figure E.4: *Operational Satellites by Country (as of 30 Sept 2019) (SOURCE: [319]).*

The world's economies, militaries and societies rely heavily on space-based systems (see (Figures E.4 - E.8)), and that reliance is increasing. The continued explosion of commercial interest in space is the biggest *space* development foreseen over the next 5-10 years. This growth in commercial space includes new launch capabilities (e.g. SpaceX and RocketLab); the increasing use of low-cost smallsats for communication or earth observation; on-orbit repair or salvage; large-scale constellations of communication



(a) Orbits of Operational Satellites *(b) Operational Satellites by User*

Figure E.5: *Operational Satellites (as of 30 Sept 2019) (SOURCE: [319]).*

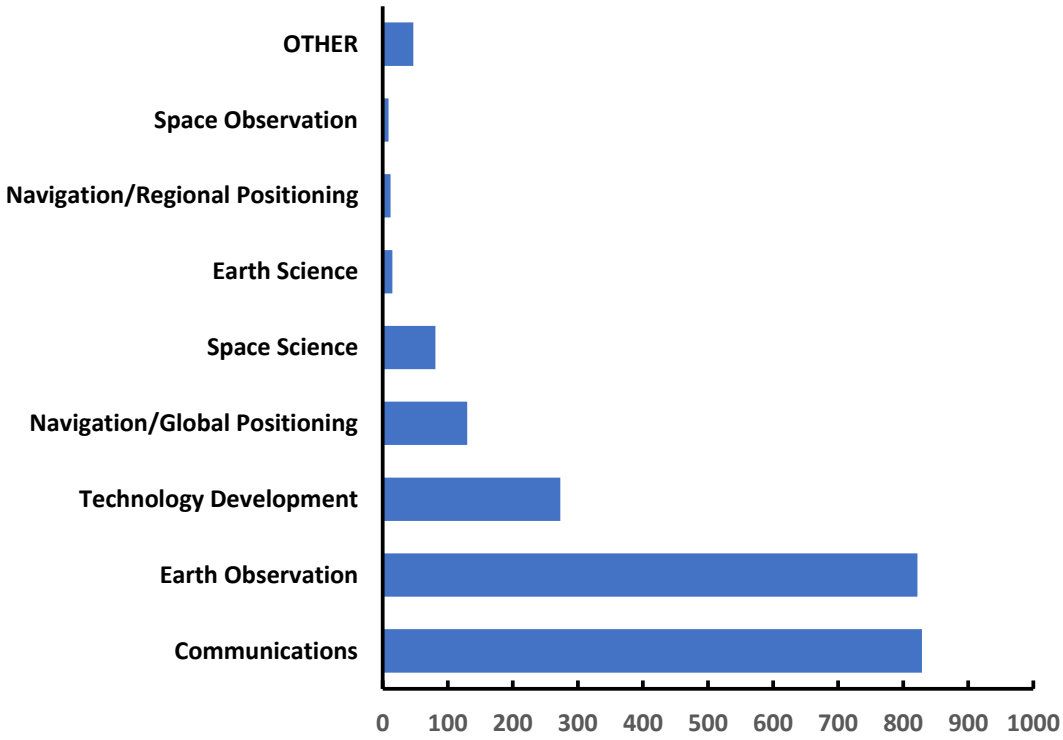


Figure E.6: *Purpose of Operational Satellites (as of 30 Sept 2019) (SOURCE: [319]).*

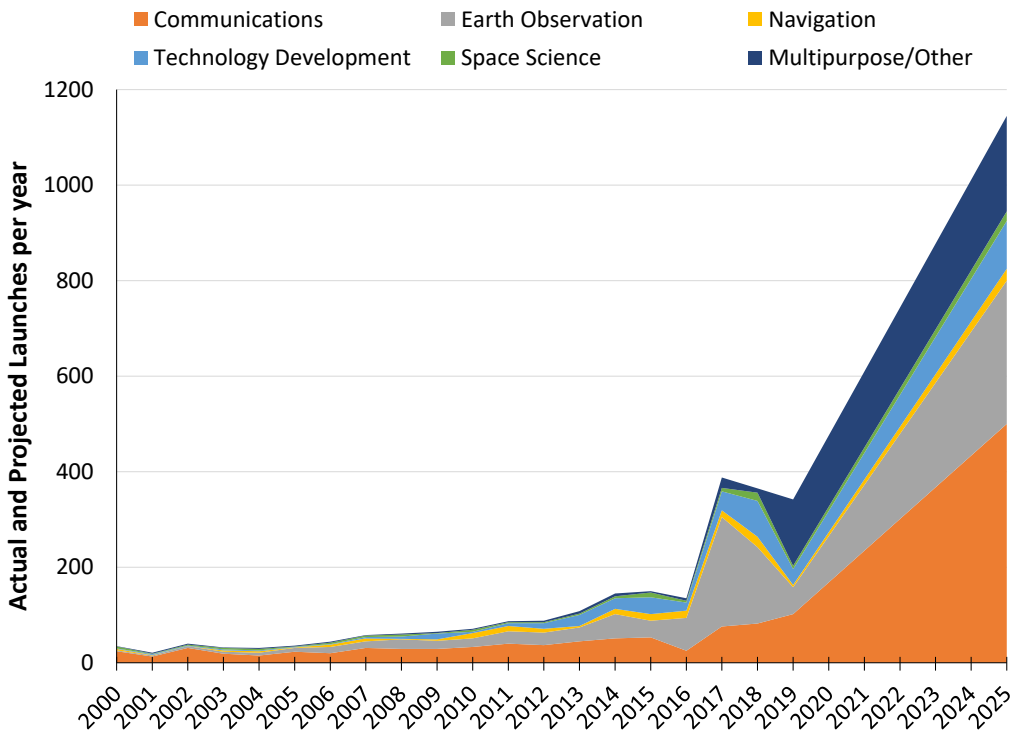


Figure E.7: *Actual and Forecast Satellite Launches per Year (SOURCE:[320]).*

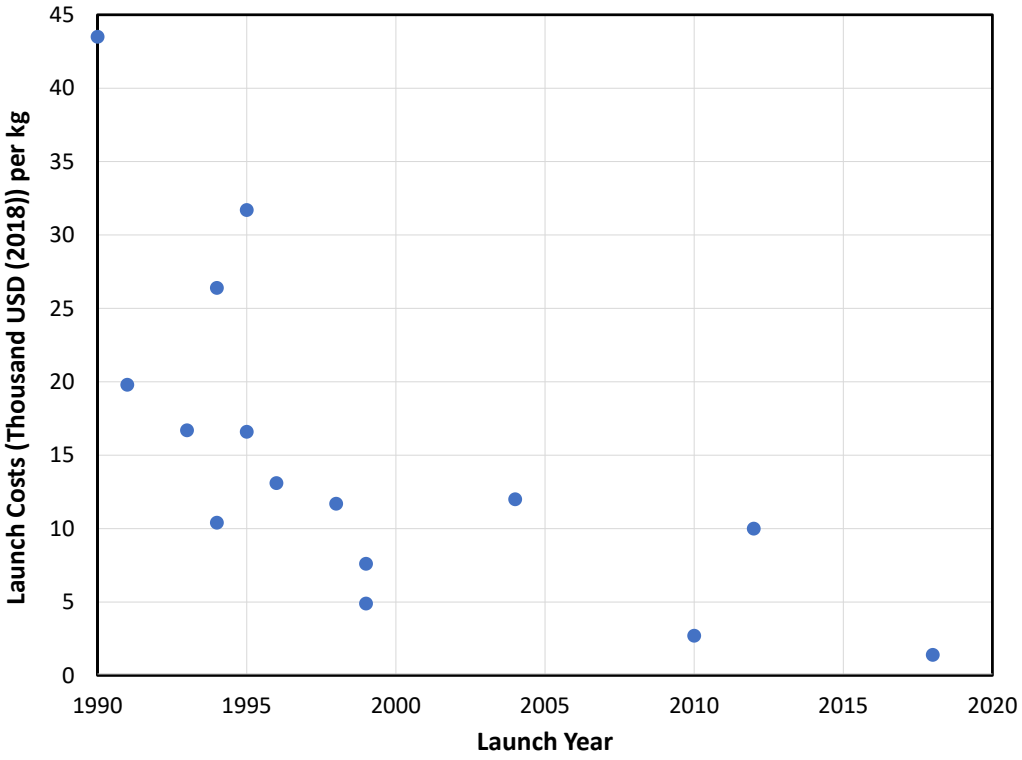


Figure E.8: *Launch Costs by Year (Thousands USD Per kg) (SOURCE: [321]).*

(internet, media, etc.) satellites; and space tourism. Over a 20-year horizon, new commercial activities in resource extraction (e.g. moon, asteroids, etc.) and human exploration will expand many times over. Figure E.7 provides some context around this growth. As of the publication of this report more than 2000 satellites are in orbit, a number driven in no small measure by the exponential decay in per kg launch costs. The number of satellites is expected to quintuple by 2030, with 1,100 expected to be launched per year in 2025 alone (almost four times the number launched in 2018) [320]. SpaceX alone is planning on placing 12,000 small satellites in orbit by 2027 to support its *Starlink* communication constellation. With all this activity, by 2040, the global space industry is forecast to grow from $350M (US) to $1 - 2.7 trillion [322].

Along with the use of space, the threats to space assets are developing as well [323, 324, 325]. While a number of countries have experimented with counter satellites weapons (e.g Figure E.9), recent actions by Russian *space apparatus inspectors* [326], as well as Chinese [327] and Indian [141, 328] anti-satellite (ASAT) activities are of significant concern. These physical threats are in addition to the spectre of cyber-attacks [329] (including ransomware) on space infrastructure (e.g. [330, 331, 332]) or the hijacking of existing satellites [333, 334], the use of direct energy weapons to blind satellite systems [335, 336] or more traditional jamming of satellite communication and control. On-orbit robotic servicing technologies will probably open the door to the development of new ASAT weapons such as *parasitic* microsatellites, designed to hijack, jam, re-purpose, exploit, destroy or covertly monitor satellite activity. As such, there will be a growing need by Alliance nations to design resilient satellites that are capable of defending themselves (passively or actively) from such threats. As noted by Gen Andre Lanata (Supreme Allied Commander Transformation (SACT)) [337]: *"Until now, space was considered by everybody as a safe haven ... It's not the case anymore."*

Figure E.9: *ASM-135A Launched From a Highly Modified F-15A, Sept. 13, 1985 (CREDIT: USAF (Paul Reynolds)).*

Military Implications

BLUE

Space is an underpinning technology for NATO operations and Alliance activities. The following developments will impact a broad range of NATO space capabilities and uses (PNT, indications and warning, environmental monitoring, and C4ISR):

1. **Smallsats**: Smallsats support many different military capabilities as they can perform military missions that once were reserved for large spacecraft. Today, smallsats of different size and degrees of autonomy are already used for ISR collection activities, taking advantage of very short revisit times, rapid launch and flexible positioning. Increased use of smallsats with new low powered passive and active sensors will increase situational awareness around the planet, and increase space situational awareness. In the future swarms, increased autonomy and large constellations will further improve C4ISR capabilities.

2. **Microwave Photonics**: Microwave photonics can strongly impact space based functionalities and performance for high-frequency of radars and EW systems. Photonics integration can help in

reducing size and weight, and in increasing the robustness in terms of electromagnetic interference insensitivity. The integrated photonic technology has already been demonstrated to be space qualified for military applications.

3. **PCL**: The increase in detection ranges for ground base PCL radars, augmented by space-based receivers, will allow a real-time RAP (Recognised Air Picture) over a much wider area over RED or neutral territory. It will enable a deep view onto activity over a wide area and provide detection, precise tracking and identification of targets using adversary or neutral nation transmitters of opportunity. An advantage of such an approach will be the possibility of more complete TBM and hypersonic launch detection and tracking.

4. **Quantum**: One of the main benefits of quantum technologies will be realised in the medium term through improved sensing applications; in particular, the ability to detect submerged or concealed objects. Improved imaging through various techniques may enable more rapid and accurate identification of threats. QKD potentially offers a significant improvement in secure communications, but there are several challenges to be overcome concerning distance and network size. Nevertheless, rapid identification of intrusion could be a substantial aid to cyber intelligence.

5. **Terahertz Sensors**: Terahertz sensors will support exo-atmospheric high-resolution sensing. Interception and countermeasures capabilities into this region of the spectrum would prevent other actors from being able to exploit such capabilities against NATO.

6. **Situational Awareness**: With Space as an operational domain, space situational awareness will become even more critical. Dealing with debris, hunter-killer satellites [325, 338], congested orbits, commercial space-derived intelligence, mega-constellations, space weather and increased human activity in space will all require increase space situational awareness.

RED

Peer or near competitors will leverage the same advantages as BLUE. However, the use by asymmetric forces is expected to grow predominately through the leveraging of commercial space imagery and communication systems. Cyber attacks against BLUE (commercial or military) space control centres open up additional areas of vulnerability and the possibility of *ransomware*, covert monitoring or hijacking of commercial space assets [339]. More specifically:

- **Smallsats**: Since smallsats can be developed in short times and with affordable budgets, they may also be used as a threat to NATO space assets. However, the major limitation will be placing smallsats in relevant orbits requiring launch vehicle capability, which is today only owned by a small number of space fairing nations. However, launch capacity may be obtained from Russia, China or growing commercial sources. The rapidly falling price of space launches and increased miniaturisation will greatly increase access to space, including access to criminal or asymmetric threats.

- **Microwave Photonics**: The applications of microwave photonics in communications wireless systems and distributed sensor networks will make this technology available worldwide. This availability will allow RED to develop increasingly smaller and more functional satellites and constellations.

- **PCL**: Peer or near-peer forces will obtain the capability for covert detection and tracking of BLUE forces activities at long distances.

- **Terahertz Sensors**: Of particular concern is the possibility that RED could detect stealthy objects more readily using space-based terahertz sensors.

- **ASAT**: The risks from ASAT (anti-satellite) (hard or soft kill) weapons or robotic parasitic systems will become more acute. Increasingly congested orbits, increased use of large constellations of smallsats and increasing levels of space debris *polluting* the near-earth environment will impact the effectiveness and reliability of space-based systems [75, 140, 141, 142, 340].

Interoperability

To date, NATO does not own satellites directly but leverages those owned by Alliance nations, exploits space derived information and uses satellite-based communication networks. As such, interoperability issues will arise around access to highly classified space derived information, operational use of commercial communication networks, sharing of exploitation results, policies on the use of data collected by commercial sensors, and procedures for the Alliance to request collection on targets by national means. Interoperability solutions will require that NATO continues to provide a forum to share information and supports missions and operations with space-based systems. Common interests and a willingness to work together are characteristic of international activities in space (e.g. Figure E.10), including those involving NATO, and such coordination and collaboration will be essential to ensure interoperability and the long term utility of space to NATO's success.

Figure E.10: *The International Space Station.*

S&T DEVELOPMENT

1. **Microwave Photonics**: Maturing with subsystems currently at TRL 5, and many components at TRL 6. Continued research will improve system performance and support further miniturisation.

2. **Small-sats**: A variety of small-sats are already used within military operations in all domains. However, these systems are limited in their usage and missions capability. To fully cover the military needs, S&T efforts are still required to increase the TRL for key technologies. With increasing required levels of autonomy, the current TRL level is decreasing. Therefore the current TRL level ranges from 3 – 9 depending on the observed technology. Additional research will need to be undertaken on low power propulsion, autonomy and satellite control, in order to enable next generation smallsat swarming or mission specific orbital adjustment.

3. **Autonomy**: Space has always pushed the boundaries of autonomy. Continued research needs to be conducted to expand on-orbit autonomous capabilities. These developments include expanding on-board AI and processing capabilities, better energy storage, more efficient thruster and propulsion technologies, and enhanced robotics. These technologies vary widely from TRL 3 – 9 depending on the observed technology.

4. **Passive Coherent Location (PCL) Radars**: The TRL level can be estimated between 2 and 3. The studies are at the present moment at the level of theoretical considerations and basic phenomena modelling. Selected field tests show the capability of passive radars to track fast objects like missiles both in lunch and ballistic phases. It is estimated that this technology will reach TRL level 4-6 in the next five years, and reach level 9 over the 20-year time-frame.

5. **Spaced Based Quantum**: The TRLs vary across the different technologies outlined above, but none are currently above TRL5. Gravitometers are up to TRL5; while mostly imagers are up to TRL4, and some RF sensors have reached TRL5. QKD is at TRL7, and has already been demonstrated in space but with substantial challenges associated with expansion to larger networks.

Within 5 to 15 years, precision navigation systems, QKD, imagers, and gravity sensors could reach TRL9.

6. **Terahertz Sensors**: In 10 - 20 years, components developed originally for automotive/ communication systems will be available for space-borne ISAR systems. This availability will allow space objects with a radar cross-section* of about 0.1m2 to be imaged with a resolution of better than a centimetre at a range of 50km.

7. **Resilience**: Resilient space assets and networks will need to be developed and maintained. Research into new methods of rapid low cost tactical launch, improved space situational awareness (including space weather), satellite hardening (new materials, impact survivability & cyber) and active/passive ASAT countermeasures should be explored.

The following table presents the assessed integrated potential impact, state and rate of development, as well as identified areas for focused research.

Table E.2: *Space (Systems) 2020-2040.*

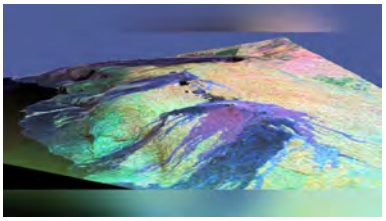
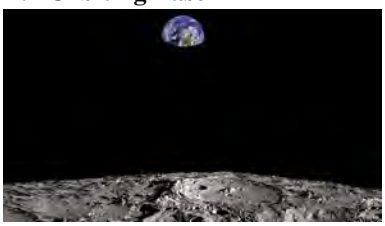
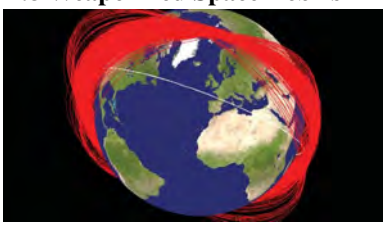
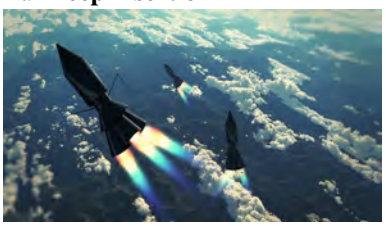
EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Space	Platforms	Moderate	Expectation	6	2025
	Operations	Moderate	Expectation	5	2030
	Sensors	High	Trigger	3	2035

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

References

[73, 74, 75, 99, 99, 141, 142, 255, 322, 327, 333, 341, 342, 343, 344, 345, 346, 347, 348]

Conjecture Card: Space

E.1 Star Wars Satellites	**E.2 Satellite**	**E.3 Solar Space Power**
		
Surgically deliver a kinetic or directed energy weapon (DEW) effect from space to targets larger than 10cm in diameter.	Conduct on orbit construction, repair, deconstruction or covert/overt modifications of C4ISR satellite systems and constellations.	Deliver very large quantities of energy everywhere on Earth provided you have the necessary equipment to receive it.
E.4 Commercial Space ISR	**E.5 Instant launch**	**E.6 Global radar**
		
Use and fuse commercial space derived data providing global situational awareness of air, space and maritime surface traffic, including identification of dark targets in real-time.	Launch single-purpose limited life satellites & swarms into low Earth orbit (LEO) from forward-operating bases.	Target from space using GPS or other EM echoes.
E.7 Orbiting Base	**E.8 Weaponized Space Debris**	**E.9 Deep insertion**
		
Employ persistent counterattack or observation bases for Earth-orbiting objects, defeating earth-oriented countermeasures.	Plausibly deny destruction of an adversarial satellite or ground strike.	Strategic resupply and force projection anywhere on Earth in hours.

F. Hypersonics

Hypersonics

"I'm sorry for everybody out there who champions some other high priority ... But there has to be a first, and hypersonics is my first ... When the Chinese can deploy [a] tactical or regional hypersonic system, they hold at risk our carrier battle groups. They hold our entire surface fleet at risk. They hold at risk our forward-deployed forces and land-based forces." - *Michael Griffin, Undersecretary of Defence Research and Engineering (USA)* [349]

Definition

Hypersonics (HWS)

(Advanced) Hypersonic Weapons Systems (missiles, vehicles, etc.) operate at speeds greater than Mach 5 (6125 kph). In such a regime, dissociation of air becomes significant, and rising heat loads pose an extreme threat to the vehicle. Hypersonic flight phases occur during re-entry from space into the atmosphere or during propelled/sustained atmospheric flight by rocket, scramjet or combined cycle propulsion. This class of weapon system includes air-launched strike missiles (HCM), manoeuvring re-entry glide vehicles (HGV), ground-sea *ship killers*, and post-stealth strike aircraft. Systems of this nature may rely primarily on kinetic effects alone or may include supplemental warheads (nuclear or non-nuclear). Countermeasures against individual, salvoed or swarms of hypersonic systems are particularly challenging due to their speed and manoeuvrability. [45].

Keywords

Hypersonic · Propulsion · Glide Vehicles · Directed Energy Weapons (DEW)

Overview

Advanced *hypersonic* weapons systems (missiles, vehicles, etc.) operate within the atmosphere at speeds higher than Mach 5 (6125 kph) [350]. At such speeds dissociation of air (i.e. the breakdown of air molecules into atoms, ions or radicals) becomes significant, and the resulting heat poses a threat to the vehicle. Hypersonic flight occurs during re-entry in the atmosphere from space or during propelled/sustained atmospheric flight by rocket, scramjet or combined cycle propulsion. A hypersonic vehicle may be an

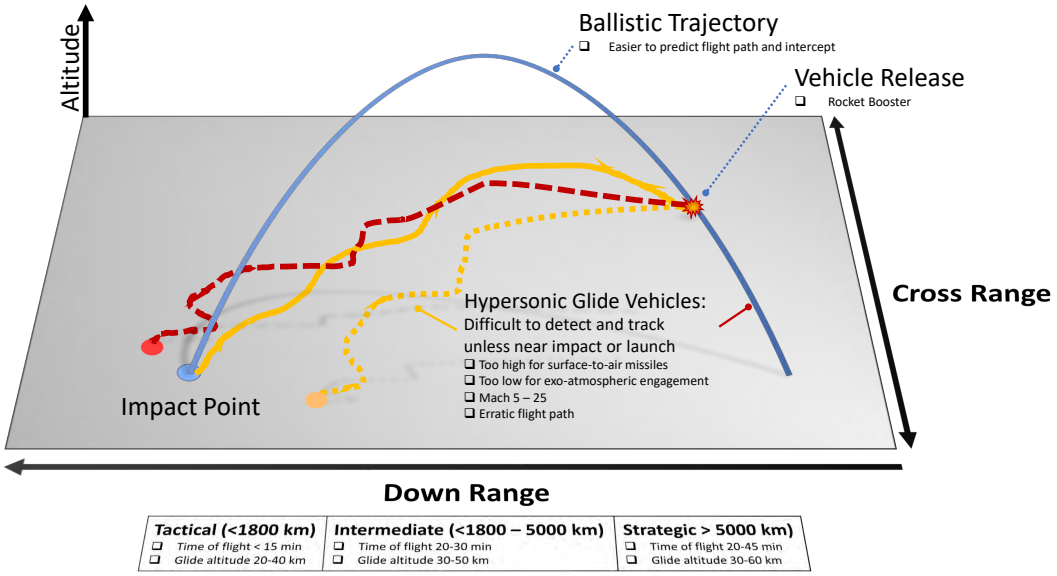


Figure F.2: *Hypersonic Glide Vehicle (HGV) (CREDIT: Adapted from [352]).*

aeroplane, missile or spacecraft. Potential applications include fast, long-range strike of high value or high threat targets, ballistic missile defence, ISR and reusable space transport vehicles.

Hypersonic weapons [350, 351] are ultra-fast *and* manoeuvrable weapon systems which typically come in three types:

(1) Boost Glide: Hypersonic Glide Vehicles (HGV) employ ballistic launch by rocket, but glide and manoeuvre un-powered at hypersonic speeds within the atmosphere. These wave-rider HGVs generally fly at altitudes between 40 to 100 km [352] reaching speeds as high as Mach 25;

(2) Cruise Missiles: Hypersonic Cruise Missles (HCM) are typically air-launched and powered by scramjets (supersonic combusting ramjets) to maintain hypersonic speeds. Scramjets use thrust produced by compressed air moving at hypersonic speeds, mixed with fuel, and then ignited. As a result, they require rockets for assisted take-off or launch in order to accelerate the HCM to Mach 3 or 4, where the scramjet begins to operate. HCMs generally fly at altitudes of 20 - 30 km [352]; and,

(3) Hypersonic Aircraft: Human-crewed aircraft or unmanned drones, that are typically used for strike or reconnaissance purposes (e.g. an aircraft similar to the Mach 3+ SR-71).

Figure F.1: *Hypersonics Glide Vehicle.*

Ballistic missiles reach similar speeds, but generally follow a prescribed (i.e. ballistic) flight path after exhausting their fuel supplies. As a result, they are excluded from this assessment. Likewise, EM rail guns [353], which fire hyper-velocity projectiles, are also excluded as they generally use non-manoeuvrable projectiles and an electromagnetic impulsive launch. The use of rail guns, rather than rockets, for the initial acceleration of scramjets has been an area of investigation[354, 355].

Given the enormous kinetic energies involved, hypersonic missile systems may rely primarily on kinetic effects or may include supplemental warheads (nuclear or non-nuclear). Countermeasures against individual, salvos or swarms of hypersonic systems are particularly challenging due to their speed and manoeuvrability [45].

The latest developments in hypersonic systems build upon a number of development cycles spread out over the last 60 years. However, the latest R&D cycle has brought with it the possibility of operational

use, as noted in [351]:

> *"Hypersonic weapons use electronic capacity, sensor quality, and miniaturisation to create a new threat ... They're fast and manoeuvrable. That combination creates a threat ... There are flight tests from Russian, China, and other countries that show accelerated progress."*.

Jet engines come in three primary varieties: turbojet, ramjets and scramjets (see Figure F.3 for a comparison). In particular, scramjets, while employing relatively few moving parts, are incredibly complex systems due to various problems with aerothermodynamics, supersonic combustion, fuels, insulation/cooling and structural material and design. Achieving a positive thrust-drag ratio is a significant engineering and technical challenge. These specialised areas include hypersonic flow physics, turbulent transport phenomena, heat transfer, the transition from laminar to turbulent flow, hypersonic inlets, supersonic combustion, advanced functional materials, thermal protection, thermal management stability and control including control effectors. Research continues to be necessary in the mid-term in order to develop affordable air-launched air-breathing hypersonic weapons capable of sustained high-temperature cruise airspeeds [202].

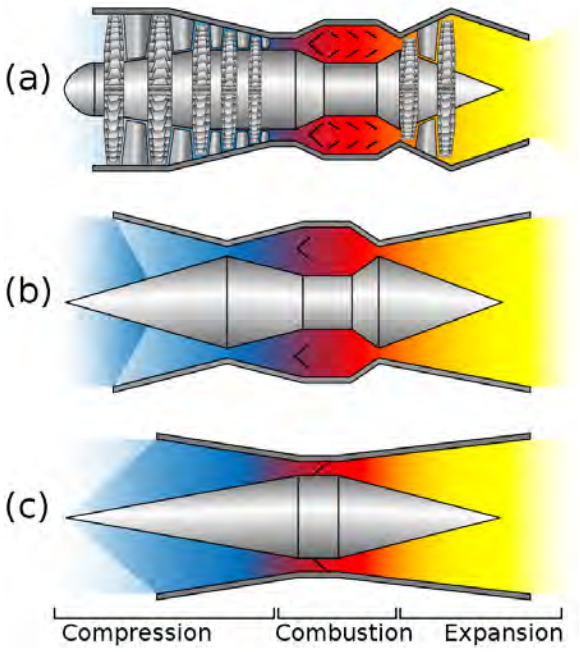
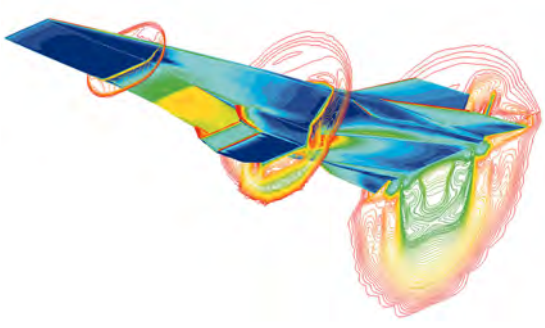
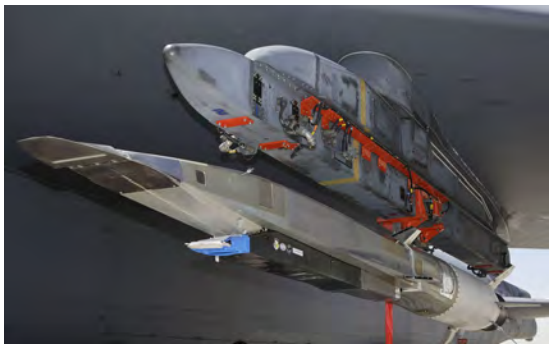


Figure F.3: *Three Types of Jet Engines: (a) Turbo; (b) Ramjet; and, (c) Scramjet. [356]*

Sustained hypersonic flight may be achieved by supersonic combustion ramjets (scramjet), but requires acceleration by rocket or other sub-to-supersonic propulsion systems to reach the scramjet's operational regime. Sustained hypersonic flight has been achieved only for a minimal duration ($\sim$ 2.5 min X-51A [357], Figure F.4). Research focused on new engine designs, and operating modes will be critical to the broader development of hypersonic capabilities. In particular, development of dual-mode engines, which transition from fuel-efficient turbine operation to ramjet mode, will support transformational changes in long-range strike (both HCM and aircraft), ISR, and would enable two-state-to-orbit (TSTO) operations significantly reducing the cost of space launch [202, 358].



(a) *X-43A Computational Fluid Dynamics (Mach 7) (2001-2004) (CREDIT: NASA Photo ID: ED97-43968-1).*



(b) *X-51A Waverider on a B-52 (2010-2013 [359])*

Figure F.4: *US Hypersonic Research Testbeds.*

Significant milestones in hypersonic flight research have been the crewed X-15 experimental rocket (1967), early human-crewed space re-entry capsules or modules (Mercury, Gemini, Apollo, Vostok,

Soyuz), the Space Shuttle, and USAF programs such as the X-43a [360] and X-51A projects [357, 359] (Figure F.4). Vehicles typically have a wave-rider configuration with a robust heat protected and cooled structure.

Experimental work in hypersonic flight is possible only for nations with highly developed R&D capabilities and very high financial resources [351], with the US alone spending $1 billion annually [361]. The USA, Russia and China are the current leaders in research and development for military hypersonic vehicle applications [361, 362, 363, 364, 365]. China in particular is demonstrating considerable S&T leadership in many aspects of hypersonic flight [366] (see Figure F.5 for one measure of such leadership). More importantly, China and Russia have both announced successful tests and development [77, 81, 82, 367, 368], while the US has expressed concerns about losing its technology edge in this area [369]. In recent years many other nations [370], such as the UK [371], France [372], Japan [373], and Australia [374] have initiated new hypersonic research programs in combination with other partners. By the 2030s, hypersonic missile technologies are expected to expand beyond delivering warheads at speeds faster than sound also to include hypersonic intelligence and reconnaissance flights [375].

