UNIDIR

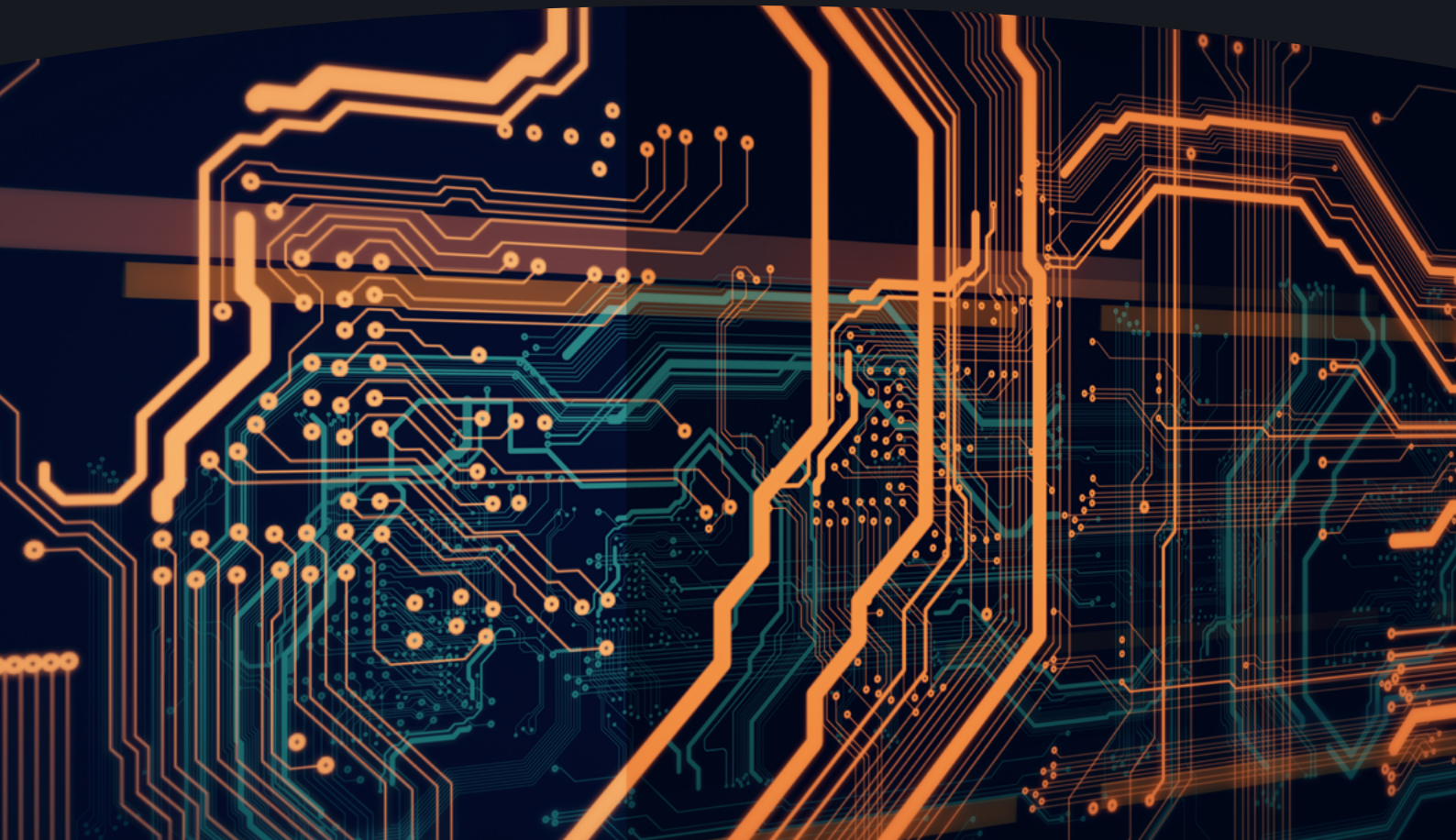
Funded by
the European Union

FULL REPORT

Enabling Technologies and International Security: A Compendium

2023 Edition

WENTING HE



Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This publication was funded by the European Union as part of UNIDIR's Security and Technology Programme, which is supported by the governments of the Czech Republic, Germany, Italy, the Netherlands, Switzerland and Norway, and by Microsoft.

The author extends sincere gratitude to Dr. Giacomo Persi Paoli for his invaluable guidance and insightful contributions throughout the drafting process. Special thanks also go to Elia Duran-Smith for her assistance with the background research. Furthermore, the author wishes to thank James Black and Sarah Grand-Clément for their thorough review and constructive feedback, which greatly enriched the final work.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual author. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, or the European Union, nor their staff members or sponsors.

Citation

He, Wenting. "Enabling Technologies and International Security: A Compendium (2023 edition)". Geneva, Switzerland: UNIDIR, 2024.

Author

Wenting He

Associate Researcher, Security and Technology

Wenting He is an Associate Researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, Wenting worked for the United Nations Office at Geneva and the Global Initiative against Transnational Organized Crime. She holds a Master's Degree in International Affairs from the Graduate Institute of International and Development Studies in Geneva, as well as a Bachelor's Degree in Diplomatic Studies from China Foreign Affairs University in Beijing. Her areas of expertise include multilateral disarmament and arms control, diplomatic practices, international policy analysis, statistical methods and emerging technologies.

Acronyms & Abbreviations

5G	Fifth-generation cellular networks
6G	Sixth-generation cellular networks
AI	Artificial intelligence
AIAAS	Artificial Intelligence as a Service
AR	Augmented reality
AWS	Amazon Web Services
CPU	Central processing unit
CSP	Cloud service provider
DOD	Department of Defense (United States)
EUV	Extreme ultraviolet
GNSS	Global navigation satellite system
GPU	Graphics processing unit
HTS	High-temperature superconductors
IAAS	Infrastructure as a service
ICRC	International Committee of the Red Cross
ICT	Information and communications technology
IOMT	Internet of Military Things
IOT	Internet of Things
ISR	Intelligence, surveillance and reconnaissance
JWCC	Joint Warfighting Cloud Capability
LEO	Low Earth Orbit
MRI	Magnetic resonance imaging
NEMS	Nanoelectromechanical systems
NM	Nanometre
NPU	Neural processing units
PAAS	Platform as a service
PQC	Post-quantum cryptography
QKD	Quantum key distribution
SAAS	Software as a service
SOC	System-on-chip
TPU	Tensor processing unit
TSMC	Taiwan Semiconductor Manufacturing Company
UAV	Uncrewed aerial vehicle
VR	Virtual reality

Contents

Executive Summary

Technological advancements in areas such as advanced materials, microchips, sensors and connectivity infrastructure are enabling innovation across other technology areas, not least in information and communications technologies (ICTs), artificial intelligence (AI) and autonomous systems. These enabling technologies are reshaping the digital landscape and hold potential applications in the military domain. While progress has been made in addressing the security implications of ICTs and AI within various intergovernmental processes, comparatively less attention has been devoted to the underlying technologies that are facilitating or driving their further development. This underscores the urgent need for a more thorough and comprehensive examination of enabling technologies as well as their potential impacts on international security.

To address this knowledge gap, this compendium is dedicated to the identification and analysis of the most salient advancements in enabling technologies, with a particular emphasis on those still in their early stages of development or application. The compendium explores four categories of enabling technologies: advanced materials (semiconductors, superconductors and nanotechnology), parts and components (microchips and sensors), processing and computing (cloud, edge and quantum computing), and infrastructure (fifth- and sixth-generation telecommunications (5G and 6G), the Internet of Things, cloud infrastructure and satellite communications).

The compendium highlights several overarching trends and developments across the technology domains under examination. The ongoing trend of hardware miniaturisation is leading to the creation of increasingly compact and efficient devices, facilitating the widespread integration of enabling technologies in military systems. These technologies offer significant enhancements in military capabilities and the potential to strengthen international security efforts. However, challenges arise from the potential for increased technological competition among States and from cybersecurity risks and vulnerabilities in the global supply chain that are associated with enabling technologies. While the role of the private sector is crucial, collaboration on dual-use technologies may introduce new risks such as jeopardising sensitive military information.

Continuous monitoring and analysis of emerging trends are therefore essential for establishing effective governance frameworks that balance the opportunities and risks that enabling technologies present.

1. Introduction

Technologies such as advanced materials, microchips and sensors, computing power and connectivity infrastructure are enabling or driving innovation and the development of capabilities across other technology areas, not least in information and communications technologies (ICTs), artificial intelligence (AI) and autonomous systems. The development of enabling technologies is revolutionising the digital ecosystem, expanding the possibilities for their being developed and applied for military purposes.[1] As these technologies continue to advance, it becomes increasingly important to address their implications for international peace and security. Continuous horizon scanning is essential to harnessing the benefits of these technologies while mitigating their potential risks.

In the 2023 report on "Current developments in science and technology and their potential impact on international security and disarmament efforts", the United Nations Secretary-General underscores the continuing concerns that developments in science and technology of relevance to security and disarmament are outpacing the capacity of normative and governance frameworks to manage the risks.[2] While various intergovernmental processes have made strides in tackling the security implications of ICTs and AI, comparatively less attention has been devoted to the underlying technologies that are enabling or driving their further developments. This underscores the urgent need for a more thorough and comprehensive examination of enabling technologies as well as their potential impacts on international security.

In an effort to bridge the knowledge gap, the present compendium is dedicated to the identification and analysis of the most salient advancements in enabling technologies. This includes those still in the early stages of their development or application but which are anticipated to have an important impact on international peace and security. This compendium is exclusively focused on exploring the first-order effects of enabling technologies on the digital ecosystem, specifically with relevance to international peace and security. However, certain technology areas may have broader implications beyond what is covered in the present report.

In the subsequent chapters, the compendium delves into four categories of enabling technologies. Category I includes advanced materials, such as semiconductors, superconductors and nanotechnology. Category II looks into parts and components, encompassing microchips and sensors. Category III covers processing and computing, that is, cloud, edge and quantum computing. Category IV is for infrastructure, from fifth- and sixth-generation telecommunications (5G and 6G), via the Internet of Things (IoT) and cloud infrastructure, to satellite communications. Each chapter presents a comprehensive analysis of the technology under examination, including the latest developments and relevant military applications, followed by an assessment of the potential implications for international security. The compendium concludes with an overarching examination of general trends and developments in the realm of enabling technologies.

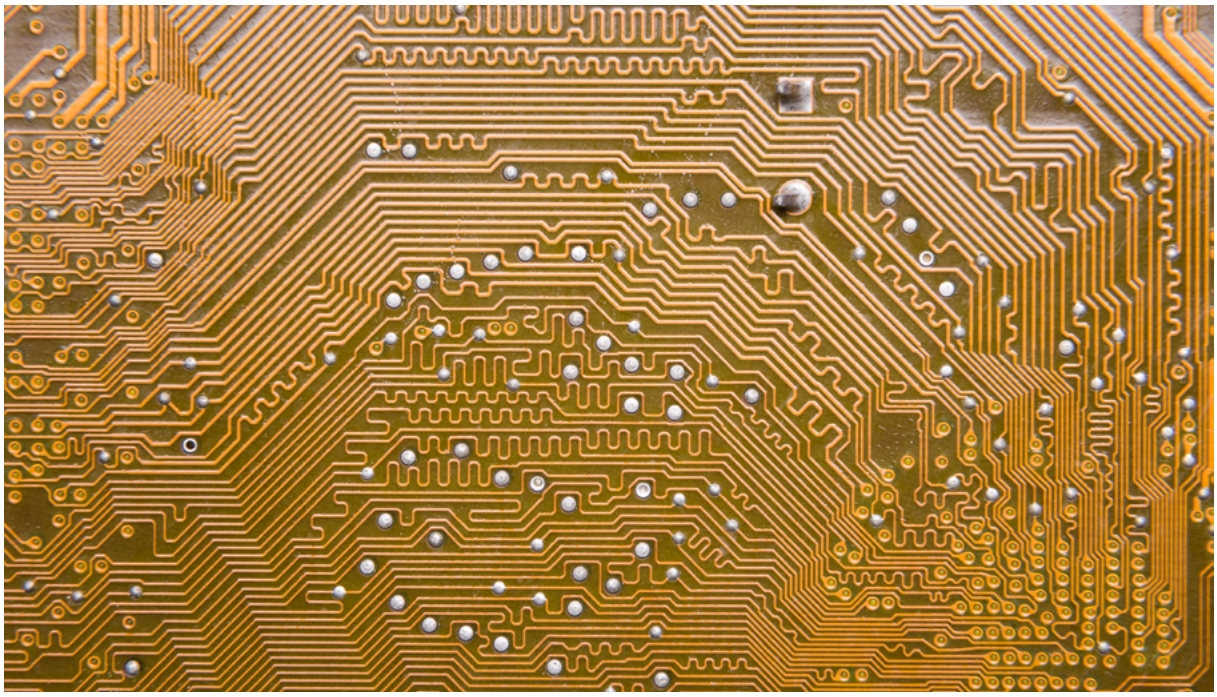
---

1 For the purpose of this compendium, enabling technologies are defined as those that enable or drive innovation and the development of capabilities across other technology areas within the scope of the work conducted by UNIDIR's Security and Technology Programme: cyber, AI and autonomy as well as system integration.

2 UNGA (2023).

2. Category I: Advanced Materials

2.1 Semiconductors



Semiconductors belong to a class of materials characterised by electrical conductivity properties that fall between those of conductors (e.g., metals) and insulators (e.g., glass). The electrical conductivity of a semiconductor can be controlled and modified, enabling it to serve as a building block for modern electronic devices and components including diodes, transistors and integrated circuits.

The unique electrical properties of semiconductors have transformed the technology landscape, leading to the development of increasingly compact, potent and energy-efficient electronic devices and systems. In the electronics industry, silicon is the most commonly used semiconductor material, but other materials such as gallium arsenide and germanium are also used in specialised applications. Silicon wafers often provide a foundation for microchip manufacturing and play an essential role in the functioning of digital technologies.

The process node of semiconductors, now often measured in nanometres (nm),[3] is a critical factor in semiconductor technology. Reduced process nodes allow for more transistors to be packed onto a single chip, which

[3] One nanometre is equivalent to one thousandth of a micrometre, or one billionth of a metre.

often improves performance and energy efficiency. Semiconductor node size has reduced significantly over the decades, from the initial measurement in micrometres (μm)[4] to the current, most cutting-edge level of 3-nm technology.[5] Taiwan Semiconductor Manufacturing Company (TSMC), one of the most advanced semiconductor manufacturers, is planning to produce the next-generation 2-nm semiconductors starting in 2025. This is projected to achieve processing speeds that are 10–15 per cent higher than those of 3-nm chips.[6]

The driving force behind the process node evolution is what has become known as Moore's Law. This is an empirical observation by Gordon Moore, one of Intel's co-founders, that the number of transistors on a microchip has historically tended to double approximately every two years. The law therefore claims that the computing performance will continue to grow while the cost of computers decreases. Even though the theory has largely held true into the 21st century, engineers have begun to reach the limits of traditional semiconductor materials within the current understanding of the laws of physics. As such, some observers have even proclaimed the demise of Moore's Law.[7] The industry is now seeking innovative solutions to pursue future semiconductor improvements.

In place of silicon, other materials have been identified as potential alternatives to meet the increasing demands of computing power. Compound semiconductors, for example, combine multiple elements to produce materials capable of outperforming silicon. Such materials are poised to play a pivotal role in advancing new connectivity technologies and autonomous vehicles.[8] Gallium arsenide, the second most commonly used semiconductor material after silicon, is a compound known for its superior electron mobility, leading to greater efficiency than silicon. It also exhibits a higher tolerance to overheating. However, large-scale production of gallium arsenide will need to overcome significant challenges, including reliance on toxic chemicals, raising concerns about impacts on public health and the environment.[9]

Ongoing research efforts are exploring novel materials that show significant potential in enabling the development of increasingly compact and efficient devices. Recent studies have highlighted the effectiveness of a material known as cubic boron arsenide in addressing certain limitations that traditional silicon-based semiconductors pose, with the potential to become "the best semiconductor material ever found".[10] Despite the promising properties, cubic boron arsenide is currently in the experimental phase, leaving its real-world applications yet to be fully determined. Alongside this, other emerging semiconductor materials are also gaining traction, including high-power gallium nitride, antimonide-based and bismuthide-based materials, and two-dimensional (2D) materials such as graphene.[11]

---

4 For instance, Intel's 4004 processor launched in 1971: **https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html**

5 As of September 2023, only two companies in the world are able to manufacture 3-nm semiconductors: TSMC (**https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm**) and Samsung (**https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture**).

6 Ryugen, Hideaki (2023).

7 Arcuri and Shivakumar (2022).

8 IEEE (n.d.-a).

9 IEEE (n.d.-b).

10 Chandler (2022).

11 IEEE (n.d.-b).

These materials offer distinct physical properties that have proven advantageous in specific applications. Nevertheless, their widespread use is hindered by cost implications and the complexity of their production.

The continued innovation in semiconductor materials will play a pivotal role in future military systems. Semiconductors have concrete applications in an array of critical components of electronic devices, ranging from sensors, actuators and memory chips to electro-optical systems and microcontrollers.[12] These semiconductors form the backbone of cutting-edge electronic devices that feature prominently in sophisticated military systems, including high-speed communications devices, radar systems and precision-guided weaponry. Moreover, semiconductor technology serves as a catalyst for transformative innovations such as artificial intelligence and the Internet of Things (IoT). The emergence of new semiconductor materials thus holds the potential to strengthen national defence capabilities, although it may also usher in a new era of technological competition among States.

In addition, supply chain vulnerabilities currently present a key challenge. The semiconductor supply chain is a highly complex and interconnected global network that involves various production stages and companies from different regions. It is also characterised by a high degree of specialisation, with, for instance, a concentration of advanced semiconductor production facilities in East Asia. Any disruptions to the manufacturing capabilities in the region, whether stemming from geopolitical tensions or natural disasters, could have a negative impact on the availability of semiconductors and have severe consequences for national security. However, the development of alternative semiconductor materials has the potential to reshape the existing paradigm and increase diversification within the global supply chain.

Semiconductors: Highlights for 2023

- Continuous advancements are under way in the creation of more compact and efficient semiconductors. Leading semiconductor manufacturers such as **TSMC** and **Samsung** are actively pursuing the development of next-generation 2-nm semiconductor technology, projected to increase processing speeds by 10–15 per cent compared to the currently most advanced 3-nm semiconductors.
- Silicon remains the most commonly used semiconductor material, but it is approaching its physical limitations. Ongoing research efforts are exploring novel semiconductor materials that hold the potential for improved performance, including **cubic boron arsenide** and **2D materials**.
- The semiconductor supply chain is vulnerable to disruptions due to its complex and interconnected nature, which can present a significant challenge to national security. However, the exploration of alternative semiconductor materials could potentially enhance diversification in the global supply chain.

[12] Gargeyas (2022).

2.2 Superconductors

Superconductors are materials that can conduct electricity without any resistance or energy loss and can repel magnetic fields when cooled below a specific critical temperature. This unique property allows an electric current to flow indefinitely within a superconductor.

The exceptional electromagnetic characteristics of superconductors have the potential to enhance various fields, including electronics, quantum computing, energy transmission and storage, and magnetic resonance imaging (MRI) technology. However, their practical use is limited for now by the requirement for extremely low temperatures, which necessitates expensive cryogenic engineering and high energy consumption for the cooling process. Most superconductor materials exhibit critical temperatures that range between absolute zero and 10 Kelvin (approximately –273 to –263 degrees Celsius).[13] As a result, the large-scale application of superconductors is currently impractical.

The primary focus of superconductor research has revolved around the quest to discover materials with significantly higher critical temperatures. High-temperature superconductors (HTS) have been discovered that can exhibit superconductivity at warmer temperatures than conventional materials. Despite being termed “high temperature”, HTS refer to materials that conduct above 77 Kelvin (–196.2 degrees Celsius), the boiling point

[13] NCCR (2021). The critical temperature refers to the temperature at which the electrical resistance of a superconductor falls to zero.

of liquid nitrogen.[14] In recent years, there has been a growing emphasis within the scientific community on pushing the boundaries further by striving to develop room-temperature superconductivity. While this research is ongoing, no breakthrough has been achieved thus far.

Future research and development may effectively reduce operational costs and make superconductor technology more accessible for practical applications. The use of advanced superconductors in military contexts is anticipated to be transformative. Development of scalable room-temperature superconductor materials could revolutionise the field of electronics, leading to promising applications such as ultra-high-speed and energy-efficient computer chips, low-latency broadband wireless communications and highly efficient electricity grids.[15] Additionally, superconductors can be utilised to construct qubits (the basic units of quantum processors), offering vast opportunities for quantum computing.[16] New superconductor materials are being developed to generate qubits that are resilient to external disturbances, a characteristic that could make quantum computers much more reliable.[17] Nevertheless, the emergence of room-temperature superconductors may fuel a fresh technological competition among States, potentially leading to international disputes concerning patents, technology transfers and market access.[18]

Superconductors: Highlights for 2023

- The practical application of superconductors is currently hindered by the need for extremely low temperatures, requiring costly cryogenic engineering and high energy consumption. Scientific efforts are pushing towards achieving room-temperature superconductivity.
- The development of scalable room-temperature superconductors holds promise for revolutionising the field of electronics, but their emergence may lead to **international disputes** concerning patents, technology transfers and market access.

14 Clynes (2023).

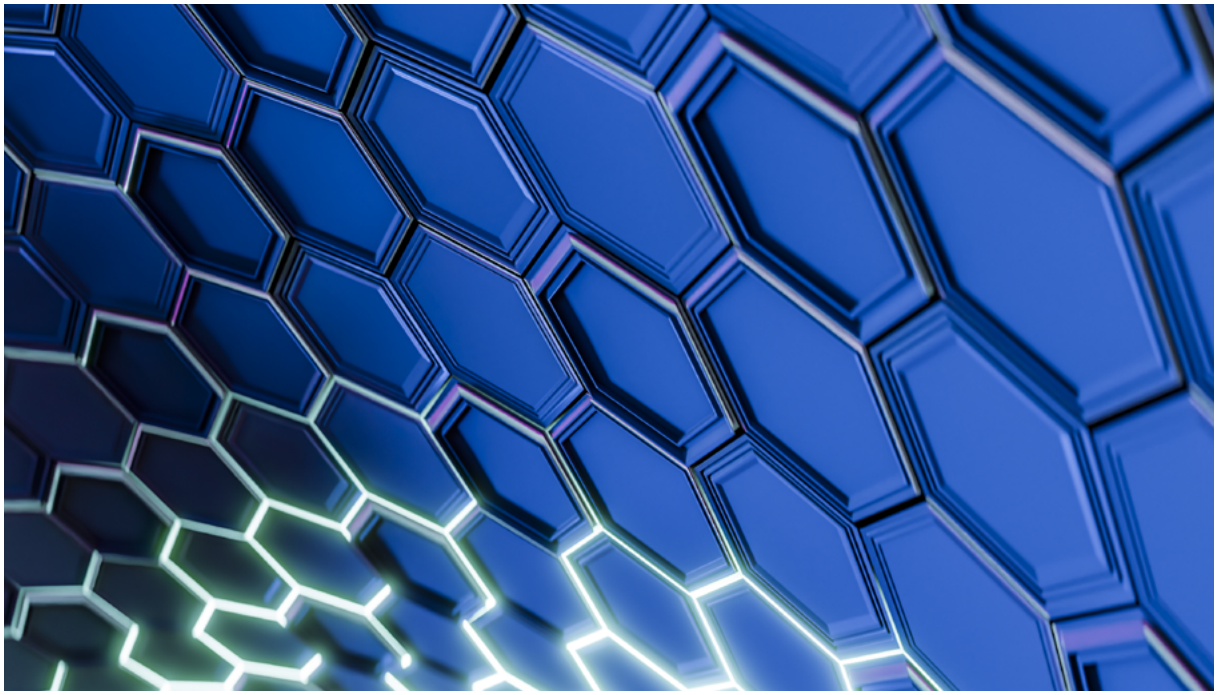
15 Pedram (2023).

16 For a detailed analysis of quantum computing and the latest developments see Section 4.3 below.

17 Feldman (2023).

18 Roa (2023).

2.3 Nanotechnology



Nanotechnology contributes to the design, manufacture and application of materials at the nanoscale, typically 1–100 nanometres (one nanometre is one billionth of a metre).

At the nanoscale, unique and often novel properties emerge as a result of quantum effects and surface behaviour.[19] Such properties can be harnessed for various applications, including in nanomaterials and nanoelectronics. In modern electronics, the ongoing trend of device miniaturisation is being significantly facilitated by the advancements in nanoelectromechanical systems (NEMS). These systems can be used to create smaller and more efficient sensors, actuators and other devices with critical applications in advanced sensing, computing and communications.