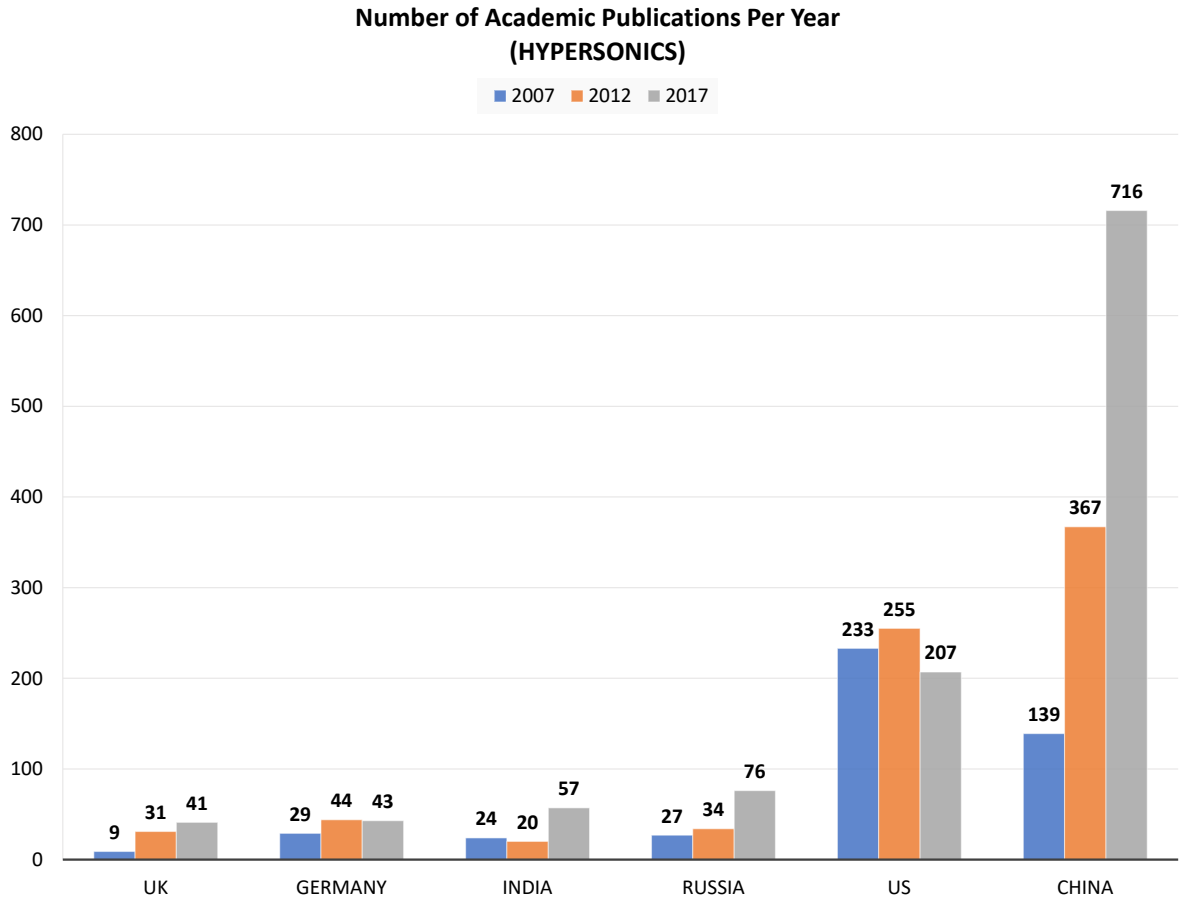


Figure F.5: *Number of Academic Publications (Selected Countries) [366].*

As advanced hypersonic weapon systems become more and more widely deployed, the need to develop countermeasures will become more and more acute. Use of interceptors (e.g. Glide Breaker [202, 376]), electronic countermeasures, lasers and other directed energy systems (DEW) (e.g. high power radio frequency weapons) offer some options for countering hypersonic threats. As noted in [45, 77, 81, 368, 377, 378, 379], the current development of hypersonic systems may be considered revolutionary, in no small measure due a lack of countermeasures and the concern that they lower the bar for the use of military force. Others have noted that while hypersonic weapons are an emerging threat, they are not quite the existential threat suggested by some [380, 381, 382, 383] given the significant technical challenges presented in operating at such high-speeds.

Military Implications

Military application is possible both for propelled and un-propelled hypersonic flight vehicles. Powered hypersonic vehicles can be used for reconnaissance purposes such as a successor to the SR-71 or for fast, long-range strike with a hypersonic cruise missile. They may provide a considerably enhanced capability for quick and precision response below the ICBM/nuclear level. The application will likely be more strategic than tactical and for high value or high threat targets only because of the very high system cost. Such high speeds allow for a rapid strike against time-critical targets from safe standoff distances, keeping the launch platform well outside contested areas. Advanced Anti-Access/Area Denial capabilities have pushed out the boundaries of contested areas. Hypersonic flight counters this trend and allows greater standoff operations for the first strike. Also, the extreme speed of hypersonic penetrating systems makes kinetic intercept very difficult.

Propelled hypersonic vehicles (e.g. HCM) will fly at very high altitude with speeds around Mach 6 – 8 and with limited manoeuvre capability. This presents significant countermeasure and intercept challenges.

Un-propelled hypersonic vehicles (e.g. HGV) may be used as warheads on a ballistic missile having the advantage of manoeuvring capability for targeting precision and defence penetration. These vehicles will reach higher hypersonic speed (> Mach 10) but for a shorter duration. Thermal problems can be addressed by heat protection/insulation.

Long-range Intelligence, Surveillance, Reconnaissance is another potential application. While manned systems are possible, long-range ISR by a hypersonic UAV would be more flexible than reconnaissance satellites with a possible option for weapon delivery. Hypersonic missiles could also be used for defence purposes as for intercept of high value/high threat time-critical targets and potentially hypersonic cruise missiles. Hypersonic flight is also possible for reusable space transport vehicles, e.g. the state-of-the-art US Air Force X-37 space-plane [384]

Significant concerns have been expressed (e.g. [45]) on the potential destabilising nature of strategic use of hypersonic weapons for decapitation strikes. Even the threat of such a strike reduces the decision space for Integrated Tactical Warning and Attack Assessment (ITW&AA).

BLUE

In particular:

1. **Strike**: The use of hypersonic systems will allow rapid, highly challenging to engage and precise high energy (kinetic) strike. In swarm or salvo, this would enable increased kinetic kill probability of high-value targets. HCMs, in particular, would provide a significant capability for penetrating RED air defences due to their high speed of operation, manoeuvrability and operating altitudes between the engagement space of traditional air and ballistic missile defence systems [352]. Such capabilities are also valuable for engaging high-value time-sensitive targets or for rapid re-targeting during flight.

2. **Defensive Countermeasures**: Hypersonic systems are challenging to defend against by their very nature (speed and manoeuvrability). New defensive countermeasures will need to be available to BLUE forces, capable of engaging such targets en-mass and in a sustained manner. Given the speeds involved, these will most likely be electromagnetic (directed energy, hypersonic rail guns, jamming, space-based missiles, etc.) in nature, although this is not without significant technical challenges.

3. **Aircraft**: Hypersonic aircraft will sustain Alliance capabilities in a post-stealth operational environment, providing a technological edge in a *post-stealth* world [77]. Such systems may enable rapid deployment of special forces or materials around the world in the matter of a few hours.

4. **ISR**: Propelled hypersonic vehicles will be used for high-altitude rapid ISR collection (e.g. as a successor to the SR-71), as an alternative to collection by satellites or HALE UAVs.

RED

Over the 20 year horizon of this report, hypersonic weapon systems will remain the province of peer or near-peer competitors due to significant technical challenges and high capability costs. Increased strike capabilities, more effective defensive countermeasures [385] and hypersonic aircraft will challenge Alliance operations. In particular, the possibility of a non-nuclear (kinetic) decapitation strike against strategic and operational high-value targets (e.g. critical bases, capital ships [386] etc.) will significantly compress strategic and operational decision times in a manner that is potentially profoundly destabilising [45].

Both China and Russia have demonstrated advanced HGV and HCM programs [81, 82], although their true operational status is subject to debate (e.g. Chinese DF-ZF (WU-14) and Russia (Russian YU-74 Avangard)). At the end of 2019, the Russian Defence Minister Sergei Shoigu announced that the Avangard HGV had entered service, with President Putin further stating [387]:

Figure F.6: *Kh-47M2 Kinzha (Dagger): 2018 Moscow Victory Day Parade (CREDIT: kremlin.ru).*

> *"Not a single country possesses hypersonic weapons, let alone continental-range hypersonic weapons ... [other nations are] playing catch-up with us ... The Avangard is invulnerable to intercept by any existing and prospective missile defence means of the potential adversary"*

Prior to this, on 1 March 2018, Russia successfully tested the air-launched Kinzhal hypersonic missile and official reports indicate that they have entered limited service (Figure F.6) [388]. Later in March Russian announced it had tested a new HCM (Zircon), a ship-launched anti-ship and land-attack missile system [389]. Similar Chinese development of hypersonic glide vehicles has culminated in the operational deployment (as of 2019) of the DF-17 and development of anti-ship missiles [382, 390, 391].

To date, research and development of hypersonic flight is possible only for nations with highly developed R&D capabilities and significant financial resources.

Interoperability

Given the high cost associated with hypersonic R&D, interoperability issues are expected to be small, as these systems will remain firmly under national control. Hypersonic defence systems may present some interoperability challenges, but these are expected to be consistent with the deployment of conventional systems. More critical will be the (offensive & defensive) capability disparity within the Alliance, along with C2 issues associated with integrated tactical warning and threat assessment.

S&T Development

Hypersonic research has gone through several major cycles over the last 70 years. However, recent advances in materials, propulsion, guidance, control have provided new approaches to dealing with significant thermal, manoeuvrability, pressure and energy challenges. In particular, future research will need to be focused on:

1. **Platforms**: Novel heat resilient materials; new modes of propulsion; miniaturisation, weight reduction; modelling & simulation; new vehicle designs; scramjet propulsion; stealth materials and design; autonomous behaviour (AI and swarms); and, advanced flight control. More specifically,

    - **Materials**: Surface temperatures of HCM/HGV systems can reach over 1000 °C. The development of new mechanically strong and heat-tolerant materials will be necessary [352].

- **Propulsion**: Propulsion systems will need to be expanded and further refined, including increased reliability, efficiency [352, 358] and alternative launch (e.g. EM).
- **Control**: Flight dynamics at hypersonic speeds is complicated by unusual airflow characteristics, necessitating improved modelling and simulation (i.e. computational fluid dynamics (Figure F.4)). This, in turn, will help enable research on vehicle control and guidance, which is especially important to improve accuracy, loss of control and autonomous behaviour.

2. **Defensive Counter-Measures**: Countering hypersonic threats will be necessary as the high speeds, manoeuvrability and operating altitudes make this a challenging prospect [392, 393]. More specifically,

   - **Sensors & Tracking**: Countering HCM & HGV will require improved terrestrial and space-based sensors for detection, identification and tracking, as well as improved navigation and control to ensure successful intercepts. Integrated data fusion and autonomous functions will need to be improved to support the short decision times available.
   - **Hard Kill**: Development of new anti-hypersonic missiles or hyper-velocity projectiles suitable for the counter-hypersonic role will present a major technological challenge. Directed energy weapons (DEW) may also provide a hard-kill capability, but the very nature of hypersonic vehicles will make this a challenge.
   - **Soft Kill**: The use of cyber, EW, DEW and decoys as a means of countering hypersonic weapon systems.

The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table F.1: *Hypersonic (Systems) 2020-2040.*

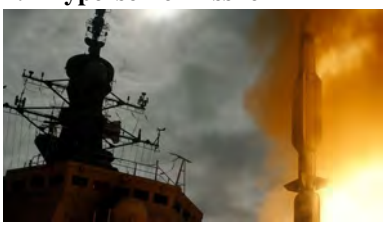
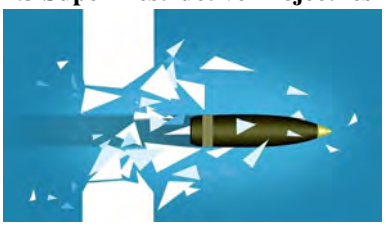
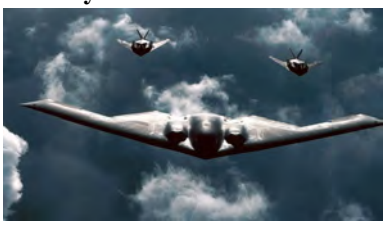
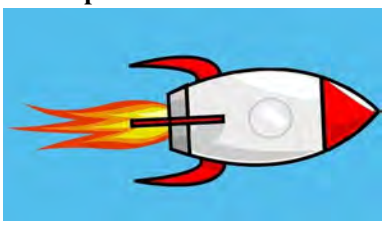
EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Hypersonics	Platforms and Propulsion	High	Trigger	5	2025
	Countermeasures	High	Trigger	3	2030

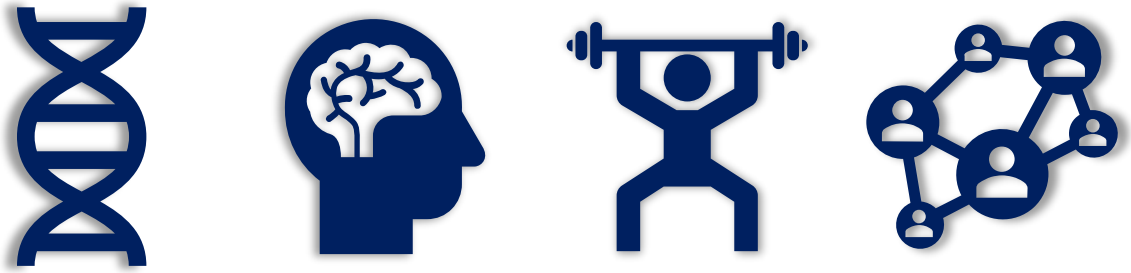
Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

References

[45, 78, 79, 80, 350, 352, 361, 363, 364, 366, 367, 368, 370, 379, 385, 390, 393]

Conjecture Card: Hypersonics

F.1 Energy Beam Self Defense  Automatically defend air, maritime and land assets from incoming hypersonic missiles or enemy systems using high powered energy beam weapons (e.g. lasers).	**F.2 Hypersonic Missile**  Launch a precision hypersonic attack from ground, surface, air or orbit capable of absolute destruction of a large building, aircraft carrier, air terminal or complex.	**F.3 Super Destructive Projectiles**  Propel hypersonic projectiles over great distances, without the need for chemical propellant, delivering destructive power through kinetic effect.
F.4 Underwater Launch  Launch hypersonic weapons (glide or cruise) while submerged for strike or ISR missions.	**F.5 Very Fast Air**  Employ manned aircraft, UAVs and missile systems supporting hypersonic cruise, increasing responsiveness, situational awareness and survivability.	**F.6 Hypersonic Swarms**  Precision control of swarms of hypersonic vehicles or missiles in-flight targeting air, land or naval forces.
F.7 Propulsion and Materials  Exploit next generation materials, propulsion and manufacturing to greatly reduced the cost and availability of hypersonic systems.	**F.8 Defensive Shield**  Simultaneously identify and destroy multiple incoming ballistic or hypersonic missiles inside or outside the atmosphere.	**F.9 EM Countermeasures**  Disable targeted electronic systems on hypersonic vehicles, even those with electromagnetic shielding or countermeasures.



G. Biotechnology & Human Enhancement

Biotechnology and Human Enhancement
"Modern technologies that actively seek to combine bio, nano, info and neuro elements can give us the ability to 'enhance' human beings in ways that we want. This ability — to make soldiers more capable of defeating their enemies and surviving the perils of conflict — is of great interest to militaries throughout the world." - *Adam Henschke* [394].

Definition

Bio & Human Enhancement Technologies (BHET)
Biotechnologies use organisms, tissues, cells or molecular components derived from living things, to act on living things; or, act by intervening in the workings of cells or the molecular components of cells, including their genetic material [101]. *Human Enhancement Technologies* (**HET**) are biomedical interventions that are used to improve human form or to function beyond what is necessary to restore or sustain health. HET may enhance physiological, cognitive or social functions.

Keywords

Medicine · Supplements · Mixed Reality · Prophylaxis · CRISPR · Synthetic Biology · Human Enhancement Technologies (HET) · Bio-Engineering · Genetics · Medical Countermeasures · Genetic Engineering · Micro-Fluidics · Neural Interface · Prosthetics · Exoskeleton · Molecular Engineering · Brain-Machine Interface · Neural Prostheses · Neural Interface · Biosensors · Bioinformatics · Micro-Arrays · Bioelectronics

Overview

Bio and Human Enhancement Technologies (BHET) are comprised of four major R&D areas (with substantial overlap and synergies between them). These are listed below with example applications or areas of research:

(1) **Bioinformatics & Biosensors**: In vitro / ex vitro sensors, medical imaging, quantum biology, applied BDAA;

(2) **Human Augmentation**: Mixed reality, virtual reality, social networks, robotics, AI, prosthetics, exo-skeletons, neuro-electronics, rehabilitation, neuroscience, robotics, teleoperations, autonomy, cognitive performance, computational, artificial intelligence, trusted autonomy, perceptual enhancements;

(3) **Medical Countermeasures and Bio-medical technologies**: Chemical-Biological-Radiological-Nuclear (CBRN) counter-measures and detection, personalized medicine, biomarkers, bio-engineering, supplements, nutrition, physiology, resilience, stress resistance; and,

(4) **Synthetic Biology**: Genetic engineering, DNA sequencing and exploitation, bio-manufacturing, modified microbiome, living sensors.

Advances in materials, information systems and the human sciences are setting the stage to significantly enhance human capabilities, pushing the physiological, cognitive and social human performance frontiers. R&D in these areas is enabled by rapid parallel developments in RAS, AI, BDAA, miniaturisation and innovative materials/manufacturing. As a result, BHET developments are moving at a breathtaking rate, driven by research breakthroughs (e.g. the discovery of CRISPR/Cas9 for gene editing [395]), substantial national investments and increasing commercial interest. The limits on development are around the need for baseline research, as well as ethical, legal and policy concerns. In particular, there are serious issues around the use of genetic engineering; the release of personal bio-data; use of pharmacological enhancements; and, ethical testing of new therapeutics and countermeasures.

Figure G.1: *Bioinformatics.*

Bioinformatics, and the related field of computational biology is concerned with the storage, retrieval, organisation and analysis of biological data, and in particular that associated with humans or human activity. The processing of such large volumes of data available for exploitation and assessment (often in real-time) has enabled a much greater understanding of biological, biochemical, physiological, cognitive and social behaviours. In turn, this has supported new technological developments in medicine, genetics and biology. Especially over the last 15 years, bioinformatics has transformed the biological sciences to the point where:

> *"It might be that a new, "theoretical biology" is emerging, where models and their predictions can now be assessed by experimental biology, in analogy to the interplay between theoretical and experimental physics. This moment might have come faster than expected. The merging of computation into the fabric of biosciences and biomedicine by 2020 ...will possibly necessitate a redefinition of computational biology as a distinct discipline in the not-so-distant future." [396].*

Developments in biosensors (especially cheap and widely available ones) have significantly contributed to this data explosion. Biosensors are devices that measure biological (immunological, pressure, thermal, etc.) or biochemical processes and convert them into an electrical signal. These are widely used today and come in many forms. They may be employed for many purposes, such as nano-sensors embedded in smart clothing for detection of CBRN agents; treatment monitoring (e.g. diabetes); silicon photonic biosensors (e.g. fibre Bragg gratings [397]); rapidly applied *tattoos* to monitor physiological or cognitive stress [398]; and in support of biomedical research [399]. Human physiological monitoring technologies are already commercially available and more advanced sensor packages will mature in the midterm. Advances and technological convergence in material, information and human sciences are allowing new cheaper, smaller and more robust biosensors to be developed.

S&T development in bioinformatics and biosensors, as they related to NATO capabilities, will be predominately around their novel use, application of new analytical methods (e.g. AI, quantum

biology [400], new sensors (in vivo / ex vivo) and the identification of new biomarkers). This continued development will support predictive combat casualty care and diagnostics; operational readiness (e.g. over-training, nutritional deficiencies, immunocompetence, cardiac health and muscular-skeletal injury); and assessment of CBRN exposure.

State-of-the-art sensors are typically designed for optimal detection only. As an example, terrorism threats and military conflicts have motivated research in novel sensors for detecting explosives and chemical warfare agents (CWAs). The focus of today's research on (bio)sensors goes far beyond the optimisation of the sensing material; it includes the ability to make decisions and act – *smart sensing*. Research in this area includes the application of [401]: sensor material designs employing carbon nanotubes, polymer nanowires, and porous silicon; machine learning, and DNA-based molecular computing for smart biosensor function; and, bioelectronics and neuroelectronics, such as nerve cell microelectrode arrays for creating novel transducers and physiological biosensors.

Figure G.2: *The Future Soldier (CREDIT: US-ARMY/DARPA).*

Enhanced bioinformatics and biosensors will improve monitoring and bio-situational awareness through the application of advanced data collection and predictive analytics. Leveraging such techniques will support improved military health, operational readiness and training, through predictive and pre-emptive responses to environmental or individual issues [202].

Human augmentation, human enhancement or soldier systems are broadly understood to mean technologies used to improve human form or to function beyond what is necessary to restore or sustain health. Concerning BHET relevant to NATO, we take these to cover the range of human domains - physiological, cognitive & social, and the use of robotic exoskeletons, smart textiles, drugs, and seamless man-machine interfaces.

The development of new human augmentation technologies (physical, pharmacological, neurological or social) has the potential to change the capabilities of the individual soldier, sailor or aviator significantly [402, 403, 404, 405, 406] and create integrated human-machine symbiotes of unparalleled capabilities. Examples of such augmentation across a variety of sensory modalities are [402]:

- Ocular enhancements to imaging, sight, and situational awareness through implants, glasses or contact lens. These visual enhancements will support team data sharing; enhanced target identification; man-machine teaming; and, expansion of vision beyond the visible spectrum. [407];
- Restoration and programmed muscular control through an optogenetic bodysuit sensor web;
- Auditory enhancement for communication and protection; and
- Direct neural enhancement of the human brain for two-way data transfer.

The first three of these technologies are expected to be widely available within the next 20 years. The last, direct neural enhancement, is potentially the most disruptive but is also unlikely to be widely available before 2050, putting it outside the scope of this study. Nevertheless, the development of direct neural-silica connections supporting bi-directional data transfer and mesh networks are a real possibility. Given recent advances in understanding the brain's neurological components and cognitive architecture,

neuroelectronic components that can efficiently implement brain-like algorithms and interface directly with biological *wetware* offer possibilities for new technological capabilities that could significantly impact both the civilian and military domains. Very high speed, very low power neuromorphic electronic components that feature non-von Neumann architectures and analogue-like processors offer the possibility of autonomous systems and heterogeneous computer architectures that incorporate these devices. Such systems would be able to perform tasks that the brain excels at but which currently thwart classical computers, such as extensive heterogeneous data analysis and visual scene processing. Interfacing these devices with biological systems will offer new treatment methods for neurological diseases and improved interface mechanisms between the brain and electronic devices for better control of artificial limbs.

In the near term, significant changes in advancing heads-up displays over the past five years will be refined to offer:

- Improvements in the power efficiency of micro-displays;
- Advancements in optical fabrication techniques for free-form optical surfaces; and
- Integration and proliferation of smartphones and wireless data links.

The broad deployment of exoskeletons in commercial sectors will probably remain quite limited for the short term, due to their high cost (more than $25,000 per suit). Nevertheless, *"it's clear that the era of the exoskeleton has begun"* [408] in areas such as logistics (e.g. warehouses), construction and manufacturing (e.g. cars and aviation) to ease worker burden, improve efficiency and reduce injuries. It is predicted that by 2025 the exoskeleton market will be 1.8 billion USD, up from 68 million USD in 2014 [409]. The US Army and others are moving forward quickly with development and exploring the operational effectiveness of exoskeletons in theatre [410, 411].

Other methods of human augmentation include the development of new physiological and pharmacological cognitive (PCE) enhancements, with attendant reproducibility, medical, ethical, legal and policy considerations (e.g. [412, 413]). Direct peripheral nerve stimulation and other non-invasive methods may also be used to increase synaptic plasticity for improved cognitive performance and learning [202], supporting rapid and practical training of military personnel in complex multi-faceted tasks.

Figure G.3: *Future Gear.*

Ethical, legal, and policy issues arise around the entire spectrum of human enhancement technologies, but especially with pharmacological enhancements. As noted by [414]:

> *"Militaries have long sought to enhance the physical and cognitive performance of warfighters directly, and indeed some human performance enhancement drugs are widely used across the US military today, such as caffeine. Existing technologies have demonstrated the ability to improve individual physical and cognitive performance above baseline levels and in key areas central to military competition: strength, focus, attention, learning, and resistance to fatigue. Many of these technologies are already being used in civilian settings, in licit or illicit contexts."*

Mixed reality, is another example of human augmentation, blending the real and virtual worlds to create new digital or manufactured realities, where physical and digital objects co-exist and interact in real-time. Applications include heads up or head-mounted displays for pilots and soldiers for real-time situational awareness, digital cockpits/windows, realistic training environments or providing hands-free job performance aids. Augmented Reality and Virtual Reality are subsets of Mixed Reality. Computer

simulation models are often used to deliver these experiences. Recent attempts at large-scale commercial product releases for head-worn, see-through, virtual displays have reopened interest in the use of head or body-worn virtual displays.

Figure G.4: *Visual Enhancement.*

Reference [402] notes that these technologies will rapidly mature over the next 20 year and be primarily driven by the commercial market. This bio-economy is already at the earliest stages of development (e.g. Google glasses [415]), while the pharmaceutical industry is one of the world's most significant contributing over 200M euro to the EU economy alone.

The social domain is an essential element of human existence, and technology has provided social enhancement technologies in the form of social networks and media. A social network is a network of social interactions and personal relations. Social media is a set of mediums that can be used for social networking. Social media and networks have helped reshape the social, economic and political world over the last 15 years [416, 417], with over 3.5 billion daily users (45% of the world's population). Social media has been embraced widely and quickly, and it has gained tremendous power to affect the perceptions and behaviours of individuals and societies. As such, it has become critical for the defence, security and safety of the Alliance, and it is the prime human-terrain for operations in the cyber/information domain. The amount and variety of social media (whether text, audio, photographic or video in nature) is immense and growing at an astounding rate.

Although social media is a product of the Internet era and most notably the 21st Century, the research on social networks predates the internet by a wide margin. One of the first major social networking studies in the 20th Century resulted in the *Six Degrees of Separation (SDS) Theory*, first proposed by Frigyes Karinthy in 1929. In 2008, well after the advent of the internet, Microsoft conducted a study demonstrating that the average e-mail chain length was 6.6 hops. However, in 2016, researchers at Facebook reported that social networking had reduced the chain length to three and a half degrees of separation. As such, social media and social networks may be best understood as a means for human social augmentation, and they have been highly successful at it.

The growth of the global information network presents significant challenges in understanding dynamic information flows within the network, and the associated velocity, variety and veracity challenges. Understanding the dynamics and spread of information, whether, by individuals, groups, societies or states, within social networks is essential to our understanding of weaponised information and the role this plays in hybrid warfare [418]. Understanding how this dynamic may be exploited is of considerable commercial (e.g. Google, Facebook, Amazon, etc.) and military interest [26, 202].

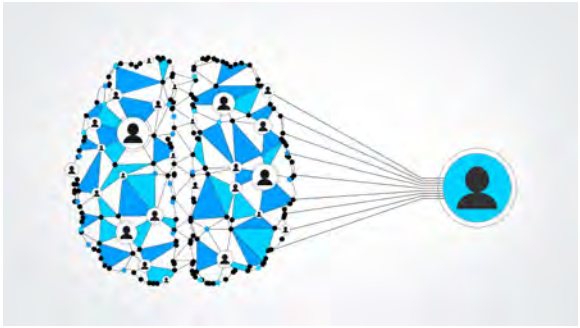


Figure G.5: *Social Augmentation and Enhancement.*

The development of new *Medical countermeasures* and more generally *Biomedical Technologies* pulls together and applies parallel developments in bioinformatics, biosensors, human augmentation and synthetic biology. For example, applied research in casualty care and neural interfaces will help to support evidence-based medicine, operational readiness, increased immunocompetence, disease/biothreat forecasting & detection, patient-centric medicine, rapid development of CBRN countermeasures, improve rehabilitation through new neural interfaces & AI-enabled robotic prosthetic limb technology, and provide new diagnostic and treatment options for mTBI (mild traumatic brain injury) and PSTD (post-traumatic

stress disorder) [202].

Figure G.6: *Casualty Care.*

Combat casualty care may also be significantly enhanced through the use of improved bioinformatics and biosensors, remote monitoring, molecular & cellular biology, AI for rapid diagnostics, bioinformatics, surgical techniques & tools, novel materials to improve rapid identification, and treatment of tissue damage and infection. These technologies have the potential to reduce significantly mortality and morbidity resulting from injuries on the battlefield, improve the efficacy of follow-on care and enhance rehabilitation efforts.

Fundamental research is also ongoing in understanding the dynamics of complex biological systems, such as the human biome. Research is focused on understanding complex dynamical biological systems-of-systems and developing mechanisms for assessment and optimal control [202].

Synthetic biology involves the precise genetic manipulation and engineering of organisms for scientific research and the development of unique characteristics and capabilities not seen in nature. Furthermore, synthetic biological processes can yield new organic molecules, novel materials that cannot be manufactured directly or even new bio-manufacturing paradigms. Synthetic biology builds upon a human tradition of genetic manipulation (e.g. crop breeding, domestication, etc.). Still, it has begun to evolve very rapidly due to the confluence of molecular biology, systems engineering, information science and other emergent technical fields.

The complex convergence of several fundamental technical domains such as molecular biology, systems engineering, etc. precludes a concise and comprehensive characterisation of all relevant and enabling science and technology involved in the field of synthetic biology. Synthetic biology is not a single technology but rather an integrated environment of synergistic technologies (e.g. CRISPR/Cas9 [419]) involved in the manipulation of DNA sequences and exploitation of the resulting complex molecules. The latter involves specialised bio and chemical engineering for scaling biological processes to produce meaningful quantities of new organisms and their products. The former includes the involvement of data and information sciences to architect new molecules. The technologies involved in synthetic biology are globally becoming more advanced and refined as both public and private sector investment are increasingly applied to this field in pursuit of both economic and national security objectives.