In sensing applications, nanotechnology is applied in environmental monitoring of air and water quality as well as pollutant detection. The incorporation of nanotechnology can make smaller and more sensitive sensors for military field operations that can, for example, detect biological and chemical threat agents. Compared with conventional methods of biothreat detection, nanomaterial-based biosensors can achieve higher sensitivity and accuracy even with reduced sample volume, preparation time and assay costs.[20] Nanosensors can be used to provide real-time information about potential threats for military operations, thereby enhancing situational awareness on the battlefield. They could equally benefit disarmament verification efforts in the biological and chemical weapon domains.

In the computing field, nanotechnology paves the way for next-generation computing by

---

19 US National Nanotechnology Coordination Office (n.d.).

20 Rowland et al. (2016).

facilitating the development of nanomaterials such as carbon nanotubes, graphene and quantum dots. As conventional silicon technology is approaching its physical limits, interest has grown in alternative materials and approaches for new computing paradigms. In recent years, carbon nanotubes have been identified by researchers to be an attractive alternative to replace silicon in transistor manufacturing.[21] The use of this highly conductive nanomaterial can facilitate the creation of more compact and efficient transistor designs, capable of surpassing silicon-based transistors.[22] However, their advantage in real-world applications has yet to be conclusively proven.[23] In addition, quantum dots (i.e., nanoscale crystals synthesised through the process of nanofabrication) can potentially revolutionise the field of quantum computing. Due to their quantum properties, quantum dots can be utilised as qubits that form the very foundation of quantum computers, enabling the structure of a scalable, cost-effective and fault-tolerant working machine.[24] However, the technology remains in its infancy and there are several technical and commercial obstacles that must be overcome before practical and large-scale production of quantum computers can be achieved.[25]

Furthermore, nanotechnology can facilitate advanced communications for military operations, offering multiple benefits including lower energy consumption, miniaturised communication devices and enhanced connectivity. In wireless communications systems, the development of nanotechnology leads to smaller, cheaper, less power-consuming and more efficient wireless sensor devices and makes 5G networks possible.[26] Nanomaterials can also be used to create highly efficient antennas that allow for improved signal efficiency and reliability. For instance, nanoscale antennas have been developed by researchers to enable light-speed data transfer between different core processors with little loss.[27]

While nanotechnology holds considerable promise for enhancing military information and communications systems, its development and deployment also come with certain risks. Studies have indicated that nanoparticles can display a wide range of toxicity and environmental hazards, thereby posing significant threats to both human health and ecological well-being.[28] The size and composition of nanoparticles allow them to breach the physiological barriers of living organisms and they can cause harmful biological reactions within the human body (e.g., lung inflammation and cardiac problems).[29] Nanomaterials produced through manufacturing processes can enter the environment through both deliberate and accidental releases. Once deposited into the soil, they possess the potential to contaminate the ground and subsequently migrate into water systems.[30]

---

21 Fadelli (2023).

22 Basheer et al. (2022).

23 Fadelli (2023).

24 Hecht (2022).

25 For a detailed analysis of quantum computing and the latest developments see Section 4.3 below.

26 Hamza and Jaafar (2022).

27 Kullock et al. (2020).

28 Kumah et al. (2023).

29 Ibid.

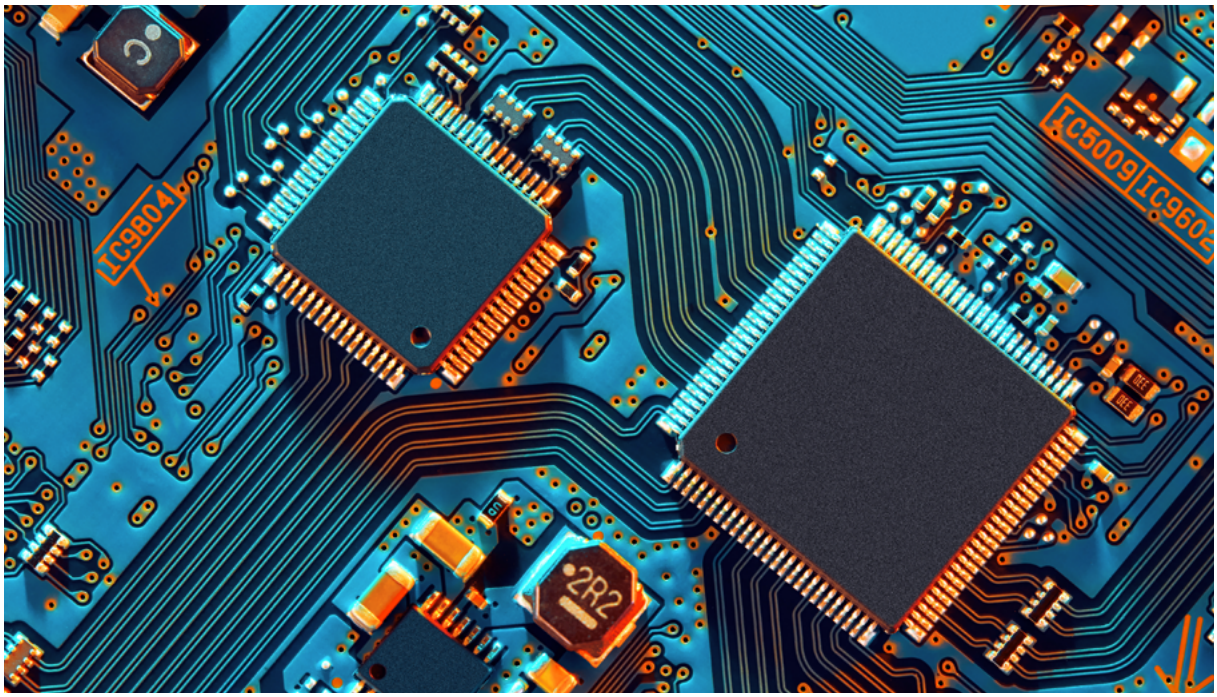
30 Ray, Paresh et al. (2009).

Nanotechnology: Highlights for 2023

- Ongoing progress in nanotechnology is consistently improving advanced sensing, computing and communications. Nanomaterials such as **carbon nanotubes** and **quantum dots** have the potential to drive next-generation computing, including the emerging field of quantum computing. However, challenges persist in achieving practical and large-scale production.
- Nanotechnology offers potential benefits for military information and communications systems, but it also presents risks. **Research** indicates that nanoparticles can be toxic and environmentally hazardous, posing significant threats to human health and ecological well-being.

3. Category II: Parts and Components

3.1 Microchips



Microchips or chips, also known as integrated circuits, are compact assemblies of miniaturised electronic components including transistors, diodes and resistors on one small flat piece of semiconductor material, usually a silicon wafer.

The significance of microchip technology cannot be overstated. It forms the cornerstone of modern electronics and computing systems, creating devices that are not only smaller but also more powerful, cost-effective and energy-efficient than those constructed of discrete components. Microchips can perform various critical functions, including information processing, data storage and instruction execution, and they can be used as memory chips, central processing units (CPUs) and graphics processing units (GPUs).

Microchips are constantly evolving, with advancements in the semiconductor materials leading to novel functionalities and higher performance at lower costs.[31] As described above, the semiconductor industry continues to push the boundaries of miniaturisation to develop transistors with smaller process nodes. Reduced size allows for more transistors to be packed onto a single microchip, resulting in increased processing power and energy efficiency. However, as the current silicon-based semiconductor technology is

[31] For a detailed analysis of semiconductor technology and the latest developments see Section 2.1 above.

gradually approaching its physical limits, alternative materials and approaches are being sought to ensure the continued growth and transformation of microchip technology.

Innovation in the field is also driven by improved chip design. Alternative chip-design methods have been put forward such as "multi-die systems" and "chiplet-based design".[32] Unlike the traditional monolithic chips, multi-die architecture consists of a collection of specialised chips such as memory and CPUs that can be linked to create a complex and integrated system-on-chip (SoC) package. The innovative chip design is believed to be capable of supporting AI machine learning at scale, enhancing silicon yields and minimising waste in the chip-manufacturing process.[33] Custom SoCs have been designed by companies such as Apple, Google/Alphabet and Amazon Web Services (AWS) to optimise chip performance for specific applications and workloads – this is known as the "custom silicon" approach.[34]

Specialised microchips are being designed to enable other technological applications such as 5G and artificial intelligence. 5G connectivity necessitates the development of advanced microchips that can meet the technology's high speed and low latency requirements. AI capabilities also rely largely on the processing power of specialised microchips such as tensor processing units (TPUs) and neural processing units (NPUs). The cutting-edge AI chips can be tens to thousands of times faster and more efficient than general-purpose chips such as CPUs.[35]

Moreover, extreme ultraviolet (EUV) lithography technology currently plays an important role in the manufacturing of the world's most advanced microchips. It facilitates the creation of ultra-small and highly precise components on silicon wafers and contributes to the continuous miniaturisation of microchips. To further the miniaturisation process, a more complex method, known as high numerical aperture EUV lithography, has been identified by researchers to achieve mass production of the next generation 2-nm node technology.[36] The new manufacturing systems are expected to be fully operational by 2025.[37] In addition, advanced packaging methods also continue to enhance microchip performance and energy efficiency, notably the three-dimensional (3D) stacking and packaging techniques that integrate multiple chips in a 3D structure.[38]

New developments in microchip technology will continue to shape the technological landscape in the coming years, with important implications for international security. The pervasive role of electronic systems in modern warfare means that enhanced microchip performance can benefit various aspects of military operations. These include increasing the precision and effectiveness of advanced weaponry, boosting capabilities for intelligence, surveillance and reconnaissance (ISR), enhancing communications systems, and facilitating the integration of AI and autonomy within military systems. However, the technology also introduces new security challenges. The microchip supply chain is highly global and complex, from chip design and manufacturing to packaging, testing and distribution.

---

32 MIT Technology Review Insights (2023).

33 Ibid.

34 Shilov (2023).

35 Khan and Mann (2020).

36 IBM (2023).

37 ASML (n.d.).

38 Moore (2022).

The most advanced technologies and manufacturing capabilities are often concentrated in certain regions, creating potential supply chain vulnerabilities. For instance, ASML in the Netherlands is currently the only company with the capacity to manufacture the EUV lithography machines used for large-scale production of the world's most advanced microchips.[39]

Another challenge pertains to the dual-use nature of the technology and potential proliferation. Microchips used in civilian applications, such as smartphones and laptops, can fall outside of export control regulations and so can be exploited for military purposes or integrated within military systems.[40] There are also cybersecurity concerns associated with the use of microchips. Hardware vulnerabilities are difficult to detect given the complexity of the integrated circuit architecture. Physical modifications might be effectively concealed among the vast array of valid components and functions and stay undetected for a long time.[41] Compared to software issues, hardware flaws are often significantly more difficult and costly to fix, which opens a vulnerability window and puts the broader digital systems at risk.[42]

Microchips: Highlights for 2023

- Advancements in semiconductor technology continue to drive higher microchip performance and functionality at lower costs through miniaturisation. Exploring alternative semiconductor materials and approaches holds the potential to sustain the growth and transformation of microchip technology.
- Progress in the field is also driven by improved chip design and production techniques. Innovative chip designs, such as the "**multi-die systems**", offer complex integrated chip systems and can support AI machine learning at scale. The ongoing development of **high numerical aperture EUV lithography** aims to enable mass production of next-generation 2-nm node technology by 2025.
- Despite the potential benefits of improved microchip performance for military operations, challenges include supply chain vulnerabilities, the dual-use nature of the technology and cybersecurity concerns.

39 ASML (n.d.).

40 Gilchrist (2023).

41 Levine and Pipikaite (2019).

42 Giles (2019).

3.2 Sensors

Sensors are devices designed to detect physical properties and environmental conditions and subsequently convert this information into output signals.

Sensors – encompassing motion sensors, proximity sensors, biometric sensors and image sensors, among others – have a broad range of applications and functionalities. They have become indispensable in almost every facet of military systems, from ground vehicles, ships and uncrewed aerial vehicles (UAVs) to missiles and satellites. Advancements in sensor technology thus play a crucial role in modernising defence capabilities, with the capacity to enhance the overall effectiveness of military operations. Advanced sensor applications can provide military forces with more accurate and timely data collection, enhance situational awareness and protection on the battlefield, improve targeting precision and threat detection, and facilitate decision-making in dynamic operational environments.

Numerous advancements have emerged in the realm of sensor technology for military purposes. Sensor fusion represents one key area of innovation. Armed forces have increasingly sought to combine multiple sensor sources to obtain more accurate and comprehensive information about the battlefield. Multi-sensor systems integrate and analyse data from diverse sensor types (e.g., acoustic, radar, electro-optical and infrared sensors), enhancing situational awareness to a level beyond what can be normally achieved by analysing these sources individually. In ground-based military vehicles, sensor-fusion technology provides the crew or commander with a comprehensive 360-degree view of their surroundings and facilitates information-sharing with other systems.[43]

---

[43] Eshel (2022).

Quantum sensing harnesses the inherent sensitivity of quantum states to disturbances, not only enabling more accurate and sensitive measurements but also unlocking the potential to measure previously unmeasurable phenomena.[44] Quantum sensing holds the potential to transform military capabilities. For example, researchers have developed quantum sensors that can detect objects concealed behind walls and other barriers, which can help with military applications such as reconnaissance.[45] In addition, quantum sensing technology could improve the accuracy of inertial navigation systems used in ships, submarines and aircraft. This would significantly enhance positioning and navigation capabilities in GNSS-denied environments.[46]

Sensors are increasingly integrated with AI technologies to provide intelligent data collection and analysis, thus improving the efficiency of military decision-making. Cognitive radar systems employ machine learning capabilities to adapt to changes in the environment or in the behaviour of an adversary.[47] Additionally, wearable biometric sensors have also been developed to monitor in real time soldiers' vital signs (e.g., heart rate, body temperature and hydration), as well as mental states including fatigue and stress levels. The integration of AI into future systems will be critical in expediting the filtration and interpretation of data collected from soldier wearables.[48] This new development could potentially assist commanders with military decisions and lead to improved performance of military personnel.

In addition to enhancing military capabilities, advancements in sensor technology present novel opportunities for international peace and security. Remote sensing technology can aid in the monitoring of ongoing armed conflicts and compliance with peace agreements.[49] Leveraging advanced sensors also enhances the efficiency of detecting hazardous substances, such as chemical and biological agents, in the environment. These applications can facilitate early threat detection, enabling swift response and mitigation measures, and they hold the potential to strengthen disarmament verification regimes.

However, the use of sensors also introduces a unique set of challenges that must be addressed. Sensors, particularly those involved in data-sharing across different systems, largely rely on networks and are thus susceptible to cyberattacks. Malicious actors may attempt to disrupt or manipulate sensor systems, thereby compromising data integrity and leading to flawed decision-making. As the technology advances, sensors gain the ability to generate increasingly larger volumes of data within the systems, which can potentially result in significant lag times and affect data quality.[50] This may hinder military decision-making unless accompanied by improved network architecture. Lastly, by collecting and storing information related to both military personnel and civilians, sensor applications may raise valid concerns regarding personal privacy and surveillance practices.

---

44 van Amerongen (2021).

45 UK National Quantum Technologies Programme (n.d.).

46 Coggins et al. (n.d.).

47 UK Defence Science and Technology Laboratory (2022).

48 Hamblen (2023).

49 Avtar et al. (2021).

50 Macri (2022).

Sensors: Highlights for 2023

- Sensor fusion, which integrates data from diverse sources (e.g., acoustic, radar and infrared sensors), provides comprehensive battlefield awareness.
- Quantum sensing shows promise in military applications by leveraging the sensitivity of quantum states to disturbances, enabling more accurate measurements, **object detection** behind barriers, and improving inertial navigation systems in **GNSS-denied environments**. Integration of sensors with AI technologies enhances data collection and analysis, leading to improved military decision-making.
- Advanced sensor technology can contribute to international security efforts, aiding in the monitoring of **ongoing armed conflicts and compliance with peace agreements**, as well as early detection of hazardous substances. Nevertheless, it is essential to address cybersecurity concerns and other challenges, including **potential lag times** resulting from increased data volume.

4. Category III: Processing and Computing

4.1 Cloud Computing

Cloud computing facilitates user access to computing resources without the necessity of maintaining on-premises infrastructure. It offers the flexibility to scale resources as requirements change.

Cloud computing operates with the backing of the integrated hardware and software components of cloud infrastructure.[51] In recent years, the capabilities of cloud computing have served as a catalyst for innovation across a diverse spectrum of applications, including big data analytics, machine learning, serverless computing, augmented reality (AR), virtual reality (VR) and various other cutting-edge technologies. Cloud-based platforms now enable the outsourcing of AI as a Service (AIaaS), which facilitates widespread access to the transformative capabilities of AI.[52] Moreover, cloud-native technology has emerged as a novel approach to building, testing, deploying and managing applications in cloud computing environments, providing the benefits of increased efficiency, cost reduction and scalability.[53]

---

51 For a detailed analysis of cloud infrastructure and the latest developments see Section 5.3 below.

52 Marr (2023).

53 Google (n.d.) and AWS (n.d.)

Cloud computing holds the potential to fuel innovation in the military sector. Specifically, harnessing cloud technology can accelerate the processes of designing, developing and testing software for military systems.[54] This can enhance capabilities in diverse military applications, ranging from artificial intelligence and machine learning to software modernisation and cybersecurity.[55] In military training, cloud-based platforms can provide personnel with access to realistic and immersive training environments, enabled by emerging technologies such as VR or AR. Since September 2022, the British Army has collaborated with a private company to develop and scale a cloud-distributed immersive simulation of land warfare that has been designed to facilitate large-scale, collective training for both physical and virtual users in various locations.[56] Moreover, cloud computing provides the high-speed computing power essential for handling large-scale data processing in military operations. Given the complexity and sheer volumes of military data, cloud technology enables the deployment of tools that assist armed forces in analysing data more effectively. This allows them to stay ahead of rapidly evolving threats while maintaining security.[57]

Nevertheless, cloud technology introduces potential threats and challenges. The integration of cloud computing into military operations raises concerns about data security, particularly when third-party cloud service providers (CSPs) are involved.[58] In addition, connectivity problems, such as high latency in remote or challenging environments, can affect the reliability of cloud-based services and thus have an impact on operational efficiency and real-time decision-making. Lastly, the intensifying global competition in cloud technology may emerge as a potential catalyst for heightened international tension, with States potentially seeking to tighten export controls on advanced cloud technologies in alignment with their national security interests.[59]

Cloud Computing: Highlights for 2023

- Cloud computing continues to fuel innovation across a range of cutting-edge applications, including big data analytics, machine learning, serverless computing, AR and VR. Cloud-based platforms currently allow the outsourcing of **AI as a Service (AIaaS)**, democratising access to transformative AI capabilities.
- In the military sector, cloud technology can facilitate **realistic and immersive training environments**, enabled by emerging technologies such as VR or AR. Cloud computing equally provides the **high-speed computing power** crucial for handling large-scale data processing in military operations. However, connectivity problems, such as high latency in remote environments, may have an impact on the reliability of cloud-based services.

---

54 Microsoft (2023).

55 US Department of Defense (2023).

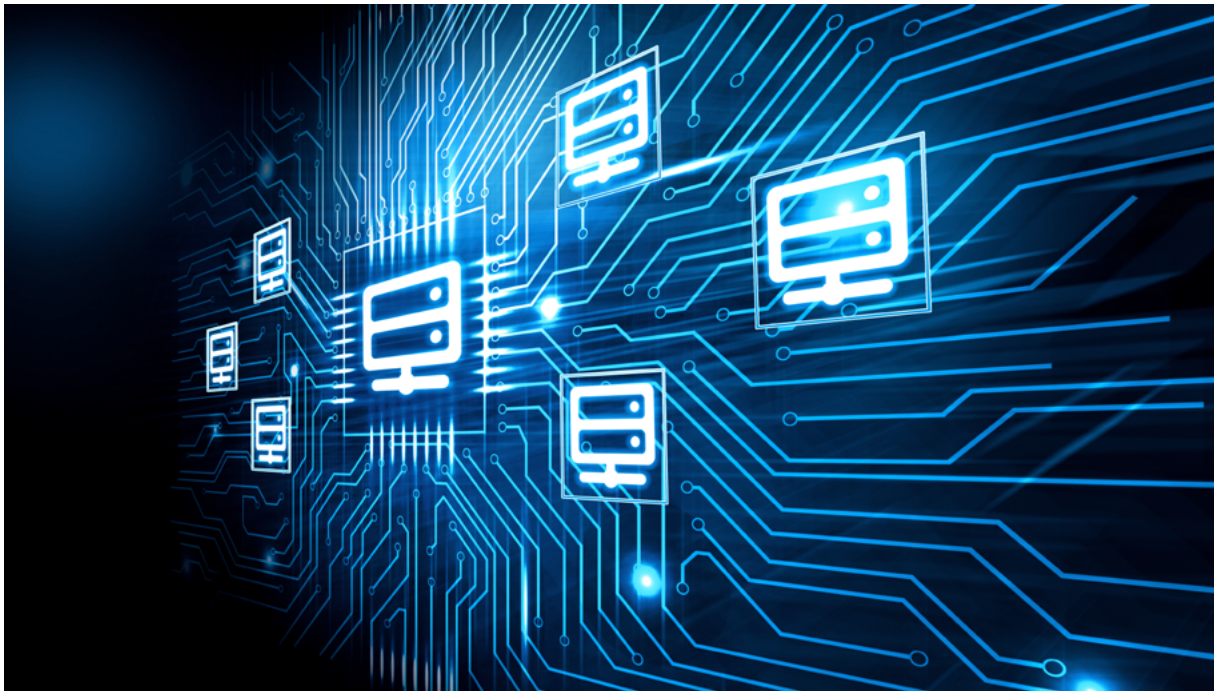
56 Hadean (2022).

57 Microsoft (2023).

58 For a further analysis of the data security issues associated with cloud technology see Section 5.3 below.

59 Hayashi and McKinnon (2023).

4.2 Edge Computing



Edge computing employs a distributed computing paradigm that relocates data storage and computation closer to the data source or "edge" of the network, rather than relying on a centralised cloud-based system.

In edge computing, data processing occurs on a device or a local server situated at the "edge" of a network. When data requires processing in the centralised cloud data centre, only the critical information is transmitted.[60] As a result, edge computing minimises latency and enhances computing power by storing and processing data locally and alleviating potential bottlenecks in cloud networks and data centres. These advantages are particularly significant for edge devices that require real-time processing, as evident in applications such as the Internet of Things, autonomous vehicles and AR.

The development of edge computing holds the potential to transform the way in which the military sector operates, enhancing communication, data processing and decision-making capabilities.[61] Deploying edge computing in the field enables instant data-sharing among forces connected within the same edge network, facilitating real-time communication and coordination. It also brings computational resources to the tactical edge of military operations and reduces dependence on cloud data centres. Large data sets from the field, such as sensor data and video feeds for surveillance and reconnaissance, can be analysed locally at edge locations, accelerating response times and improving situational awareness. The adoption of an edge architecture in the battlefield can therefore enhance the Internet of Military Things (IoMT) applications and allow military personnel to quickly react to potentially dangerous situations.[62]

---

60 Microsoft Azure (n.d.).

61 Lee et al. (n.d.).

62 Cameron (2018).

Edge computing ensures that data resources and computation are available in remote locations with intermittent Internet connectivity and even under extreme operational environments. Advanced AI analytics can run effectively on edge platforms when completely offline in harsh environments, thereby supporting critical missions such as search and rescue operations.[63] Yet, AI applications deployed on military edge devices such as UAVs, satellites and ground vehicles often face limitations and may be inferior to state-of-the-art models due to constraints in processing speed, working memory and power.[64] Moreover, Amazon Web Services recently introduced AWS Snowblade, a new edge computing product specifically designed for the Joint Warfighting Cloud Capability (JWCC) contract with the United States Department of Defense (DOD).[65] AWS Snowblade enables military users of the JWCC to run operations in edge locations that may be subject to extreme temperatures, vibrations or shocks.

Nevertheless, edge computing presents certain security challenges for military applications. The distributed computing framework may increase the attack surface, providing more endpoints for cyberattacks. Edge computing is vulnerable to a range of cybersecurity threats, including Denial-of-Service (DoS) attacks, side-channel attacks, malware-injection attacks, and authentication and authorisation attacks.[66] Edge computing facilities are also susceptible to physical damage, potentially leading to disruptions and data breaches in the edge networks.[67] To address these vulnerabilities, ongoing efforts are being made to enhance the security measures of edge computing systems. For instance, AWS Snowblade edge devices have incorporated advanced encryption technology to ensure data security and prevent unauthorised access from potential adversaries.[68]

Edge Computing: Highlights for 2023

- Edge computing holds the potential to transform military operations, enhancing communication, data-processing and decision-making capabilities. Moreover, in remote or extreme environments, edge computing plays a critical role in securing data and providing necessary computational resources.
- Edge platforms empower AI analytics to operate efficiently offline in challenging environments, supporting critical missions such as **search and rescue operations**. **Limitations** in processing speed, memory and power can affect AI applications on military edge devices.
- Persistent security challenges in military edge computing include the expanded surface for cyberattacks and vulnerability to physical damage. Ongoing efforts to enhance security measures, such as advanced encryption in **AWS Snowblade**, are being implemented.