Biological engineering is a developing area of research that holds significant promise. The goal of biological engineering is the design and construction of multi-cellular biological systems or systems-of-systems, including the use of AI and genetic design. The goal is to create biological materials with engineered properties. Developments in this area include AI optimised xenobots (i.e specialised bio-robots) for nano-scale manufacturing [420, 421] and living bio-sensors (e.g. persistent living aquatic or terrestrial sensors, or CBRN monitoring) [202].

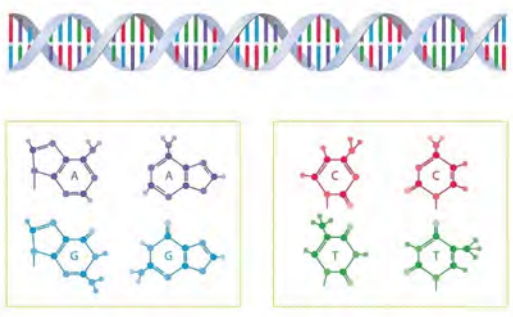


Figure G.7: *DNA.*

The scope and magnitude of the future contributions that synthetic biology will make to civil and national security sectors are currently quite speculative; however, there is little doubt that this technology domain will have substantive impacts wherever it is applied or exploited. Examples of practical applications of synthetic biology are the development of new macro-phages [422], plants, insects [423], viruses constructed batteries [104] and *xeno-bots* for nano-scale manufacturing [420, 421]. Nevertheless, there remain many technical barriers to be overcome in order to realise its full hypothesised potential as well

as many ethical and institutional challenges to be mitigated. The broad global awareness and proliferation of the underlying enabling technologies for synthetic biology largely preclude its comprehensive control; potential adversaries and economic competitors can be expected to have few, if any barriers, to its exploitation for their national or organisational objectives.

Biotechnology, nanotechnology and genomics are advancing rapidly in the short to midterm. These advances are mostly driven by the private sector but can easily be transferred to the military sector where appropriate.

MILITARY IMPLICATIONS

BLUE

BHET are expected to create disruption in:

1. **Readiness**: Use of biomarkers (phenotypic and genetic) for predictive diagnostics will enable predeployment identification of medical issues or weaknesses (e.g. muscular-skeletal, psychological, immunological, physiological or nutritional). Improved diagnosis and novel countermeasures will result in increased occupational readiness and effectiveness for forces in high-risk high-threat environments. Human state monitoring in real-time to near real-time will allow individual and team performance to be optimised.

2. **Operations**: Wearable biomedical systems that provide the ability to monitor soldier health continuously could provide knowledge of the inception and progress of injury over time. Knowledge of the health status of soldiers on the battlefield could be of great benefit for BLUE forces in providing essential information needed for force condition status assessment. Forces, leveraging bioinformatics, sensors and enhancement technologies, should be able to operate in smaller groups, which has implications on affordability (i.e. a smaller number of soldiers, sailors or aviators can achieve similar results). Virtual reality and ultimately, neural interfaces will support significant improvements in situational awareness and operations of autonomous systems. Heads up displays, currently used in aviation and to a lesser extent in automobiles, could also find uses in dismounted soldier systems. Heads-up, eyes-out targeting could be achieved by overlaying targeting symbols on top of real-world targets. Mixed reality could be used to assist planners and mission rehearsal. Immersive visualisation of rapidly generated accurate 3D representations of the physical environment (terrain + buildings + infrastructure) from open source and military data and observations could provide staff with a realistic feel for the terrain before being exposed to it in real life. Mixed Reality setups are already used to provide practical, cost-effective training environments. Advances in computer networking, processing and analytics will see such setups used in the battlefield as well as expensive labs. Neurological interfaces will increase response times, situational awareness and the effectiveness of man-machine teaming.

3. **Medical Countermeasures and Care**: Use of biomarkers, biosensors (in vivo & in vitro) [424] and microarrays (microfluidic devices integrating computing chips with living cells and tissue) will allow rapid (pre-symptomatic) diagnosis and response to synthetic or natural pathogens, chemicals, as well as real-time monitoring of treatment options. Use of biomarkers, novel pharmaceuticals, gene therapy and bio-engineering (e.g. robotics, prosthesis, neural interfaces, etc.) will dramatically increase the effectiveness of combat casualty care and rehabilitation, especially in such areas as post-traumatic stress disorder (PTSD), environmental exposure and mild-traumatic brain injury (mTBI).

4. **Performance**: Rapid advances in material, computer and human sciences, as well as convergence between these fields, is setting the stage to enhance human capabilities and push the human performance frontiers significantly. Optimising the performance of each individual, be it in the cognitive, physical or resilience domains, in addition to improving team cohesiveness and effectiveness, will enable Alliance forces to make better decisions faster, and can produce actions better tuned to

the needs of the situation. Current and future advances in physiological and psychological state monitoring will maximise overall human performance and readiness through specific user group algorithm applications. Benefits include better leadership assessment of force status; increased training program adaptation and effectiveness through real-time performance metrics; and increased health and safety monitoring as well as injury protection. Bioinformatics and biosensors, along with increased use of personalised and virtualised training, will improve training effectiveness. Muscular-skeletal augmentation (e.g. exoskeletons) will increase load carrying capacity during operations, reduce debilitating injuries and increase combat performance.

5. **Social Networks**: Social media supports military activities in six key ways [26]: intelligence collection; (geo-) targeting; cyber operations; command and control; defense; and, psychological warfare (inform and influence). Fusing social media (as part of OSINT (open-source intelligence)) with other data, and integrating social network operations into broader operational and strategic actions will be a critical success factor in countering hybrid and memetic warfare operations.

RED

BHET threats will increase driven, in no small measure by, the democratisation of associated technologies. Significant Alliance ethical, legal and policy are not shared by a peer or near-peer strategic threats. However, more worrisome perhaps, will be their use by security threats (both criminal and otherwise) or the use of non-sanctioned enhancements by individuals. With globalisation and the increased pace of scientific discoveries, there is a high likelihood that an adversary force will have access to the knowledge necessary to create similar capabilities. The implications on the battlefield are that RED would have a significant performance advantage if such a force is not constrained by the same ethical considerations in implementing these new technologies.

In particular:

1. **Synthetic Biology**: New pathogens, novel biological agents or chemical agents, with explicitly engineered and targeted effects (e.g. increased virulence, physical, neurological or physiological impact, genetic susceptibility, etc.), will potentially increase casualties, reduce combat effectiveness and present a strategic challenge to Alliance societies as a whole. The impact of unknown biological agents will challenge the capacity of medical and logistics systems to cope, while countermeasures themselves may present significant health and safety challenges.

2. **Designer Pharmaceuticals**: Criminal and non-state actors will increasingly have the ability to develop low cost targeted pharmacological agents. These may be used to explicitly to disrupt Alliance operations or destabilise alliance societies through targeted psycho-social effects.

3. **Super-Soldiers**: BHET will enable pharmacologically, neurologically and physiologically enhanced opponents. In combination with more effective partnering with autonomous and semi-autonomous systems, these will significantly challenge Alliance forces, force structure and effectiveness.

Interoperability

Alliance interoperability will be challenged by differing legal, policy, training, operational effectiveness and ethical standards amongst the nations driven by BHET. Development of standards for personal biosensors, the handling of bio-data, the sharing of medical countermeasures, man-machine interfaces (including neurological) and bio-mechanical systems will be critical enablers of effective alliance BHET enabled operations and capabilities.

S&T Development

BHET research over the next 20 years (across the innovation system) is expected to include R&D in:

- **Bioinformatics and Biosensors**: The collection, classification, storage, retrieval and analysis of biological and biochemical data leveraging new sensor materials, AI and BDAA. The research will explore new biosensor (including bio-engineered) and bio-data collection methods for detection of biomarkers, as well as the processing and exploitation of massive amounts of personalised, cohort, ISR and environmental data. In addition to increased situational awareness, this will support the development of increasingly sophisticated and predictive models and simulations supporting clinical interventions, personalised medicine, individualised training, assessment of natural or artificial biological threats. [202].
- **Medical Countermeasures and Technologies**: The development of new diagnostics, therapeutics and vaccines (employing bioinformatics, genetic engineering and biosensors) to support predictive diagnostics, CBR threat identification, modelling and treatments. Combat casualty care will apply advances in molecular and cellular biology, AI, bioinformatics, and novel materials to improve rapid identification and treatment of tissue damage and infection.
- **Human Augmentation (Physiological & Cognitive)**: The use of genetic modifications, pharmacological agents, electro-mechanical devices, and neurological interfaces to increase human physiological, neurological performance beyond normal limits.
- **Human Augmentation (Social)**: Increased computational and modelling capabilities to understand information flow within complex social networks (social media). Development of novel quantitative methods will be essential if a deeper understanding of information network dynamics is to be advanced, and countermeasures developed in the context of hybrid-warfare.
- **Synthetic Biology**: The deliberate design, engineering and creation of novel synthetic or modified biological components or systems. This includes the engineering of multi-cellular bio-sensor systems for surveillance and manufacturing.

The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table G.1: *Biotechnologies and Human Enhancement 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Biotechnologies	Bioinformatics	Moderate	Expectation	6	2025
	Human Augmentation	High	Expectation	5	2030
	Medical Countermeasures	High	Trigger	4	2030
	Synthetic Biology	High	Trigger	6	2025

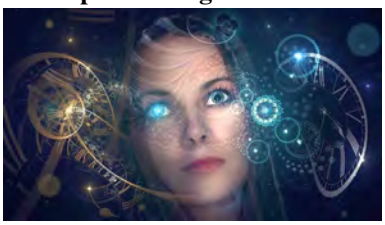
Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

References

[101, 207, 394, 400, 402, 414, 424, 425, 426, 427, 428, 429, 430]

Conjecture Card: Biotechnology

G.1 Super Sensings



Enhance human senses and cognitive abilities to super-human levels to increase speed of learning/comprehension and reduce reaction times.

G.2 Body Self-Repair

Heal wounds, injury or illness using DNA restructuring or synthetic biology solutions (e.g. artificially grown body parts).

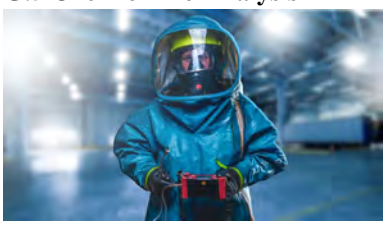
G.3 Bio-Databases

Store or process massive amounts of data in living organisms.

G.4 Human-Machine

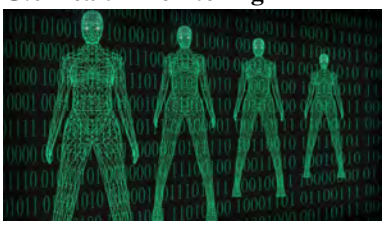
Mechanically augment the human body either with exoskeleton or internal mechanical parts to gain super strength, balance and speed.

G.5 Chem or Bio Analysis



Instantly analyse and identify chemical or biological substances remotely or using hand-carried or unmanned systems.

G.6 Health Monitoring



Continuously monitor health and well-being of entire populations at the individual level, activating drugs or hormones or genes on demand.

G.7 Train in Reality

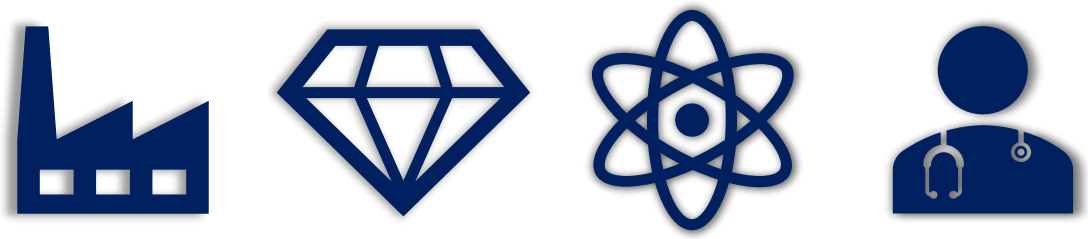
Deploy realistic virtual or augmented reality training environments to prepare soldiers in real-time for mission tasks.

G.8 Psychotic Effects

Remotely induce mass hysteria or hallucinations in groups or individuals.

G.9 Genetic Targeting

Design and develop targeted pathogens, antidotes or neutralising agents for CBRN agents from materials and knowledge available at low cost and to everyone.



H. Novel Materials and Manufacturing

Novel Materials and Advanced Manufacturing

"Advances in materials and manufacturing will have a profound effect on Defence and national security over the coming decades. The use of novel materials with additive and hybrid manufacturing will make for more efficient, lower waste products, highly customised design and production, and embedded electronics and sensors enabling the collaborative, rapid design and manufacture of spare parts for weapons, combat vehicles, and other equipment." - *A. Zelinsky* [431]

Definition

Novel Materials and Manufacturing (NMM)

Advanced (novel) materials are artificial materials with unique and novel properties. Advanced materials may be manufactured using techniques drawn from nanotechnology or synthetic biology. Development may include coatings with extreme heat resistance, high strength body or platform armour, stealth coatings, energy harvesting & storage, superconductivity, advanced sensors & decontamination, bulk production of food, fuel and building materials. Research into graphene, other novel 2-D materials, and topological materials are an area of high potential and growing interest. *Additive Manufacturing*, which is often used as a synonym for *3-D printing* [102], is the process of creating an almost arbitrary 3D solid object from a digital model through layered addition of materials. Additive Manufacturing can be used for: rapid prototyping; in situ production & repair of deployed military equipment; and production of precision, custom or unique parts.

Keywords

Novel Materials · Additive Manufacturing · Agile Manufacturing · Bio-materials · Graphene · 2D Materials · Black Silicon · Flexible Displays · Nanotechnologies · Smart Coatings · Bio-fabrication · Bio-manufacturing

Overview

Novel materials and manufacturing (NMM) research underlies much of the success of the industrial revolution, and that is expected to continue. Over the next 20 years, three main areas of R&D activity are seen to be disruptive: **(1)** Novel Materials; **(2)** Additive Manufacturing; and, **(3)** Energy.

Research into novel materials and advanced manufacturing is a vast field of study [431, 432], touching on the truly unique and surprising properties of 2-D materials, new 3-D fabrication methods, unique designs, smart materials, quantum M&S, nanotechnologies, and bio-manufacturing. These, in turn, have a wide range of applications, with perhaps the generation and storage of energy (e.g. batteries) being one of the most disruptive.

A revolution in 2-D materials research [432, 433, 434, 435] has emerged since the isolation and initial characterisation of graphene and more recently, the families of topological insulators and transition metal dichalcogenides. These and other novel materials have generated considerable R&D excitement, kick-started by the discovery of graphene in 2004, and the awarding of the 2010 Nobel prize in Physics to its discoverers Geim and Novoselov [436]. Graphene is a new carbon-based material with a wide range of extreme mechanical, physical, chemical and electrical properties not found in any other known material. It is chemically stable, non-toxic, lightweight and relatively easy to produce from widely available raw materials. Graphene's individual properties exceed those of conventional materials, and its combination of these properties is unique. It is widely expected to lead to significantly improved materials for applications in aerospace (composite structures), high-frequency electronics (terahertz, radar, cooling), functional coatings (anti-icing, corrosion protection), energy storage (batteries, ultra-capacitors), camouflage (radar absorbers), weapon technologies (energetics, missiles), protection (armour, textiles), sensors (photodetectors, pressure/strain, chemical) and portable devices (displays). Other novel 2-D materials such as phosphorene [437], hexagonal boron nitride [438] and transition metal dichalcogenides [436] have also demonstrated unique and surprising characteristics.

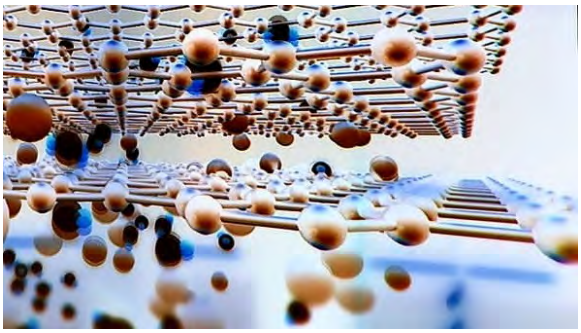


Figure H.1: *2-D Materials.*

2-D materials R&D is taking place around the world. China, in particular, has taken a leading role in 2-D material research [439], and is making significant progress towards commercialisation, as is South Korea. In January 2013 graphene was identified as one of the two European Union Future and Emerging Technology Flagship projects with a budget of 1B€ over 10 years, forming Europe's most significant ever research initiative [440].

The fundamental properties of these 2D materials may be critical enablers for a range of future technologies. While challenges remain in terms of manufacture and scalability, graphene and other 2-D materials will offer game-changing technological improvements — eventually. However, military capability development and application over the next 10-15 years will most likely be evolutionary. Advances will almost certainly be found from combining 2D materials to form new classes of layered heterostructure materials, as well as with use of traditional bulk materials. Early experiments around stacked two-layer, three-layer and twisted graphene sheets [441] have also demonstrated remarkable electrical properties (i.e. superconductivity) [442] and yielded promising biosensors [443].

In general, improved robustness, operational life and reduced weight/size can be expected. This research will lead to novel enhanced devices and uses, such as: • Integration with conventional semiconductor devices to improve infra-red photo-detection for thermal imaging or to achieve faster optical modulation for broadband communications • Biological and chemical warfare detectors • Barriers to specific biochemical molecules • Conductive membranes for flexible or printed electronics [444] • High-speed electronics to support the development of imaging and ranging (radar) as well as Terahertz (THz) communication frequencies [444] • Cooling of electronics leveraging the superior thermal conductivity of graphene [444]. • Development of graphene optoelectronics and photonics for solar cells, touch screens, photodetectors and ultrafast lasers [445, 446].

Current 2D materials research is extremely broad, ranging from energy generation and storage, through optoelectronics and bio-chemical sensing as well as flexible, lightweight yet mechanically strong fabrics and conducting polymers. From a defence perspective, the focus might sensibly be directed toward those

technologies that can provide key advantages in the near to medium term; one of these key areas is likely to be optoelectronics. Testing is being done in industry on the application of graphene to a variety of technologies relevant to sectors such as electronics, medicine, aerospace, automotive, energy storage, water desalination, composites, coatings and paints, solar technologies, oil and communications.

Other materials are also being explored for application to defence problems. Silicon, although well studied and widely applied, has additional properties or states which are of interest. An example is black silicon, micro-structured silicon, which absorbs visible and infrared light strongly due to surface micro-spike traps [447]. It has potential applicability in the production of photo-detectors, night-vision systems and solar cells. Another type of material being explored are topological materials [103], a class of quantum materials whose quantum states are unnaturally stable under environmental changes. Topological insulators [448] are of particular interest due to an unusual combination of insulating and conducting properties.

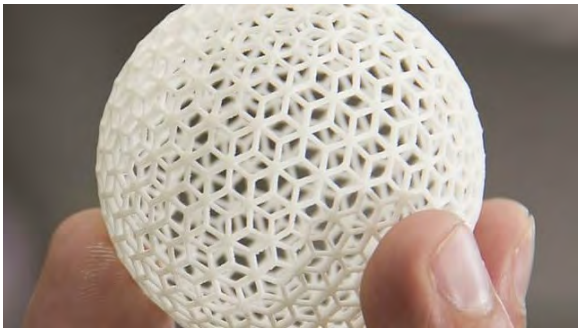


Figure H.2: *3D Printing.*

Additive manufacturing (AM) or 3D printing as it is also known creates three-dimensional solid objects of virtually unlimited shape from digital models and a wide variety of metals, plastics and resins [449]. AM is achieved using an additive material process, whereby successive layers of material are laid down in different forms. AM is distinct from traditional material removal or machining techniques, which rely on cutting, milling or drilling (subtractive processes). AM is already heavily influencing commercial production and supply chains. Some caveats for AM application are limitations in component size, precision and surface quality and the potential need for post-fabrication machining. The resulting manufactured materials may have unique material properties and may be impractical or impossible to produce using conventional manufacturing methods. AM technologies may be used for, among other things, rapid prototyping, in-site production and repair of deployed military equipment, precision, custom and unique parts production. Industry is leading the development of 3D printing, with the global 3D printing market rising from 5.8 billion USD in 2016 to 55.8 billion USD by 2027 [450].

Over the last 20 years, AM techniques, equipment and technology have been developing at a rapid pace [451, 452, 453], where they have become a key component of high-value manufacturing and agile manufacturing. AM (or 3D printing) is a broad term encompassing 7 core technologies [102]: • VAT photopolymerisation • Material jetting • Binder jetting • Material extrusion • Powder bed fusion • Sheet lamination • Directed energy deposition.

Figure H.3: *SpaceX Super Draco Printed Thrust Chamber [454] (CREDIT: SpaceX)*

Current AM techniques are mostly applicable for limited production runs, specialised designs or prototyping [4]. AM systems (limited as they are) are growing in popular both in the home and industrial market. As such they are becoming widely available and have moved well beyond printing simple 3-D plastic models (e.g. Figure H.3). Roughly two-thirds of US manufacturers have already adopted 3D printing with around 50 per cent already using it for prototyping and final products. Nevertheless, AM systems are not yet at a level of maturity necessary to replace traditional machining and manufacturing methods for widespread, full-sized industrial production. This is changing, and the availability of 3D printing capabilities is enabling agile manufacturing and edge production in a variety of industries.

Potential 3D printing applications are seen to be: • Concept modelling and prototyping. • Low-volume complex parts, such as rocket engines • Replacement (obsolescent) parts • Structures using lightweight, high strength materials • Mixed-materials and embedding additively manufactured electronics directly in/on parts • Repair parts on the battlefield, on-board ship or in space • Large structures directly in location thus circumventing transport vehicle size limitations • Manufacture of novel designs or use of unique materials • Large structures [455] such as buildings (using local materials) or weapon systems (such a ship [456]) • Bio-materials such as replacement tissues, organs and body parts.

The related process of 4D printing [457] merges 3D printing with advanced materials sensitive to environmental conditions. These materials are programmed to change their form or physical behaviour when subject to an environmental trigger (e.g. heat, pressure, current, light, etc.).

A related technology, nanotechnologies, are those processes for the manipulation of materials at the atomic scale, often leading to novel material characteristics. The Ministry of Defence in the UK predicts that medical nanobots and nano-enhanced C4ISR devices (e.g. micro-radar for miniature UxVs) will begin to be used from 2030 on-wards [458].

Current AM (3D/4D) and nano-technologies have direct implications for defence and security [460]. However, these technologies are also widely available and *dual-use in nature* [4], thus providing near-peer and non-state actors with similar advantages. This also supports a massive increase in RED's ability to leverage system designs obtained through illicit means or provide embargoed parts such as those needed for advanced aircraft or missiles [461].

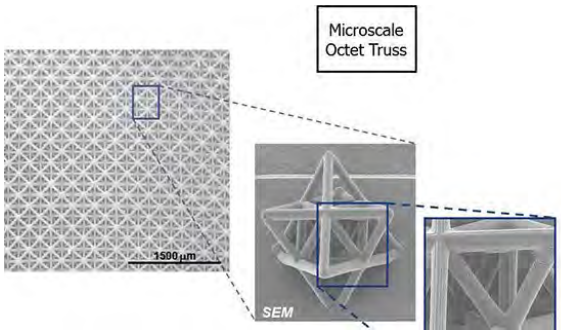


Figure H.4: *3D Micromaterials [459] (CREDIT: DARPA)*

The development of increasingly sophisticated techniques and tools to sequence, synthesise and manipulate genetic material has led to the rapidly maturing discipline of synthetic biology. These developments, in turn, have opened up new approaches to materials R&D, nano-scale manufacturing, bio-fabrication and bio-manufacturing. These approaches utilise engineered biological agents (cells, proteins, fungi, etc.) to assemble or build a wide variety of products, ranging from pharmaceuticals, organs, tissues, leather and even concrete [462]. Specialised bio-robots or *xenobots* for nano-scale manufacturing are also at the early stage of development [420].

Energy, storage and generation, is a critical aspect of battlefield sustainment and the increasingly multi-domain and nonlinear nature of modern conflict demands prodigious amounts [463]. Over the last 10 years, in particular, electric storage and renewables have leapt ahead. These advances are based on the development of novel materials, manufacturing methods, energy management (e.g. use of AI), and approaches to energy collection. Lithium-ion batteries, in particular, are an enabling technology for sensors, vehicles, edge computing, mobile devices etc. The importance of the science behind lithium-ion batteries was recognised by the awarding of the 2019 Nobel Prize in Chemistry to John B. Goodenough, M. Stanley Whittingham and Akira Yoshino.

Energy research spans a wide range of topics and approaches, with societal and military demands increasing yearly. This demand cannot be addressed via existing technologies, and major breakthroughs continue to be needed [464]. Research into new energy collection, generation, storage and management continues at an accelerating pace. This includes research into • Renewable energy such as solar, wind, geothermal and biofuels • Hydrogen • Fusion (inertial confinement fusion, magnetic containment) • Fission (molten salt, thorium, mini-reactors, etc.) • Energy harvesting (wireless, bio-mechanical) • Grid storage • AI enabled power management; • Batteries (graphene, carbon nano-tubes, solid state, metal-air etc.)

Military Implications

BLUE

There are many defence applications of advanced materials, nanotechnologies and 3D/4D manufacturing. It can be assumed that future systems will be lighter weight, stronger and more power-efficient due to the incorporation of advanced materials. In particular, graphene and other 2-D materials will enable:

- Reduced equipment burden (by the nature of being able to replace bulky components with lightweight materials and devices), particularly important for long-range operations and critical for aircraft systems;
- Integral lightweight, flexible electronics woven into fabrics for covert wearable devices;
- Faster electronics for communications (wider bandwidths) and improved computation;
- Improved detection of (weak) signals, (RF/microwave or optical) extending the physical range of operating platforms (either for communications, range-finding or thermal imaging/heat-seeking).
- Membranes that protect against bio-chemical attack, or provide higher sensitivity to detection (as well as selectivity) of explosive vapours;
- Lightweight high-impact resistant materials for new armour and soldier systems, substantially lighter than current technologies. Graphene has been shown to improve the fracture toughness of ceramics, and this is expected to translate into improved ballistic protection if applied to ceramics used for armour. Graphene may improve the strength and elastic properties of ballistic fibres such as ultrahigh molecular weight polyethene.
- Reduced radar reflections from all platforms (land, sea and air) by adding graphene to polymers for radar-absorbing coatings.
- Energy storage in ultra-capacitors and batteries using graphene-based storage. Some products are already certified for space applications.
- Wearable technologies. It is expected that graphene may be useful as a coating on textiles for uniforms, to improve weather resistance and for condition, monitoring using smart/intelligent textiles. Chemical protection of gloves, masks, etc. may also be improved.
- Increase vehicle survivability through the reduction of reflection and radiation of electromagnetic waves by smart coatings.

Specific applications of AM supporting Alliance operations or capability development are:

- Improved product development, via shortened design cycles and increased cost/time effective development. AM can also support design optimisation unlimited by conventional machining constraints;
- Improved maintenance and logistics by reducing stocks of spare parts (at home, on ships or abroad), increasing parts availability and reducing shipping expenses. Spare parts could be manufactured on demand locally, replacing hardware storage by storage of printable designs. Such parts could be produced on-site based on a 3D scan of the component, thereby significantly extending operational life, reducing the logistic tail and minimising life-cycle costs.;
- Cost reduction and increased effectiveness of new designs and high-cost items, especially in the aerospace or maritime environments. For example, single-crystal turbine blades coated with thermal barrier coatings or ultra-quiet submarine propellers involve intricate designs and complex material processing. They are, therefore, costly. The effective repair of such components using AM will significantly reduce the cost of ownership and increase operational availability.

- Production of task-tailored autonomous weapon systems on-demand and on-site [465].

Synthetic biology and nanotechnology specific applications include:

- Production of commodity-like materials, with increased efficiencies enabling production economies of scale, e.g. fuel, food, and building materials;
- Fielding unique capabilities for sensing of environmental and other phenomena not currently detectable or at scales needed across the battlespace; and,
- Creating speciality materials having special chemical or physical properties, including drugs, nutritional supplements, and other substances requiring nano-scale manufacturing assembly processes.

RED

The benefits for RED are similar to those available to BLUE. More specifically for AM:

- Since progress in AM is mainly driven by civil/commercial interests it is probable that these technologies will be available to a wide range of countries, non-state actors and military forces. As such, the novel use by asymmetric threats (firearms, IED's, task tailored weapons, etc.) must be anticipated and may pose a considerable threat to BLUE.
- There are serious concerns around the management of AM technologies for defence applications. Digital designs are required for AM, and these are easily reproduced (e.g. via 3D scanning), shared, hacked, modified, counterfeited and stolen.
- The broad availability of AM and associated novel designs will encourage the proliferation of defence technology to non-state players; non-friendly states; and, counterfeiting of components. Embargoed parts could also be readily produced (e.g. F-14 parts [466]) limiting the effectiveness of sanctions.

Interoperability

No specific interoperability challenges are foreseen with the development or use of 2D materials. Nevertheless, this may lead to some technical disparities amongst NATO forces.

Development of AM as an integral NATO capability will require design, software, IP, cyber, certification and manufacturing standards be developed if advanced 3D/4D printed parts are to be used in advanced weapon systems. Safety requirements alone suggest that if we are to exploit AM parts routinely in high-stress areas such as aerospace, then we must address their certification and qualification as original or replacement parts. This requirement will require an extensive understanding of all factors that lead to variability in properties, and methods to accurately inspect, characterise and certify components. Use of digital designs, scanning and 3D printing of parts may violate contractors IP or may increase the risk of legal action against Alliance forces, while limiting operational agility and reducing operational availability.

Figure H.5: *Standards for Push-Button Replication.*

S&T Development

Graphene and 2D materials research are at an early but promising stage of development. The range of potential applications for graphene and related technologies makes it impossible to generalise at this point. Some applications (ultra-capacitors), adhesives and elastomers (rubber tyres) are commercially

available, so the TRL for these applications is 9. Most applications, however, are at relatively low TRL. The rate of development is fast in some areas, driven by broad public and private investment. In the short term (0 - 7 years), evolution will occur in the application to ultra-capacitors, adhesives, elastomers, non-demanding fibre composites (sports equipment), some coatings will achieve TRL 9. In the medium term (8 - 20 years) thermal interface materials for electronic cooling will reach TRL 9 at the beginning of the period. Some sensors and electronic applications will be reaching commercialisation, and many coatings will be available for corrosion resistance. Significant progress (TRL 6) will have been achieved in multi-functional (structural) camouflage coatings by the end of the period.

Figure H.6: *Stem Cell Bio-Printing.*

The application of bio-manufacturing at nano-scales is now at the lowest technology readiness levels. It is anticipated that many heretofore unidentified synthetic biological materials and applications will develop over the next ten to fifteen years, having by then reached TRL 6 or higher. The current TRL of some of the enabling synthetic biological technologies for applications in the midterm time-frame are likely already manifested in technology readiness levels one through three.

For 3D/4D AM the technology is already used today within various industries for many different purposes, while at the same time rapidly evolving and expanding. The specific TRLs and attention levels are very material, application and process specific [467]. TRL for a military application can be rated between 4 - 6.

The following table presents the assessed potential impact, state and rate of development, as well as identified areas for focused research.