---

63 Thomas (2021).

64 Miller and Lohn (2023).

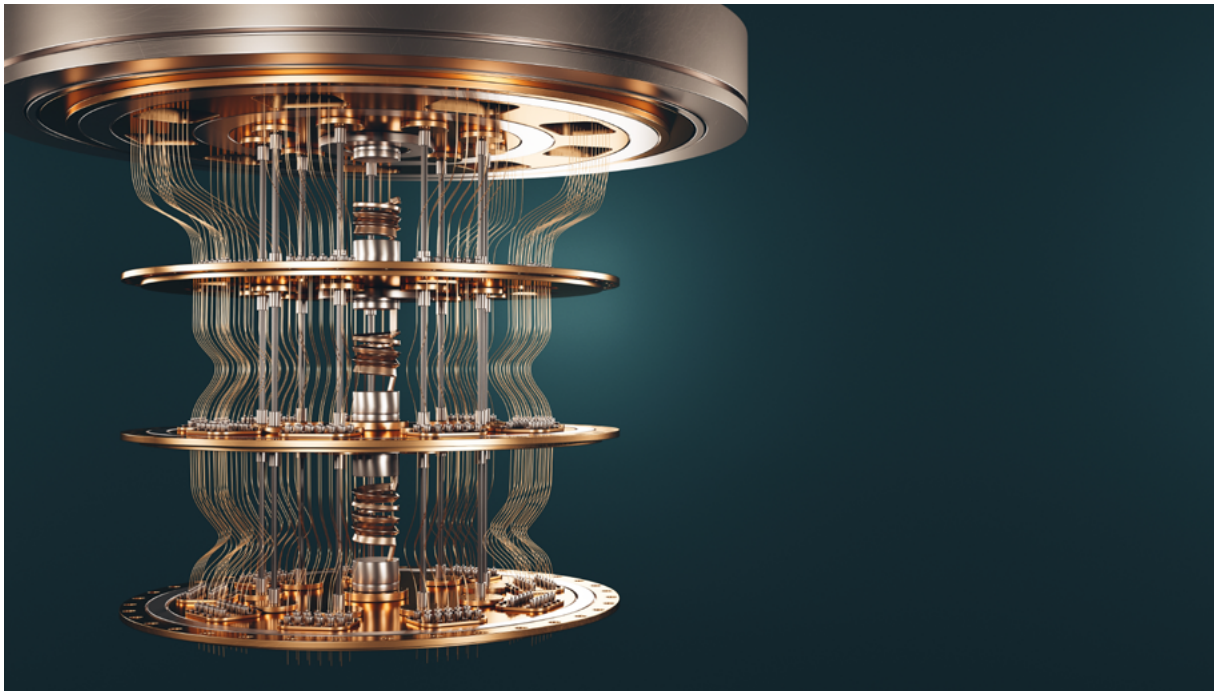
65 AWS (2023).

66 Xiao et al. (2019).

67 NATO CCDCOE (2022).

68 Konkel (2023).

4.3 Quantum Computing[69]



Quantum computing is an emerging field that leverages the principles of quantum mechanics to tackle problems of complexity beyond the capabilities of classical computers.

The potential for quantum computer to outperform classical computers is attributed to unique quantum phenomena, notably superposition and entanglement. Quantum bits or qubits, the fundamental unit of information in quantum computing, can exist simultaneously in multiple states (0 and 1) due to superposition. When qubits become entangled, the state of one qubit becomes directly linked to the state of another, irrespective of the physical distance between them. Quantum entanglement can be harnessed to achieve significant increases in computational speed, which enables quantum computers to perform specific calculations more efficiently than their classical counterparts.

The field of quantum computing has witnessed considerable progress. Private companies including IBM, Google/Alphabet and Microsoft have invested heavily in the research and development of practical quantum computers. IBM, for instance, has steadily increased the number of qubits on a single chip. In December 2023, IBM unveiled the Condor processor, which features 1,121 qubits, a notable advance from the previous 433-qubit Osprey processor.[70] Concurrently, the company introduced the Heron, its highest-performing quantum processor to date, equipped with 133 high-quality qubits.[71] Notably, Heron

---

69 A forthcoming report from UNIDIR, titled "International Security in a Quantum New World: A Primer", will provide further analysis on the field of quantum computing and its relevant implications for international security.

70 Gambetta (2023).

71 Ibid.

processors have the capability to directly connect with other Heron processors, potentially facilitating the scalability of quantum computers.[72]

Nonetheless, amid these advancements, the field still grapples with substantial challenges that remain to be addressed. One key issue is known as decoherence, a quantum phenomenon resulting from insufficient isolation of a physical qubit from its environment, which can introduce noise into calculations. Overcoming decoherence and correcting quantum errors have thus become critical.[73] Additionally, although mathematical proofs suggest quantum advantages over classical models, empirical evidence is still lacking due to the unavailability of quantum computers with a sufficient number of qubits.[74] For instance, researchers have estimated that the decryption of the state-of-the-art cryptography in eight hours would require 20 million qubits.[75]

While the practical applications of quantum computing still remain on the horizon, potential future developments hold profound implications for military practices and international security. Quantum computing has the potential to revolutionise diverse technological areas, particularly in enhancing artificial intelligence and machine learning. The success of classical machine learning algorithms often depends on extensive parameters and substantial training data. In contrast, quantum machine learning, by leveraging the diverse states available to quantum particles, can potentially reduce the required number of parameters and data.[76] Empirical research has shown that hybrid networks, which combine features of both classical and quantum computers, can achieve improved training of machine learning models.[77] These advancements could transform future military AI applications, especially in developing more accurate lethal autonomous weapons systems.[78]

Furthermore, quantum computing can reshape the cybersecurity landscape, presenting both challenges and opportunities. Quantum computers have the capacity to solve certain mathematical problems exponentially faster than classical computers, which could compromise the security of some commonly used cryptographic algorithms (e.g., such as RSA and ECC encryption schemes). Quantum algorithms capable of decrypting digital communications, notably Shor's algorithm, have been developed and can be executed once practical quantum computers become available.[79] This introduces new cybersecurity vulnerabilities and can give rise to Harvest Now Decrypt Later (HNDL) attacks, where malicious actors acquire sensitive, encrypted data now with the intention of decoding it later, following possible breakthroughs in decryption technology. Such attacks can lead to national security concerns, allowing adversaries to gain access to sensitive military information.[80] In response to potential quantum threats, ongoing efforts are being made to develop post-quantum cryptography (PQC). This involves creating

---

72 Brooks (2023a).

73 Lidar (2023).

74 Brooks (2023b).

75 Ibid.

76 Ibid.

77 Xu (2023).

78 US Congressional Research Service (2023).

79 van Amerongen (2021).

80 US Congressional Research Service (2023).

cryptographic systems that can withstand future attacks by quantum computers. Emerging quantum technologies, such as quantum key distribution (QKD)[81] and quantum random number generation (QRNG),[82] also offer the opportunities to enhance encryption mechanisms and secure communications.

Quantum Computing: Highlights for 2023

- Considerable progress has been made in quantum computing. IBM, for instance, has consistently increased the number of qubits on a single chip, reaching a milestone with the introduction of the **1,121-qubit Condor processor** in 2023. Simultaneously, the company launched the Heron processor with the ability to directly connect with other Heron processors, potentially facilitating **enhanced scalability.**
- Empirical research has shown that **hybrid networks** combining both classical and quantum computers can achieve improved training of machine learning models. This development holds profound implications for military AI applications, particularly for the development of **more accurate lethal autonomous weapons systems.**
- However, the development of quantum computing presents significant cyber and information security challenges, notably the risk of Harvest Now Decrypt Later attacks, given the **potential** of practical quantum computers to compromise widely-used cryptographic algorithms. Consequently, there are ongoing efforts to develop post-quantum cryptography in response to emerging quantum threats.

81 NATO (2022).

82 Argillander et al. (2023).

5. Category IV: Infrastructure

5.1 5G and 6G

5G stands for the fifth-generation technology standard for cellular networks, which provides advanced broadband connections that surpass its predecessors, such as 4G LTE. **6G** refers to the ongoing development of sixth-generation cellular technology designed to surpass 5G, delivering even more advanced network capabilities.

The current generation of connectivity infrastructure is characterised by significant progress in wireless technology, notably the widespread implementation of fifth-generation (5G) cellular networks. 5G technology presents various advantages over its predecessors, owing to new features such as network slicing and the ability to operate on the millimetre wave (mmWave) spectrum, a high-frequency band of radio spectrum in the range 30–300 GHz.[83] 5G significantly elevates connectivity by providing faster speeds, reducing latency, enhancing network reliability and supporting the concurrent connection of a greater number of devices. These innovative capabilities of 5G are instrumental in meeting the growing demands of technological innovations, particularly in IoT-based applications, enabling the connection of more devices and objects to networks.

---

[83] Gerwig and Goss. (2023).

5G technology can unlock immense potential for transformative military applications, facilitating enhanced communication, swift data transfer and real-time decision-making capabilities on the battlefield. Its high-speed, low-latency connectivity capacity can support critical military functions, from communications and logistics to ISR as well as command and control. Recent research has underscored three concrete military applications made possible by the implementation of 5G: the tracking of items and equipment using smart tags for improved operations; leveraging high-band 5G networks in data transfer for large sensor data sets; and the use of remote 5G communications for command and control to enhance multinational coordination.[84] The use of smart tag tracking in shipments via a 5G network also holds promise for advancing arms control efforts by potentially mitigating the risks associated with the diversion of conventional weapons and ammunition. In addition, 5G can serve as a powerful catalyst for cutting-edge AI and IoT applications within the military domain, paving the way for enhanced capabilities. High-speed 5G networking can facilitate the integration of AI for efficient processing of vast amounts of sensor data on the battlefield. For instance, adversary signals can be transmitted in real-time through a secure 5G network for further analysis using advanced signal-processing algorithms.[85]

Nevertheless, the integration of 5G technology introduces new risks, particularly in the realm of cybersecurity. With the surge in data volumes and interconnected devices within 5G networks, potential security vulnerabilities can be amplified, providing malicious actors with increased opportunities for exploitation and disruption. The characteristics of 5G technology, including open interfaces and its cloud-based nature, also create additional security threats, resulting in an expansive threat landscape for 5G deployments.[86] A diverse array of cybersecurity threats can manifest across the multiple 5G subsystems, which span from 5G user equipment and the radio access network (RAN) to the core network, cloud services and multi-access edge computing (MEC), among other critical components.[87]

The development of 6G cellular networks is currently under way, holding even greater promise than the present advancements witnessed with 5G technology. It is expected to bring further improvements in speed, latency and connectivity, as well as the capacity to enable a wider range of novel technological applications. Compared to previous generations of communications networks, the research and development of 6G place a greater focus on achieving comprehensive network coverage ”on land, at sea, and in air and space”, by combining terrestrial cellular mobile networks with aerial and satellite platforms.[88] This integrated satellite–terrestrial network architecture should offer significant potential for ensuring global Internet coverage and providing ubiquitous communication support for the Internet of Things.[89] The rollout of 6G technology is expected to begin around the year 2030.[90]

---

84 Lee et al. (2023).

85 Tucker (2022).

86 Śliwa and Suchański (2022).

87 NATO CCDCOE (2022).

88 Chen et al. (2023).

89 Tirmizi et al. (2022).

90 Kharpal (2023) and Chen et al. (2023).

5G and 6G: Highlights for 2023

- The current progress in 5G technology unlocks transformative potential in **military applications**, supporting enhanced communications, swift data transfer and real-time decision-making on the battlefield. 5G can also facilitate the integration of cutting-edge AI and IoT applications, thus enhancing military capabilities.
- However, the introduction of 5G technology amplifies potential cybersecurity vulnerabilities due to increased data volumes and interconnected devices. The open interfaces and its cloud-based nature also create **an expansive threat landscape** for 5G deployments.
- The ongoing research and development of 6G cellular networks focus on **achieving comprehensive coverage** across land, sea, air and space through an integrated satellite–terrestrial network, with an anticipated rollout by 2030.

5.2 Internet of Things

The **Internet of Things (IoT)** links an extensive network of physical devices, appliances, vehicles and other objects integrated with sensors, software and network connectivity, facilitating the collection and exchange of data between devices and systems. By enabling these devices to communicate and collaborate with one another via the Internet or other communications networks, IoT creates an interconnected ecosystem that can be monitored and controlled remotely.

Recent developments within the Internet of Things (IoT) domain are intertwined with technological innovations in other areas, notably edge computing, 5G networks and the integration of artificial intelligence.[91] The rise of edge computing has fostered a more localised approach to data processing and storage, effectively reducing latency and enhancing real-time processing capabilities for IoT devices.[92] Meanwhile, the rollout of 5G networks has also accelerated IoT development by providing higher data-transfer speeds, lower latency and increased network capacity.[93] Furthermore, the integration of AI technologies, specifically machine learning, can support real-time analysis and interpretation of the large amount of data generated by IoT applications, leading to more efficient decision-making and automation.

IoT technology is being increasingly leveraged in military systems to optimise operations and enhance efficiency, which has facilitated a shift towards a more connected and data-driven

---

91 Coughlin (2023).

92 For a detailed analysis of edge computing and the latest developments see Section 4.2 above.

93 For a detailed analysis of 5G cellular networks and the latest developments see Section 5.1 above.

military landscape. The Internet of Military Things (IoMT) can employ a diverse array of sensors deployed across various domains, aiming to attain comprehensive situational awareness and effective control within complex and diverse conflict environments.[94] The incorporation of sensor networks and uncrewed systems within the IoMT framework can significantly elevate surveillance and reconnaissance capabilities, enabling military forces to track the battlefield environment, manage equipment and vehicles, and monitor soldiers' health conditions.[95] Leveraging IoT/IoMT technology has the potential to enhance targeting precision and minimise the risk of civilian casualties during military operations, as sensors integrated within an IoT/IoMT network can guide weapons more accurately to their intended target.[96]

Furthermore, advancements in IoT/IoMT technology have also significantly improved military communications systems. The IoT facilitates seamless data-sharing and connectivity, thus enhancing collaboration among joint and coalition forces and across different domains.[97] In addition, the integration of secure communications protocols and the use of encryption and digital signatures in IoT-enabled systems can effectively safeguard communications channels, ensuring the confidentiality, integrity and availability of sensitive military information.[98] Yet, without robust communications protocols, the widespread adoption of IoT technology can introduce substantial cybersecurity threats to interconnected military systems. IoMT networks present a large attack surface comprising IoMT devices, the communication channels linking these devices, IoMT-specific back-end applications, as well as the back-end data storage.[99] The implications of cyber operations involving IoT devices can extend beyond military systems, potentially causing indiscriminate disruptions to other connected systems, including medical facilities, educational institutions and other sensitive networks.[100]

Internet of Things: Highlights for 2023

- IoT technology is increasingly being applied in military systems for operational optimisation (known as the Internet of Military Things). The IoMT employs a diverse array of sensors across domains for **comprehensive situational awareness and control**. Sensors integrated within an IoT/IoMT network can also enhance targeting precision in military operations, with the potential to **minimise the risk of civilian casualties.**
- However, in the absence of robust communications protocols, the widespread adoption of IoT in military systems can introduce cybersecurity risks. IoMT networks create a significant attack surface with potential implications beyond military systems, affecting **other critical sectors** including medical facilities, educational institutions and other sensitive networks.

---

94 Withrington (2023).

95 Khawaja (2023).

96 Douglass (2022).

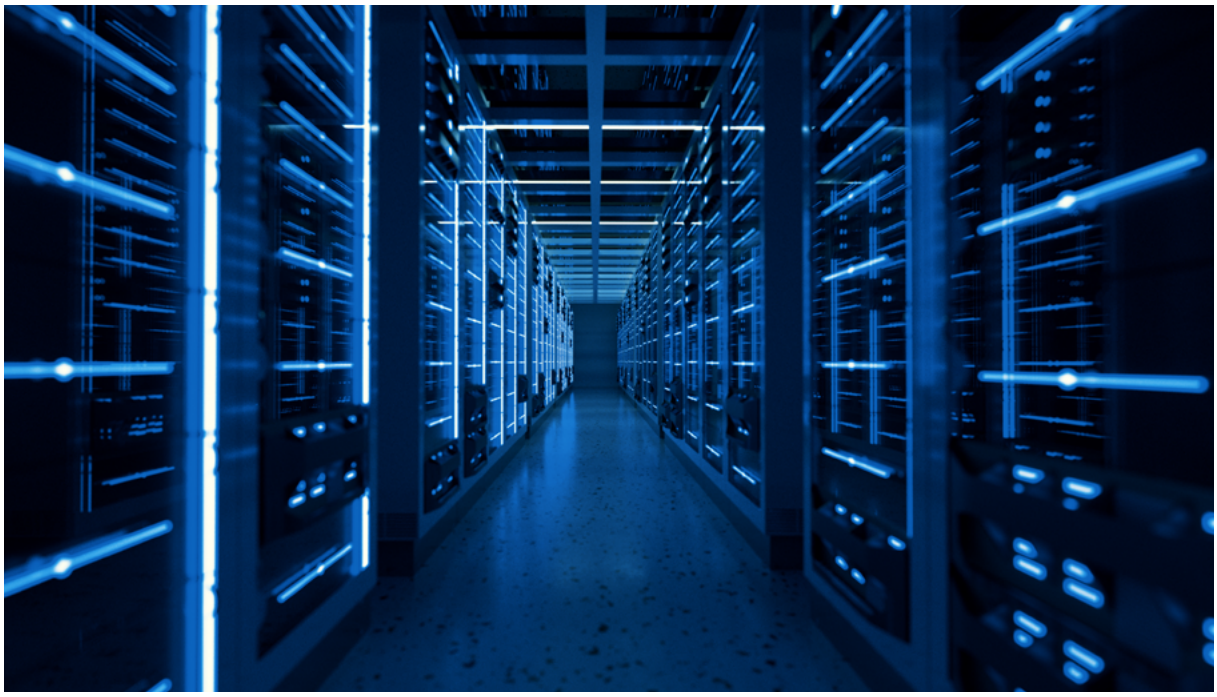
97 Breaking Defense (2023).

98 Kannan et al. (2023).

99 Withrington (2023).

100 Renals (2021).

5.3 Cloud Infrastructure



Cloud infrastructure consists of both hardware and software components essential for delivering cloud services over the Internet. This includes hardware such as servers, storage, networking components and data centres, as well as software such as virtualisation software.

Cloud infrastructure provides the foundation on which cloud computing services are built and delivered.[101] Cloud services have expanded in recent years, with private companies playing a critical role as cloud service providers (CSPs). Major CSPs include Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Oracle Cloud and Alibaba Cloud. They offer a diverse range of cloud services, which can be grouped into three primary categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). CSPs have continued to rapidly extend the coverage of their cloud infrastructure around the globe, establishing a presence on every continent.[102]

Cloud technology has been increasingly leveraged to enhance operational efficiency and data management in military settings. Military forces have not only developed their internal cloud infrastructure but have also adopted commercial cloud capabilities and services from private CSPs. As an example, in December 2022, the US Department of Defense awarded contracts to four leading CSPs (AWS, Google, Microsoft and Oracle) to support the DOD's Joint Warfighting Cloud Capability.[103] Cloud infrastructure enables military

---

101 For a detailed analysis of cloud computing and the latest developments see Section 4.1 above.

102 A global map of cloud infrastructure across eight major cloud service providers: https://www.cloudinfrastructuremap.com/

103 US Department of Defense (2022).

forces to store and manage large volumes of military data, from ISR data to logistical information and other mission-critical data. This can facilitate communication and coordination between military personnel and units from diverse locations.

Ensuring data security has been a critical consideration in the deployment of cloud technology within military contexts. Cloud infrastructure often offers enhanced security for sensitive information, through robust encryption, identity and access management, and other advanced security features. Notably, the Ukrainian Government's proactive move to migrate a significant portion of its critical data to the cloud elevated the country's readiness to withstand unprecedented cyberattacks.[104] Both governments and CSPs have continued to strengthen the security measures of their cloud infrastructure, including the adoption of a zero-trust approach in cloud computing environments.[105]

Nevertheless, cloud environments, like other digital platforms, remain susceptible to potential cyber risks and vulnerabilities. The transfer of sensitive data to cloud systems can heighten security concerns, as evidenced by previous cloud security incidents. In February 2023, a substantial volume of sensitive military emails was exposed due to a misconfigured email server on the Microsoft Azure Government Cloud platform. [106] While utilising commercial cloud services from major CSPs offers the advantages of robust security protocols and high concentrations of expertise, it also introduces the potential for incidents that affect the cloud infrastructure of these providers to have widespread effects.[107] Furthermore, the International Committee of the Red Cross (ICRC) has highlighted the growing involvement of civilians in digital operations during armed conflicts, potentially leading to an increased use of civilian infrastructure, including cloud infrastructure, for military purposes.[108] This trend poses a heightened risk of civilians and civilian infrastructure being targeted, undermining the universally supported principle of distinction.[109]

Cloud Infrastructure: Highlights for 2023

- Military forces have increasingly embraced cloud infrastructure to enhance operational efficiency and data management. While advanced security measures, such as robust encryption, are being implemented, the integration of cloud environments in military settings remains vulnerable to cyber risks, as evidenced by **past incidents.**
- Furthermore, **the ICRC** has highlighted the growing civilian involvement in digital operations during armed conflicts, potentially increasing the use of civilian infrastructure, including cloud infrastructure, for military purposes. This raises the risk of civilians and civilian infrastructure being targeted, undermining the principle of distinction.

---

104 Lewis (2023).

105 US Department of Defense (2023).

106 Martin et al. (2023).

107 Maurer and Hinck (2020).

108 ICRC (2023).

109 Ibid.

5.4 Satellite Communications

Satellite communications involve the use of artificial satellites to establish communication links between diverse locations on Earth.

Satellite communications systems play a critical role in ensuring global Internet coverage, bridging the digital divide and increasing the resilience of the connectivity infrastructure, especially in areas where traditional terrestrial communications networks are limited or unavailable. Satellite technologies are integral to military operations, and ongoing advancements in the field continue to drive innovation in the defence sector. The current rise in deployments of Low Earth Orbit (LEO) satellite constellations is poised to significantly increase the number of satellites orbiting the Earth. Compared to traditional geosynchronous satellites, large constellations of smaller satellites in LEO can substantially reduce latency, increase bandwidth capacity and offer consistent global coverage. Private entities are primarily leading developments in LEO satellites, including SpaceX's Starlink, OneWeb and Amazon's Project Kuiper.[110]

The enhanced connectivity provided by LEO systems can be leveraged by military forces to enable real-time data transfers, improving precision and efficiency in military operations. As observed in the conflict between Russia and Ukraine, SpaceX's LEO satellite constellation Starlink has played a crucial role in facilitating critical communication for both civilian and military purposes in Ukraine, including deployment on UAVs for surveillance and reconnaissance.[111] Beyond defence applications, LEO constellations also hold the potential to bridge the global digital gap, providing high-speed Internet in remote or rural areas where traditional ground infrastructure is challenging to deploy.[112]

Another notable innovation in satellite

---

110 Borowitz (2022).

111 Jayanti (2023).

112 Marquina (2022).

communications is the integration of quantum technologies. Quantum key distribution (QKD) can secure satellite communications by applying the principles of quantum mechanics to create and exchange encryption keys between two parties. In September 2022, the European Space Agency announced a collaboration with the European Commission and more than 20 European space companies to introduce the first space-based QKD system in the region, known as the Eagle-1 satellite.[113] This satellite-enabled connectivity system will pave the way for an ultra-secure network in Europe. Concurrently, countries including China[114] and Singapore[115] are also pursuing the development of QKD technology to enhance security in satellite communications.

While satellite technology opens up vast possibilities for global connectivity and secure communications, it also introduces a range of security concerns. One challenge pertains to the susceptibility of satellite systems to cyber threats and potential data breaches.

Satellite communications are indispensable in transmitting sensitive information crucial for military operations, and any compromising of the systems can result in significant strategic disadvantages. Military satellite communications systems have become targets for cyber-attacks, leading to outages and disruptions of critical services.[116] The deployments of satellites in orbit, particularly the large number of LEO satellites, can also present security concerns such as those related to space traffic and increasing space debris, which poses a threat to space security and sustainability.[117] Furthermore, given the pivotal role played by private entities in the field of satellite communications, military forces will continue to leverage commercial technologies to their advantage. Nevertheless, the dependence on commercial actors for critical communication infrastructure during conflicts has underscored potential pitfalls arising from differences in incentives, operating principles and accountability mechanisms between private and public entities.[118]

Satellite Communications: Highlights for 2023

- Significant innovations in satellite communications include the surge in LEO satellite constellations, led by **private entities** such as SpaceX's Starlink. These not only help to improve **global connectivity** but also plays a vital role in military operations by facilitating **critical communication** during conflicts. Moreover, the integration of quantum key distribution technology into **satellite systems** paves the way for achieving more secure communications.
- However, satellite communications can also pose security challenges, including vulnerabilities to **cyber threats** and concerns about **space debris.** In addition, as military forces continue to leverage commercial satellite technologies, it is crucial to highlight **potential pitfalls** related to differences in incentives, operating principles and accountability mechanisms between public and private entities.