Table H.1: *(Novel) Materials 2020-2040.*

EDT	Technology Focus Areas	Impact	Attention	TRL	Horizon
Materials	Novel Materials	High	Trigger	2	2040
	Additive Manufacturing	Moderate	Enlightenment	7	2025
	Energy Storage	Moderate	Trigger	5	2030

Relevance: Low Medium High							
Capability Hierarchy	PREPARE	PROJECT	ENGAGE	C3	SUSTAIN	PROTECT	INFORM
S&T Domain	HUMAN		INFORMATION			PHYSICAL	

References

[257, 429, 431, 444, 453, 464, 467, 468, 469, 470]

Conjecture Card: Materials

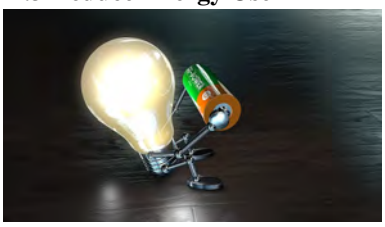
H.1 Synthetic Biology

Use artificially grown or 3D printed human body parts for use for transplants to heal injured people or to upgrade humans.

H.2 Smartlite Armor

Wear lightweight body amour or clothes that are extremely flexible, but resistant to bullets or directed energy fire.

H.3 Reduce Energy Use

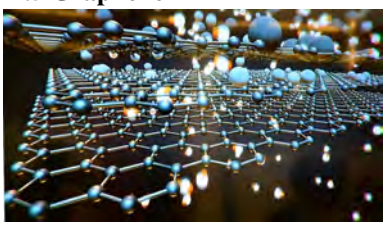


Harvest, store and optimise use of energy reducing resupply needs without significant loss of capability.

H.4 Self-Charging Batteries

Generate and store renewable energy adequate for the daily needs of an individual soldier in ways that are soldier portable.

H.5 Graphene



Use diamond hard graphene composite armour and corrosion resistant plating an order of magnitude lighter than 20th century systems.

H.6 Temporary Shelters

Build large stable shelters from extremely resilient extremely lightweight material that remembers how it was packed and self-packs in minutes.

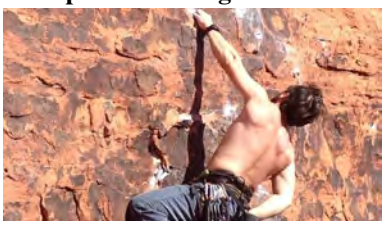
H.7 Platform Printing

Rapidly develop and deploy task tailored land vehicles, naval vessels, aircraft, habitation and space craft.

H.8 Textured Explosives

3D print embedded and hidden energetic materials in structures and systems (available to state, non-state actors, and individuals).

H.9 Spider climbing



Climb walls or windows with sticky material applied to hands and knees or feet.

I. Methodology

Forecasting:
"Mieux vaut prévoir sans certitude que de ne pas prévoir du tout." - *Henri Poincaré* [471]

I.1 Description

The approach and key data sources used to conduct this assessment are described in the following sections.

I.2 NATO Reports and Studies

The following NATO publicly released documents were used in the preparation of this report:

I.2.1 The Science & Technology Office: Tech Trends Report 2017 - Empowering the Alliance's Technological Edge

This report, published in 2017 [10, 42], provides highlights of technology trends assessed by the NATO STO. It was the first report on emerging trends in science and technology published by the NATO STO. It drew upon insights generated by the STO Panels and Group captured in Technology Watch Cards, highlighting potentially disruptive developments in science and technology.

The report identified twelve technology areas:

Additive Manufacturing	*Everywhere Computing*	*Predictive Analytics*
Social Media	*Unmanned Air Vehicles*	*Advanced Materials*
Mixed Reality	*Sensors are Everywhere*	*Artificial Intelligence*
Electromagnetic Dominance	*Hypersonic Vehicles*	*Soldier Systems*

I.2.2 Framework for Future Alliance Operations (2018)

To maintain a decision and capability advantage (credible, networked, aware, agile and resilient) in future operations, NATO must continually evolve, adapt, and innovate. *The Framework for Future Alliance Operations 2018* (FFAO) [24] provides a possible futures perspective supporting such developments. It informs the Alliance of opportunities to improve its defence and deterrence posture together with its ability to project stability, ensuring it remains continuously proactive, ready and responsive. It describes how NATO forces can keep the edge and retain the ability to defeat potential adversaries on the battlefields of the future. Finally, it provides military advice identifying force characteristics and abilities needed by

the Alliance to retain the military edge, address upcoming challenges, and seize the opportunities of the future.

The FFAO identifies several *instability situations*, potential events of critical significance, that could reach the threshold requiring the Alliance to use military forces. These instability situations provide a useful framework for consideration of the impact of EDTs, both from a threat and opportunities perspective, and are listed below:

Weapons of Mass Destruction	*Conventional War*	*Threat Escalation*
Hybrid War	*Irregular War*	*Terrorism*
Global Commons Disruption	*Critical Infrastructure Attack*	*Information Warfare*
Cyberattack	*Governance Challenges*	*Endangerment of Civilian Populations*
Mass Migration	*Pandemic Disease*	*Natural or Man-made Disaster*

The report identifies anticipated future operational challenges. These include the impact of technological advances; new concepts of operation (e.g. global strike, hybrid, and cyberspace operations); and, shifts in the geopolitical landscape. Of interest to the assessment of EDTs, the report notes that future armed conflict is expected to be characterised by any combination of:

- Adversaries (state and non-state) global in scope and employing indirect approaches;
- A greater role of super-empowered individuals and non-state actors that produce hard to predict effects;
- A compression of strategic, operational and tactical decision making, blurring decision-making processes;
- More inter-connectivity across air, land, sea, cyber, space and information domains;
- Small units fighting over greater distances;
- Operations in the cyberspace domain, global commons, urban areas, and subterranean areas;
- Rapidly emerging and widely available technologies;
- The use of human enhancement and the rising importance of the human-machine interface;
- The use of automated and potentially autonomous systems and operations in which humans are not directly involved in the decision cycle;
- New classes of weapons that can cause widespread destruction;
- Greater number of sensors and the proliferation of the internet of things;
- An expanded access to knowledge, including the ability to conduct large-scale advanced data analytics to gain military advantage; and,
- Weaponized information activities intended to influence populations alone or in support of armed conflict.

I.2.3 Technology Trends Survey: Future Emerging Technology Trends (2015)

"Technology Trends Survey - A Food-for-Thought Paper to Support the NATO Defence Planning Process" [472], published in 2015 by NATO ACT, considered the impact of advances in technology to support the NATO Defence Planning Process. It identifies no notably radial or disruptive technologies; however, it describes significant incremental changes across a broad range of technology areas. The report represents a holistic approach to foresight. It can best be understood as a guide book to emerging technologies, developed to position NATO to exploit such areas to its advantage. Though this document provides a primer for overall knowledge development, its primary objective was to support the derivation of long term requirements within the NATO Defence Planning Process (NDPP). In particular, it identifies the following technologies of note:

Biotechnology	*Robotics*	*Information Technology*
Nanotechnology and Materials	*Energy*	*Space and Hypersonic Systems*

I.2.4 Emerging or Disruptive Technologies Roadmap

Following the July 2019 NATO Defence Minister's meeting, the NATO IS/ESC (International Staff / Emerging Security Challenges), NATO ACT and the STO engaged in a vigorous debate around the issue of emerging or disruptive technologies. As noted in [9] the Defence Ministers approved an EDT Roadmap in October 2019. Work underlying this report informed, and was in turn informed by, these developments. The EDT taxonomy used in this report reflects an agreed-upon set of seven EDTs, with the addition of Materials (Novel Materials and Agile Manufacturing) based on STO foresight activities. The inclusion of an eighth EDT recognises that aspects of materials and manufacturing research are both well-developed technologically yet are becoming increasingly disruptive (e.g. 3D/4D manufacturing) while at the same time, some aspects are emergent (e.g. novel materials, bio-manufacturing and nanotechnologies).

I.3 NATO STO Technology Watch

I.3.1 Collaborative Research Program (CPoW) NATO S&T Priority Areas

A set of NATO research priorities guides S&T conducted under the auspices of the STO, as agreed to by the Nations through the S&T Board. These priorities serve to influence medium to long-term S&T planning across the NATO and inform S&T investment decisions within the Nations. Through engagement with the over 6000 active scientists, engineers and analysts who participate in the collaborative research program (CPoW), the STO's maintains an understanding of current and future S&T, including broad themes and EDTs.

The STO S&T priorities are organised into 10 S&T Areas, spanning the human, information and physical sciences. Each area has specific defined *Targets of Emphasis (TOE)*. While there are many different ways of organising S&T activities, the 10 S&T Areas provide a broad and useful reference frame for research activities, while the targets of emphasis provide selective focus and orientation. The priorities are constructed independent of physical domains, scientific disciplines, or specific applications, while the language is situated between the words used to express requirements and S&T solutions. The employment of the priorities focuses on S&T efforts that support cutting-edge capabilities for the Alliance's forces, inform future military specifications, and provide strategic advice to senior decision-makers. Table I.1 summarises these priorities and associated targets of emphasis.

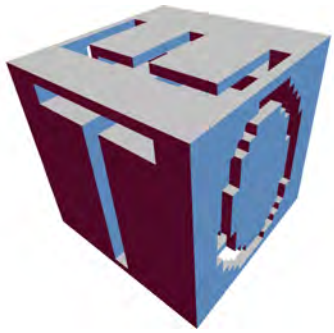


Figure I.1: *Targets of Emphasis (ambigram) [473].*

Table I.1: *NATO S&T Priorities.*

Domain	NATO S&T Priority Areas	Targets of Emphasis
HUMAN	Advanced Human Performance & Health	Medical Solutions for Health Optimisation
		Human Resiliency
		Enhanced Cognitive Performance
		Human & Machine Interfaces
	Cultural, Social & Organisational Behaviours	Social Influence
		Political Influence
		Cultural Communications
		Group & Organisational Behaviour
INFORMATION	Data Collection and Processing	EM Sensors
		Non-EM Sensors
		Sensor Integration & Networks
		Advanced Signal Processing
	Information Analysis & Decision Support	Big Data & Long Data Processing and Analysis
		Big Data & Human Decision Making
		Multi-Domain Situational Awareness
		Planning and Managing Uncertainties
	Advanced Systems Concepts	Integrated Human - Machine Hybrid Force
		Clusters & Swarms
		Modular, Scalable Systems
		High Assurance Engineering & Validation
	Autonomy	Artificial Intelligence
		Mission Autonomous Systems
		Human-Autonomous Machine Teaming
	Communications & Networks	Secure and Resilient Communications
		Trusted Multi-Domain Information Sharing
		Ad hoc and Heterogeneous Networks
PHYSICAL	Precision Engagement	Precision Control
		Weapons - Techniques and Systems
		Weapons - Effects
		Active & Passive EM, Acoustic & Optical Countermeasures
	Platforms & Materials	Fast and Agile Platforms
		Unmanned Platforms
		Hypersonic Platforms
		Advanced and Adaptive Materials
		In-Theatre Fabrication & Production of Equipment
	Power & Energy	Power & Energy Storage
		Alternative & Renewable Energy Sources
		Propulsion
		Enhanced Energy Efficiency & Management

Targets of emphasis do not naturally align with the more broadly identified EDTs nor do they provide sufficient resolution of potential or current development areas found within the identified EDTs. For purposes of this report Technical Focus Areas (Table I.2) (TFA) were defined. TFAs are essentially sub-aspects of EDTs suitable for focused research. These were then mapped to existing NATO S&T *Targets of Emphasis* (TOE) (many-to-many). These do not cover all potential mappings, but rather those that are deemed to require research focus. Highlighted TOEs are those considered to be most closely aligned with their respective EDT (i.e. primary drivers of development in this area).

Table I.2: *EDT Technology Focus Areas (TFA).*

EDT	Technology Focus Area (TFA)	NATO S&T Targets of Emphasis	TOE
Data	Advanced Analytics	**Big data & Long Data Processing and Analysis**	IA&DS-2
	Communications	Ad hoc and Heterogeneous Networks	C&N-3
		Advanced Signal Processing	DC&P-4
		Trusted Multi-Domain Information Sharing	C&N-2
		Secure and Resilient Communications	C&N-1
	Advanced Decision Making	**Human Decision Making**	IA&DS-1
		Multi-Domain Situational Awareness	IA&DS-3
		Planning and Managing Uncertainties	IA&DS-4
	Sensors	Sensor Integration & Networks	DC&P-3
Artificial Intelligence	Advanced Algorithms	**Artificial Intelligence**	**A-1**
		Big Data & Long Data Processing and Analysis	**IA&DS-2**
		Advanced Signal Processing	**DC&P-4**
	Human-Machine Symbiosis	Human & machine interfaces	AHP&H-4
		Integrated Human – Machine Hybrid Forces	ASC-1
		Human-Autonomous Machine Teaming	**A-3**
	Applied AI	**Multi-Domain Situational Awareness**	**IA&DS-3**
		Planning and Managing Uncertainties	IA&DS-4
		Human Decision Making	IA&DS-1
Autonomy	Autonomous Systems	**Mission Autonomous Systems**	**A-2**
		Unmanned Platforms	**P&M-2**
	Countermeasures	Active & Passive EM, Acoustic and Optical Countermeasures	PE-4
	Human-Machine Teaming	**Human & machine Interfaces**	**AHP&H-4**
		Human-Autonomous Machine Teaming	**A-3**
		Integrated Human – Machine Hybrid Forces	**ASC-1**
	Autonomous Behavior	**Clusters and Swarms**	**ASC-2**
		Sensor Integration & Networks	**DC&P-3**
		Secure & Resilent Communications	C&N-1
		Rules of Engagement, Legal and Ethical Implications	**PE-5**
Space	Operation	Clusters and Swarms	ASC-2
		Precision Control	**PE-1**
	Platforms	High Assurance Engineering and Validation	ASC-6
		Modular, Scalable Systems	ASC-3
		Propulsion	**P&E-3**
		Fast & Agile Platforms	**P&M-1**
		Enhanced Energy Efficiency & Management	P&E-4
		Active & Passive EM, Acoustic and Optical Countermeasures	PE-4
		Weapons - Techniques and Systems	PE-2
	Sensors	EM Sensors	DC&P-1
		Non-EM Sensors	DC&P-2
		Sensor Integration & Networks	DC&P-3
Hypersonics	Countermeasures	Active & Passive EM, Acoustic and Optical Countermeasures	PE-4
		Weapons – Techniques and Systems	PE-2
		Weapons effects	PE-3
	Platforms and Propulsion	Fast and Agile Platforms	P&M-1
		Hypersonic Platforms	**P&M-3**
		Enhanced Energy Efficiency & Management	P&E-4
		Propulsion	P&E-3
Quantum	Communication	**Secure and Resilient Communications**	**C&N-1**
		Trusted Multi-Domain Information Sharing	C&N-2
	Information Science	**Big Data & Long Data Processing and Analysis**	**IA&DS-2**
	Precision Navigation	**Precision Control**	**PE-1**
	Sensors	**EM Sensors**	**DC&P-1**
		Non-EM Sensors	DC&P-2
Biotechnologies	Bioinformatics	Big data & Long Data Processing and Analysis	IA&DS-2
		Human Resiliency	**AHP&H-1**
		Cultural Communications	CS&OB-3
		Group and Organisational Behaviour	CS&OB-4
		Medical Solutions for Health Optimisation	AHP&H-1
		Political Influence	CS&OB-2
		Social Influence	CS&B-1
		EM Sensors	DC&P-1
		Non-EM Sensors	**DC&P-2**
	Synthetic Biology	**Human Resiliency**	**AHP&H-1**
		Medical Solutions for Health Optimisation	**AHP&H-2**
		Advanced and Adaptive Materials	P&M-4
	Human Augmentation	**Enhanced Cognitive Performance**	**AHP&H-3**
		Human & Machine Interfaces	**AHP&H-4**
		Integrated Human – Machine Hybrid Forces	ASC-1
		Alternative and Renewable Energy Sources	P&E-2
	Medical Countermeasures	**Human Resiliency**	**AHP&H-1**
		Medical Solutions for Health Optimisation	**AHP&H-2**
Materials	Additive Manufacturing	**In-theatre Fabrication & Production of Equipment**	**P&M-3**
	Energy	Power and Energy Storage	P&E-2
		Alternative and Renewable Energy Sources	**P&E-2**
	Novel Materials	**Advanced and Adaptive Materials**	**P&M-4**
		Hypersonic Platforms	**P&M-3**

I.3.2 Technology Watch Cards (TWC)

Recognising the pressing need to maintain the Alliance's technological edge, the STO actively pursues *Technology Watch* for the Alliance. The STO Panels and Group have embraced a culture of continually identifying and documenting potentially disruptive science or technology in *Technology Watch Cards*. These cards contain assessments of the maturity of the science or technology and offer commentary on how science or technology may affect the capabilities of the Alliance and potential adversaries in the future. The current S&T Trends report relies heavily on the almost 100 Technology Watch Cards developed by the STO Panels and Group, to deliver a short synthesis of observed technology trends. TWC assessments and text were especially helpful in drafting the more detailed appendices in this report.

I.3.3 Von Karman Horizon Scanning (vKHS)

To address emerging challenges, the von Karman Horizon Scan is an instrument to quickly perform a technology scan on a particular S&T topic within a short time frame (typically two to 6 months). Drawing upon internationally recognised S&T expertise and experienced senior military, the process assesses the state of leading-edge research in a specific S&T area; the outlook for the next decade; its relevance for the armed forces; and, potential avenues for investment. Von Karman Horizon Scans have been undertaken on laser weapons, quantum technologies, as well as optronic 3D imaging systems.

I.4 Workshops

Two unclassified workshops were held by the STO, with strong support from both NATO ACT and NCI Agency, in 2018. During these workshops, NATO and partner science workers, along with military personnel, identified and assessed the disruptive impact of various current and emerging technologies. The workshops were unclassified and focused on:

- Sharing of national and NATO perspectives on EDTs;
- Technology trends identified through open-source materials;
- Logical and historical inference of potential technological development and impact; and,
- Global technological progress;

The workshops identified ten EDTs:

New Weapons *Autonomous Systems and Countermeasures* *Energy*
Assured Connectivity *Human Capability Enhancement* *Computing Superiority*
Space *Applications of Artificial Intelligence* *Sensors*
Manufacturing

The workshops also identified three disruptive themes:

Ethics *Culture* *The Environment.*

I.5 Alliance and Partner Research Programs

The vast majority of STO sponsored S&T activity is undertaken through national collaborative research activities. As such, the STO maintains cross-alliance visibility on national research activities and priorities. These activities provided insights into emerging technology areas and activities, of importance to the Alliance. In particular, the following research programs were of considerable value in understanding national stretch objectives in defence and security S&T: [202, 241, 474, 475, 476, 477, 478, 479].

I.6 Attention Analysis

An assessment of EDT public attention was conducted partially based on data pulled from Google Trends [54] and a review of the Gartner Hype Cycle for Emerging Technologies, 2019 and 2018 [50]. Figure I.2 presents the Gartner consolidated assessment for all emerging technologies considered to be of interest to a general business audience as assessed in 2019.

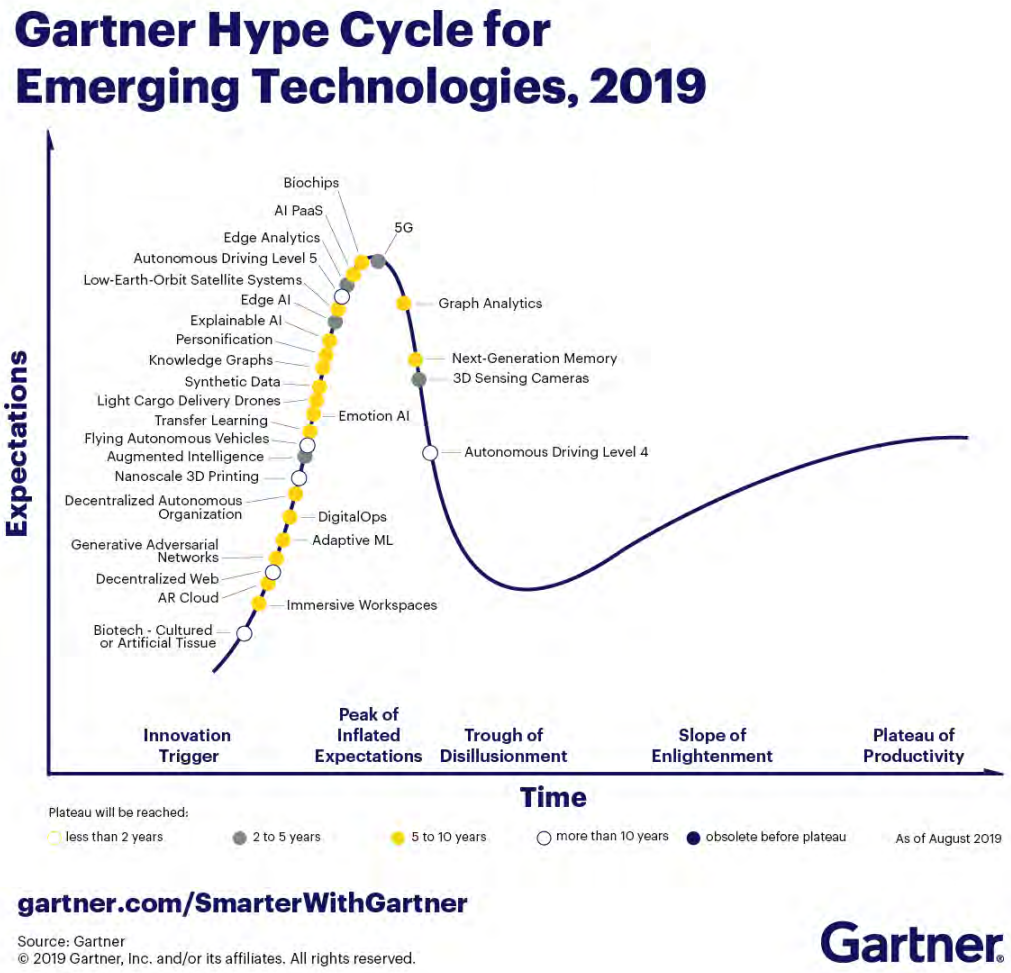


Figure I.2: *Gartner Hype Cycle 2019 (CREDIT: Gartner[480]).*

Figure I.3 presents the Gartner assessment for sub-areas associated with AI, considered to be of interest to a general business audience as assessed in 2019.

Google Trend data are presented in Figures I.4, I.5, I.6 and I.7. Figure I.4 compares raw web search data with a 12-month moving average. Use of a moving average smooths out noise due to random events and better supports an assessment of topic attention development over time. It is important to note that the general shape of the Google Trends data does not match that used in Gartner as it reflects attention (good or bad), while the Gartner cycle reflects a more idealised subjective assessment of expectations. Both perspectives were useful in understanding the current level of interest in a particular EDT.

The remaining graphs (Figures I.5, I.6) show 12-month moving averages of world-wide *interest over time* or attention in a topic area. The vertical axis shows the relative interest based on google search activity around a topic normalised by the maximum search volume over the period. In other words, 100 represents the maximum searches (as a percentage of the reporting period) recorded for this topic with all other points representing a percentage of this normalised search volume.

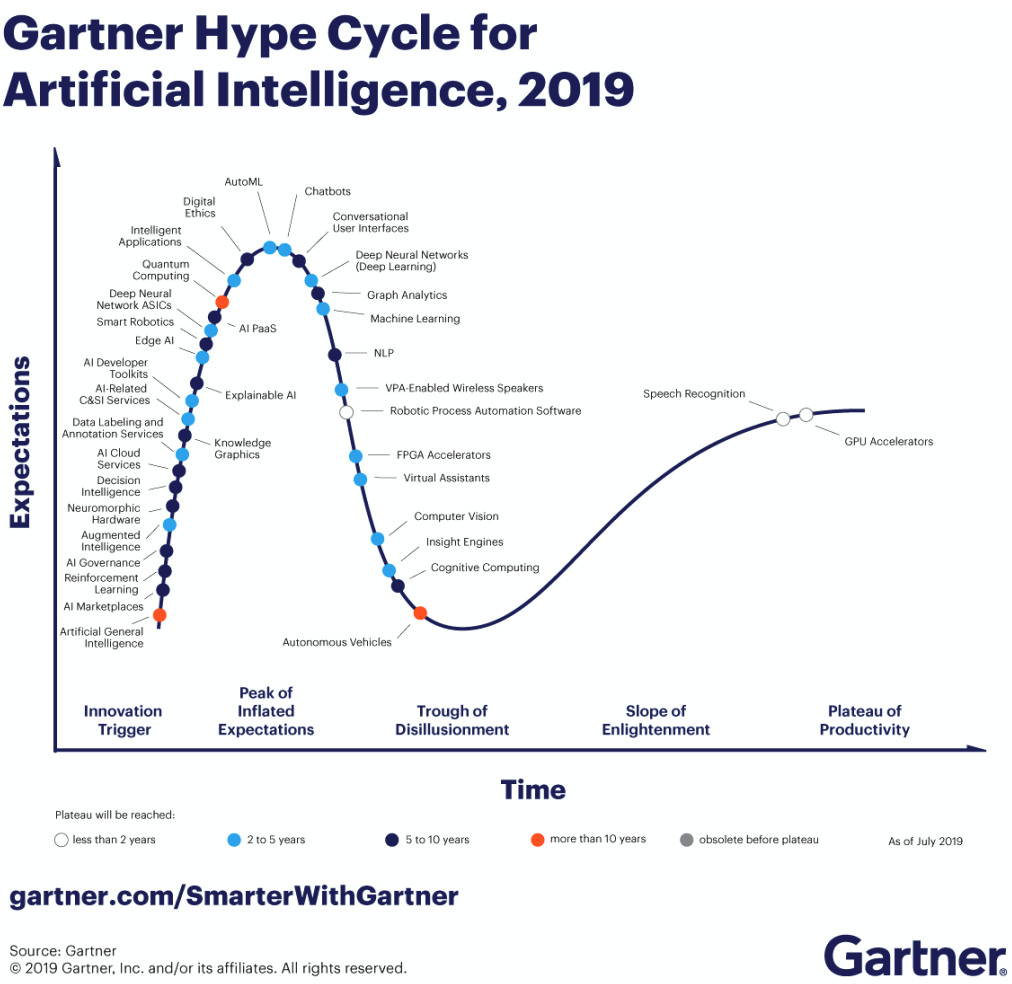


Figure I.3: *Gartner Hype Cycle - Artificial Intelligence 2019 (CREDIT: Gartner[481]).*

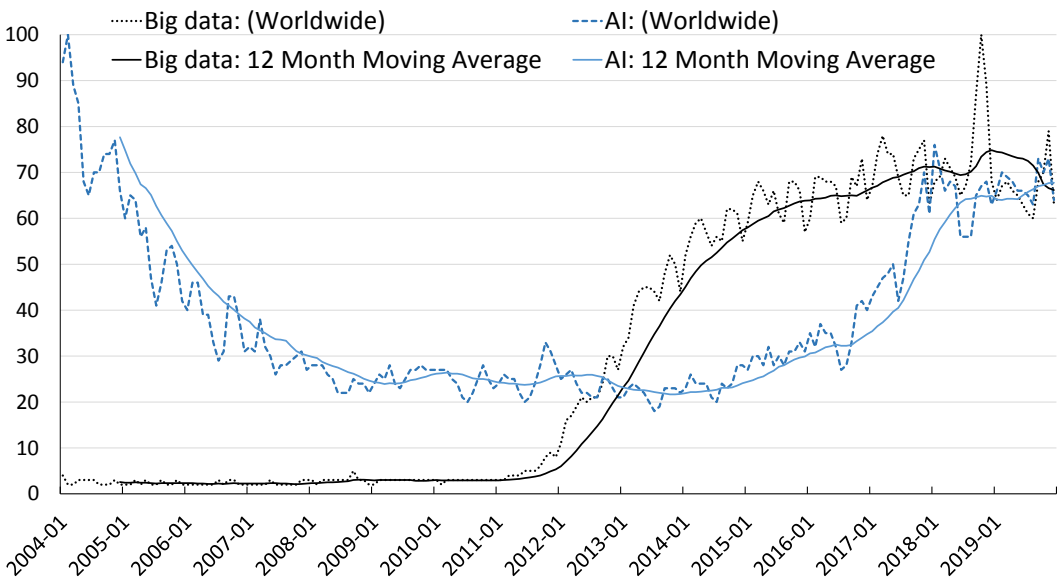


Figure I.4: *Google Trends (World Wide 2004-2020): Raw data and 12 Month Moving Average (AI, Big Data).*

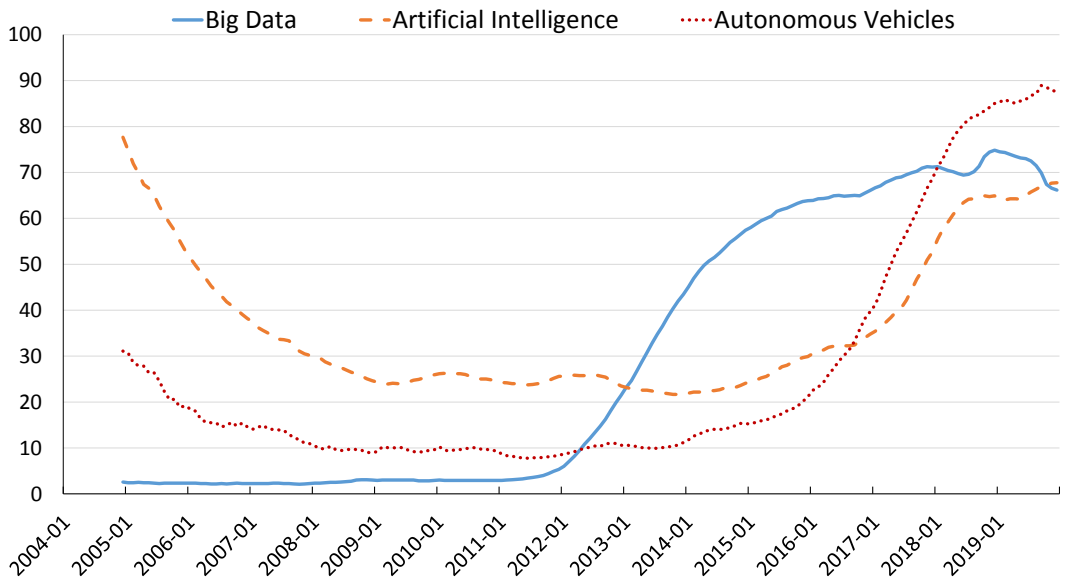


Figure I.5: *Google Trends (World Wide 2004-2020): 12 Month Moving Average (AI, Big Data, Autonomous Vehicles).*

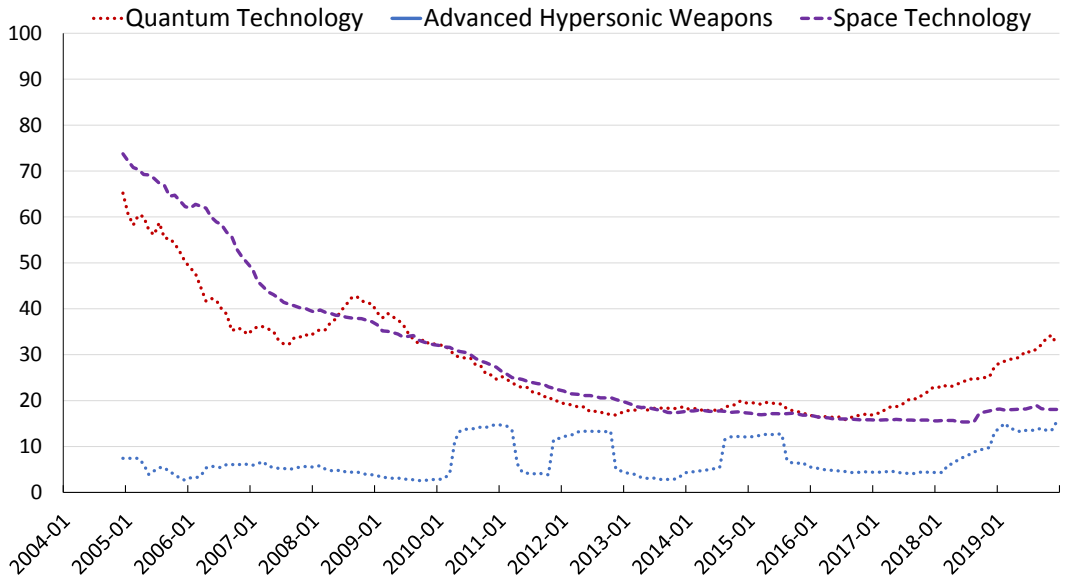


Figure I.6: *Google Trends (World Wide 2004-2020): 12 Month Moving Average (Quantum Technologies, Space Technologies, Advanced Hypersonic Weapons).*

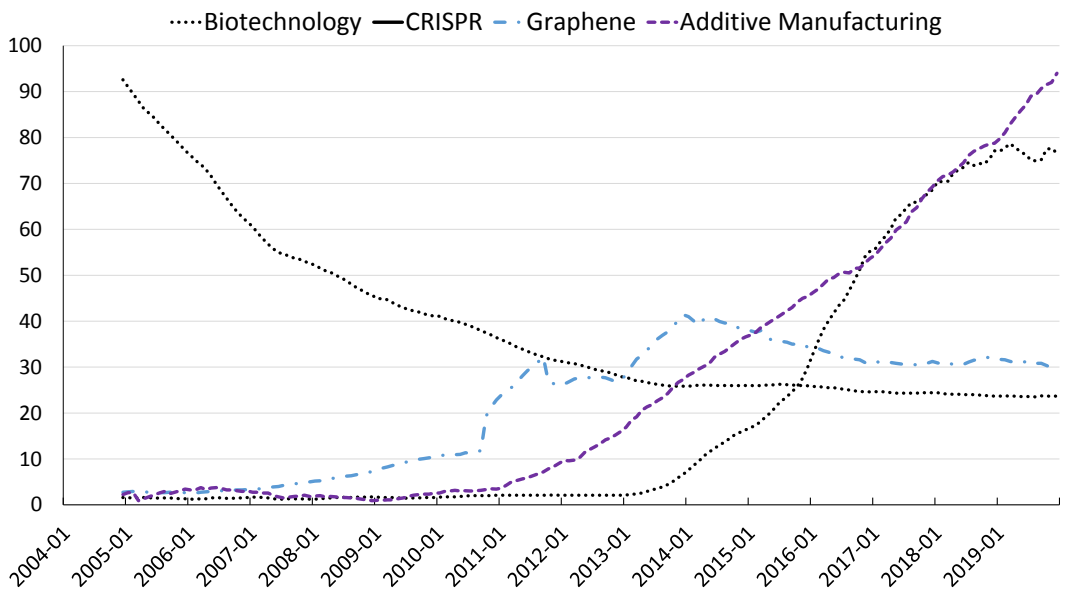
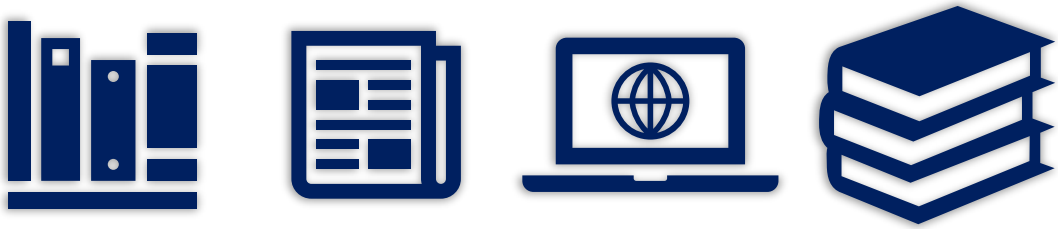


Figure I.7: *Google Trends (World Wide 2004-2020): 12 Month Moving Average (Bio & Human Enhancement Technologies, & Novel Materials and Manufacturing).*

I.7 Studies and Meta-Analyses

A considerable body of relevant literature exists on S&T trends, much of it referenced as required within the body of this report. These span the gamut of national defence and security studies, open literature and news articles, meta-studies and innovation research. In particular, the following documents were found to be of particular value in drafting this assessment:

- Technology Trends (Defence & Security): [37, 44, 45, 118, 122, 163, 181, 257, 482, 483, 484, 485, 486]
- Technology Trends (Civilian): [32, 33, 41, 43, 128, 132, 487, 488, 489, 490]
- Future Security Environment: [24, 116, 117, 119, 122, 181, 184, 491]
- Articles: [23, 492, 493, 494]
- Other: [2, 83, 495, 496, 497]



Bibliography

[1] quoteinvestigator. It's Difficult to Make Predictions, Especially About the Future – Quote Investigator (2013). URL https://quoteinvestigator.com/2013/10/20/no-predict/.

[2] Marino, T. Maintaining NATO's Technological Edge: Strategic Adaptation And Defence Research & Development. General Report, NATO Parliamentary Assembly, Brussels (2017). URL https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20174%20STC%2017%20E%20bis%20-%20MAINTAINING%20NATO%27S%20TECHNOLOGICAL%20EDGE.pdf.

[3] STO. Charter of the Science and Technology Organization (2012). URL https://www.sto.nato.int/publications/STO%20Documents/01%20STO%20Charter/STO_CHARTER_C-M(2012)0046.pdf?Mobile=1&Source=%2Fpublications%2F%5Flayouts%2Fmobile%2Fview%2Easpx%3FList%3D048e1603%2Ddaa8%2D4e61%2D970b%2D1880486ded63%26View%3D3b5c269e%2D459d%2D4a65%2Dbcf8%2D82c0b05fcc56%26RootFolder%3D%252Fpublications%252FSTO%2520Documents%252F01%2520STO%2520Charter%26CurrentPage%3D1.

[4] Breedlove, P. & Kosal, M. E. Emerging Technologies and National Security: Russia, NATO, & the European Theater. *Governance in an Emerging World (Hoover Institution)* (2019). URL https://www.hoover.org/research/emerging-technologies-and-national-security-russia-nato-european-theater. Library Catalog: www.hoover.org.

[5] Under Secretary Of Defense, A. T. A. L. Defence Science Board 2006 Summer Study on 21st Century Strategic Technology Vectors.pdf. Technical Report ADA464370, Office of the Under Secretary of Defense, for Acquistion, Technology, and Logistics, Washington, D.C. (2007). URL https://apps.dtic.mil/docs/citations/ADA464370.

[6] Possony, S., Pournelle, J. & Kane, F. *The Strategy of Technology* (University Press of Cambridge (1970), New York, Dunellen, 1970), 1 edn. URL https://www.jerrypournelle.com/jerrypournelle.c/slowchange/Strat.html.

[7] Chin, W. Technology, war and the state: past, present and future. *International Affairs* **95**, 765–783 (2019). URL https://academic.oup.com/ia/article/95/4/765/5513164.

[8] North Atlantic Council, N. Brussels Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 11-12 July 2018 (2018). URL http://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[9] NATO. NATO: Ready for the Future - Adapting the Alliance (2018-2019). Tech. Rep., NATO, Brussels (2019). URL https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf.

[10] Killion, T. NATO 2017 STO Technology Trends Report (NU). Tech. Rep. NATO STO AC_323-D(2017)0006 (INV), NATO S&T Organisation, Brussels (2017). URL https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20180522_TTR_Public_release_final.pdf.

[11] Kott, A. & Perconti, P. Long-Term Forecasts of Military Technologies for a 20-30 Year Horizon: An Empirical Assessment of Accuracy. *arXiv:1807.08339 [cs]* (2018). URL http://arxiv.org/abs/1807.08339. ArXiv: 1807.08339.

[12] Roland, A. War and Technology - Foreign Policy Research Institute (2009). URL https://www.fpri.org/article/2009/02/war-and-technology/.

[13] Kranzberg, M. Technology and History: "Kranzberg's Laws". *Technology and Culture* **27**, 544–560 (1986). URL http://www.jstor.org/stable/3105385.

[14] Eaton, J. NATO STO Technology Trends Workshop - Summary. Tech. Rep., NATO Office of the Chief Scientist, Brussels (2018).

[15] Gallo, C. Apple's Unique Website Tribute To Steve Jobs (2012). URL https://www.forbes.com/sites/carminegallo/2012/10/05/apples-unique-website-tribute-to-steve-jobs/.

[16] Hoffman, F. Healthy Skepticism about the Future of Disruptive Technology and Modern War - Foreign Policy Research Institute (2019). URL https://www.fpri.org/article/2019/01/healthy-skepticism-about-the-future-of-disruptive-technology-and-modern-war/.

[17] Sutherland, B. The advanced military technology that will win future wars (2017). URL https://www.gq-magazine.co.uk/article/advanced-military-technology.

[18] Barrons, G. S. R. The nature of warfare is changing. *Wired UK* **11** (2017). URL https://www.wired.co.uk/article/innovation-will-win-the-coming-cybersecurity-war-richard-barrons-opinion.

[19] Brown, Z. T. Unmasking War's Changing Character (2019). URL https://mwi.usma.edu/unmasking-wars-changing-character/.

[20] TRADOC. The Operational Environment and the Changing Character of Future Warfare (2017). URL https://www.pdf-archive.com/2017/07/28/theoperationalenvironment/theoperationalenvironment.pdf.

[21] Hoffman, F. G. Will War's Nature Change in the Seventh Military Revolution. *Parameters - The US Army War College Quarterly* **47**, 13 (2017). URL https://publications.armywarcollege.edu/pubs/3554.pdf.

[22] Oxford, P. C. The Changing Character of War Centre (2019). URL http://www.ccw.ox.ac.uk.

[23] Carter, A. Shaping Disruptive Technological Change for Public Good (2018). URL https://www.belfercenter.org/publication/shaping-disruptive-technological-change-public-good?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=.

[24] NATO Allied Command Transformation, S. P. a. P. & Mercier, G. F. A. F. D. Framework for Future Alliance Operations - 2018 Report. Strategic Foresight, NATO Allied Command Transformation, Norfolk, VA (2018). URL http://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf.

[25] NRC. Emerging Technologies and Canadian Society - Artificial Intelligence (2017).

[26] NATO Strategic Communications. *Social media as a tool of hybrid warfare* (NATO Strategic Communications Centre of Excellence, Riga, 2016). URL http://www.stratcomcoe.org/social-media-tool-hybrid-warfare. OCLC: 987389645.

[27] Hoffman, F. G. The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War | The Heritage Foundation (2015). URL https://www.heritage.org/military-strength-topical-essays/2016-essays/the-contemporary-spectrum-conflict-protracted-gray.

[28] Allen, J. & Hussain, A. On Hyper-War (2017). URL https://fortunascorner.com/2017/07/10/on-hyper-war-by-gen-ret-john-allenusmc-amir-hussain/. Library Catalog: fortunascorner.com Section: Afghanistan.

[29] Giesea, J. It's Time to Embrace Memetic Warfare. Open Publications, NATO StratCom, Riga, Latvia (2017). URL https://www.act.nato.int/images/stories/media/doclibrary/open201705-memetic1.pdf.

[30] Hybrid and Next-Generation Warfare: The Future of Conflict (2016). URL https://www.youtube.com/watch?v=tR_BER01NTw.

[31] Gartner. Gartner Top 10 Strategic Technology Trends 2019 (2018). URL https://www.youtube.com/watch?v=nRTRyfIDp4k.

[32] Deloitte. Tech Trends 2018: The Symphonic Enterprise. Tech. Rep., Deloitte (2018). URL https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/tech-trends-2018.html.

[33] Webb, A. Tech Trends Report 2019 - 12th Annual Edition (2019). URL https://futuretodayinstitute.com/2019-tech-trends/.

[34] Thomas, J. Implications of Technological Trends for NATO's Defense Posture (2020).

[35] Goldfein, D. & Raymond, J. America's future battle network is key to multidomain defense (2020). URL https://www.defensenews.com/opinion/commentary/2020/02/27/americas-future-battle-network-is-key-to-multidomain-defense/.

[36] Stillon, J. & Clark, B. What it Takes to Win: Succeeding in 21st Century Battle Network Competitions. Tech. Rep., Center for Strategic and Budgetary Assessments (2015). URL https://csbaonline.org/research/publications/what-it-takes-to-win-succeeding-in-21st-century-battle-network-competitions. Library Catalog: csbaonline.org.

[37] Martin, L. 5 Trends Shaping the Future of Defense (2019). URL https://www.lockheedmartin.com/en-us/news/features/2018/trends-shaping-future-defense.html.

[38] Walker, R. *Defence S&T Strategy 2006* (Defence R&D Canada, Ottawa, 2006).

[39] Hawco, R. D. Canada and the Future Security Environment (2016). URL https://www.queensu.ca/kcis/sites/webpublish.queensu.ca.kciswww/files/files/2016/P2-Hawco.pdf.

[40] Murray, W. *Military Adaptation in War With Fear of Change* (Cambridge University Press, Cambridge, 2011). URL https://books.google.be/books?id=VnwbwaxH41sC&printsec=frontcover&hl=nl&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

[41] O'Hanlon, M. Forecasting change in military technology, 2020-2040. Tech. Rep., Foreign Policy at Brookings Institution, Washington, D.C. (2018). URL https://www.brookings.edu/wp-content/uploads/2018/09/FP_20181218_defense_advances_pt2.pdf.

[42] Eaton, J. Overview of 2017 NATO Technology Trends (2017).

[43] Kikiras, P. European Defence Matters - 10 EDTs 2017 edm-issue-14_web.pdf. *European Defence Matters* **2017** (2017).

[44] Augustyn, J. Emerging Science and Technology Trends: 2017-2047: A Synthesis of Leading Forecasts. Future Security Environment, Office of the Deputy Assistant Secretary of the Army (Research & Technology) (2017). URL https://apps.dtic.mil/dtic/tr/fulltext/u2/1043071.pdf.

[45] Bidwell, C. & MacDonald, B. Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security. Tech. Rep., Federation of American Scientists (2018). URL https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf.

[46] Kealey, P. & Serna, M. von Kármán Horizon Scanning on Quantum Capabilities for Sensing and Communications - Summary Report (2018).

[47] Gerard, D. The Gartner Hype Cycle is ... hype. Don't use it as an excuse. (2019). URL https://davidgerard.co.uk/blockchain/2019/10/03/the-gartner-hype-cycle-is-hype-dont-use-it-as-an-excuse/.

[48] Fosdick, H. The Sociology of Technology Adoption. *Enterprise Systems Journal* (1992). URL http://rexxinfo.org/Sociology%20of%20Technology%20Adoption/SOCIOL_1.HTM.

[49] Moran, G., Moran, G. & Moran, G. Fostering Greater Creativity By Celebrating Failure (2014). URL https://www.fastcompany.com/3028594/a-real-life-mad-man-on-fighting-fear-for-greater-creativity. Library Catalog: www.fastcompany.com.

[50] Gartner. Hype Cycle Research Methodology (2019). URL https://www.gartner.com/en/research/methodologies/gartner-hype-cycle.

[51] Fenn, J. & Blosch, M. Understanding Gartner's Hype Cycles (2018). URL https://www.gartner.com/en/documents/3887767/understanding-gartner-s-hype-cycles. Library Catalog: www.gartner.com.

[52] Voiovich, J. T. Unhyping the Hype Cycle: Five Secrets to Building an Attention Dashboard for Any Innovation (2019). URL https://medium.com/swlh/unhyping-the-hype-cycle-five-secrets-to-building-an-attention-dashboard-for-any-innovation-858a3251cd1b.

[53] Lucker, J., Hogan, S. K. & Sniderman, B. Is it the next big thing or merely a shiny new object? *Deloitte Insights* 17 (2018). URL https://www2.deloitte.com/us/en/insights/deloitte-review/issue-23/hype-innovation-inflated-expectations.html.

[54] Google. Google Trends (2020). URL https://trends.google.com/trends/?geo=US.

[55] Mai, T. Technology Readiness Level (2015). URL http://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html.

[56] MITRE. *The MITRE Systems Engineering Guide* (The MITRE Corporation, 202 Burlington Road, Bedford, MA, 2014). URL https://www.mitre.org/publications/systems-engineering-guide/about-the-seg.

[57] Enspire. TRL Scale in Horizon 2020 and ERC - Explained (2018). URL https://enspire.science/trl-scale-horizon-2020-erc-explained/.

[58] Fedkin, M. 2.3 Emerging, converging, disruptive technologies | EME 807: Technologies for Sustainability Systems (2018). URL https://www.e-education.psu.edu/eme807/node/8.

[59] C3B, N. Consultation, Command and Control Board (C3b) C3 Taxonomy Baseline 3.1 (2019). URL https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_09/20190912_190912-C3-Taxonomy-baseline.pdf. Publically Disclosed PDN(2019)0013.

[60] Walker, R. Looking Forward - Staying Ahead 2005. Tech. Rep., Defence R&D Canada (2006).

[61] Patrick, D., Allen, D. & Gilbert, D. P. The Information Sphere Domain Increasing Understanding and Cooperation. In Czosseck, C. & Geers, K. (eds.) *Virtual Battlefield: Perspectives on Cyber Warfare*, 132–42 (IOS Press, Amsterdam, 2009). URL https://books.google.be/books?hl=en&lr=&id=BKDbN5eUhV0C&oi=fnd&pg=PA132&dq=related:a3rS7i4eshIkmM:scholar.google.com/&ots=v3K_spRqaR&sig=NfIAHOFRclxDU_sdfqWqox2K_uM&redir_esc=y#v=onepage&q&f=false.

[62] USAF. USAF AI Annex to DoD AI Strategy. Tech. Rep., United States Air Force (2019). URL https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf.

[63] Varian, H. Open source and open data (2019). URL https://blog.google/technology/research/open-source-and-open-data/.

[64] Team, I. The Power Of Open Source AI (2019). URL https://www.forbes.com/sites/insights-intelai/2019/05/22/the-power-of-open-source-ai/.

[65] Kohli, T. AI's contribution to the global economy will bypass that of China and India by 2030, to reach $15.7 trillion (2019). URL https://www.weforum.org/agenda/2019/09/artificial-intelligence-meets-biotechnology/.

[66] Zacharias, G. *Autonomous horizons: the way forward* (Air University Press ; Curtis E. LeMay Center for Doctrine Development and Education, Maxwell Air Force Base, Alabama, 2019).

[67] Endsley, M. R. Autonomous Horizons: Autonomy in the Air Force—A Path to the Future. Vol. 1, Human Autonomy Teaming. Air Force Science and Technology AF/ST TR 15-01, US Air Force, Washington, D.C. (2015).

[68] Williams, A. P. & Scharre, P. D. (eds.) *Autonomous Sytems - Issues for Defence Policy Makers* (NATO Allied Command Transformation, Norfolk, VA, 2015). URL http://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf.

[69] Boulet, M. T. The Autonomous Systems Tidal Wave. *Lincoln Laboratory Journal* **22**, 6 (2017). URL https://www.ll.mit.edu/sites/default/files/page/doc/2018-06/22_2_1_Boulet.pdf.

[70] Marr, B. The 4 Ds Of Robotization: Dull, Dirty, Dangerous And Dear (2017). URL https://www.forbes.com/sites/bernardmarr/2017/10/16/the-4-ds-of-robotization-dull-dirty-dangerous-and-dear/#77a69c6b3e0d.

[71] DCDC. The UK Military Space Primer. Primer, Development, Concepts and Doctrine Centre, Shrivenham (UK) (2010). URL https://www.gov.uk/government/publications/the-uk-military-space-primer.

[72] Winick, E. Rocket Lab: The small firm that launched the 3D-printed space revolution - MIT Technology Review (2019). URL https://www.technologyreview.com/s/613792/rocket-lab-the-small-firm-that-launched-the-3d-printed-space-revolution/.

[73] Rose, F. A. Safeguarding the Heavens: The United States and the Future of Norms of Behavior in Outer Space. Policy Brief, The Brookings Institution, Washington, D.C. (2018). URL https://www.brookings.edu/wp-content/uploads/2018/06/FP_20180614_safeguarding_the_heavens.pdf.

[74] Albrecht, M. & Graziani, P. Op-ed | Congested space is a serious problem solved by hard work, not hysteria (2016). URL https://spacenews.com/op-ed-congested-space-is-a-serious-problem-solved-by-hard-work-not-hysteria/.

[75] Williams, M. S. The Growing Problem of Space Debris (2019). URL https://interestingengineering.com/the-growing-problem-of-space-debris.

[76] Medrano, K. What is a hypersonic railgun? How the superweapon China may be building works (2018). URL https://www.newsweek.com/china-secretly-building-superweapon-leaked-photos-first-hypersonic-railgun-798565.

[77] Tirpak, J. A. The Great Hypersonic Race (2018). URL https://www.airforcemag.com/article/the-great-hypersonic-race/.

[78] Speier, R. H., Nacouzi, G., Lee, C. & Moore, R. M. *Hypersonic missile nonproliferation: hindering the spread of a new class of weapons* (RAND, Santa Monica, CA, 2017). URL https://www.rand.org/pubs/research_reports/RR2137.html.

[79] Board, U. S. A. USAF Scientific Advisory Board Study Technology Readiness for Hypersonic Vehicles. USAF Scientific Advisory Board Study, United States Air Force (2016). URL https://www.scientificadvisoryboard.af.mil/Portals/73/documents/AFD-140728-026.pdf.

[80] Osborn, K. U.S. Air Force Chief Scientist Says Hypersonic Weapons Ready by 2020s (2016). URL http://www.scientificadvisoryboard.af.mil/News/Article-Display/Article/461171/us-air-force-chief-scientist-says-hypersonic-weapons-ready-by-2020s/.

[81] Brimelow, B. The US has no defenses against China and Russia's hypersonic weapons - Business Insider (2018). URL https://www.businessinsider.com/us-china-russia-hypersonic-weapons-2018-3?r=US&IR=T.

[82] Mizokami, K. Russian Military - Hypersonic Weapons - Ballistic Missiles (2019). URL https://www.popularmechanics.com/military/weapons/a30346798/russia-new-hypersonic-weapon-mach-27/.

[83] de Touzalin, A. *et al.* Quantum Manifesto - A New Era of Technology. Future and Emerging Technologies Flagship Consultations, European Commission (2016). URL http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf.

[84] Lewis, A. M., Krämer, M. & Travagnin, M. Quantum Technologies: Implications for European Policy. Science Policy, European Commission (2016). URL https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/quantum-technologies-implications-european-policy-issues-debate.

[85] Lewis, A., Ferigato, C., Travagnin, M. & Florescu, E. The Impact of Quantum Technologies on the EU's Future Policies: Part 3 Perspectives for Quantum Computing. EUR - Scientific and Technical Research Reports 978-92-79-96730-6, European Union (2018). URL https://publications.jrc.ec.europa.eu/repository/bitstream/JRC110412/quantum_computing_report_v5.4.pdf.

[86] Travagnin, M. & Adam, L. The Impact of Quantum Technologies on the EU's Future Policies: Part 2 Quantum Communications: from science to policies. Text, European Commission, Ispra, Italy (2018). URL https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/impact-quantum-technologies-eu-s-future-policies-part-2-quantum-communications-science.

[87] Reding, D., Rivest, J. & McMillan, C. A Quantum Strategy for DRDC (2016).

[88] Pritchard, J. & Till, S. UK Quantum Technology Landscape 2014. DSTL Publication DSTL/PUB75620, Defence Science and Technology Laboratory, Porton Down (2014). URL https://epsrc.ukri.org/newsevents/pubs/dstl-uk-quantum-technology-landscape-2014/.

[89] Desjardins, J. Quantum Computers And Their Applications [INFOGRAPHIC] (2016). URL https://www.valuewalk.com/2016/03/quantum-computers-applications-graphic/.

[90] Roblin, S. No More 'Stealth' Submarines: Could Quantum 'Radar' Make Submarines Easy to Track (And Kill)? | The National Interest (2019). URL https://nationalinterest.org/blog/buzz/no-more-stealth-submarines-could-quantum-radar-make-submarines-easy-track-and-kill-54547.

[91] Mizokami, K. The Air Force Wants to Unleash a Robotic "Golden Horde" on Adversaries (2019). URL https://www.popularmechanics.com/military/a29995819/us-air-force-golden-horde/.

[92] O'Donnel, W. Quantum Radar a Game Changer for Offensive Stealth Operations (2019). URL https://incyberdefense.com/editors-picks/quantum-radar-a-game-changer-for-offensive-stealth-operations/.

[93] Battersby, S. Core Concept: Quantum sensors probe uncharted territories, from Earth's crust to the human brain. *Proceedings of the National Academy of Sciences* **116**, 16663–16665 (2019). URL https://www.pnas.org/content/116/34/16663.

[94] Majumdar, D. Quantum Radars: China's New Weapon to Take Out U.S. Stealth Fighters (Like the F-22)? (2019). URL https://nationalinterest.org/blog/buzz/quantum-radars-chinas-new-weapon-take-out-us-stealth-fighters-f-22-44652.

[95] Chan, D. Asia Times | Stealth killer: Quantum radar actually works | Article (2019). URL https://www.asiatimes.com/2019/09/article/stealth-killer-quantum-radar-actually-works/.

[96] Vincent, J. IBM's new quantum computer is a symbol, not a breakthrough (2019). URL https://www.theverge.com/2019/1/8/18171732/ibm-quantum-computer-20-qubit-q-system-one-ces-2019.

[97] CNBC.com, J. T., Special to. IBM sees quantum computing going mainstream within five years (2018). URL https://www.cnbc.com/2018/03/30/ibm-sees-quantum-computing-going-mainstream-within-five-years.html.

[98] Moskvitch, K. Gil Kalai's Argument Against Quantum Computers (2018). URL https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/.

[99] Erwin, S. Pentagon sees quantum computing as key weapon for war in space (2018). URL https://spacenews.com/pentagon-sees-quantum-computing-as-key-weapon-for-war-in-space/.

[100] Greene, T. Understanding quantum computers: The noise problem (2018). URL https://thenextweb.com/artificial-intelligence/2018/10/25/understanding-quantum-computers-the-noise-problem/.

[101] Ladisch, M. *Opportunities in Biotechnology for Future Army Applications* (National Academies Press, Washington, D.C., 2001). URL http://www.nap.edu/catalog/10142.

[102] AMRG. The 7 categories of Additive Manufacturing, Additive Manufacturing Research Group, Loughborough University (2018). URL https://www.lboro.ac.uk/research/amrg/about/the7categoriesofadditivemanufacturing/.

[103] Gibney, E. Thousands of Exotic "Topological" Materials Discovered through Sweeping Search (2018). URL https://www.scientificamerican.com/article/thousands-of-exotic-topological-materials-discovered-through-sweeping-search/.

[104] Oberhaus, D. The Next Generation of Batteries Could Be Built by Viruses | WIRED (2020). URL https://www.wired.com/story/the-next-generation-of-batteries-could-be-built-by-viruses/.

[105] Arun, C. Artificial Intelligence of Things(AIoT) Explained! - Arun C - Medium (2020). URL https://medium.com/@arun.cthomas3/artificial-intelligence-of-things-aiot-explained-eedd4376f027.

[106] Giesea, J. Hacking Hearts and Minds: How Memetic Warfare is Transforming Cyberwar. Open Publications, NATO StratCom, Riga, Latvia (2017). URL https://www.act.nato.int/images/stories/media/doclibrary/open201706-memetic2.pdf.

[107] Villoresi, P. Quantum Communications in Space (2019). URL https://www.unoosa.org/documents/pdf/copuos/stsc/2019/tech-43E.pdf.

[108] Timmer, J. A neural network picks promising antibiotics out of a library of chemicals | Ars Technica (2020). URL https://arstechnica.com/science/2020/02/a-neural-network-picks-promising-antibiotics-out-of-a-library-of-chemicals/.

[109] Sagoff, J. Scientists pair machine learning with tomography to learn about material interfaces (2020). URL https://phys.org/news/2020-03-scientists-pair-machine-tomography-material.html.

[110] University, C. Machine learning illuminates material's hidden order (2020). URL https://phys.org/news/2020-03-machine-illuminates-material-hidden.html.

[111] Borealis, S. The Canadian response to Ebola: a new science diplomacy? (2014). URL https://blog.scienceborealis.ca/the-canadian-response-to-ebola-a-new-science-diplomacy/.

[112] Matys, M. Researchers are leading a unique Ebola study in Toronto (2018). URL http://health.sunnybrook.ca/sunnyview/researchers-ebola-study-toronto/. Library Catalog: health.sunnybrook.ca Section: Featured.

[113] Grant, K. How Canada developed pioneer drugs to fight Ebola. *The Global and Mail* (2014). URL https://www.theglobeandmail.com/life/health-and-fitness/health/how-canada-developed-pioneer-drugs-to-fight-ebola/article20184581/.

[114] quotesearch. Plans Are Worthless, But Planning Is Everything – Quote Investigator (2917). URL https://quoteinvestigator.com/2017/11/18/planning/. Library Catalog: quoteinvestigator.com.

[115] Voltaire. *Oeuvres Complete de Voltaires*, vol. 38 (Imprimerie de la Société Littéraire-Typographique, 1785). URL https://books.google.nl/books/about/Oeuvres_completes_de_Voltaire.html?id=iGARzQEACAAJ&redir_esc=y.

[116] MOD, U. Global Strategic Trends - The Future Starts Today (Sixth Edition). Strategic Trends, UK Ministry of Defence (2018). URL https://www.gov.uk/government/publications/global-strategic-trends.

[117] Canadian Department of National Defence *et al.* The Future Security Environment 2013-2040. Future Security Environment, Government of Canada, Ottawa (2015). URL http://epe.lac-bac.gc.ca/100/201/301/weekly_checklist/2015/internet/w15-11-F-E.html/collections/collection_2015/mdn-dnd/D4-8-2-2014-eng.pdf. 911139027.

[118] Augustyn, J. Emerging Science and Technology Trends: 2016-2045 A Synthesis of Leading Forecasts. Future Security Environment, Office of the Deputy Assistant Secretary of the Army (Research & Technology) (2016). URL https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/2016_SciTechReport_16June2016.pdf.

[119] Gizewski, P. Army 2040 The Global Security Environment: Emerging Trends And Potential Challenges. In *Annual Meeting of the Canadian Political Science Association*, 15 (Carleton University, Ottawa, Canada, 2009). URL https://www.cpsa-acsp.ca/papers-2009/Gizewski.pdf.

[120] National Intelligence Council (U.S.). *Global trends: paradox of progress* (National Intelligence Council, 2017). URL http://heinonline.org/HOL/Page?handle=hein.usfed/globtpdxrs0001&id=1&collection=usfed. OCLC: 968133230.

[121] Godefroy, A. B. & Centre de guerre aérospatiale des Forces canadiennes. *Projection de la puissance: la Force aérienne du Canada en 2035* (Le Centre de guerre aérospatiale des Forces canadiennes, Ottawa, 2009). URL https://central.bac-lac.gc.ca/.item?id=D2-247-2009-fra&op=pdf&app=Library. OCLC: 594920193.

[122] Miller, D. T., Nye, J. S., CSIS International Security Program & Center for Strategic and International Studies (Washington, D. *Defense 2045: assessing the future security environment and implications for defense policymakers* (Center for Strategic & International Studies, 2015). URL http://csis.org/files/publication/151106_Miller_Defense2045_Web.pdf. OCLC: 1013334310.

[123] Ghosh, I. Ranked: The Most Innovative Economies in the World (2020). URL https://www.visualcapitalist.com/world-most-innovative-economies/. Library Catalog: www.visualcapitalist.com.

[124] Jamrisko, M. & Lu, W. Germany Breaks Korea's Six-Year Streak as Most Innovative Nation (2020). URL https://www.bloomberg.com/news/articles/2020-01-18/germany-breaks-korea-s-six-year-streak-as-most-innovative-nation.

[125] Moretti, E., Steinwender, C. & Van Reenen, J. The Intellectual Spoils of War? Defense R&D, Productivity and International Spillovers. Tech. Rep. w26483, National Bureau of Economic Research, Cambridge, MA (2019). URL http://www.nber.org/papers/w26483.pdf.

[126] Sargent, J. F. U.S. Research and Development Funding and Performance: Fact Sheet. CRS Report R44307, Congressional Research Service, Washington, D.C. (2020). URL https://fas.org/sgp/crs/misc/R44307.pdf.

[127] Sargent, J. F. Government Expenditures on Defense Research and Development by the United States and Other OECD Countries: Fact Sheet. CRS Report R45441, Congressional Research Service, Washington, D.C. (2018). URL https://www.everycrsreport.com/reports/R45441.html.

[128] OECD, O. S. *OECD Science, Technology and Innovation Outlook 2018: Adapting to Technological and Societal Disruption* (OECD Publishing, Paris, 2019). URL https://doi.org/10.1787/sti_in_outlook-2018-en.

[129] FLIA. China's New Generation of Artificial Intelligence Development Plan (2017). URL https://flia.org/notice-state-council-issuing-new-generation-artificial-intelligence-development-plan/. Library Catalog: flia.org Section: Blog.

[130] Emanuel, E., Gadsden, A. & Moore, S. How the U.S. Surrendered to China on Scientific Research. *Wall Street Journal* (2019). URL https://www.wsj.com/articles/how-the-u-s-surrendered-to-china-on-scientific-research-11555666200.

[131] OECD. Research and Development Statistics (RDS) - OECD (2020). URL https://www.oecd.org/sti/inno/researchanddevelopmentstatisticsrds.htm.

[132] OECD. Key nanotechnology indicators (2018). URL https://www.oecd.org/sti/emerging-tech/nanotechnology-indicators.htm.

[133] Nielsen, P. C., Michael. Science Is Getting Less Bang for Its Buck (2018). URL https://www.theatlantic.com/science/archive/2018/11/diminishing-returns-science/575665/.

[134] Cowen, T. & Southwood, B. Innovation & scientific progress (2019). URL https://www.brown.edu/academics/political-theory-project/sites/brown.edu.academics.political-theory-project/files/uploads/Innovation%20%26%20scientific%20progress.pdf.

[135] Qureshi, Z. Advanced tech, but growth slow and unequal: paradoxes and policies (2018). URL https://www.technologyreview.com/s/612021/advanced-tech-but-growth-slow-and-unequal-paradoxes-and-policies/.

[136] Friedman, U. Bill Gates: 'The Idea That Innovation Is Slowing Down Is ... Stupid' (2014). URL https://www.theatlantic.com/international/archive/2014/03/bill-gates-the-idea-that-innovation-is-slowing-down-is-stupid/284392/.

[137] Wells, B. A Think Piece on Innovation (2019).

[138] Christensen, C. M., Raynor, M. E. & McDonald, R. What Is Disruptive Innovation? *Harvard Business Review* (2015). URL https://hbr.org/2015/12/what-is-disruptive-innovation.

[139] NATO. NATO: READY FOR THE FUTURE Adapting the Alliance (2018-2019) (2019). URL https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf.

[140] Langbroke, M. Why India's ASAT Test Was Reckless – The Diplomat (2019). URL https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/.

[141] Weeden, B. & Samson, V. Op-ed | India's ASAT test is wake-up call for norms of behavior in space (2019). URL https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space/.

[142] Keck, Z. China Will Soon Be Able to Destroy Every Satellite in Space (2018). URL https://nationalinterest.org/blog/buzz/china-will-soon-be-able-destroy-every-satellite-space-27182.

[143] Stoltenberg, J. NATO - Opinion: Press conference by NATO Secretary General Jens Stoltenberg folowing the meeting of the North Atlantic Council at the level of Foreign Ministers, 20-Nov.-2019 (2019). URL https://www.nato.int/cps/en/natohq/opinions_171022.htm.

[144] Von Spreckelsen, M. Electronic Warfare – The Forgotten Discipline (2018). URL https://www.japcc.org/electronic-warfare-the-forgotten-discipline/.

[145] Friedman, B. The Russian Understanding of War (2020). URL https://www.realcleardefense.com/articles/2020/03/24/the_russian_understanding_of_war_115142.html. Library Catalog: www.realcleardefense.com.

[146] Lim, L. & Bergin, J. Inside China's audacious global propaganda campaign. *The Guardian* (2018). URL https://www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping.

[147] Zgryziewicz, R., Grzyb, T., Fahmy, S. & Shaheen, J. Daesh information campaign and its influence. Tech. Rep., NATO Strategic Communications Center of Excellence, Riga, Latvia (2015). URL https://www.stratcomcoe.org/daesh-information-campaign-and-its-influence-1.

[148] Hall, J. S. F. O. O. P. A. 2019-DOD-Arctic-Strategy. Report to Congress, Office of the Under Secretary of Defense for Policy (USA), Washington, D.C. (2019). URL https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF.

[149] GoC. Canada's Arctic and Northern Policy Framework (2019). URL https://www.rcaanc-cirnac.gc.ca/eng/1560523306861/1560523330587.

[150] Norway, N. M. Norway's Arctic Strategy – between geopolitics and social development. Strategy, Norwegian Ministries, Oslo (2017). URL https://www.regjeringen.no/contentassets/76dc3d09a93a460c8fe649390a722689/arctic-strategy_kort-versjon.pdf.

[151] Centre, E. P. S. Walking on Thin Ice: A Balanced Arctic Strategy for the EU. EPSC Strategic Notes 31, European Union, Brussels (2019).

[152] Schmitt, L. Walking on Thin Ice: A Balanced Arctic Strategy for the EU (2019). URL https://ec.europa.eu/epsc/publications/strategic-notes/walking-thin-ice-balanced-arctic-strategy-eu_en.

[153] Kuo, M. A. The US and China's Arctic Ambitions (2019). URL https://thediplomat.com/2019/06/the-us-and-chinas-arctic-ambitions/.

[154] Allan, I. Arctic Narratives and Political Values: Russia, China and Canada in the High North. Russian Executive Summary, NATO Strategic Communications Center of Excellence, Riga, Latvia (2018). URL https://www.stratcomcoe.org/russias-arctic-strategy.

[155] Aliyev, N. Russia's Military Capabilities in the Arctic (2019). URL https://icds.ee/russias-military-capabilities-in-the-arctic/. Library Catalog: icds.ee.

[156] Boulègue, M. Russia's Military Posture in the Arctic Managing Hard Power in a 'Low Tension' Environment. Research Paper, Chatham House, The Royal Institute of International Affairs, London (2019). URL https://www.chathamhouse.org/sites/default/files/2019-06-28-Russia-Military-Arctic_0.pdf.

[157] Melino, M., Conley, H. A. & Bermundez, J. S. J. Ice Curtain: Why Is There a New Russian Military Facility 300 Miles from Alaska? CSIS Briefs, Center for Strategic and International Studies, Washington, DC (2020). URL https://www.csis.org/analysis/ice-curtain-why-there-new-russian-military-facility-300-miles-alaska. Library Catalog: www.csis.org.

[158] Goldstein, L. J. What Does China Want with the Arctic? (2019). URL https://nationalinterest.org/feature/what-does-china-want-arctic-78731. Library Catalog: nationalinterest.org Publisher: The Center for the National Interest.

[159] Bodnar, J. & Collins, S. NATO Joint Military Operations in an Urban Environment //A Capstone Concept. *The Three Swords Magazine* 6 (2019). URL http://www.jwc.nato.int/images/stories/_news_items_/2017/UrbanOps.pdf.

[160] DESA, U. 68% of the world population projected to live in urban areas by 2050, says UN (2018). URL https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html.

[161] Hoornweg, D. & Pope, K. Socioeconomic Pathways and Regional Distribution of the World's 101 Largest Cities. Global Cities Institute Working Paper 4, University of Toronto, Toronto (2014). URL https://shared.uoit.ca/shared/faculty-sites/sustainability-today/publications/population-predictions-of-the-101-largest-cities-in-the-21st-century.pdf.

[162] Press, A. U. Primer on Urban Operations (2016). URL https://www.armyupress.army.mil/Online-Publications/Primer-on-Urban-Operations/.

[163] Kaspersen, A., Eide, E. B. & Shelter-Jones, P. 10 trends for the future of warfare (2016). URL https://www.weforum.org/agenda/2016/11/the-4th-industrial-revolution-and-international-security/.

[164] Raso, F. & Mekone, V. Towards Rule of Law in the Digital Environment. Tech. Rep., NATO STRATCOM COE, Riga, Latvia (2019). URL https://www.stratcomcoe.org/towards-rule-law-digital-environment.

[165] Ekman, E. Here's One Reason the U.S. Military Can't Fix Its Own Equipment. *The New York Times* (2019). URL https://www.nytimes.com/2019/11/20/opinion/military-right-to-repair.html.

[166] Keck, C. Lack of Right-to-Repair Protections Is Even Screwing With the U.S. Military (2019). URL https://gizmodo.com/lack-of-right-to-repair-protections-is-even-screwing-wi-1839969876.

[167] Finkel, M. Even The American Military Is Struggling With Right-To-Repair (2020). URL https://foxtrotalpha.jalopnik.com/even-the-american-military-is-struggling-with-right-to-1841531517.

[168] Aitoro, J. Forget Project Maven. Here are a couple other DoD projects Google is working on (2019). URL https://www.c4isrnet.com/it-networks/2019/03/13/forget-project-maven-here-are-a-couple-other-dod-projects-google-is-working-on/.

[169] ICRC. Autonomy, artificial intelligence and robotics: Technical aspects of human control. Tech. Rep., International Committee of The Red Cross, Geneva (2019). URL https://www.icrc.org/en/document/autonomy-artificial-intelligence-and-robotics-technical-aspects-human-control.

[170] Haider, A. & Catarrasi, B. Future Unmanned System Technologies - Legal and Ethical Implications of Increasing Automation. Tech. Rep., Joint Air Power Competence Center (JAPCC), Kalkar, Germany (2016). URL https://www.japcc.org/wp-content/uploads/Future_Unmanned_System_Technologies_Web.pdf.

[171] Santoni de Sio, F. & van den Hoven, J. Meaningful Human Control over Autonomous Systems: A Philosophical Account. *Frontiers in Robotics and AI* **5**, 15 (2018). URL http://journal.frontiersin.org/article/10.3389/frobt.2018.00015/full.

[172] Etzioni, A. & Etzioni, O. Pros and Cons of Autonomous Weapons Systems. *MILITARY REVIEW* 10 (2017). URL https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/.

[173] Union européenne & Groupe européen d'éthique des sciences et des nouvelles technologies. Statement on artificial intelligence, robotics and autonomous' systems. Tech. Rep., European Commission, Luxembourg (2005). URL http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf. OCLC: 1082425583.

[174] Sharkey, N. Saying 'No!' to Lethal Autonomous Targeting. *Journal of Military Ethics* **9**, 369–383 (2010). URL http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.537903.

[175] Chavannes, E. & Arkhipov-Goyal, A. Towards Responsible Autonomy - The Ethics of RAS in a Military Context.pdf. Tech. Rep., The Hague Centre for Strategic Studies, The Hague (2019). URL https://hcss.nl/report/towards-responsible-autonomy-ethics-ras-military-context.

[176] Army, A. Robotic & Autonomous Systems Strategy. Tech. Rep., Commonwealth of Australia, Canberra, Australia (2018). URL https://www.army.gov.au/our-future/australian-army-research-centre-aarc/australian-army-research-centre-publications/robotic.

[177] Wagner, M. Autonomy in the Battlespace: Independently Operating Weapon Systems and the Law of Armed Conflic. *International Humanitarian Law and the Changing Technology of War* 24 (2012). URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2211036.

[178] Weaver, M. UK public faces mass invasion of privacy as big data and surveillance merge | UK news | The Guardian (2017). URL https://www.theguardian.com/uk-news/2017/mar/14/public-faces-mass-invasion-of-privacy-as-big-data-and-surveillance-merge.

[179] Matsakis, L. How the West Got China's Social Credit System Wrong | WIRED (2019). URL https://www.wired.com/story/china-social-credit-score-system/.

[180] NOAA. 2019 Arctic Report Card (2019). URL https://arctic.noaa.gov/Report-Card.

[181] Boey, S., Dortmans, P. & Nicholson, J. Forward 2035 - DSTO Foresight Study. DSTO Foresight Study, Defence Science and Technology Group, Canberra, Australia (2014). URL https://www.dst.defence.gov.au/sites/default/files/publications/documents/Forward-2035.pdf.

[182] Lu, D. & Flavelle, C. Rising Seas Will Erase More Cities by 2050, New Research Shows - The New York Times (2019). URL https://www.nytimes.com/interactive/2019/10/29/climate/coastal-cities-underwater.html.

[183] OECD. OECD Science, Technology and Innovation Outlook: Adapting to Technological and Societal Distruption. Tech. Rep., OECD Committee for Scientific and Technological Policy (CSTP), Paris (2018). URL https://read.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-innovation-outlook-2018_sti_in_outlook-2018-en#page1.

[184] DND, C. The Future Security Environment 2008-2030 (2009). URL https://www.publicsafety.gc.ca/lbrr/archives/cn8160-eng.pdf.

[185] Lucas, L. China in 2050: will it be a global player or split the world economy? (2019). URL https://www.ft.com/content/7500eb04-dfb6-11e9-b8e0-026e07cbe5b4.

[186] Crooke, A. America's Technology and Sanctions War Will End, by Bifurcating the Global Economy (2018). URL https://www.strategic-culture.org/news/2018/12/18/america-technology-sanctions-war-will-end-by-bifurcating-global-economy/.

[187] Amerson, K. & Meredith, S. B. The Future Operating Environment 2050: Chaos, Complexity and Competition (2018). URL https://smallwarsjournal.com/jrnl/art/the-future-operating-environment-2050-chaos-complexity-and-competition.

[188] Thucydides. *History of the Peloponnesian War* (Project Gutenberg, USA, 2004). URL http://www.gutenberg.org/ebooks/7142.

[189] Farley, R. Intellectual Property, Defense Technology, and the Future of Great Power Relations | The Diplomat (2019). URL https://thediplomat.com/2019/03/intellectual-property-defense-technology-and-the-future-of-great-power-relations/.

[190] NATO. Remarks by NATO Secretary General Jens Stoltenberg at the Lowy Institute (Sydney) (2019). URL http://www.nato.int/cps/en/natohq/opinions_168351.htm.

[191] Ratcliffe, S. *Oxford Essential Quotations (4 ed.)* (Oxford University Presss, Oxford, 2016), 4 edn. URL https://www.oxfordreference.com/view/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00018679.

[192] Piatetsky-Shapiro, G. Big Data Hype (and Reality) (2012). URL https://hbr.org/2012/10/big-data-hype-and-reality.

[193] Dörner, D. *The Logic of Failure* (Basic Books, 1997), 2 edn. URL https://www.amazon.com/gp/product/0201479486/ref=as_li_qf_asin_il_tl?ie=UTF8&tag=dlishego07-20&creative=9325&linkCode=as2&creativeASIN=0201479486&linkId=0fd667e314743f3aca48db4252057dc9.

[194] Lishego, D. Dietrich Dorner & The Logic of Failure (2019). URL https://medium.com/@dlishego/dietrich-dorner-the-logic-of-failure-9cda6a9360cc.

[195] Woodie, A. Why Gartner Dropped Big Data Off the Hype Curve (2015). URL https://www.datanami.com/2015/08/26/why-gartner-dropped-big-data-off-the-hype-curve/.

[196] Wu, J. X. & Li, L. An Introduction to Wearable Technology and Smart Textiles and Apparel: Terminology, Statistics, Evolution, and Challenges. *Smart and Functional Soft Materials* (2019). URL https://www.intechopen.com/books/smart-and-functional-soft-materials/an-introduction-to-wearable-technology-and-smart-textiles-and-apparel-terminology-statistics-evoluti. Publisher: IntechOpen.

[197] Trevithick, J. Russia Plans To Set Up Massive New Radar Array To Help "Control" The Arctic Region (2019). URL https://www.thedrive.com/the-war-zone/31271/russia-plans-to-set-up-massive-new-radar-array-to-help-control-the-arctic-region. Library Catalog: www.thedrive.com.

[198] Episkopos, M. Russia's New Radar Can Track 5,000 Objects (Including Hypersonic Missiles) (2018). URL https://nationalinterest.org/blog/buzz/russias-new-radar-can-track-5000-objects-including-hypersonic-missiles-38177. Library Catalog: nationalinterest.org Publisher: The Center for the National Interest.

[199] Humpert, M. Satellite Images Reveal New Russian Long-Range Radar in the Arctic (2019). URL https://www.highnorthnews.com/en/satellite-images-reveal-new-russian-long-range-radar-arctic. Library Catalog: www.highnorthnews.com.

[200] Kuper, S. Next-gen HF radar technology to be developed in SA lab (2019). URL https://www.defenceconnect.com.au/key-enablers/4076-next-gen-hf-radar-technology-to-be-developed-in-sa-lab. Library Catalog: www.defenceconnect.com.au Section: key enablers.

[201] Marr, B. What Is Digital Twin Technology - And Why Is It So Important? (2017). URL https://www.forbes.com/sites/bernardmarr/2017/03/06/what-is-digital-twin-technology-and-why-is-it-so-important/. Library Catalog: www.forbes.com Section: Tech.

[202] DARPA. Defense Advanced Research Projects Agency • Budget Estimates FY 2020 • RDT&E Program. Tech. Rep., DARPA (2019). URL https://www.darpa.mil/attachments/DARPA_FY20_Presidents_Budget_Request.pdf.

[203] Banafa, A. Ten Trends of Internet of Things in 2020 (2019). URL https://www.bbvaopenmind.com/en/technology/digital-world/ten-trends-of-internet-of-things-2020/. Library Catalog: www.bbvaopenmind.com.

[204] FinExtra. EU sets out plans for Big Data and AI (2020). URL https://www.finextra.com/newsarticle/35315/eu-sets-out-plans-for-big-data-and-ai. Library Catalog: www.finextra.com.

[205] Ortiz, B. *et al.* A Common Operating Picture Framework Leveraging Data Fusion and Deep Learning. *arXiv:2001.05982 [cs]* (2020). URL http://arxiv.org/abs/2001.05982. ArXiv: 2001.05982.

[206] Forrester, B. Integrating Social Media Tools with Command and Control (C2). Scientific Report DRDC-RDDC-2016-R073, Defence R&D Canada / Recherche et développement pour la défense Canada, Valcartier, QC (CANADA) (2016).

[207] JASON, M. C. Data Analysis Challenges. JASON Study JSR-08-142, The MITRE Corporation, McLean, Virginia 22102-7539 (2008). URL https://fas.org/irp/agency/dod/jason/data.pdf.

[208] DND, C. The Department of National Defence and Candian Armed Forces Data Strategy (2019). URL https://www.canada.ca/en/department-national-defence/corporate/reports-publications/data-strategy.html.

[209] Clark, L. Data analytics' big problem: 'The tools are nice, but how do you get people to use them?' | ZDNet (2019). URL https://www.zdnet.com/article/data-analytics-big-problem-the-tools-are-nice-but-how-do-you-get-people-to-use-them/.

[210] Custers, B., van de Herik, J., de Laat, C., Rademaker, M. & Veenman, C. Enabling Big Data Applications for Security - Responsible by Design. Tech. Rep., The Hague Security Delta, The Hague (2017). URL https://www.thehaguesecuritydelta.com/media/com_hsd/report/126/document/Big-Data-HR.pdf.

[211] Yudkowsky, E. Artificial Intelligence as a Positive and Negative Factor in Global Risk. In Bostrom, N. & Ćirković, M. M. (eds.) *Global Catastrophic Risks*, 308–345 (NewYork:OxfordUniversityPress., 2008). URL https://intelligence.org/files/AIPosNegFactor.pdf.

[212] DoD, U. Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity. Summary Report, US Department of Defense, Washington (2018). URL https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

[213] Crow, L. Demis Hassabis on AI's potential (2020). URL https://theworldin.economist.com/edition/2020/article/17385/demis-hassabis-ais-potential.

[214] Franklin, J., Carmody, C., Keller, K., Levitt, T. & Buteau, B. Expert system technology for the military: selected samples. *Proceedings of the IEEE* **76**, 1327–1366 (1988). URL http://ieeexplore.ieee.org/document/16329/.

[215] Intel. Neuromorphic Computing - Next Generation of AI (2019). URL https://www.intel.com/content/www/uk/en/research/neuromorphic-computing.html.

[216] GAO. TECHNOLOGY ASSESSMENT Artificial Intelligence Emerging Opportunities, Challenges, and Implications. Report to the Committee on Science, Space, and Technology, House of Representatives GAO-18-142SP, United States Government Accountability Office, Washington, D.C. (2018). URL https://www.gao.gov/assets/700/690910.pdf.

[217] Bufithis, G. Oh, crap! Even MORE stuff to worry about: malevolent machine learning can derail AI (thank you, Enron data set!) – Gregory Bufithis (2019). URL http://www.gregorybufithis.com/2019/03/26/oh-crap-even-more-stuff-to-worry-about-malevolent-machine-learning-could-derail-ai/.

[218] Wiyatno, R. R., Xu, A., Dia, O. & de Berker, A. Adversarial Examples in Modern Machine Learning: A Review. *arXiv:1911.05268 [cs, stat]* (2019). URL http://arxiv.org/abs/1911.05268. ArXiv: 1911.05268.

[219] Torres, M., Hart, G. & Emery, T. The Dstl Biscuit Book - Artificial Intelligence, Data Science and (mostly) Machine Learning. Dstl Biscuit Book DSTL/PUB115968, Ministry of Defence (2019). URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/850129/The_Dstl_Biscuit_Book_WEB.pdf.

[220] Shetty, J. & Adibi, J. The Enron Email Dataset Database Schema and Brief Statistical Report. Technical Report, University of Southern California, Information Sciences Institute, California (2004). URL https://foreverdata.org/1009HOLD/Enron_Dataset_Report.pdf.

[221] Defence, B. DoD Growth In Artificial Intelligence: The Frontline Of A New Age In Defense (2019). URL https://breakingdefense.com/2019/09/dod-growth-in-artificial-intelligence-the-frontline-of-a-new-age-in-defense/.

[222] Miller, H. & Stirling, R. Government AI Readiness Index 2019. Tech. Rep., Oxford Insights and the International Development Research Centre, London England (2019). URL https://www.oxfordinsights.com/ai-readiness2019.

[223] Duranton, S., Erlebach, J. & Pauly, M. Mind the (AI) Gap - Leadership Makes a Difference. Tech. Rep., Boston Consulting Group, Frankfurt (2018). URL https://image-src.bcg.com/Images/Mind_the%28AI%29Gap-Focus_tcm108-208965.pdf.

[224] Dellinger, A. The robot apocalypse has been delayed until further notice (2019). URL https://www.mic.com/p/artificial-intelligence-development-is-starting-to-slow-down-facebook-head-of-ai-says-19424331.

[225] Knight, W. Progress in AI isn't as impressive as you might think (2017). URL https://www.technologyreview.com/s/609611/progress-in-ai-isnt-as-impressive-as-you-might-think/.

[226] Browne, J. Don't Panic about AI (2019). URL https://blogs.scientificamerican.com/observations/dont-panic-about-ai/.

[227] Cumbers, J. Can Synthetic Biology Inspire The Next Wave Of AI? (2019). URL https://www.forbes.com/sites/johncumbers/2019/11/23/can-synthetic-biology-inspire-ai/#ca0f39b50176.

[228] Vincent, J. This is when AI's top researchers think artificial general intelligence will be achieved (2018). URL https://www.theverge.com/2018/11/27/18114362/ai-artificial-general-intelligence-when-achieved-martin-ford-book.

[229] Hutson, M. AI protein-folding algorithms solve structures faster than ever. *Nature* (2019). URL https://www.nature.com/articles/d41586-019-01357-6. Publisher: Nature Publishing Group.

[230] Mitchum, R. & Lerner, L. How AI could change science (2019). URL https://news.uchicago.edu/story/how-ai-could-change-science. Library Catalog: news.uchicago.edu.

[231] Falk, D. How Artificial Intelligence Is Changing Science (2019). URL https://www.quantamagazine.org/how-artificial-intelligence-is-changing-science-20190311/. Library Catalog: www.quantamagazine.org.

[232] Ober, A. How artificial intelligence is changing science (2018). URL https://news.stanford.edu/2018/05/15/how-ai-is-changing-science/.

[233] Shrestha, D. How Artificial Intelligence Will Impact Scientific Research (2019). URL https://medium.com/@fusemachines/how-artificial-intelligence-will-impact-scientific-research-4e6f4face1ae. Library Catalog: medium.com.

[234] Craig, C. *et al.* Machine learning: the power and promise of computers that learn by example. Tech. Rep., Royal Society (Great Britain) (2017). URL https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf. OCLC: 1016323791.

[235] RSGB. The AI revolution in scientific research. Tech. Rep., The Royal Society (Great Britian), London (2019). URL https://royalsociety.org/-/media/policy/projects/ai-and-society/AI-revolution-in-science.pdf?la=en-GB&hash=5240F21B56364A00053538A0BC29FF5F.

[236] Tonin, M. Artificial Intelligence: Implications for NATO's Armed Forces. NATO Parlimentary Assemby Report 149 STCTTS 19 E rev. 1 fin, NATO, Brussels (2019).

[237] Simonite, T. AI Could Revolutionize War as Much as Nukes | WIRED (2017). URL https://www.wired.com/story/ai-could-revolutionize-war-as-much-as-nukes/.

[238] Paul, C. & Posard, M. N. Artificial Intelligence and the Manufacturing of Reality (2020). URL https://www.rand.org/blog/2020/01/artificial-intelligence-and-the-manufacturing-of-reality.html.

[239] Gibney, E. Self-taught AI is best yet at strategy game Go. *Nature News* (2017). URL http://www.nature.com/news/self-taught-ai-is-best-yet-at-strategy-game-go-1.22858.

[240] Meyer, S. P. A Looming AI War: Transparency v. IP Rights | Lexology (2019). URL https://www.lexology.com/library/detail.aspx?g=5ec0ae23-5a2c-401c-993e-9d807ba9745b.

[241] USAF. U.S. Air Force Science and Technology Strategy - Strengthening USAF Science and Technology for 2030 and Beyond (2019). URL https://www.af.mil/Portals/1/documents/2019%20SAF%20story%20attachments/Air%20Force%20Science%20and%20Technology%20Strategy.pdf.

[242] Slijper, F., Beck, A., Kayser, D. & PAX (Project). State of AI: artificial intelligence, the military and increasingly autonomous weapons. Tech. Rep., PAX, Utrecht, NL (2019). URL https://www.paxvoorvrede.nl/media/files/state-of-artificial-intelligence--pax-report.pdf. OCLC: 1102502855.

[243] HLEG, A. A Definition of AI: Main Capabilities And Disciplines. Independent High-Level Expert Group On Artificial Intelligence, European Commission, Brussels (2009). URL https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.

[244] Kasapoğlu, C. & Kırdemir, B. Artificial Intelligence and the Future of Conflict. In *New Perspectives on Shared Security_ NATO's Next 70 Years*, 112 (Carnegie Endowment for International Peace, Washington, D.C., 2019). URL https://carnegieendowment.org/files/NATO_int_final1.pdf.

[245] Press, G. Top Artificial Intelligence (AI) Predictions For 2020 From IDC and Forrester (2019). URL https://www.forbes.com/sites/gilpress/2019/11/22/top-artificial-intelligence-ai-predictions-for-2020-from-idc-and-forrester/#8bb5ea9315a1.

[246] Gunning, D. *et al.* XAI—Explainable artificial intelligence | Science Robotics. *Science Robotics* **4**, 2 (2019). URL https://robotics.sciencemag.org/content/4/37/eaay7120.full?utm_medium=twitter&utm_source=dlvr.it.

[247] Allison, G. Is China Beating America to AI Supremacy? (2019). URL https://nationalinterest.org/feature/china-beating-america-ai-supremacy-106861.

[248] Zeigler, B., Muzy, A. & Yilmaz, L. Artificial Intelligence in Modeling and Simulation. In Meyers, R. (ed.) *Encyclopedia of Complexity and System Science*, 44 (Springer, Heidelberg, Germany, 2009).

[249] De Spiegeleire, S., Maas, M. & Sweijs, T. *Artificial Intelligence And The Future Of Defense: Strategic Implications For Small And Medium-Sized Force Providers* (The Hague Centre for Strategic Studies, 2017). URL https://mafiadoc.com/artificial-intelligence-and-the-future-of-defense-hcss_5981b1491723ddeb563a0af6.html.

[250] McKendrick, J. Artificial Intelligence Only Goes So Far In Today's Economy, Says MIT Study. *Forbes* 2 (2019). URL https://www.forbes.com/sites/joemckendrick/2019/09/14/artificial-intelligence-only-goes-so-far-in-todays-economy-says-mit-study/#429a1ca71162.

[251] Scharre, P. Killer Apps. *Foreign Affairs* **May/June 2019** (2019). URL https://www.foreignaffairs.com/articles/2019-04-16/killer-apps.

[252] Tarraf, D. *et al. The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations* (RAND Corporation, 2019). URL https://www.rand.org/pubs/research_reports/RR4229.html.

[253] Besser, H.-L., Göge, D., Huggins, M. & Zimper, D. Platform Autonomy: State-of-the-Art and Future Perspectives from an S&T Point of View. *The Journal of the JAPCC* **20** (2015). URL https://www.japcc.org/platform-autonomy/.

[254] Bernard, D. *et al.* Autonomy and software technology on NASA's Deep Space One. *IEEE Intelligent Systems and their Applications* **14**, 10–15 (1999).

[255] University of Sheffield *et al.* Space Robotics and Autonomous Systems: Widening the horizon of space exploration. UKRAS White Paper, UK-RAS Network (2018). URL https://www.ukras.org/wp-content/uploads/2018/09/UK_RAS_wp_Urban_010618_print.pdf.

[256] Fong, T. Autonomous Systems NASA Capability Overview (2018). URL https://www.nasa.gov/sites/default/files/atoms/files/nac_tie_aug2018_tfong_tagged.pdf.

[257] Ivanova, K. & Gallasch, G. E. Analysis of Emerging Technologies and Trends for ADF Combat Service Support 2016. DST Group Report DST-Group-GD-0946, Defence Science and Technology Group Land Division, Edinburgh SA 5111 (2016). URL https://www.dst.defence.gov.au/publication/horizon-scan-emerging-technologies-and-trends-adf-combat-service-support-2016.

[258] Singer, P. W. How the U.S. Can Win the Robot Revolution (2010). URL https://www.popularmechanics.com/technology/military/robots/how-to-win-robot-military-revolution.

[259] Rane, S. Building a cyber-physical immune system (2019). URL https://www.computerweekly.com/opinion/Building-a-cyber-physical-immune-system.

[260] Reim, G. US Army looks for autonomous medevac vehicles, including UAVs | News | Flight Global (2019). URL https://www.flightglobal.com/fixed-wing/us-army-looks-for-autonomous-medevac-vehicles-including-uavs/135489.article.

[261] Dhingra, A. Miniaturization of sensors opening new vistas in data collection (2019). URL https://www.geospatialworld.net/blogs/miniaturization-of-sensors-opening-new-vistas-in-data-collection/.

[262] Seffers, G. DARPA's Ocean of Things Ripples Across Research Areas (2019). URL https://www.afcea.org/content/darpas-ocean-things-ripples-across-research-areas.

[263] Jackson, R. Small is beautiful: Nano drone tech is advancing (2017). URL https://www.defenceiq.com/defence-technology/articles/nano-drone-tech-is-advancing. Library Catalog: www.defenceiq.com.

[264] Spencer, T. DE&S Technology Office procures cutting-edge Nano UAVs (2019). URL https://des.mod.uk/des-pocures-nano-uavs/. Library Catalog: des.mod.uk Section: News.

[265] Kirve, P. Small Drones Take Flight for Military, Surveillance Applications (2018). URL https://www.roboticsbusinessreview.com/unmanned/small-drones-military-surveillance/. Library Catalog: www.roboticsbusinessreview.com Section: Unmanned Systems.

[266] Praczyk, T., Szymak, P., Naus, K., Pietrukaniec, L. & Hożyń, S. Report on Research with Biomimetic Autonomous Underwater Vehicle — Navigation and Autonomous Operation. *Scientific Journal of Polish Naval Academy* **213**, 53–67 (2018). URL https://content.sciendo.com/view/journals/sjpna/213/2/article-p53.xml. Publisher: Sciendo Section: Scientific Journal of Polish Naval Academy.

[267] Ayers, J. *et al.* A Modular Behavioral-Based Architecture for Biomimetic Autonomous Underwater Robots. In *Proc. of the Autonomous Vehicles in Mine Countermeasures Symposium* (Naval Postgraduate School, Naval Postgraduate School, 1998). URL http://www.neurotechnology.neu.edu/biomimeticrobots98.html.

[268] EDA. EDA expands work on autonomous underwater vehicles (2019). URL https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/09/27/eda-expands-work-on-autonomous-underwater-vehicles.

[269] McMullan, T. How swarming drones will change warfare - BBC News (2019). URL https://www.bbc.com/news/technology-47555588.

[270] TRADOC, U. A. The U.S. Army Robotic and Autonomous Systems Strategy. Tech. Rep., U.S. Army, 950 Jefferson Ave, Fort Eustis, VA (2017). URL https://www.tradoc.army.mil/portals/14/documents/ras_strategy.pdf.

[271] Martin, B. *et al. Advancing Autonomous Systems: An Analysis of Current and Future Technology for Unmanned Maritime Vehicles* (RAND Corporation, 2019). URL https://www.rand.org/pubs/research_reports/RR2751.html.

[272] DARPA, O. ACTUV "Sea Hunter" Prototype Transitions to Office of Naval Research for Further Development (2018). URL https://www.darpa.mil/news-events/2018-01-30a.

[273] Lockwood, F. *et al.* Global Marine Technology Trends Autonomous Systems.pdf. Global Marine Technology Trends, 7 Lloyd's Register Group Ltd, QinetiQ and University of Southampton., Southampton (2017). URL https://cdn.southampton.ac.uk/assets/imported/transforms/content-block/UsefulDownloads_Download/F9AFACCCB8B444559D4212E140D886AF/68481%20Global%20Marine%20Technology%20Trends%20Autonomous%20Systems_FINAL_SINGLE_PAGE.pdf.

[274] NASC. X-47B First to Complete Autonomous Aerial Refueling (2015). URL https://www.navy.mil/submit/display.asp?story_id=86710.

[275] South, T. Soldiers soon to see robotic mules and tougher bomb bots in the field (2019). URL https://www.armytimes.com/news/your-army/2019/11/22/soldiers-soon-to-see-robotic-mules-and-tougher-bomb-bots-in-the-field/. Library Catalog: www.armytimes.com Section: Your Army.

[276] Judson, J. After protest, Army launches new competition for robotic mule (2020). URL https://www.defensenews.com/land/2020/02/18/after-protest-army-launches-new-competition-for-robotic-mule/. Library Catalog: www.defensenews.com Section: Land.

[277] Gettinger, D. & Michel, A. H. Loitering Munitions. Technical Report, The Center for the Study of the Drone at Bard College, Washington, D.C. (2017). URL https://dronecenter.bard.edu/files/2017/02/CSD-Loitering-Munitions.pdf.

[278] Gao, C. Why Loitering Munitions Are the Newest and Deadliest Threat | The National Interest (2019). URL https://nationalinterest.org/blog/buzz/why-loitering-munitions-are-newest-and-deadliest-threat-81241.

[279] Ministry of Defence, U. Coalition Autonomous Systems – the future of military logistics (2019). URL https://www.gov.uk/government/news/coalition-autonomous-systems-the-future-of-military-logistics.

[280] Pawlyk, O. Air Force Wants to Decrease Manning for Its UAVs (2018). URL https://www.military.com/daily-news/2018/02/24/air-force-wants-decrease-manning-its-unmanned-vehicles.html. Library Catalog: www.military.com Section: Headlines.

[281] Porat, T., Oron-Gilad, T., Rottem-Hovev, M. & Silbiger, J. Supervising and Controlling Unmanned Systems: A Multi-Phase Study with Subject Matter Experts. *Frontiers in Psychology* **7** (2016). URL https://www.frontiersin.org/articles/10.3389/fpsyg.2016.00568/full. Publisher: Frontiers.

[282] Moniz, A. B. Robots and humans as co-workers? The human-centred perspective of work with autonomous systems. IET Working Papers Series No. WPS03/2013, Universidade Nova de Lisboa, Monte de Caparica, Portugal (2013).

[283] Mizokami, K. Gremlin First Flight | C-130 Will Be a Flying Aircraft Carrier (2020). URL https://www.popularmechanics.com/military/aviation/a30612943/gremlin-drone-first-flight/.

[284] Axe, D. Missile Plane: How the C-17 Cargo Plane Could Be Modified to Carry Deadly Weapons | The National Interest (2020). URL https://nationalinterest.org/blog/buzz/missile-plane-how-c-17-cargo-plane-could-be-modified-carry-deadly-weapons-134642.

[285] DARPA, O. OFFensive Swarm-Enabled Tactics (OFFSET) (2019). URL https://www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics.

[286] Atherton, K. D. Russia will test swarms for anti-robot combat in 2020 (2019). URL https://www.defensenews.com/unmanned/2019/12/13/russia-will-test-swarms-for-anti-robot-combat-in-2020/.

[287] Cole, S. Counter-drone technologies are evolving to "counter" countermeasures (2020). URL http://mil-embedded.com/articles/counter-drone-technologies-are-evolving-to-counter-countermeasures/.

[288] EDM. Remote Defence: Unmanned & Autonomous Systems Take Hold in Military Toolboxes. *European Defence Matters* (2018). URL https://www.eda.europa.eu/docs/default-source/eda-magazine/edm16.

[289] McFadden, C. A Brief History of Military Robots Including Autonomous Systems (2018). URL https://interestingengineering.com/a-brief-history-of-military-robots-including-autonomous-systems.

[290] Harper, J. Spending on Drones Projected to Soar (2019). URL https://www.nationaldefensemagazine.org/articles/2019/4/15/spending-on-drones-projected-to-soar.

[291] Research and Markets. Global $172.3 Bn Autonomous Vehicle Markets, 2019-2024: Long Haul Trucking Market will Grow at a CAGR of Over 60% (2019). URL https://www.prnewswire.com/news-releases/global-172-3-bn-autonomous-vehicle-markets-2019-2024-long-haul-trucking-market-will-grow-at-a-cagr-of-over-60-300818667.html.

[292] Osborn, K. Army Soldiers Will Control AI-enabled Robot Tanks (2020). URL https://defensemaven.io/warriormaven/land/army-soldiers-will-control-ai-enabled-robot-tanks-rUoQ33J80EeRUd5n2SmQbw.

[293] Kallenborn, Z. & Bleek, P. C. Swarming destruction: drone swarms and chemical, biological, radiological, and nuclear weapons. *The Nonproliferation Review* **25**, 523–543 (2018). URL https://doi.org/10.1080/10736700.2018.1546902. Publisher: Routledge _eprint: https://doi.org/10.1080/10736700.2018.1546902.

[294] Blum, G. Invisible Threats. In Berkowitz, P. (ed.) *Emerging Threats in National Security and Law* (Hoover Institution, Stanford University, Standford, CA, 2012). URL https://www.hoover.org/sites/default/files/research/docs/emergingthreats_blum.pdf.

[295] Razzouk, N. & Blas, J. Saudi Oil Production Cut in Half After Drone Attack from Yemen - Bloomberg (2019). URL https://www.bloomberg.com/news/articles/2019-09-14/saudi-aramco-contain-fires-at-facilities-attacked-by-drones.

[296] Block, I. "Massive swarm" strike on Saudi oil facility demonstrates destructive potential of drones (2019). URL https://www.dezeen.com/2019/09/16/drone-strike-saudi-arabia-aramco-oil-supply/. Library Catalog: www.dezeen.com Section: all.

[297] Gonzales, D. & Harting, S. *Designing unmanned systems with greater autonomy: using a federated, partially open systems architecture approach* (RAND Corporation, Santa Monica, 2014). OCLC: ocn890435458.

[298] Marr, B. 20 Mind-Boggling Facts About Quantum Computing Everyone Should Read (2018). URL https://www.forbes.com/sites/bernardmarr/2018/02/23/20-mind-boggling-facts-about-quantum-computing-everyone-should-read/.

[299] Coakley, A. Quantum computing: Is it really all it's cracked up to be? | DW | 05.11.2019 (2019). URL https://www.dw.com/en/quantum-computing-is-it-really-all-its-cracked-up-to-be/a-51118334.

[300] NIST. The Second Quantum Revolution (2018). URL https://www.nist.gov/topics/physics/introduction-new-quantum-revolution/second-quantum-revolution.

[301] Dowling, J. P. & Milburn, G. J. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **361**, 1655–1674 (2003). URL https://royalsocietypublishing.org/doi/10.1098/rsta.2003.1227.

[302] Schwab, K. The Fourth Industrial Revolution: what it means and how to respond (2016). URL https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[303] Smith-Goodson, P. Quantum USA Vs. Quantum China: The World's Most Important Technology Race (2019). URL https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/.

[304] Turnbull, G. Quantum leap: atomic sensing for the military - Global Defence Technology | Issue 96 | February 2019. *Global Defence Technology* (2019). URL https://defence.h5mag.com/global_defence_technology_feb19/quantum_leap_atomic_sensing_for_the_military.

[305] Roblin, S. Quantum Radars Could Unstealth the F-22, F-35 and J-20 (Or Not) (2018). URL https://nationalinterest.org/blog/the-buzz/quantum-radars-could-unstealth-the-f-22-f-35-j-20-or-not-25772. Library Catalog: nationalinterest.org Publisher: The Center for the National Interest.

[306] University, P. Quantum Computing Breakthrough: Silicon Qubits Interact at Long-Distance (2019). URL https://scitechdaily.com/quantum-computing-breakthrough-silicon-qubits-interact-at-long-distance/.

[307] Meetings, L. N. L. Quantum technologies to revolutionize 21st century (2016). URL https://phys.org/news/2016-06-quantum-technologies-revolutionize-21st-century.html.

[308] Wittek, P. Bayesian Deep Learning and Near-Term Quantum Computers: A Cautionary Tale In Quantum Machine Learning (2019). URL https://www.kdnuggets.com/2019/07/bayesian-deep-learning-near-term-quantum-computers.html.

[309] Simonite, T. Quantum Computing Is Here! But Also Not Really | WIRED (2019). URL https://www.wired.com/story/quantum-computing-here-but-not-really/.

[310] Popkin, G. Physics - Waiting for the Quantum Simulation Revolution (2019). URL https://physics.aps.org/articles/v12/112.

[311] NATO. Doorstep statement by NATO Secretary General Jens Stoltenberg ahead of the meeting of NATO Ministers of Foreign Affairs (2019). URL http://www.nato.int/cps/en/natohq/opinions_171016.htm.

[312] JAPCC. Filling the Vacuum: A Framework for a NATO Space Policy. Tech. Rep., Joint Air Power Competence Center (JAPCC), von-Seydlitz-Kaserne, DEU (2012). URL http://www.japcc.org/wp-content/uploads/SPP_2012_web.pdf.

[313] Mabrouk, E. What are SmallSats and CubeSats? (2015). URL http://www.nasa.gov/content/what-are-smallsats-and-cubesats.

[314] Dormehl, L. DARPA is Building a Robotic Space Mechanic to Fix Satellites in Orbit (2020). URL https://www.digitaltrends.com/cool-tech/darpa-robot-arm-in-space-rsgs-spacecraft/. Library Catalog: www.digitaltrends.com Section: Emerging Tech.

[315] Choudhary, M. On-orbit satellite servicing: Process, Benefits and Challenges (2018). URL https://www.geospatialworld.net/article/on-orbit-satellite-servicing-process-benefits-and-challenges-2/.

[316] Griffiths, H. Passive Radar - From Inception to Maturity (2017). URL https://in.bgu.ac.il/en/engn/ece/radar/Radar2017/Documents/Prof.%20Hugh%20Griffiths%20-%20Passive%20Radar%20-%20From%20Inception%20to%20Maturity.pdf.

[317] Cave, D. Intelligence for sale: Commercial space sensors and their use (2016). URL https://www.army.gov.au/our-future/blog/situational-awareness/intelligence-for-sale-commercial-space-sensors-and-their-use.

[318] Carmichael, D. Laser Communications Small Satellite Mission Demonstrates Tech First (2018). URL http://www.nasa.gov/feature/ames/nasa-s-laser-communications-small-satellite-mission-demonstrates-technology-first.

[319] of Concerned Scientist, U. USC Satellite Database (2019). URL https://www.ucsusa.org/resources/satellite-database.

[320] Ryan-Mosley, T. The number of satellites orbiting Earth could quintuple in the next decade (2019). URL https://www.technologyreview.com/s/613746/satellite-constellations-orbiting-earth-quintuple/.

[321] Jones, H. W. The Recent Large Reduction in Space Launch Costs. In *ICES-2018-81* (International Conference on Environmental Systems, Albuquerque, New Mexico, 2018). URL https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20200001093.pdf.

[322] Foust, J. A trillion-dollar space industry will require new markets (2018). URL https://spacenews.com/a-trillion-dollar-space-industry-will-require-new-markets/.

[323] DIA. Challenges to Security in Space. Tech. Rep., Defense Intelligence Agency, Washington, D.C. (2019). URL www.dia.mil/Military-Power-Publications.

[324] Ryan-Mosely, T., Winick, E. & Kakaes, K. Defense intelligence chief paints bleak picture of the space battlefield (2019). URL https://spacenews.com/defense-intelligence-chief-paints-bleak-picture-of-the-space-battlefield/.

[325] Dormehl, L. Space Force Needs to Prepare for a New Cold War in Earth's Orbit (2020). URL https://www.digitaltrends.com/cool-tech/space-force-cold-war-space-chris-bogdan/. Library Catalog: www.digitaltrends.com Section: Emerging Tech.

[326] Wall, M. Space Weapon? US Calls Out Russian Satellite's 'Very Abnormal Behavior' (2018). URL https://www.space.com/41503-russian-satellite-possible-space-weapon.html.

[327] Gruss, M. U.S. Official: China Turned to Debris-free ASAT Tests Following 2007 Outcry (2016). URL https://spacenews.com/u-s-official-china-turned-to-debris-free-asat-tests-following-2007-outcry/.

[328] Langbroek, M. Why India's ASAT Test Was Reckless – The Diplomat (2019). URL https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/.

[329] Tucker, P. The NSA Is Studying Satellite Hacking (2019). URL https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/.

[330] Roadknight, T. Space: the final frontier for cybersecurity? (2016). URL https://www.nexor.com/space-final-frontier-cybersecurity/.

[331] Livingstone, D. & Lewis, P. Space, the Final Frontier for Cybersecurity? Research Paper, Chatham House, The Royal Institute of International Affairs, London (2016). URL https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[332] Rouland, C. Securing satellites: The new space race (2019). URL https://www.helpnetsecurity.com/2019/05/09/securing-satellites/.

[333] STUFF. Lack of rules could turn space exploration into the 'wild west' | Stuff.co.nz (2019). URL https://www.stuff.co.nz/national/118257315/lack-of-rules-could-turn-space-exploration-into-the-wild-west.

[334] Kallberg, J. Why older satellites present a cyber risk (2018). URL https://www.fifthdomain.com/opinion/2018/12/28/why-older-satellites-present-a-cyber-risk/.

[335] SpaceNews. NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft (2006). URL https://spacenews.com/nro-confirms-chinese-laser-test-illuminated-us-spacecraft/.

[336] Shachtman, N. Is This China's Anti-Satellite Laser Weapon Site? *Wired* (2009). URL https://www.wired.com/2009/11/is-this-chinas-anti-satellite-laser-weapon-site/.

[337] Gehrke, J. Russia is stalking US satellites in orbit, a NATO general warns - Business Insider (2020). URL https://www.businessinsider.com/russia-stalking-us-satellites-in-orbit-a-nato-general-warns-2020-2?r=US&IR=T.

[338] Takahashi, K., Charles, C., Boswell, R. W. & Ando, A. Demonstrating a new technology for space debris removal using a bi-directional plasma thruster. *Scientific Reports* **8**, 14417 (2018). URL http://www.nature.com/articles/s41598-018-32697-4.

[339] Akoto, W. All Those Low-Cost Satellites in Orbit Could Be Weaponized by Hackers, Warns Expert (2020). URL https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932.

[340] Berger, E. India proudly showcases its anti-satellite weapon at an arms bazaar (2020). URL https://arstechnica.com/science/2020/02/india-proudly-showcases-its-anti-satellite-weapon-at-an-arms-bazaar/.

[341] McDonald, A. W. & Hanlon, B. Shaping Defence Science and Technology in the Aerospace Domain 2017–2027 (2017). URL https://www.dst.defence.gov.au/publication/shaping-defence-science-and-technology-aerospace-domain-2017-2027.

[342] Lewis, D. *et al.* NATO Space - S&T Developments to Enhance Resiliency and Effectiveness of NATO Operation - Final Report of Specialists' Meeting SCI-268-SM Jun 2014 at ALTEC, Turin, Italy. STO Technical Report, NATO Science and Technology Organisation (2014).

[343] Desai, S. PLA SSF: Why China will be ahead of everyone in future cyber, space or information warfare (2019). URL https://theprint.in/opinion/pla-ssf-why-china-will-be-ahead-of-everyone-in-future-cyber-space-or-information-warfare/342772/.

[344] Cronin, P. M. & Neuhard, R. Securing the High Ground in Outer Space | The National Interest (2019). URL https://nationalinterest.org/feature/securing-high-ground-outer-space-100572.

[345] Winter, L. NATO declares space an 'operational domain' | News | Al Jazeera (2019). URL https://www.aljazeera.com/ajimpact/nato-declares-space-operational-domain-191204155031893.html.

[346] Teller Report. Military Alliance: NATO Prepares for Wars in Space (2019). URL https://www.tellerreport.com/news/2019-11-19---military-alliance--nato-prepares-for-wars-in-space-.S1ZcVIq-3B.html.

[347] Dorrian, G. & Whittaker, I. Space may soon become a war zone – here's how that would work (2019). URL https://phys.org/news/2019-10-space-war-zone.html.

[348] Moon, M. THE SPACE DOMAIN AND ALLIED DEFENCE. REPORT: Sub-Committee on Future Security and Defence Capabilities www. 162 DSCFC 17 E rev.1 fin, NATO Parliamentary Assembly, Brussels (2017). URL https://www.nato-pa.int/document/2017-space-domain-and-allied-defence-moon-report-162-dscfc-17-e-rev1-fin.

[349] Mehta, A. Hypersonics 'highest technical priority' for Pentagon R&D head (2018). URL https://www.defensenews.com/pentagon/2018/03/06/hypersonics-highest-technical-priority-for-pentagon-rd-head/.

[350] Besser, H.-L., Göge, D., Huggins, M., Shaffer, A. & Zimper, D. Hypersonic Vehicles. *The Journal of the JAPCC* **24**, 11–27 (2017). URL https://www.japcc.org/hypersonic-vehicles/.

[351] Booz-Allen-Hamilton. The Threat of Hypersonic Weapons (2019). URL https://www.boozallen.com/d/insight/blog/the-threat-of-hypersonic-weapons.html.

[352] GAO. HYPERSONIC WEAPONS. Tech. Rep. GAO-19-705SP Hypersonic Weapons, United States Government Accountability Office, Washington, D.C. (2019). URL https://www.gao.gov/assets/710/701369.pdf.

[353] LaGrone, S. Navy Quietly Fires 20 Hyper Velocity Projectiles Through Destroyer's Deckgun (2019). URL https://news.usni.org/2019/01/08/navy-quietly-fires-20-hyper-velocity-projectiles-destroyers-deckgun.

[354] Youngquist, R. C., Cox, R. B. & Starr, S. O. The Feasibility of Railgun Horizontal-Launch Assist. NASA Technical Report 20110005535, NASA, NASA Kennedy Space Center, Florida (2011). URL https://ntrs.nasa.gov/search.jsp?R=20110005535.

[355] Pacella, R. M. NASA Engineers Propose Combining a Rail Gun and a Scramjet to Fire Spacecraft Into Orbit (2010). URL https://www.popsci.com/technology/article/2010-11/nasa-engineers-propose-combining-rail-gun-and-scramjet-fire-spacecraft-orbit/.

[356] Trafalgar, G. English: Side-by-side comparative diagram of (a) turbojet; (b) ramjet; (c) scramjet sections. (2010). URL https://commons.wikimedia.org/wiki/File:Turbo_ram_scramjet_comparative_diagram.svg.

[357] Belfiore, M. The X-51A Hypersonic Plane: What Went Wrong? (2012). URL https://www.popularmechanics.com/military/a8262/the-x-51a-hypersonic-plane-what-went-wrong-14124408/.

[358] Engines, R. Sabre :: Reaction Engines (2019). URL https://www.reactionengines.co.uk/sabre.

[359] USAF. X-51A Waverider > U.S. Air Force > Fact Sheet Display (2011). URL https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104467/x-51a-waverider/.

[360] USAF. AEDC team members recall their time spent supporting NASA's X-43A proj (2019). URL https://www.afmc.af.mil/News/Article-Display/Article/1853352/aedc-team-members-recall-their-time-spent-supporting-nasas-x-43a-project/.

[361] Stone, R., 2020 & Am, . 'National pride is at stake.' Russia, China, United States race to build hypersonic weapons (2020). URL https://www.sciencemag.org/news/2020/01/national-pride-stake-russia-china-united-states-race-build-hypersonic-weapons. Library Catalog: www.sciencemag.org.

[362] Axe, D. How the U.S. Is Quietly Winning the Hypersonic Arms Race. *The Daily Beast* (2019). URL https://www.thedailybeast.com/how-the-us-is-quietly-winning-the-hypersonic-arms-race.

[363] Lewis, M. & White, M. Department of Defense Press Briefing on Hypersonics (2020). URL https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2101062/department-of-defense-press-briefing-on-hypersonics/. Library Catalog: www.defense.gov.

[364] Wilson, J. The emerging world of hypersonic weapons technology (2019). URL https://www.militaryaerospace.com/power/article/14033431/the-emerging-world-of-hypersonic-weapons-technology. Library Catalog: www.militaryaerospace.com.

[365] Pickrell, R. The US military just took a big step forward in the hypersonic arms race with Russia and China (2020). URL https://www.businessinsider.com/us-military-successfully-tests-glide-body-for-future-hypersonic-weapons-2020-3. Library Catalog: www.businessinsider.com.

[366] Delcker, J. China leads research into hypersonic technology: report (2019). URL https://www.politico.eu/article/china-leads-research-into-hypersonic-technology-report/. Library Catalog: www.politico.eu.

[367] Roblin, S. China's stealth drones and hypersonic missiles surpass — and threaten — the U.S. (2019). URL https://www.nbcnews.com/think/opinion/china-s-stealth-drones-hypersonic-missiles-surpass-threaten-u-s-ncna1064841.

[368] Brumfiel, G. Nations Rush Ahead With Hypersonic Weapons Amid Arms Race Fear (2018). URL https://www.npr.org/2018/10/23/659602274/amid-arms-race-fears-the-u-s-russia-and-china-are-racing-ahead-with-a-new-missil.

[369] Lague, D. & Lim, B. K. Special Report: New missile gap leaves U.S. scrambling to counter China. *Reuters* (2019). URL https://www.reuters.com/article/us-china-army-rockets-specialreport-idUSKCN1S11DH.

[370] Sayler, K. M. Hypersonic Weapons: Background and Issues for Congress. CRS Report, Congressional Research Service, Washington DC (2020).

[371] Martin, S. Watch out, Putin! UK developing hypersonic missile capable of reaching Moscow in 24 mins (2019). URL https://www.express.co.uk/news/science/1166598/uk-russia-vladimir-putin-hypersonic-missiles-tempest-ministry-of-defence-rolls-royce-bae. Library Catalog: www.express.co.uk Section: Science.

[372] Peck, M. Now France Wants Hypersonic Missiles by 2021 (2019). URL https://nationalinterest.org/blog/buzz/now-france-wants-hypersonic-missiles-2021-43202.

[373] Yeo, M. Japan unveils its hypersonic weapons plans (2020). URL https://www.defensenews.com/industry/techwatch/2020/03/13/japan-unveils-its-hypersonic-weapons-plans/.

[374] Beale, C. US and Australia test hypersonic missiles that fly at a mile a second | The Independent (2017). URL https://www.independent.co.uk/news/us-and-australia-test-hypersonic-missiles-that-fly-at-a-mile-a-second-a7842961.html.

[375] Keller, J. The Air Force's New Hypersonic Spy Plane Is Coming Soon | The National Interest (2019). URL https://nationalinterest.org/blog/buzz/air-forces-new-hypersonic-spy-plane-coming-soon-85636.

[376] Howell, E. DARPA's hypersonic 'Glide Breaker' could blast missile threats out of the sky | Space (2020). URL https://www.space.com/darpa-glide-breaker-hypersonic-vehicle-defense.html.

[377] Simon, S. Opinion | Hypersonic Missiles Are a Game Changer. *The New York Times* (2020). URL https://www.nytimes.com/2020/01/02/opinion/hypersonic-missiles.html.

[378] Peake, E. Hypersonic missiles are coming to change warfare forever. *Wired UK* (2017). URL https://www.wired.co.uk/article/this-is-how-hypersonic-missiles-could-change-the-future-of-warfare.

[379] White, R. An Emerging Threat: The Impact of Hypersonic Weapons on National Security, Crisis Instability, and Deterrence Strategy (2018). URL https://potomacinstitute.org/images/studies/Intern_Projects/Rylie%20White-Hypersonic%20Weapons%20(1).docx.

[380] Peck, M. Expert: The U.S. Army Doesn't Need Hypersonic Missiles | The National Interest (2019). URL https://nationalinterest.org/blog/buzz/expert-us-army-doesnt-need-hypersonic-missiles-79566.

[381] Ghoshal, D. Playing Catch Up: How the U.S. Plans to Counter Hypersonic Missiles (2019). URL https://www.defenceiq.com/air-land-and-sea-defence-services/articles/playing-catch-up-how-the-us-plans-to-counter-hypersonic-missiles.

[382] Acton, J. M. China's Ballyhooed New Hypersonic Missile Isn't Exactly a Game-Changer (2019). URL https://carnegieendowment.org/2019/10/04/china-s-ballyhooed-new-hypersonic-missile-isn-t-exactly-game-changer-pub-79998.

[383] Axe, D. The Problem with Hypersonic Missiles: "None of this stuff works yet." | The National Interest (2019). URL https://nationalinterest.org/blog/buzz/problem-hypersonic-missiles-none-stuff-works-yet-97252.

[384] Erwin, S. Air Force X-37B secret spaceplane lands after 780 days in orbit - SpaceNews.com (2019). URL https://spacenews.com/air-force-x-37b-secret-spaceplane-lands-after-780-days-in-orbit/.

[385] Wang, B. Russia developing hypersonic weapons expects breakthroughs in combat laser and electromagneticweapons – NextBigFuture.com (2017). URL https://www.nextbigfuture.com/2017/01/russia-developing-hypersonic-weapons.html.

[386] Levick, E. The warship is dead - Australian Defence Magazine (2019). URL https://www.australiandefence.com.au/news/the-warship-is-dead. Library Catalog: www.australiandefence.com.au.

[387] BBC. Russia deploys hypersonic missile system. *BBC News* (2019). URL https://www.bbc.com/news/world-europe-50927648.

[388] Alliance, M. D. A. Hypersonic Weapon Basics – Missile Defense Advocacy Alliance (2019). URL https://missiledefenseadvocacy.org/missile-threat-and-proliferation/missile-basics/hypersonic-missiles/.

[389] Mizokami, K. Zircon Missile | Russia Tests Its Hypersonic Anti-Ship Missile (2020). URL https://www.popularmechanics.com/military/weapons/a31159727/zircon-hypersonic-missile-test/.

[390] Panda, A. Hypersonic Hype: Just How Big of a Deal Is China's DF-17 Missile? (2019). URL https://thediplomat.com/2019/10/hypersonic-hype-just-how-big-of-a-deal-is-chinas-df-17-missile/.

[391] Seidel, J. 'Impossible to defend': China goes rogue with new weapon - NZ Herald (2019). URL https://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=12285008.

[392] Osborn, K. The U.S. Military Wants to Destroy Russia and Chinese Hypersonic Missiles in a War | The National Interest (2019). URL https://nationalinterest.org/blog/buzz/us-military-wants-destroy-russia-and-chinese-hypersonic-missiles-war-107221.

[393] Ali, S. All the Secret (Or Not) Ways to Kill a Hypersonic Missile | The National Interest (2019). URL https://nationalinterest.org/blog/buzz/all-secret-or-not-ways-kill-hypersonic-missile-64031.

[394] Henschke, A. 'Supersoldiers': Ethical concerns in human enhancement technologies (2017). URL https://medium.com/law-and-policy/supersoldiers-ethical-concerns-in-human-enhancement-technologies-fa9bf1e06889.

[395] Markus, D. CRISPR developer Jennifer Doudna on Reset podcast: How the gene-editing technology works - Vox (2020). URL https://www.vox.com/2020/2/28/21154930/jennifer-doudna-crispr-gene-editing-babies.

[396] Ouzounis, C. A. Rise and Demise of Bioinformatics? Promise and Progress. *PLoS Computational Biology* **8** (2012). URL https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3343106/.

[397] Luan, E., Shoman, H., Ratner, D. M., Cheung, K. C. & Chrostowski, L. Silicon Photonic Biosensors Using Label-Free Detection. *Sensors (Basel, Switzerland)* **18** (2018). URL https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6210424/.

[398] Starr, M. These Incredible Real Tattoos Change Colour as Biomarkers Like Glucose Levels Shift (2019). URL https://www.sciencealert.com/there-is-now-an-actual-tattoo-that-can-change-colour-based-on-glucose-levels.

[399] Bhalla, N., Jolly, P., Formisano, N. & Estrela, P. Introduction to biosensors. *Essays in Biochemistry* **60**, 1–8 (2016). URL https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4986445/.

[400] Turin, L. *et al.* A Foresight Activity on Research in Quantum Biology (FarQBio). ESF Forward Look, European Science Foundation, Strasbourg (2015). URL https://pdfs.semanticscholar.org/dd61/6f945beacc23823ebd7fec64c19535b09c65.pdf?_ga=2.140450679.555855977.1579206493-1087385114.1579206493.

[401] Knopf, G. K. & Bassi, A. S. *Smart Biosensor Technology* (CRC Press, Baca Raton FL, 2018). URL https://www.crcpress.com/Smart-Biosensor-Technology/Knopf-Bassi/p/book/9781498774482.

[402] Emanuel, P. *et al.* Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DOD. Tech. Rep. CCDC CBC-TR-1599, TRADOC - US ARMY, Fort Eustis, VA (2019). URL https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/300458.

[403] Seidel, J. Future soldiers: human biotechnology push for defence | The Advertiser (2018). URL https://www.adelaidenow.com.au/news/national/the-biotechnology-revolution-is-here-and-so-are-superhumans/news-story/1c685c6fb7b545665764e62674f974ab.

[404] Ryan, M. & Keane, T. Biotechnology and Human Augmentation: Issues for National Security Practitioners (2019). URL http://intellibriefs.blogspot.com/2019/02/biotechnology-and-human-augmentation.html.

[405] Thorpe, J. B., Girling, K. D. & Auger, A. Maintaining Military Dominance In The Future Operating Environment: A Case For Emerging Human Enhancement Technologies That Contribute To Soldier Resilience. *Small Wars Journal* 18 (2017).

[406] Cook, M., Heshmat, S. & Solutions, C. T. The Symbiosis of Humans and Machines: Planning for Our AI-Augmented Future. Tech. Rep., The Center for the Future of Work (2019). URL https://www.cognizant.com/whitepapers/planning-for-our-ai-augmented-future-codex4744.pdf.

[407] Keller, J. DARPA is Eyeing a High-Tech Contact Lens Straight Out of 'Mission: Impossible' (2019). URL https://nationalinterest.org/blog/buzz/darpa-eyeing-high-tech-contact-lens-straight-out-mission-impossible-54617.

[408] Best, J. Robotic exoskeletons: Coming to a factory, warehouse or army near you, soon (2019). URL https://www.zdnet.com/article/robotic-exoskeletons-coming-to-a-factory-warehouse-or-army-near-you-soon/.

[409] Thilmany, J. Exoskeletons in Construction: Everything You Need to Know (2019). URL https://constructible.trimble.com/construction-industry/exoskeletons-for-construction-workers-are-marching-on-site.

[410] Husseini, T. US Army exoskeletons: which companies are designing military suits? (2019). URL https://defence.nridigital.com/global_defence_technology_apr19/military_exoskeletons_the_next_phase.

[411] Robitzski, D. The Army is spending millions on powered exoskeletons (2019). URL https://futurism.com/the-byte/army-soldiers-powered-exoskeletons.

[412] Maslen, H., Faulmüller, N. & Savulescu, J. Pharmacological cognitive enhancement—how neuroscientific research could advance ethical debate. *Frontiers in Systems Neuroscience* **8** (2014). URL https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4052735/.

[413] Dimkov, P. *The Philosophy of Human Cognitive Pharmacological Enhancement: The Genesis of Pharmacometaphysics* (PREPRINT, South-West University, AUS, 2018). URL https://www.researchgate.net/publication/324866218_The_Philosophy_of_Human_Cognitive_Pharmacological_Enhancement_The_Genesis_of_Pharmacometaphysics.

[414] Scharre, P. & Fish, L. Human Performance Enhancement (2018). URL https://www.cnas.org/publications/reports/human-performance-enhancement-1.

[415] Statt, N. Google opens its latest Google Glass AR headset for direct purchase (2020). URL https://www.theverge.com/2020/2/4/21121472/google-glass-2-enterprise-edition-for-sale-directly-online.

[416] Mohsin, M. 10 Social Media Statistics You Need to Know in 2020 [Infographic] (2019). URL https://www.oberlo.com/blog/social-media-marketing-statistics.

[417] Guzman, A. 6 ways social media is changing the world (2016). URL https://www.weforum.org/agenda/2016/04/6-ways-social-media-is-changing-the-world/.

[418] Biały, B. Social Media—From Social Exchange to Battlefield. *The Cyber Defense Review* **2**, 69–90 (2020). URL https://www.jstor.org/stable/10.2307/26267344.

[419] Plumer, B. A simple guide to CRISPR, one of the biggest science stories of the decade (2018). URL https://www.vox.com/2018/7/23/17594864/crispr-cas9-gene-editing.

[420] Guardian, T. Scientists use stem cells from frogs to build first living robots. *The Guardian* (2020). URL https://www.theguardian.com/science/2020/jan/13/scientists-use-stem-cells-from-frogs-to-build-first-living-robots.

[421] Kriegman, S., Blackiston, D., Levin, M. & Bongard, J. A scalable pipeline for designing reconfigurable organisms. *Proceedings of the National Academy of Sciences* **117**, 1853 (2020). URL http://www.pnas.org/content/117/4/1853.abstract.

[422] Yang, H. *et al.* Engineering macrophages to phagocytose cancer cells by blocking the CD47/SIRP. *Cancer Medicine* **8**, 4245–4253 (2019).

[423] Bextine, B. Insect Allies (2018). URL https://www.darpa.mil/program/insect-allies.

[424] Dove, A. In vitro veritas: Biosensors and microarrays come to life (2018). URL https://www.sciencemag.org/features/2018/03/vitro-veritas-biosensors-and-microarrays-come-life.

[425] Juengst, E. & Moseley, D. Human Enhancement. In Zalta, E. N. (ed.) *The Stanford Encyclopedia of Philosophy* (Metaphysics Research Lab, Stanford University, 2019), summer 2019 edn. URL https://plato.stanford.edu/archives/sum2019/entries/enhancement/.

[426] McCarty, K. Building a Better Soldier: Human Enhancement Technologies in the 21st Century. *Paideia* **1** (2014). URL http://digitalcommons.calpoly.edu/paideia/vol1/iss1/6.

[427] Ruck, H. (ed.) *Human Performance Modification: Review of Worldwide Research with a View to the Future* (National Academies Press, Washington, D.C., 2012). URL http://www.nap.edu/catalog/13480.

[428] Mortier, R., Haddadi, H., Henderson, T., McAuley, D. & Crowcroft, J. Human-Data Interaction: The Human Face of the Data-Driven Society. *arXiv:1412.6159 [cs]* (2014). URL http://arxiv.org/abs/1412.6159. ArXiv: 1412.6159.

[429] Antón, P. S., Silberglitt, R. S. & Schneider, J. *The global technology revolution: bio/nano/materials trends and their synergies with information technology by 2015* (RAND, Santa Monica, CA, 2001). URL https://www.rand.org/pubs/monograph_reports/MR1307.html.

[430] of Medical Sciences, T. A. Human enhancement and the future of work: Report from a joint workshop hosted by the Academy of Medical Sciences, the British Academy, the Royal Academy of Engineering and the Royal Society. Tech. Rep., Academy of Medical Sciences; British Academy; Royal Academy of Engineering; The Royal Society (2012). URL https://acmedsci.ac.uk/file-download/35266-135228646747.pdf.

[431] Burnett, M. *et al.* Advanced Materials and Manufacturing – Implications for Defence to 2040. Tech. Rep. DST-Group-GD-1022, Defence Science and Technology Group (2018). URL https://www.dst.defence.gov.au/publication/advanced-materials-and-manufacturing-%E2%80%93-implications-defence-2040.

[432] NATURE. Nature Index 2019 Materials Science. *NATURE* **576** (2019). URL https://www.nature.com/collections/hdjhficcjj.

[433] Harper, T. 2-Dimensional Materials Create New Tools for Technologists - Scientific American (2016). URL https://www.scientificamerican.com/article/2-dimensional-materials-create-new-tools-for-technologists/.

[434] Garner, C. Graphene, 2D Materials and Carbon Nanotubes: IDTechEx's latest insights (2019). URL https://www.scitecheuropa.eu/graphene-2d-materials/95799/.

[435] IOPScience. Focus Issues in 2D Materials - 2D Materials - IOPscience (2020). URL https://iopscience.iop.org/journal/2053-1583/page/Focus-issues.

[436] van Bremen, R. PhD Defence Rik van Bremen | NANOSCALE PROPERTIES OF 2D MATERIALS | Science and Technology Faculty (TNW) (2020). URL https://www.utwente.nl/en/tnw/events/2020/1/142446/phd-defence-rik-van-bremen-nanoscale-properties-of-2d-materials.

[437] Akhtar, M. *et al.* Recent advances in synthesis, properties, and applications of phosphorene. *npj 2D Materials and Applications* **1**, 1–13 (2017). URL https://www.nature.com/articles/s41699-017-0007-5.

[438] Park, H. J. *et al.* One-dimensional hexagonal boron nitride conducting channel | Science Advances. *Science Advances* **6** (2020). URL https://advances.sciencemag.org/content/6/10/eaay4958.

[439] Ghaffarzadeh, K. Graphene: can China retain its leading position? (2019). URL https://www.idtechex.com/en/research-article/graphene-can-china-retain-its-leading-position/17235.

[440] Crew, I. About Graphene Flagship (2019). URL http://graphene-flagship.eu:80/project/Pages/About-Graphene-Flagship.aspx.

[441] Mutalik, P. When Magic Is Seen in Twisted Graphene, That's a Moiré (2019). URL https://www.quantamagazine.org/when-magic-is-seen-in-twisted-graphene-thats-a-moire-20190620/. Library Catalog: www.quantamagazine.org.

[442] Wogan, T. Squeezed graphene becomes a superconductor (2019). URL https://physicsworld.com/a/squeezed-graphene-becomes-a-superconductor/.

[443] Illinois, U. o. Crumpled graphene makes ultra-sensitive cancer DNA detector (2020). URL https://phys.org/news/2020-03-crumpled-graphene-ultra-sensitive-cancer-dna.html.

[444] Zirath, H. *et al.* Graphene Roadmap. Tech. Rep., Swedish Electronics (2019). URL https://siografen.se/app/uploads/2019/06/SIO-Grafen-Roadmap-Swedish-Electronics_v1.3.pdf.

[445] Bonaccorso, F., Sun, Z., Hasan, T. & Ferrari, A. C. Graphene photonics and optoelectronics. *Nature Photonics* **4**, 611–622 (2010). URL https://doi.org/10.1038/nphoton.2010.186.

[446] Fogden, S. A faster future: Graphene based optoelectronics (2016). URL https://graphene-flagship.eu/news/Pages/A-Faster-Future-Graphene-Based-Optoelectronics.aspx.

[447] Lv, J., Zhang, T., Zhang, P., Zhao, Y. & Li, S. Review Application of Nanostructured Black Silicon. *Nanoscale Research Letters* **13**, 110 (2018). URL https://nanoscalereslett.springeropen.com/articles/10.1186/s11671-018-2523-4.

[448] Shen, Z.-X. Topological Insulators | Shen Laboratory (2019). URL https://arpes.stanford.edu/research/quantum-materials/topological-insulators.

[449] Übel, M. v. The 3D Printing Materials Guide | All3DP (2019). URL https://all3dp.com/1/3d-printing-materials-guide-3d-printer-material/.

[450] Smithers. Reasons Why 3D Printing is Reaching Mainstream (2017). URL https://www.smithers.com/resources/2017/jul/reasons-why-3d-printing-is-reaching-the-mainstream.

[451] Allison, A. & Scudamore, R. Additive Manufacturing: Strategic Research Agenda. AM SRA Consultation Document, AM Platform (2014).

[452] Hague, R., Reeves, P. & Jones, S. Mapping UK Research and Innovation in Additive manufacturing. Tech. Rep., Innovate UK (2016). URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/505246/CO307_Mapping_UK_Accessible.pdf.

[453] Scott, C. DARPA Highlights its Work with 3D Printing and Advanced Manufacturing - 3DPrint.com | The Voice of 3D Printing / Additive Manufacturing (2018). URL https://3dprint.com/226516/darpa-3d-printing-manufacturing/.

[454] SpaceX. SpaceX Launches 3D-Printed Part to Space, Creates Printed Engine Chamber | SpaceX (2014). URL https://www.spacex.com/news/2014/07/31/spacex-launches-3d-printed-part-space-creates-printed-engine-chamber-crewed.

[455] Jamie, D. 3D Printing: The Future of Construction - 3Dnatives (2018). URL https://www.3dnatives.com/en/3d-printing-construction-310120184/.

[456] Maxley, K. "Print Me a Cruiser" : The Future of the US Fleet (2013). URL https://www.engineering.com/3DPrinting/3DPrintingArticles/ArticleID/5542/Print-Me-a-Cruiser-The-Future-of-the-US-Fleet.aspx.

[457] Joel, C. Australian researches taking 4D printing to the next level (2019). URL https://www.3dprintersonlinestore.com/australian-researches-taking-4d-printing-to-the-next-level?gclid=CjwKCAiA1fnxBRBBEiwAVUouUlumELIsNBX6tXZKrFZXPgVrKYPi20ZFd0M5hsvp_1ZdjerU-kG6ehoCj9wQAvD_BwE.

[458] Soutter, W. Nanotechnology in the Military (2012). URL https://www.azonano.com/article.aspx?ArticleID=3028.

[459] Paschkewitz, J. S. Materials with Controlled Microstructural Architecture (MCMA) (2018). URL https://www.darpa.mil/program/materials-with-controlled-microstructural-architecture.

[460] Vicente, P. L. Additive manufacturing in defence (2019). URL https://www.eda.europa.eu/webzine/issue14/cover-story/additive-manufacturing-in-defence.

[461] Hallex, M. Digital Manufacturing and Missile Proliferation. Public Interest Report, Federation of American Scientists, Washington DC (2013). URL https://fas.org/pir-pubs/digital-manufacturing-and-missile-proliferation/. Library Catalog: fas.org.

[462] Lee, S. Suzanne Lee: Why "biofabrication" is the next industrial revolution | TED Talk (2019). URL https://www.ted.com/talks/suzanne_lee_why_biofabrication_is_the_next_industrial_revolution/transcript?language=en.

[463] Aliberti, K. & Bruen, T. L. Energy on Demand. *Army Logistician* **39** (2007). URL https://alu.army.mil/alog/issues/JanFeb07/energy_demand.html.

[464] Stringer, J. & Horton, L. Basic research needs to assure a secure energy future. A report from the Basic Energy Sciences Advisory Committee. Tech. Rep. 811872, Oak Ridge National Lab., TN (US) (2003). URL http://www.osti.gov/servlets/purl/811872-ezwpeg/native/.

[465] Lumb, D. US Military tests system for on-demand 3D-printed drones (2017). URL https://www.engadget.com/2017/12/18/us-military-tests-system-for-on-demand-3d-printed-drones/. Library Catalog: www.engadget.com.

[466] Singh, S. Here's how 3D printers could become a global nonproliferation nightmare - Atlantic Council (2018). URL https://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-how-3d-printers-could-become-a-global-nonproliferation-nightmare/.

[467] Duchêne, V. *et al.* Identifying current and future application areas, existing industrial value chains and missing competences in the EU, in the area of additive manufacturing (3D-printing). Tech. Rep., European Union, Brussels (2016). URL http://publications.europa.eu/resource/cellar/b85f5e09-7e2b-11e6-b076-01aa75ed71a1.0001.01/DOC_1.

[468] Silberglitt, R. S. & (U.S.), N. I. C. (eds.) *The global technology revolution 2020, executive summary: bio/nano/materials/information trends, drivers, barriers, and social implications* (RAND Corporation, Santa Monica, CA, 2006). OCLC: ocm65537907.

[469] Armitage, C. Remastering matter: materials science goes to market. *Nature* **576**, S19–S19 (2019). URL https://www.nature.com/articles/d41586-019-03763-2.

[470] Savage, N. Tomorrow's industries: from OLEDs to nanomaterials. *Nature* **576**, S20–S22 (2019). URL https://www.nature.com/articles/d41586-019-03764-1.

[471] Poincaré, H. *La science et l'Hypothèse*. Bibiliothèque de Philosophie Scientifique (Ernest Flammarion, Paris, 1917). URL http://henripoincarepapers.univ-lorraine.fr/chp/hp-pdf/hp1917sh.pdf.

[472] Tocher, M. & Goffettre, L. R. Technology Trends Survey - A Food-for-Thought Paper to Support the NATO Defence Planning Process (2015). URL https://www.act.nato.int/images/stories/events/2012/fc_ipr/technology_trend_survey_v3.pdf.

[473] Schreiber, M. Wolfram Demonstrations Project:Simple Three-Letter Cube (2008). URL https://demonstrations.wolfram.com/SimpleThreeLetterCube/.

[474] Collet-Billon, L. Document de Présentation de l'Orientation de la S&T: Période 2014-2019. Tech. Rep., Direction générale de l'armement, Paris (2013). URL http://www.defense.gouv.fr/content/download/463109/7360240/file/post_dga_2014_2019.pdf.

[475] Winter, M. Naval S&T Strategy - Innovations for the Future Force. Tech. Rep., Office of Naval Research, Washington, D.C. (2015). URL https://apps.dtic.mil/dtic/tr/fulltext/u2/a619266.pdf.

[476] Cocking, J. DST Group and Industry – partnering for next generation technologies (2018). URL https://crca.asn.au/wp-content/uploads/2018/05/JanisCocking.pdf.

[477] Gallo, M. E. Defense Advanced Research Projects Agency: Overview and Issues for Congress. CRS Report R45088, Congressional Research Service, Washington, D.C. (2018). URL https://fas.org/sgp/crs/natsec/R45088.pdf.

[478] UK, M. MOD Area of Research interest (2018). URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673821/20171124-MOD_ARI-O.pdf.

[479] Durrant-Whyte, H. Science and Technology Strategy 2017. Tech. Rep., UK Ministry of Defence (2017).

[480] Panetta, K. Gartner Top 10 Strategic Technology Trends for 2020 (2019). URL https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/.

[481] Goasduff, L. Artificial intelligence trends (2019). URL https://www.gartner.com/smarterwithgartner/top-trends-on-the-gartner-hype-cycle-for-artificial-intelligence-2019/.

[482] Augustyn, J. Emerging Science and Technology Trends: A Synthesis of Leading Forecasts-5th Edition. Tech. Rep., Office of the Deputy Assistant Secretary of the Army (Research & Technology), Washington (2019). URL https://apps.dtic.mil/dtic/tr/fulltext/u2/1078879.pdf.

[483] Kott, A. *et al.* Potential Science and Technology Game Changers for the Ground Warfare of 2050: Selected Projections Made in 2017. Technical Report ARL-TR-8283, Army Research Laboratory (2018). URL https://www.arl.army.mil/arlreports/2018/ARL-TR-8283.pdf.

[484] The Mad Scientist Initiative. 52. Potential Game Changers (2018). URL https://madsciblog.tradoc.army.mil/52-potential-game-changers/.

[485] Kindvall, G., Lindberg, A., Trane, C. & Westman, J. Exploring Future Technology Development. Tech. Rep. FOI-R–4196–SE, FOI (2017). URL https://www.foi.se/rest-api/report/FOI-R--4196--SE.

[486] Auger, A. Emerging Technologies in the FOE - CANIC 2019 (2019).

[487] Gokhberg, L., Sokolov, A. & Chulok, A. Russian S&T Foresight 2030: Looking for New Drivers of Growth. *Foresight* **91**, 441–446 (2017). URL https://www.emerald.com/insight/content/doi/10.1108/FS-07-2017-0029/full/html.

[488] OECD. Innovation statistics and indicators - OECD (2017). URL https://www.oecd.org/sti/inno/inno-stats.htm.

[489] Webb, A. 2020 Tech Trends Report - 13th Annual Edition. Tech. Rep., Future Today Institute, New York (2020). URL https://futuretodayinstitute.wetransfer.com/downloads/14f623f321798cdb7a4370c3b140f47920200225171335/6498cf.

[490] Likens, S. The Essential Eight technologies (2019). URL https://www.pwc.com/gx/en/issues/technology/essential-eight-technologies.html.

[491] DGRIS. Strategic Horizons. Tech. Rep., Ministere des Armees, Paris (2013). URL https://www.defense.gouv.fr/english/dgris/strategic-thinking/defense-foresight/en/strategic-horizons.

[492] Cag, D. 11 Awesome Disruptive Technology Examples 2019 (MUST READ) (2019). URL https://richtopia.com/emerging-technologies/11-disruptive-technology-examples.

[493] Webber, A. Emergent v. Disruptive Technologies | Asymmetric Insights (2011). URL http://www.asymmetricinsights.org/2011/08/emergent-v-disruptive-technologies/.

[494] Economist, T. What NATO is doing to keep abreast of new challenges. *The Economist* (2019). URL https://www.economist.com/special-report/2019/03/14/what-nato-is-doing-to-keep-abreast-of-new-challenges.

[495] Alleslev, L. NATO Science and Technology: Maintaining the Edge and Enhancing Alliance Agility. Special Report 183 STC 18 E rev.1 fin, NATO Parliamentary Assembly, Brussels (2018). URL https://www.nato-pa.int/download-file?filename=sites/default/files/2018-12/183%20STC%2018%20E%20-%20NATO%20SCIENCE%20AND%20TECHNOLOGY%20EDGE%20-%20ALLESLEV%20REPORT.pdf.

[496] Collingridge, D. *The Social Control of Technology* (St. Martin's Press, 1980). URL https://books.google.be/books?id=hCSdAQAACAAJ.

[497] UNESCO. UNESCO Science Report (2015). URL https://en.unesco.org/unescosciencereport.

Symbols, Abbreviations and Acronyms

$\hbar$	$h/(2\pi)$
c	Speed of Light in a Vacuum ($2.99792458 \times 10^{+8} m/s$)
h	Planck Constant ($6.62607004 \times 10^{-34} m^2 kg/s$)
2-D *or* 2D	2-Dimensional
3-D *or* 3D	3-Dimensional
4-D *or* 4D	4-Dimensional
5G	Fifth Generation (Wireless Technologies)
5V	Volume, Velocity, Variety, Veracity and Visualisation (Challenges of Big Data)
A2AD *or* A2/AD	Anti-Access and Area Denial
ACT	Allied Command Transformation
ADF	Australian Defence Force
AFRL	Air Force Research Lab (USA)
AGI	Artificial General Intelligence
AI	Artificial Intelligence
AI HLEG	Artificial Intelligence High Level Experts Group
AIoT	Artificial Intelligence of Things
AIS	Automatic Identification System
AM	Additive Manufacturing
AMRG	Additive Manufacturing Research Group
ARL	Army Research Lab (USA)
ASAT	Anti-Satellite Weapons

ASW	Anti-Submarine Warfare
BDA	Battle Damage Assessment
BDAA	Big Data and Advanced Analytics
BHET	Bio and Human Enhancement Technologies
BLUE	Friendly Forces
C2	Command & Control
C3	Consultation, Command and Control
C4ISR	Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR)
CBRN	Chemical, Biological, Radiological and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CI	Computational Imaging
CMRE	Centre for Maritime Research and Experimentation
COA	Courses of Action
COP	Common Operating Picture
CPoW	Collaborative Program of Work
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CSBA	Center for Strategic and Budgetary Assessments
CWA	Chemical Warfare Agent
DARPA	Defense Advanced Research Projects Agency (US)
DCDC	Development, Concepts and Doctrine Centre
DEW	Directed Energy Weapon
DGA	Direction Générale de L'armement
DGRIS	Direction Générale des Relations Internationales et de la Stratégie
DIA	Defense Intelligence Agency
DIM	Deception, Identification & Monitoring
DIME	Diplomatic, Information, Military and Economic
DNA	Deoxyribonucleic Acid
DND	Canadian Department of Defence
DOD	US Department of Defence
DOTMLPF-I	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability

DRDC	Defence Research and Development Canada
DST	Defence Science and Technology Group (AUS)
dstl	Defence Science and Technology Laboratory (UK)
DSTO	Defence Science and Technology Organisation (AUS)
EDA	European Defence Agency
EDT	Emerging And/Or Disruptive Technology
ELINT	Electronic Intelligence
EM	Electromagnetic
EO	Electro-Optical
EOD	Explosive Ordnance Disposal
EW	Electronic Warfare
FAS	Federation of American Scientists
FLIA	Foundation for Law & International Affairs
fm	Femtometer $(10^{-15}m)$
FOI	Foi Totalförsvarets Forskningsinstitut / Swedish Defence Research Agency
GAI	Generalised Artificial Intelligence
GAN	Generative Adversarial Network
GAO	(US) General Accounting Office
GDP	Gross Domestic Product
GEO	Geosynchronous Equatorial Orbit
GNSS	Global Navigation Satellite System
GoC	Government of Canada
GPS	Global Positioning System
HALE	High Altitude Long Endurance
HCM	Hypersonic Cruise Missile
HDMS	His/Her Danish Majesty's Ship
HEO	Highly Elliptical Orbit
HET	Human Enhancement Technologies
HGV	Hypersonic Glide Vehicle
HT	Hypersonic Technologies
I2D2	Intelligent, Interconnected, Distributed & Digital
IED	Improvised Explosive Device

IoT	Internet of Things
IP	Intellectual Property
IR	Infrared
IS/ESC	NATO International Staff / Emerging Security Challenges
ISR	Intelligence, Surveillance and Reconnaissance
ISTAR	Intelligence, Surveillance, Targeting and Reconnaissance
ITW&AA	Integrated Tactical Warning and Attack Assessment
JAIC	(NATO) Joint Artificial Intelligence Center
JALLC	(NATO) Joint Analysis and Lessons Learned Centre
JAPCC	(NATO) Joint Air Power Competence Centre
LEO	Low Earth Orbit
LIDAR	Light Detection and Ranging
M&S	Modelling and Simulation
Mach 1	Speed of Sound (340.3 m/s; 1,235 km/s; 767 mph) In Dry Air at Mean Sea Level and Standard Temperature of 15°C)
MASINT	Measurement and Signature Intelligence
MC	Military Committee
MCM	Mine Countermeasures
MEO	Medium Earth Orbit
MIMO	Multiple-Input and Multiple-Output,
MIoP	Military Instruments of Power
ML	Machine Learning
MOD	(UK) Ministry of Defence
mTBI	Mild Traumatic Brain Injury
NAC	North Atlantic Council
NASC	Naval Air Systems Command
NATO	North Atlantic Treaty Organization
NCIA	NATO Communication and Information Agency
NDPP	NATO Defence Planning Process
NGO	Non-Governmental Organisations
nm	Nano-Metre ($10^{-9}m$)
NRC	National Research Council (Canada)

OCS	NATO Office of The Chief Scientist
OECD	The Organisation for Economic Co-Operation and Development
OGD	Other Government Departments
ONR	Office of Naval Research (USA)
OODA	Observe, Orient, Decide, and Act
OR&A	Operational (Operations) Research & Analysis
OTH	Over-The-Horizon
PAL	Phase Alternating Line
PCE	Physiological and Pharmacological Cognitive Enhancements
PCL	Passive Coherent Location (Radar)
pm	Picometer ($10^{-12}m$)
PNT	Positioning, Navigation and Timing
PTSD	Post-Traumatic Stress Disorder
QC	Quantum Communication
QIS	Quantum Information Science
QKD	Quantum Key Distribution
QO	Quantum Optics
QT	Quantum Technologies
R&D	Research and Development
RAP	Recognised Air Picture
RAS	Robotics and Autonomous Systems
RCAF	Royal Canadian Air Force
RDDC	Recherche et Développement Pour La Défense Canada
RDS	Research and Development Statistics
RED	Hostile Forces
RF	Radio Frequency
ROE	Rules of Engagement
RSGB	Royal Society (Great Britian)
S-AIS	Satellite - Automatic Identification System
S&T	Science and Technology
SA	Situational Awareness
SACEUR	Supreme Allied Commander Europe

SACT	Supreme Allied Commander Transformation
SAR	Synthetic-Aperture Radar
ST	Space Technologies
STO	Science & Technology Organization
TBM	Theatre Ballistic Missile
TCPED	Tasking, Collection, Processing, Exploitation, and Dissemination
TFA	Technology Focus Area
THz	Terahertz ($10^{12} Hertz$)
TOE	Targets of Emphasis
TRADOC	U.S. Army Training and Doctrine Command
TRL	Technology Readiness Levels
TSTO	Two State to Orbit
TWC	Technology Watch Card
UAV	Unmanned Air Vehicles
UCAV	Unmanned Combat Aerial Vehicle
UGV	Unmanned Ground Vehicle
UK	United Kingdom
UMS	Unmanned Maritime Systems
UNESCO	United Nations Educational, Scientific and Cultural Organization
US	United States
USA	United States of America
USD	US Dollars
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicles
UV	Ultraviolet
vKHS	Von Kármán Horizon Scan
VV&A	Verification, Validation, & Accreditation
WEF	World Economic Forum
µm	micrometer($10^{-6} m$)


ASSESSMENT
TECHNOLOGIES
TRAINING
TECHNOLOGY
MODELLING
NATO
APPLICATIONS
VEHICLES
SUPPORT
MILITARY
EO
IR
RADAR
SIMULATION
DESIGN
SPACE
CYBER
ANALYSIS
SYSTEMS
OPERATIONAL
DEVELOPMENT
DEFENCE
FUTURE
OPERATIONS
MANAGEMENT