---

113 ESA (2022).

114 Laursen (2022).

115 SpeQtral (2022).

116 Menn (2023).

117 Mukherjee (2021).

118 Jayanti (2023).

6. Conclusion

Across the technology domains examined here, several overarching trends and developments have emerged. In particular, a persistent trend in hardware technology is the ongoing process of miniaturisation, leading to the creation of increasingly compact and efficient devices. Recent breakthroughs in semiconductor materials, nanotechnology, microchips and sensors have all played pivotal roles in driving this transformative shift. This trend is facilitating the widespread adoption of enabling technologies in military weaponry and systems, contributing to the modernisation of military equipment.

Harnessing enabling technologies will markedly elevate various military capabilities. These include improved situational awareness, streamlined command and control, accelerated data transfer and processing, and heightened precision of advanced weaponry. Notably, certain enabling technologies, such as microchips, cloud computing and quantum computing, act as catalysts for innovation in military applications. They facilitate the integration of transformative technologies such as AI and machine learning capabilities, further amplifying the potential for advancements in military operations. Moreover, enabling technologies have the potential to strengthen international security efforts by reinforcing disarmament verification and conflict monitoring mechanisms. This can be achieved, for instance, through the use of advanced sensors to detect chemical and biological agents in the environment as well as to monitor compliance with peace agreements.

However, recent advancements in enabling technologies also pose significant risks and challenges. While innovations in cloud technology and quantum key distribution can enhance the security of communication, information storage and data processing, the large-scale deployment of enabling technologies introduces heightened vulnerability to cybersecurity risks. This expansion of the technological landscape can broaden the attack surface, posing increased challenges in safeguarding military systems from potential cyber threats. Quantum computing, in particular, possesses the potential to disrupt widely used encryption protocols and standards due to its anticipated code-breaking capabilities.

Furthermore, the pursuit of cutting-edge innovations in enabling technologies has the potential to escalate international tensions and fuel technological competition among States. States may seek to impose strict export controls on advanced technologies in alignment with their national security interests. In addition, supply chain vulnerabilities constitute a substantial challenge in the realm of enabling technologies. The supply chain for hardware components, such as microchips, is a highly global and complex network, with a high concentration of production specialisation in certain regions of the globe. Disruptions to manufacturing capabilities in these regions, whether stemming from geopolitical tensions or natural disasters, would have a negative impact on the availability of the technologies and have implications for international security.

Lastly, developments in many technology domains underscore the critical role played by the private sector. Private companies have been driving progress and innovation in a diverse spectrum of technological applications, encompassing cloud technology, satellite communications and quantum computing. Military forces have long begun to collaborate with private entities to leverage state-of-the-art technologies, but this involvement is not without risks. Incidents that have an impact on the infrastructure of private companies can have widespread effects, with

the risk of sensitive military information being compromised. Dependence on private actors can also lead to potential pitfalls arising from differences in incentives, operating principles and accountability mechanisms between private and public entities.

Advancements in enabling technologies will continue to have significant implications for military practices and international security. This necessitates continued horizon scanning of new and emerging trends as well as further examination of potential governance frameworks to harness opportunities while mitigating risks. In future research projects, UNIDIR will continue to identify and examine new and emerging technologies, as well as novel applications of more established ones, and provide action-oriented policy recommendations to effectively govern different technology categories.

References

Amazon Web Services (AWS). 2023. “Announcing AWS Snowblade for U.S. Department of Defense JWCC Customers”. 6 June. As of 6 December 2023: https://aws.amazon.com/about-aws/whats-new/2023/06/aws-snowblade-us-defense-jwcc-customers/

—.n.d. “What is cloud native?”. As of 6 December 2023: https://aws.amazon.com/what-is/cloud-native/

Arcuri, Gregory and Sujai Shivakumar. 2022. “Moore’s Law and Its Practical Implications”. Center for Strategic & International Studies. 18 October. As of 6 December 2023: https://www.csis.org/analysis/moores-law-and-its-practical-implications

Argillander, Joakim et al. 2023. “Quantum Random Number Generation Based on a Perovskite Light Emitting Diode”. Communications Physics 6, 157. As of 6 December 2023: https://doi.org/10.1038/s42005-023-01280-3

ASML. n.d. “EUV Lithography Systems”. As of 6 December 2023: https://www.asml.com/en/products/euv-lithography-systems

Avtar, Ram et al. 2021. “Remote Sensing for International Peace and Security: Its Role and Implications”. Remote Sensing 13, 3: 439. As of 6 December 2023: https://doi.org/10.3390/rs13030439

Basheer, Taha et al. 2022. “Nanotechnology and Computer Science: Trends and Advances”. Memories - Materials, Devices, Circuits and Systems 2, October. As of 6 December 2023: https://doi.org/10.1016/j.memori.2022.100011

Borowitz, Mariel. 2022. “The Military Use of Small Satellites in Orbit”. French Institute of International Relations. 4 March. As of 6 December 2023: https://www.ifri.org/sites/default/files/atoms/files/m._borowitz_military_use_small_satellites_in_orbit_03.2022.pdf

Breaking Defense. 2023. “When We Talk about What Will Enable JADC2, We’re Really Talking about the Internet of Warfighting Things”. 22 March. As of 6 December 2023: https://breakingdefense.com/2023/03/when-we-talk-about-what-will-enable-jadc2-were-really-talking-about-the-internet-of-warfighting-things/

Brooks, Michael. 2023a. “What’s Next for Quantum Computing”. MIT Technology Review. 6 January. As of 6 December 2023: https://www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/

Brooks, Michael. 2023b. “Quantum Computers: What are They Good For?”. Nature. 24 May. As of 6 December 2023: https://www.nature.com/articles/d41586-023-01692-9

Cameron, Lori. 2018. “Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT”. IEEE Computer Society. 1 March. As of 6 December 2023: https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt

Chandler, David L. 2022. “The Best Semiconductor of Them All?”. MIT News. 21 July. As of 6 December 2023: https://news.mit.edu/2022/best-semiconductor-them-all-0721

Chen, Zhi et al. 2023. “Experts’ Take on 6G Technology”. China Daily. 7 August. As of 6 December 2023: https://www.chinadaily.com.cn/a/202308/07/WS64d01ddca31035260b81a8d3_1.html

Clynes, Tom. 2023. “5 Big Ideas for High-Temperature Superconductors”. IEEE Spectrum. 18 September. As of 6 December 2023: https://spectrum.ieee.org/high-temperature-superconductors

Coggins, Kevin et al. n.d. “Quantum Sensing: A New Approach to Maintaining PNT in GPS-Denied Environments”. US Naval Institute. As of 6 December 2023: https://www.usni.org/magazines/proceedings/sponsored/quantum-sensing-new-approach-maintaining-pnt-gps-denied

Coughlin, Tom. 2023. “9 IoT Trends to Keep an Eye on in 2023 and Beyond”. TechTarget. 12 July. As of 6 December 2023: https://www.techtarget.com/iotagenda/opinion/IoT-trends-to-keep-an-eye-on

Douglass, Robert. 2022. ”Introduction: IoT for Defense and National Security”. In IoT for Defense and National Security (eds R. Douglass, K. Gremban, A. Swami and S. Gerali). As of 6 December 2023: https://doi.org/10.1002/9781119892199.fmatter

Eshel, Tamir. 2022. “Sensor Fusion for Land Combat Vehicles”. European Security & Defence. 26 April. As of 6 December 2023: https://euro-sd.com/2022/04/articles/exclusive/25763/sensor-fusion-for-land-combat-vehicles/

European Space Agency (ESA). 2022. “Quantum Encryption to Boost European Autonomy”. 22 September. As of 6 December 2023: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Quantum_encryption_to_boost_European_autonomy

Fadelli, Ingrid. 2023. “Researchers Demonstrate Scaling of Aligned Carbon Nanotube Transistors to below Sub-10 nm Nodes”. Phys.org. 27 July. As of 3 January 2024: https://phys.org/news/2023-07-scaling-aligned-carbon-nanotube-transistors.html

Feldman, Andrey. 2023. “New Superconductor Could Lead to Quantum Computing Breakthrough”. Advanced Science News. 18 July. As of 6 December 2023: https://www.advancedsciencenews.com/new-superconductor-could-lead-to-quantum-computing-breakthrough/

Gambetta, Jay. 2023. “The Hardware and Software for the Era of Quantum Utility is Here”. IBM. 4 December. As of 11 January: https://www.ibm.com/quantum/blog/quantum-roadmap-2033

Gargeyas, Arjun. 2022. “The Role of Semiconductors in Military and Defence Technology”. Defence and Diplomacy Journal 11, 2 (January–March). As of 6 December 2023: https://capsindia.org/wp-content/uploads/2022/07/DD-Journal-January-March-2022-Arjun-Gargeyas.pdf

Gerwig, Kate and Michaela Goss. 2023. “The Essential 5G Glossary of Key Terms and Phrases”. TechTarget. 19 October. As of 6 December 2023: https://www.techtarget.com/searchnetworking/feature/The-essential-5G-glossary-of-key-terms-and-phrases

Gilchrist, Karen. 2023. “How U.S. Microchips are Fueling Russia’s Military – Despite Sanctions”. CNBC. 7 August. As of 6 December 2023: https://www.cnbc.com/2023/08/07/how-us-microchips-are-fueling-russias-military-despite-sanctions.html

Giles, Martin. 2019. “Cybersecurity Flaws in Chips are Still Taking Too Long to Fix”. MIT Technology Review. 3 June. As of 6 December 2023: https://www.technologyreview.com/2019/06/03/135108/cybersecurity-flaws-in-chips-are-taking-too-long-to-fix/

Google. n.d. “What is Cloud Native?”. As of 6 December 2023: https://cloud.google.com/learn/what-is-cloud-native

Hadean. 2022. “Hadean Awarded British Army Contract to Build Simulation Pathfinder”. 14 July. As of 6 December 2023: https://hadean.com/news/hadean-awarded-british-army-contract-to-build-simulation-pathfinder/

Hamblen, Matt. 2023. “Stephanie Brown on Sensors Worn by Soldiers for Their Vital Data”. Fierce Electronics. 6 June. As of 6 December 2023: https://www.fierceelectronics.com/sensors/tesla-recalls-2-million-cars-software-update-provide-visual-and-audible-alerts

Hamza, Ekhlas Kadum and Shahad Nafea Jaafar. 2022. “Nanotechnology Application for Wireless Communication System”. In Nanotechnology for Electronic Applications. Materials Horizons: From Nature to Nanomaterials. Springer, Singapore. As of 6 December 2023: https://doi.org/10.1007/978-981-16-6022-1_6

Hayashi, Yuka and John D. McKinnon. 2023. “U.S. Looks to Restrict China’s Access to Cloud Computing to Protect Advanced Technology”. 4 July. As of 6 December 2023: https://www.wsj.com/articles/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613

Hecht, Jeff. 2022. “Nanomaterials Pave the Way for the Next Computing Generation”. Nature. 10 August. As of 6 December 2023: https://www.nature.com/articles/d41586-022-02147-3

IBM. 2023. “Why We Need EUV Lithography for the Future of Chips”. 26 June. As of 6 December 2023: https://research.ibm.com/blog/what-is-euv-lithography

Institute of Electrical and Electronics Engineers (IEEE). n.d.-a. “Future of Semiconductor Performance”. As of 6 December 2023: https://irds.ieee.org/topics/future-of-semiconductor-performance

—.n.d.-b. “Semiconductor Materials”. As of 6 December 2023: https://irds.ieee.org/topics/semiconductor-materials

Intel. n.d. “The Story of the Intel® 4004”. As of 6 December 2023: https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html

Jayanti, Amritha. 2023. “Starlink and the Russia–Ukraine War: A Case of Commercial Technology and Public Purpose?”. Analysis & Opinions, Belfer Center for Science and International Affairs, Harvard Kennedy School. 9 March. As of 6 December 2023: https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

Kannan, B. Maruthu et al. 2023. “Secure Communication in IoT-enabled Embedded Systems for Military Applications Using Encryption,” 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, pp. 1385–1389. As of 6 December 2023: https://doi.org/10.1109/ICECAA58104.2023.10212400

Khan, Saif M. and Alexander Mann. 2020. “AI Chips: What They Are and Why They Matter”. Center for Security and Emerging Technology. April. As of 6 December 2023: https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/

Kharpal, Arjun. 2023. “Next-gen Mobile Internet – 6G – will Launch in 2030, Telecom Bosses Say, Even as 5G Adoption Remains Low”. CNBC. 7 March. As of 6 December 2023: https://www.cnbc.com/2023/03/08/what-is-6g-and-when-will-it-launch-telco-execs-predict.html

Khawaja, Saleem. 2023. “How Military Uses of the IoT for Defence Applications are Expanding”. Army Technology. 28 March. As of 6 December 2023: https://www.army-technology.com/sponsored/how-military-uses-of-the-iot-for-defence-applications-are-expanding/

Konkel, Frank. 2023. “AWS Unveils Edge Device for Defense Customers in Most Extreme Environments”. Nextgov/FCW. 8 June. As of 6 December 2023: https://www.nextgov.com/digital-government/2023/06/aws-unveils-edge-device-defense-customers-most-extreme-environments/387302/

Kullock, René et al. 2020. “Electrically-driven Yagi-Uda Antennas for Light”. Nature Communications 11, 115. As of 6 December 2023: https://doi.org/10.1038/s41467-019-14011-6

Kumah, Elizabeth Adjoa et al. 2023. “Human and Environmental Impacts of Nanoparticles: A Scoping Review of the Current Literature”. BMC Public Health 23, 1059. As of 6 December 2023: https://doi.org/10.1186/s12889-023-15958-4

Laursen, Lucas. 2022. “As China’s Quantum-Encrypting Satellites Shrink, Their Networking Abilities Grow”. IEEE Spectrum. 25 August. As of 6 December 2023: https://spectrum.ieee.org/satellite-qkd-china

Lee, Ki et al. n.d. “Decentralized Decision Making at the Tactical Edge”. Booz Allen. As of 6 January 2024: https://www.boozallen.com/s/insight/blog/decentralized-decision-making-at-the-tactical-edge.html

Lee, Mary et al. 2023. “Opportunities and Risks of 5G Military Use in Europe”. Santa Monica, CA: RAND Corporation. As of 6 December 2023: https://www.rand.org/pubs/research_reports/RRA1351-2.html

Lee, Sukbae et al. 2023a. “The First Room-Temperature Ambient-Pressure Superconductor”. arXiv. 22 July. As of 6 December 2023: https://arxiv.org/abs/2307.12008

—. 2023b. “Superconductor Pb10−xCux(PO4)6O Showing Levitation at Room Temperature and Atmospheric Pressure and Mechanism”. arXiv. 22 July. As of 6 December 2023: https://arxiv.org/abs/2307.12037

Levine, Edlyn V. and Algirde Pipikaite. 2019. “Hardware is a Cybersecurity Risk. Here’s What We Need to Know”. World Economic Forum. 19 December. As of 6 December 2023: https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/

Lewis, James Andrew. 2023. “Accelerating Federal Cloud Adoption for Modernization and Security”. Center for Strategic & International Studies (CSIS). 28 July. As of 6 December 2023: https://www.csis.org/analysis/accelerating-federal-cloud-adoption-modernization-and-security

Lidar, Daniel. 2023. “A Scientist Explains an Approaching Milestone Marking the Arrival of Quantum Computers”. Phys.org. 20 November. As of 6 December 2023: https://phys.org/news/2023-11-scientist-approaching-milestone-quantum.html

Macri, Kate. 2022. “Army is Modernizing Sensors for Data-Driven Decision-Making”. GovCIO Media & Research. 4 March. As of 6 December 2023: https://governmentciomedia.com/army-modernizing-sensors-data-driven-decision-making

Marquina, Claudia. 2022. “How Low-Earth Orbit Satellite Technology Can Connect the Unconnected”. 18 February. As of 6 December 2023: https://www.weforum.org/agenda/2022/02/explainer-how-low-earth-orbit-satellite-technology-can-connect-the-unconnected/

Marr, Bernard. 2023. “The 10 Biggest Cloud Computing Trends In 2024 Everyone Must Be Ready For Now”. Forbes. 9 October. As of 6 December 2023: https://www.forbes.com/sites/bernardmarr/2023/10/09/the-10-biggest-cloud-computing-trends-in-2024-everyone-must-be-ready-for-now/?sh=7ab779e66d67

Martin, Peter et al. 2023. “Pentagon and Microsoft Are Investigating Leak of Military Emails”. Bloomberg. 22 February. As of 6 December 2023: https://www.bloomberg.com/news/articles/2023-02-22/pentagon-and-microsoft-investigating-leak-of-military-emails

Maurer, Tim and Garrett Hinck. 2020. “Cloud Security: A Primer for Policymakers”. Carnegie Endowment for International Peace. August. As of 6 December 2023: https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf

Menn, Joseph. 2023. “Cyberattack Knocks Out Satellite Communications for Russian Military”. Washington Post. 30 June. As of 6 December 2023: https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/

Microsoft. 2023. “BAE Systems and Microsoft Join Forces to Equip Defence Programmes with Innovative Cloud Technology”. 14 April. As of 6 December 2023: https://news.microsoft.com/en-gb/2023/04/14/bae-systems-and-microsoft-join-forces-to-equip-defence-programmes-with-innovative-cloud-technology/

Microsoft Azure. n.d. ”What is Edge Computing?” As of 6 December 2023: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing

Miller, Kyle and Andrew Lohn. 2023. “Onboard AI: Constraints and Limitations”. Center for Security and Emerging Technology (CSET). August. As of 6 January 2024: https://cset.georgetown.edu/publication/onboard-ai-constraints-and-limitations/

MIT Technology Review Insights. 2023. “Multi-die Systems Define the Future of Semiconductors”. 31 March. As of 6 December 2023: https://wp.technologyreview.com/wp-content/uploads/2023/03/Synopsys-Report-v6.pdf

Moore, Samuel K. 2022. “3 Ways 3D Chip Tech Is Upending Computing”. IEEE Spectrum. 16 March. As of 6 December 2023: https://spectrum.ieee.org/amd-3d-stacking-intel-graphcore

Mukherjee, Supantha. 2021. “Should We be Worried about Space Debris? Scientists Explain”. World Economic Forum. 24 November. As of 6 December 2023: https://www.weforum.org/agenda/2021/11/space-debris-satellite-international-space-station/

National Centre of Competence in Research (NCCR). 2021. “Superconductivity, High Critical Temperature Found in 2D Semimetal Tungsten Nitride”. Phys.org. 5 May. As of 6 December 2023: https://phys.org/news/2021-05-superconductivity-high-critical-temperature-2d.html

NATO. 2022. “Using Quantum Technologies to Make Communications Secure”. 27 September. As of 6 December 2023: https://www.nato.int/cps/en/natohq/news_207634.htm

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2022. “Military Movement: Risks from 5G Networks”. Research Report. As of 6 December 2023: https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf

Pedram, Massoud. 2023. “Room-Temperature Superconductors Could Revolutionize Electronics – An Electrical Engineer Explains the Materials’ Potential”. The Conversation. 28 March. As of 6 December 2023: https://theconversation.com/room-temperature-superconductors-could-revolutionize-electronics-an-electrical-engineer-explains-the-materials-potential-201849

Ray, Paresh et al. 2009. “Toxicity and Environmental Risks of Nanomaterials: Challenges and Future Needs”. Journal of Environmental Science and Health, Part C, 27:1, 1–35. As of 6 December 2023: https://doi.org/10.1080/10590500802708267

Renals, Pete. 2021. “Future Developments in Military Cyber Operations and Their Impact on the Risk of Civilian Harm”. ICRC Humanitarian Law & Policy. 24 June. As of 6 December 2023: https://blogs.icrc.org/law-and-policy/2021/06/24/future-military-cyber-operations/

Roa, Carlos. 2023. “Have We Created the Philosopher’s Stone? Policymakers Should Care about Room-Temperature Superconductors”. National Interest. 2 August. As of 6 December 2023: https://nationalinterest.org/feature/have-we-created-philosopher%E2%80%99s-stone-policymakers-should-care-about-room-temperature

Rowland, Clare E. et al. 2016. “Nanomaterial-Based Sensors for the Detection of Biological Threat Agents”. Materials Today, 19, 8, October. As of 6 December 2023: https://doi.org/10.1016/j.mattod.2016.02.018

Ryugen, Hideaki. 2023. “TSMC to Make Cutting-edge 2-nm Chips at New Plant in Southern Taiwan”. Nikkei Asia. 10 August. As of 6 December 2023: https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-to-make-cutting-edge-2-nm-chips-at-new-plant-in-southern-Taiwan

Samsung. 2022. “Samsung Begins Chip Production Using 3nm Process Technology with GAA Architecture”. As of 6 December 2023: https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture

SpeQtral. 2022. “SpeQtral Announces SpeQtral-1 Quantum Satellite Mission for Ultra-Secure Communications”. 9 February. As of 6 December 2023: https://speqtralquantum.com/newsroom/speqtral-announces-speqtral-1-quantum-satellite-mission-for-ultra-secure-communications

Shilov, Anton. 2023. “The Golden Age of Custom Silicon Draws Near”. EE Times. 26 July. As of 6 December 2023: https://www.eetimes.com/the-golden-age-of-custom-silicon-draws-near/

Śliwa, Joanna and Marek Suchański. 2022. “Security Threats and Countermeasures in Military 5G Systems,” 2022 24th International Microwave and Radar Conference (MIKON), Gdansk, Poland, pp. 1-6. As of 6 December 2023: https://doi.org/10.23919/MIKON54314.2022.9924818

Taiwan Semiconductor Manufacturing Company (TSMC). n.d. “3nm Technology”. As of 6 December 2023: https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm

Thomas, Arthur. 2021. “AI at the Tactical Edge for Search & Rescue Operations”. Microsoft. 22 June. As of 6 December 2023: https://www.microsoft.com/en-us/industry/blog/government/2021/06/22/ai-at-the-tactical-edge-for-search-rescue-operations/

Tirmizi, Syed Bilal Raza et al. 2022. “Hybrid Satellite–Terrestrial Networks toward 6G: Key Technologies and Open Issues”. Sensors 22, no. 21: 8544. https://doi.org/10.3390/s22218544

Tucker, Patrick. 2022. “How Will the Military Use 5G? A New Drone Experiment Offers Clues”. Defense One. 28 September. As of 6 December 2023: https://www.defenseone.com/technology/2022/09/how-will-military-use-5g-new-drone-experiment-offers-clues/377745/

UK Defence Science and Technology Laboratory. 2022. “Sensing: Defence Science and Technology Capability”. 31 March. As of 6 December 2023: https://www.gov.uk/guidance/sensing-defence-science-and-technology-capability

UK National Quantum Technologies Programme. n.d. “Look Around Corners with the Quantum Periscope”. As of 6 December 2023: https://uknqt.ukri.org/wp-content/uploads/2021/10/Look-Around-Corners-With-The-Quantum-Periscope.pdf

United Nations General Assembly (UNGA). 2023. “Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts”. UN document A/78/268, 1 August.

US Congressional Research Service. 2023. “Defense Primer: Quantum Technology”. 25 October. As of 6 December 2023: https://crsreports.congress.gov/product/pdf/IF/IF11836

US Department of Defense. 2022. “Department of Defense Announces Joint Warfighting Cloud Capability Procurement”. 7 December. As of 6 December 2023: https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/

—. 2023. “DOD Makes Headway on Cloud Computing”. 29 March. As of 6 December 2023: https://www.defense.gov/News/News-Stories/Article/Article/3345260/dod-makes-headway-on-cloud-computing/

US National Nanotechnology Coordination Office. n.d. “What Is So Special about “Nano”?”. As of 6 December 2023: https://www.nano.gov/about-nanotechnology/what-is-so-special-about-nano

van Amerongen, Michiel. 2021. “Quantum Technologies in Defence & Security”. NATO Review. 3 June. As of 6 December 2023: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

Withrington, Claire. 2023. “The Internet of Military Things”. The Cove. 24 August. As of 6 December 2023: https://cove.army.gov.au/article/internet-military-things

Xiao, Yinhao et al. 2019. “Edge Computing Security: State of the Art and Challenges,” in Proceedings of the IEEE 107, n8, pp. 1608–1631, August. As of 6 December 2023: https://doi,org/10.1109/JPROC.2019.2918437

Xu, Tammy. 2023. “Better Machine-Learning Models with Quantum Computers”. IEEE Spectrum. 15 November. As of 6 December 2023: https://spectrum.ieee.org/quantum-machine-learning-terra-quanta

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG