UNIDIR

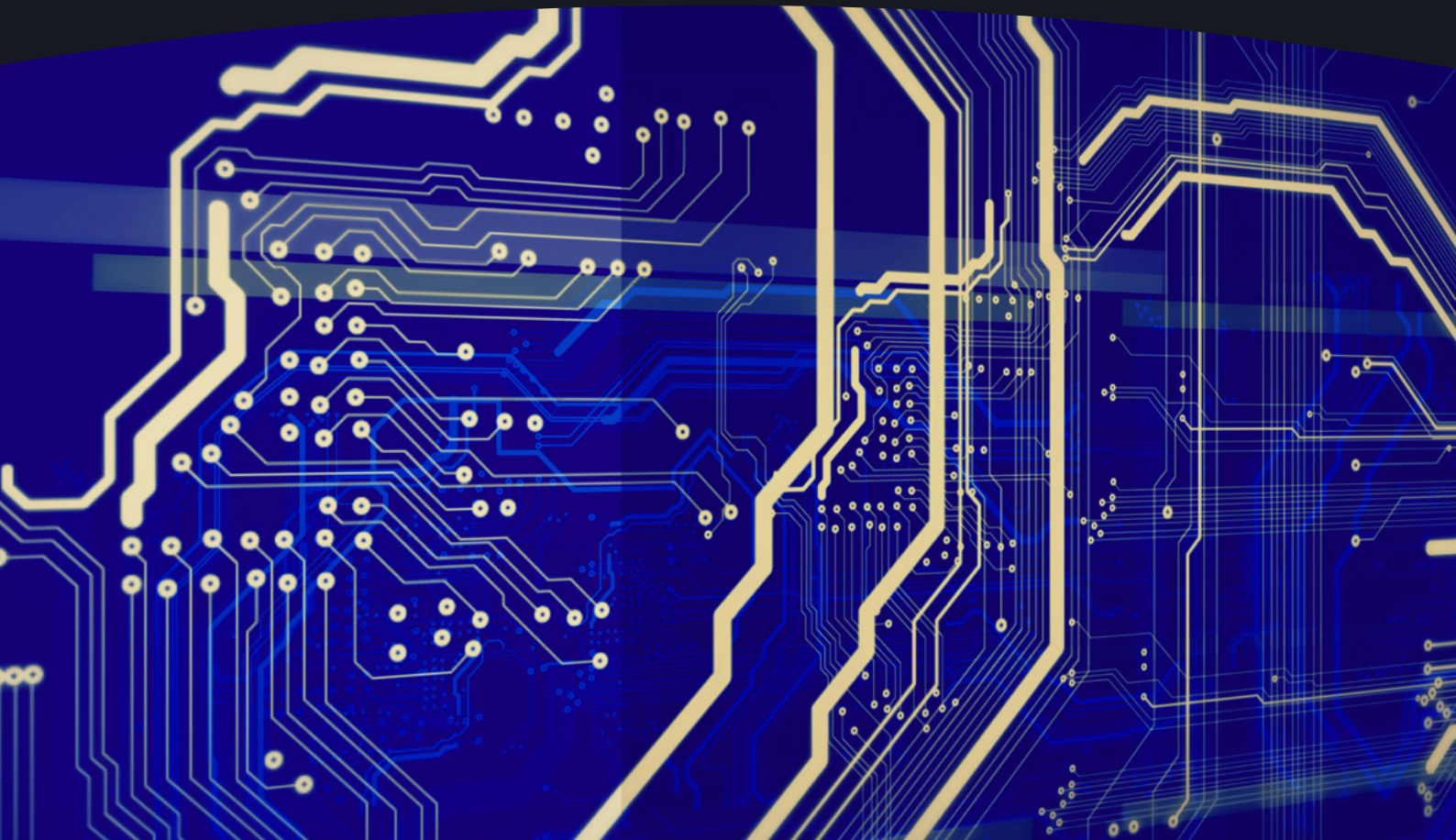
Funded by
the European Union

FULL REPORT

Enabling Technologies and International Security: A Compendium

2024 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 Czechia, France, Germany, Italy, the Netherlands, Norway and Switzerland, and by Microsoft.

The author wishes to thank Giacomo Persi Paoli and Sarah Grand-Clément of UNIDIR's Security and Technology Programme, as well as James Black of RAND Europe, for their thorough reviews 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 (2024 edition)". Geneva, Switzerland: UNIDIR, 2024.

Author

Wenting He is an Associate Researcher in the Security and Technology Programme at UNIDIR. She holds a master's degree in international affairs from the Graduate Institute of International and Development Studies, Geneva, and a bachelor's degree in diplomacy from China Foreign Affairs University, Beijing.

Acronyms & Abbreviations

2D	Two-dimensional
5G	Fifth-generation cellular networks
6G	Sixth-generation cellular networks
AI	Artificial intelligence
AIAAS	Artificial intelligence as a Service
AIOT	Artificial Intelligence of Things
AR	Augmented reality
CSP	Cloud service provider
FLIR	Forward-looking infrared
GAN	Gallium nitride
GPU	Graphics processing unit
HNDL	Harvest Now, Decrypt Later
ICT	Information and communications technology
IOMT	Internet of Military Things
IOT	Internet of Things
ISLL	Inter-satellite laser link
LAWS	Lethal autonomous weapons system
LEO	Low Earth orbit
NM	Nanometre
PNT	Position, Navigation and Timing
PQC	Post-quantum cryptography
QKD	Quantum key distribution
TMD	Transition-metal dichalcogenide
VR	Virtual reality
XR	Extended reality

Contents

Executive Summary

Enabling technologies—such as advanced materials, microchips and sensors, computing power and connectivity infrastructure—are driving innovation across other 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 significant potential for applications in both civilian and military domains. While progress has been made in addressing the security implications of ICTs and lethal autonomous weapons systems (LAWS) within various intergovernmental processes, comparatively less attention has been devoted to the underlying technologies that are enabling 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, UNIDIR's annual Compendium on Enabling Technologies and International Security focuses on identifying and analysing key advancements in enabling technologies, with a particular emphasis on those still in their early stages of development or application. This 2024 edition builds upon the 2023 compendium, providing an update on the latest developments in enabling technologies as they relate to international peace and security. While this edition addresses technological developments and applications specific to 2024, the 2023 compendium remains an essential resource for more detailed foundational analyses.

The compendium categorises enabling technologies into four areas:

- **Category I:** advanced materials, including semiconductors, superconductors and nanotechnology;
- **Category II:** parts and components, such as microchips and sensors;
- **Category III:** processing and computing, covering cloud, edge and quantum computing; and
- **Category IV:** connectivity infrastructure, spanning fifth- and sixth-generation telecommunications (5G and 6G), the Internet of Things (IoT) and satellite communications.

This compendium highlights key trends and developments in 2024 across technology domains under examination. AI's transformative impact is increasingly evident, accelerating breakthroughs in material design, advanced computing and wireless technology while fostering innovation in hardware and infrastructure to address the growing demands of sophisticated AI workloads. While advances continue to enhance civilian and military applications, significant challenges persist, including supply chain vulnerabilities, cybersecurity risks and intensified international competition. Moreover, disparities in access, ethical and legal considerations, and the growing influence of private sector entities underscore the need for responsible development and use of enabling technologies.

1. Introduction

Enabling technologies[1]—such as advanced materials, microchips and sensors, computing power and connectivity infrastructure—are driving innovation and the development of capabilities across other areas, not least in information and communications technologies (ICTs), artificial intelligence (AI) and autonomous systems. Advances in these technologies are revolutionising the digital ecosystem, expanding the possibilities for their development and use for military purposes. As enabling technologies continue to advance, it becomes increasingly important to address their implications for international peace and security. Continuous horizon scanning enables early detection of new and emerging technological developments and their applications, thus playing an important role in the timely assessment of both the benefits and potential risks of these technologies.

In the 2024 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 associated risks.[2] While various intergovernmental processes have made strides in tackling the security implications of certain technology areas, such as ICTs and lethal autonomous weapons systems (LAWS), 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.

To address the knowledge gap, the 2023 Compendium on Enabling Technologies and International Security[3] identified and analysed key advancements in enabling technologies, including those still in the early stages of their development or application but anticipated to have an important future impact on international peace and security. That report presented a comprehensive analysis of these technologies, including their latest developments, emerging military applications, along with their potential implications for international security.

This 2024 edition builds upon its predecessor, providing an update on the latest developments in enabling technologies as they relate to international peace and security. Consistent with the previous iteration, the compendium is organised into four key categories:

- **Category I:** advanced materials, including semiconductors, superconductors and nanotechnology;
- **Category II:** parts and components, such as microchips and sensors;
- **Category III:** processing and computing, covering cloud, edge and quantum computing; and

---

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 technological 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 United Nations General Assembly (2024).

3 The 2023 edition of the Compendium on Enabling Technologies and International Security can be accessed at https://unidir.org/publication/enabling-technologies-and-international-security-a-compendium-2023-edition/.

- **Category IV:** connectivity infrastructure, spanning fifth- and sixth-generation telecommunications (5G and 6G), the Internet of Things (IoT) and satellite communications.

Each section first summarises key takeaways from the 2023 compendium, followed by an analysis of new developments in 2024, including novel military applications. The report concludes with an assessment of overarching trends and advancements in enabling technologies observed during 2024. While this edition focuses on technological developments and applications specific to 2024, the 2023 compendium remains an essential resource for deeper analyses, particularly regarding potential military applications of each enabling technology and their broader international security implications.

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 electronic devices and components including diodes, transistors and integrated circuits.

For decades, the semiconductor industry has been at the forefront of technological innovation, continuously driving advancements in device miniaturisation and performance. Semiconductor technology plays a central role in the widespread adoption of AI, powering the computational capabilities required for AI models and systems.[4] As of 2023, the industry has focused on advancing the miniaturisation of semiconductor materials, particularly through the development of next-generation 2-nanometre (nm) technology.[5] This new technology holds the promise to offer significantly faster processing speeds than existing 3-nm chips. Researcher have also explored alternative materials to silicon, such as cubic boron

[4] Nature Nanotechnology (2024).

[5] Ryugen (2023) and Samsung (2023).

arsenide[6] and two-dimensional (2D) materials,[7] aiming to further enhance microchip performance.[8] Such alternative materials could potentially diversify and strengthen the semiconductor supply chain.

As Moore's Law[9] nears its physical limits, research in 2024 continues to focus on overcoming the constraints of traditional silicon technology. A key area of exploration is the development of novel materials that can surpass the performance of silicon-based devices. One such material is 2D transition-metal dichalcogenides (TMDs), which have been identified as an alternative to silicon. At just 0.7 nm thick—compared to silicon's typical 5-10 nm—TMDs offer lower power consumption, superior electron transport and enhanced computing power.[10] While mass production has been challenging, a new method was developed to rapidly fabricate these 2D crystals in several formulations.[11]

Graphene, a 2D material made of a single layer of carbon atoms arranged in a hexagonal lattice, also offers several advantages over silicon. These include exceptional electron mobility, superior heat dissipation and an ultra-thin, lightweight structure. However, integrating graphene into electronics has proven difficult due to its lack of an intrinsic electron bandgap, which is essential for enabling transistors to switch on and off.[12] Efforts to introduce a bandgap have typically compromised the material's superior electronic properties.[13] In early 2024, researchers overcame this challenge by developing a graphene-based semiconductor compatible with conventional microelectronics processing techniques.[14] This breakthrough promises computing speeds up to ten times faster than traditional silicon technology and could play a critical role in the development of quantum computing.[15]

Given the transformative potential of 2D materials, semiconductor manufacturers are making significant investments in research and integration of these materials.[16] This marks a crucial shift from laboratory development to industrial-scale applications. To guide this transition, leading scholars have proposed a strategic roadmap for advancing 2D materials, calling for a collaborative effort between academia and industry.[17] The roadmap particularly underscores the use of AI tools to meet industrial standards for 2D materials, ensuring both accuracy and efficiency in development.[18]

Other novel semiconductor materials, such as gallium nitride (GaN), are also gaining

---

6 Chandler (2022).

7 Zhang (2023).

8 Section 3.1 below provides a detailed analysis of microchips and the latest developments.

9 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.

10 Zhang (2024).

11 Ibid.

12 Johnson (2024).

13 Ibid.

14 Georgia Institute of Technology (2024).

15 Johnson (2024).

16 Hurtado (2024).

17 Qiu et al. (2024).

18 Ibid.

attention. The development of a quantum light source using GaN is seen as a major step towards functional quantum chips.[19] In addition, scientists have created a microwave chip based on GaN with a diamond substrate, offering 30 per cent higher power density than current products.[20] If widely adopted, this material could significantly improve the performance of not only civilian systems but also military applications, including the development of high-power microwave weapons, radar and communication devices in electronic warfare.[21]

Advances in semiconductor materials will continue to drive innovation, enabling smaller, more efficient devices and advancing transformative AI and quantum technologies. These breakthroughs will also enhance military capabilities, particularly in electronic warfare. However, most alternative semiconductor materials remain in the laboratory phase, and scaling them for mass production remains a work in progress, as demonstrated by the development of 2D materials.[22] Furthermore, the current silicon-based semiconductor supply chain, due to its global and specialised nature, remains vulnerable to disruptions. While novel materials hold the potential to revolutionise current production processes, their widespread adoption will require substantial investments in new manufacturing techniques and infrastructure.

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.

Superconductors are essential for constructing qubits, the fundamental units of quantum processors, and thus play a crucial role in the development of quantum computers.[23] However, as highlighted in the 2023 compendium, their practical use remains limited due to the requirement for extremely low temperatures or, in some cases, high pressures at slightly warmer environments.[24] This challenge spurs continued scientific efforts to identify materials with much higher critical temperatures,[25] particularly aiming for room-temperature superconductivity. While achieving such a breakthrough could revolutionise the field of electronics, research has highlighted the potential of international disputes over patents, technology transfers and market access.[26] This mirrors challenges faced by other cutting-edge technologies.

---

19 Ling (2024).

20 Chen (2024).

21 Ibid.

22 Nature Nanotechnology (2024).

23 Section 4.3 below provides a detailed analysis of quantum computing and the latest developments.

24 For example, superconductivity has been achieved at 203 Kelvin (-70 degrees Celsius) under 1.5 million times atmospheric pressure (https://physicsworld.com/a/superconductivity-endures-to-15-c-in-high-pressure-material/).

25 The critical temperature refers to the temperature below which a material transitions into the superconducting state, characterised by zero electrical resistance and the expulsion of magnetic fields.

26 Roa (2023).

As of 2024, research continues to focus on the search for superconductor materials with significantly higher critical temperatures.[27] One promising approach is the combination of different materials, each with unique electrical properties, to optimise superconductivity. For example, researchers have found that a novel combination of materials exhibits all the necessary characteristics for a new type of superconductivity.[28] This discovery could pave the way for more robust quantum computing.[29]

Beyond quantum computing, superconductors are expected to drastically reduce the energy required to train AI models, as they enable electric current to flow without resistance. While superconductors currently need cryogenic temperatures to function, the anticipated energy savings are expected to outweigh the costs of cooling, particularly as computational demands continue to increase.[30] Furthermore, AI is playing an increasingly important role in superconductor research and development. By leveraging AI alongside quantum mechanical simulations, researchers can now accelerate the prediction and screening of new superconducting materials, facilitating faster innovation in the field.[31]

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).

The use of nanomaterials offers vast opportunities for advancements in sensing, computing and communication technologies. As of 2023, materials such as carbon nanotubes[32] and quantum dots[33] have showed promising potential for next-generation computing, including in the emerging field of quantum computing.[34] However, challenges remain in scaling up their production for practical use. Additionally, research have raised concerns about the toxicity and environmental risks associated with nanoparticles, highlighting potential health and ecological impacts.[35]

In 2024, nanotechnology remains a key driver of device miniaturisation and optimisation. Ongoing research has propelled the development of nanomaterials with enhanced properties and applications. For instance, a more efficient method for synthesising quantum dots has been discovered, a development that is significant as quantum dots could serve as crucial building blocks for improving both quantum and classical computing systems.[36] Moreover, the use of advanced nanomaterials

---

27 For instance, Zhao and Zhang (2024) and Starr (2024).

28 Pennsylvania State University (2024).

29 Ibid.

30 Herr and Herr (2024).

31 Songshan Lake Materials Laboratory (2024).

32 Fadelli (2023).

33 Hecht (2022).

34 Section 4.3 below provides a detailed analysis of quantum computing and the latest developments.

35 Kumah et al. (2023).

36 Dailing (2024).

has enabled a novel encryption technology for visible light communication, offering high levels of security and significant benefits for point-to-point communication systems, such as those used in military operations involving uncrewed systems.[37]

AI and machine learning capabilities have opened new avenues for the development of novel nanomaterials. Advanced computational algorithms enable rapid, cost-effective analysis of nanoparticle behaviour and properties, providing a valuable alternative to traditional experimental methods in nanoscience.[38] For example, scientists have developed a genetic algorithm to design phononic crystal nanostructures that can precisely control specific material properties.[39] This innovation holds the potential to significantly enhance quantum computing and communication technologies.[40]

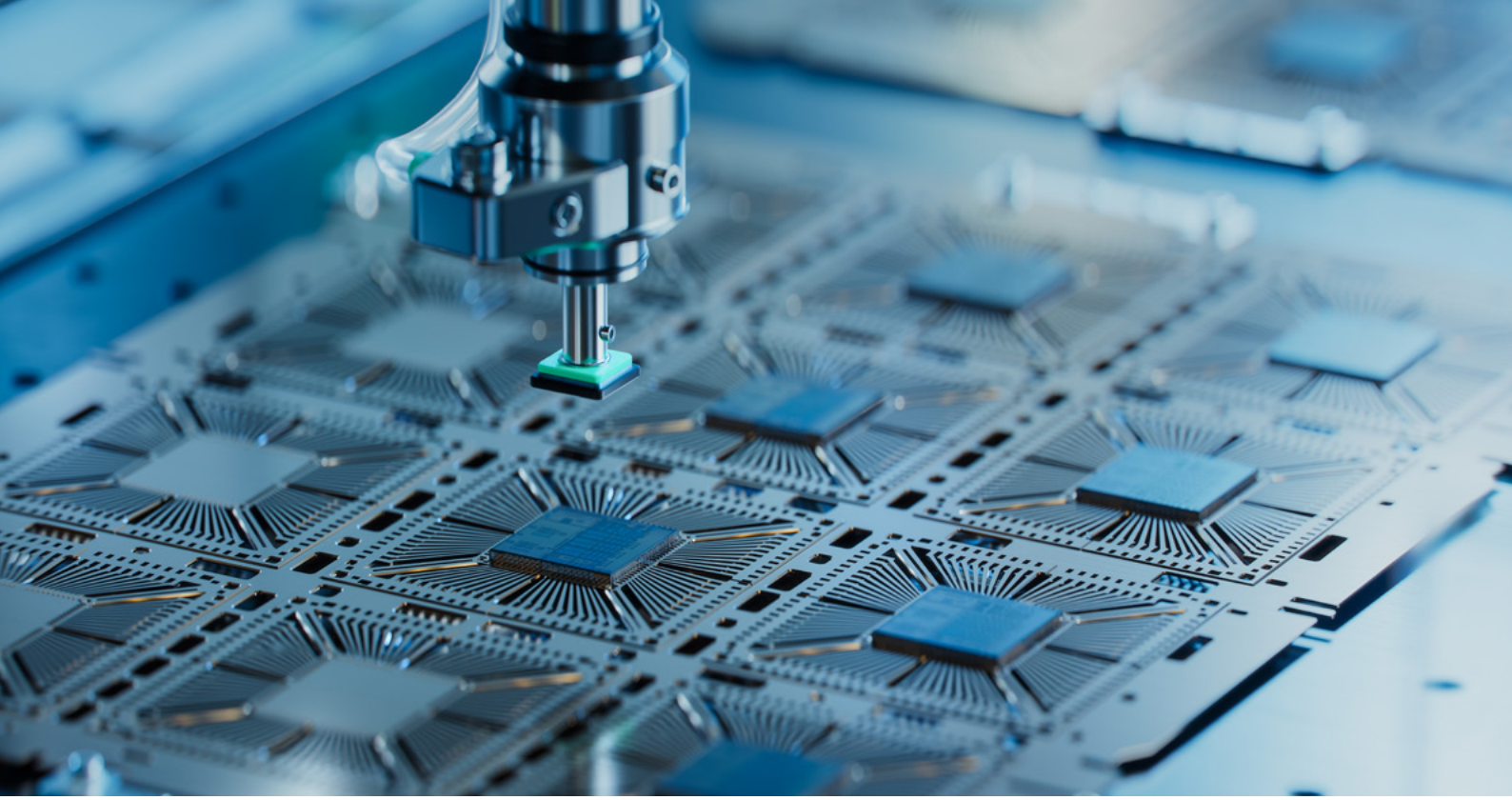
---

37 Seoul National University College of Engineering (2024).

38 Dhull (2024).

39 University of Tokyo (2024).

40 Ibid.



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.

Microchips underpin modern electronics and computing systems, performing critical functions such as information processing, data storage and instruction execution. The 2023 compendium highlighted that progress in the microchip industry has accelerated with advancements in semiconductor technology,[41] chip design and manufacturing techniques. Innovations such as multi-die systems enable highly integrated microchip architectures to support AI models and machine learning at scale,[42] while advancements in novel lithography technology[43] promise to bring next-generation microchips closer to mass production.[44] Despite these technological leaps, challenges such as supply chain vulnerabilities, potential misuse and cybersecurity risks persist.

---

41 Section 2.1 above provides a detailed analysis of semiconductors and the latest developments.

42 MIT Technology Review Insights (2023).

43 Advanced lithography technology such as extreme ultraviolet (EUV) lithography facilitates the creation of ultra-small and highly precise components on silicon wafers and contributes to the continuous miniaturisation of microchips.

44 ASML (n.d.).

Advancements in 2024 remain focused on enhancing microchip performance and tailoring designs for specialised applications. Innovations in semiconductor materials, including an ultra-thin, high-quality semiconductor just 0.7 nm thick, promise to revolutionise microchip efficiency by optimising electron flow and reducing energy consumption.[45] In parallel, photonic technology is gaining momentum.[46] Unlike traditional microchips, photonic microchips use photons—particles of light—to transmit data at higher speeds. Researchers have leveraged photonic technology to enhance processing power and reduce the energy demands of data centres and AI workloads.[47]

Chip design continues to evolve to achieve further performance gains. For instance, next-generation 2-nm microchips feature a direct power routing system that reduces wire tangling, leading to improved energy efficiency.[48] Scientists have also developed microcapacitors with ultra-high energy and power density, allowing energy storage to be integrated directly onto microchips.[49] This minimises power transfer losses between components, boosting energy efficiency in advanced electronics.[50] This advancement will greatly enhance energy efficiency in next-generation electronics. Moreover, as AI applications grow, there is a strong focus on designing specialised microchips tailored to AI workloads. Leading companies such as NVIDIA,[51] AMD[52] and Intel[53] are innovating microchip architectures to optimise performance, power consumption and scalability for AI systems.

Despite these advancements, microchip-related challenges persist. Supply chain security remains a major concern, as the industry relies on a highly globalised, specialised and complex network. For instance, many critical raw materials for microchip production are sourced from a small number of suppliers, creating vulnerabilities due to limited production capacity and potential export control restrictions.[54] Global competition over the development of cutting-edge microchips remains intense, accompanied by ongoing export controls on these advanced technologies. In response, States are increasingly localising production to enhance supply chain security and resilience. This shift has led to a gradual separation and regionalisation of the global microchip supply chain as States aim to reduce reliance on foreign sources.[55]

Furthermore, the dual-use nature of microchips continues to raise proliferation concerns. Microchips can be repurposed for unauthorised military applications, presenting risks of export control circumvention and misuse.[56] Addressing these challenges requires coordinated efforts to secure supply chains, enforce sanctions and export controls and mitigate the risks associated with dual-use technologies.

---

45 Zhang (2024).

46 Rodgers et al. (2024).

47 Winn (2024).

48 Rodgers et al. (2024).

49 Hatt (2024).

50 Ibid.

51 NVIDIA (n.d.).

52 AMD (n.d.).

53 Intel (n.d.).

54 For instance, Cassella (2024) and Dempsey and White (2024).

55 Merle (2024).

56 Zsombor (2024).

3.2. Sensors

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

Innovations in sensor technology play a crucial role in modernising defence capabilities. As noted in the 2023 compendium, armed forces have begun to leverage sensor fusion to enhance battlefield awareness by integrating data from multiple sources, including acoustic, radar and infrared sensors. Quantum sensing has also emerged as a promising tool for military applications, improving object detection[57] and navigation in GNSS-denied environments.[58] Additionally, the integration of AI into sensor systems, including at the edge, has demonstrated the potential to accelerate data processing and decision-making. Beyond military use, advanced sensors could also contribute to international security efforts, by supporting conflict monitoring[59] and hazardous substance detection. However, cybersecurity risks and network challenges constitute key concerns.

As of 2024, advanced sensors remain central to military systems, transforming how armed forces perceive, analyse and respond to threats. Enhancements in forward-looking infrared (FLIR) sensors, for example, have improved targeting accuracy and surveillance for armoured combat vehicles.[60] The ongoing development of sensor fusion technology has further enhanced battlefield intelligence by integrating data from disparate systems to provide real-time, actionable insights.[61] Quantum sensing also remains a key focus of innovation and is now reaching a level of maturity suitable for deployment in military applications.[62] Armed forces have successfully tested quantum sensing technology at sea, offering a reliable alternative for Position, Navigation and Timing (PNT) in GNSS-denied or degraded environments.[63]

As sensors generate ever-increasing volumes of data, the need for real-time processing has driven a shift toward AI-at-the-edge systems for signal analysis.[64] These systems reduce reliance on cloud infrastructure,[65] enabling faster, more secure decision-making. To further optimise processing, airborne data centres are being developed to collect and analyse intelligence directly from diverse sensor sources.[66] These mobile centres address the limitations of fixed ground stations, ensuring timely and efficient delivery of actionable intelligence.[67]

---

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

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

59 Avtar et al. (2021).

60 Keller (2024b).

61 Erwin (2024b).

62 Easley (2024a).

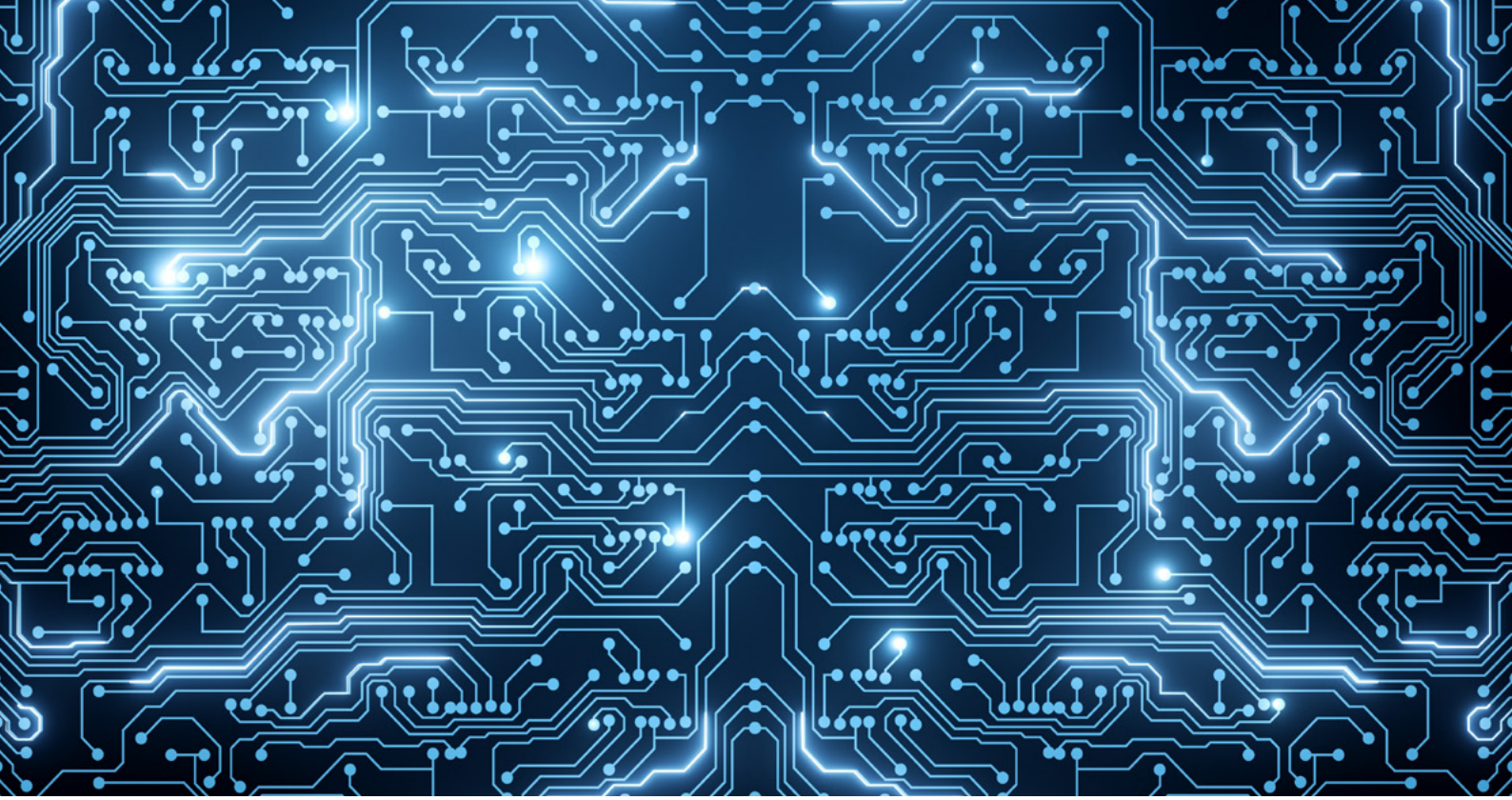
63 Royal Navy (2024).

64 Whitney (2024).

65 Section 4.1 below provides a detailed analysis of cloud computing and the latest developments.

66 Erwin (2024c).

67 Ibid.



4. Category III: Processing and Computing

4.1. Cloud Computing

Cloud computing provides 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[68] has been a catalyst for innovation across diverse technological applications, offering the computational resources necessary for transformative advancements. The 2023 compendium underscored its pivotal role in enabling big data analytics, machine learning, serverless computing and immersive technologies such as augmented reality (AR) and virtual reality (VR). Notably, Artificial intelligence as a Service (AIaaS), delivered through cloud-based platforms, could help to broaden access to advanced AI capabilities. Military forces have increasingly adopted secure cloud environments to enhance operational efficiency, streamline data management and achieve scalability. For instance, cloud computing has facilitated realistic virtual reality training environments and supported large-scale data processing essential for modern operations.

---

[68] The 2023 compendium featured two separate sections on cloud technology: cloud computing and cloud infrastructure. However, in light of recent developments and further research conducted by UNIDIR, we have decided to combine these two areas under a single Cloud Computing section to minimise potential confusion or repetition. The UNIDIR report, titled "Cloud Computing and International Security: Risks, Opportunities and Governance Challenges", provides further analysis on the field of cloud computing and its relevant implications for international security: https://unidir.org/publication/cloud-computing-and-international-security-risks-opportunities-and-governance-challenges/.

The 2023 compendium also highlighted that connectivity challenges, such as high latency in remote areas, could limit the reliability of cloud-based solutions in critical settings. While robust security measures have been implemented, the integration of cloud computing in military contexts remains susceptible to cyber threats.[69] Additionally, the growing involvement of civilians in cyber operations during armed conflicts increases the likelihood of civilian infrastructure, including cloud services, being used for military purposes. This raises concerns about the risk of civilians and civilian infrastructure being targeted during conflicts, undermining the universally supported principle of distinction.[70]

New developments have emerged during 2024 as cloud computing remains a cornerstone of the digital ecosystem. There has been an increasing focus on multi-cloud and hybrid cloud configurations,[71] including within the military domain.[72] These approaches combine the strengths of public cloud solutions with the security of private or on-premises infrastructure while leveraging services from multiple service providers to enhance resilience against potential outages or cyberattacks. To address the increasing complexity of cloud environments, new paradigms such as the adaptive cloud approach have emerged, enabling centralised management of diverse systems and resources, thus improving operational oversight and efficiency.[73]

The synergy between AI and cloud computing is also advancing rapidly. AI-powered cloud platforms are being used to automate resource allocation, optimise storage and bandwidth, and enhance security against cyber threats.[74] Conversely, the rising demand for advanced AI capabilities drives the need for specialised cloud infrastructure tailored to high-performance and energy-efficient applications. AI-centric solutions, such as graphics processing unit (GPU) clouds, provide faster processing speeds, lower latency and cost savings compared to traditional hyperscale cloud environments.[75] Specialised private clouds are also emerging for AI applications, providing dedicated infrastructure equipped with prepackaged AI ecosystems.[76]

Cloud computing is increasingly prioritised over hardware investments to democratise access to transformative technologies such as quantum computing.[77] This shift has the potential to bridge the digital divide, promote inclusive growth and support sustainable development. Robust cloud systems can provide access to cutting-edge technologies, such as AI and real-time data analytics, without the need for significant upfront infrastructure investments.[78] Moreover, integrating cloud with edge computing[79] is unlocking new performance efficiencies. While cloud computing excels in scalability and handling complex tasks, edge solutions can offer real-time, low-latency processing capabilities. This hybrid architecture

---

69 Martin et al. (2023).

70 ICRC (2023).

71 NEXTDC (2024).

72 Gill (2024).

73 MIT Technology Review Insights (2024).

74 Sharma (2024).

75 Oehme (2024).

76 Linthicum (2024).

77 Marr (2024).

78 Gelvanovska-Garcia et al. (2024).

79 Section 4.2 below provides a detailed analysis of edge computing and the latest developments.

combines the strengths of both approaches, enabling novel applications that are both high-speed and highly intelligent.[80]

Militaries continue to leverage secure cloud environments to enhance operational effectiveness. Cloud computing has the potential to provide critical support at both strategic and tactical levels, helping to achieve information superiority over adversaries,[81] in addition to facilitating information-sharing with military allies and partners or with civilian organisations. Cloud service providers (CSPs) are playing an increasingly vital role in delivering cloud services to militaries.[82] Beyond secure data storage, private-sector technology also provides access to advanced AI capabilities, including generative AI.[83] While outsourcing military cloud capabilities to CSPs offers benefits such as improved efficiency and reduced infrastructure maintenance costs, it raises concerns about security and over-reliance on these providers.[84] The concentration of cloud resources among a few major providers exacerbates these risks.[85] Furthermore, the involvement of private companies in delivering cloud services during armed conflicts could introduce complex legal considerations for CSPs as to whether they might become a legitimate military target, potentially posing risks to their employees, properties and civilian clients.[86]

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.

Edge computing reduces latency and shortens response times, making it critical for supporting time-sensitive workloads such as IoT applications.[87] As detailed in the 2023 compendium, the technology offers significant military advantages by enhancing communication, data processing and decision-making capabilities, particularly in remote or extreme environments. Edge platforms can enable AI analytics to function effectively offline, supporting critical missions such as search and rescue operations.[88] However, limitations in processing speed, memory and power could constrain the efficiency of military edge devices.[89] Additionally, the expanded attack surfaces and vulnerability to physical damage associated with edge systems highlight the need for stronger defences, including advanced encryption protocols.[90]

---

80 Marr (2024).

81 European Defence Agency (2024).

82 For instance, Australian Government (2024) and Perrigo (2024).

83 Easley (2024b).

84 European Defence Agency (2024).

85 Pendleton and Levite (2024).

86 Horowitz (2024).

87 Section 5.2 below provides a detailed analysis of IoT applications and the latest developments.

88 Thomas (2021).

89 Miller and Lohn (2023).

90 Konkel (2023).

Throughout 2024, edge computing continues to expand rapidly, driven by its integration with other emerging technologies and the rising demand for real-time data processing. A significant focus has been placed on advancing AI capabilities at the edge. Rather than relying on centralised data centres, AI processing can now occur directly on mobile devices such as smartphones and laptops. This shift enhances privacy, reduces latency and minimises dependence on internet connectivity. These advantages have driven investment in creating faster, more efficient microchips suitable for use in edge systems, with promising applications in both civilian and military domains.[91] In addition, the development of small language models (SLMs) for edge devices is also advancing, with an emphasis on optimising performance in resource-constrained environments.[92] While key challenges persist, techniques such as model compression, knowledge distillation and federated learning offer promising solutions to overcome the limitations of edge systems and improve efficiency.[93]

The deployment of edge AI continues to gain traction in the military domain. Innovations from the private sector have enhanced edge AI capabilities by integrating robust security measures, including encryption, firewalls and data isolation, with the potential to support critical military use cases including the navigation of autonomous vehicles.[94] As the volume of data processed at the edge increases, safeguarding sensitive information remains a top priority. Integrating blockchain technology has emerged as a promising solution to enhance security and integrity in edge environments. By providing a decentralised and distributed ledger, blockchain can allow each edge device to independently verify and protect locally processed data.[95]

4.3. Quantum Computing

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

Quantum computing,[96] though still in its early stages, holds transformative potential to redefine computational limits. Significant progress has been achieved by 2023, led by private sector entities such as IBM, Google/Alphabet and Microsoft. IBM, in particular, has steadily increased the number of qubits—the fundamental units of quantum information—on a single chip,[97] while making strides in scaling quantum processors.[98] Empirical research has also suggested that hybrid networks combining classical and quantum computers could enhance machine learning

---

91 O'Donnell (2024).

92 Vijayabaskar (2024).

93 Ibid.

94 Welch (2024).

95 Gu (2024).

96 The UNIDIR report, titled "Quantum Technology, Peace and Security: A Primer", provides further analysis on the field of quantum computing and its relevant implications for international security: https://unidir.org/publication/quantum-technology-peace-and-security-a-primer/.

97 Gambetta (2023).

98 Brooks (2023).

model training,[99] with notable implications for military AI, including the development of more precise lethal autonomous weapons systems.[100] However, the rapid evolution of quantum computing has also raised cybersecurity concerns, particularly the threat of 'Harvest Now, Decrypt Later' (HNDL) attacks, which could compromise widely-used cryptographic algorithms.[101] In response to emerging quantum threats, continuous efforts are underway to develop post-quantum cryptography (PQC).

While quantum computing has yet to establish a definitive advantage over classical computing in 2024, progress has been driven by increasing investments and interest from both private companies and governments.[102] Leading companies are focused on reducing error rates and enhancing system performance. For instance, IBM's latest Heron quantum processor, paired with its Qiskit quantum software, has achieved significant improvements in speed and accuracy, bringing practical quantum applications closer to reality.[103] The company's Quantum Roadmap outlines ambitious plans to achieve quantum-centric supercomputing, improve scalability and develop fully error-corrected quantum systems in the coming years.[104] AI is playing an increasingly pivotal role in advancing quantum computing. Google has partnered with NVIDIA to harness AI-driven supercomputing for designing next-generation quantum processors, aiming to overcome current hardware limitations.[105]

Quantum computing's military applications are also gaining attention despite the technology's nascent stage. Key areas of exploration include integrating quantum and quantum-hybrid technologies into machine learning to address complex computational challenges.[106] Militaries are also exploring the use of quantum key distribution (QKD) technologies to secure sensitive communications against potential eavesdropping.[107] However, ethical concerns are emerging around the use of quantum technologies in defence. The complexity of quantum algorithms, for instance, could make them difficult to reverse-engineer, creating a 'responsibility gap' where accountability for their outcomes becomes unclear.[108] This issue mirrors risks associated with the use of AI in military contexts. Moreover, the potential for quantum computers to compromise current cryptographic systems—including military-grade encryption[109]—underscores the urgent need to prioritise security and privacy in the ongoing development of quantum computing.[110]

---

99 Xu (2023).

100 US Congressional Research Service (2024).

101 van Amerongen (2021).

102 Duranton (2024) and Howard et al. (2024).

103 IBM (2024b).

104 IBM (2024a).

105 NVIDIA (2024).

106 Keller (2024a).

107 Gill (2022).

108 Taddeo et al. (2024).

109 Baker (2024).

110 University of Oxford (2024).

5. Category IV: Connectivity 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.

Wireless technology provides fundamental infrastructure for the interconnected digital ecosystem, facilitating seamless communication, enhancing network reliability and supporting a wide range of innovative applications. The 2023 compendium underscored the critical role of fifth-generation (5G) cellular networks, particularly in military applications ranging from secure communication and high-speed data transfer to integrating advanced AI and IoT systems.[111] However, the widespread adoption of 5G has also highlighted cybersecurity challenges, stemming from increased data volumes, interconnected devices, and reliance on open, cloud-based infrastructure.[112] Concurrently, research into sixth-generation (6G) networks has begun, with aspirations to provide global connectivity across land, sea, air and space using integrated satellite–terrestrial systems.[113]

---

[111] Section 5.2 below provides a detailed analysis of IoT applications and the latest developments.

[112] Śliwa and Suchański (2022).

[113] Chen et al. (2023).

While 5G coverage and adoption continue to expand in 2024, attention is shifting toward next-generation advancements. 5G-Advanced, an evolution of current 5G technology, is poised to unlock greater capabilities and efficiency.[114] This update focuses on optimising network power consumption and improving support for cutting-edge applications such as extended reality (XR),[115] autonomous vehicles, and IoT systems. Key enhancements include the integration of machine learning capabilities to enable intelligent network management.[116] The first 5G-Advanced specification, released by the 3rd Generation Partnership Project (3GPP),[117] was finalised for implementation in June 2024, marking a step towards greater performance, efficiency and resilience.[118]

Meanwhile, 6G remains in the early stages of research and development, with substantial efforts underway to define standards and explore its transformative potential. The International Telecommunication Union (ITU) has introduced the IMT-2030 Framework to guide the development of standards and radio interface technologies for 6G systems,[119] while 3GPP and industry stakeholders are also preparing detailed specifications.[120] 6G networks are expected to integrate AI more deeply into their core architecture, enabling real-time data analysis, performance optimisation and enhanced cybersecurity measures.[121]

The anticipated capabilities of AI-driven 6G technology are generating significant interest in military applications. Potential use cases include robotics, autonomous systems, virtual reality training environments and advanced sensing capabilities.[122] However, there are also concerns about relying on a profit-driven sector to supply cutting-edge wireless technology for the defence sector's increasingly complex network demands.[123] This underscores the importance of balancing innovation with security considerations as wireless technology continues to evolve.

---

[114] Nokia (n.d.).

[115] Extended reality (XR) is an umbrella term that encompasses augmented reality (AR), virtual reality (VR), mixed reality (MR) and other immersive technologies.

[116] Etengoff (2024).

[117] 3GPP is a collaborative body that brings together several telecommunications standard development organisations from different regions. Established in 1998 to create 3G mobile standards, 3GPP has since become a leading organisation in the development and standardisation of mobile telecommunications technologies.

[118] Toskala (2024).

[119] ITU (2023).

[120] Larsson (2024).

[121] IEEE (2024).

[122] Albon (2024).

[123] Heckmann (2024).

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.

The Internet of Things creates interconnected ecosystems that enhance performance and efficiency. As of 2023, there has been an increased integration of IoT technology into military systems. The Internet of Military Things (IoMT) utilises diverse sensors[124] across various domains to improve situational awareness and control,[125] as well as targeting precision, with the potential to reduce civilian casualties in combat zones.[126] However, without robust communications protocols in place, the adoption of IoT in military systems could introduce significant cybersecurity risks. IoMT networks may expand the attack surface, posing threats not only to military operations but also to other critical sectors.[127]

In 2024, civilian and dual-use IoT technology continues to evolve, driven by innovations in AI, edge computing[128] and cellular networks.[129] The integration of AI into IoT systems, termed the Artificial Intelligence of Things (AIoT), has emerged as a transformative trend. By combining IoT's data-collection capabilities with AI's pattern recognition and decision-making, AIoT enhances the efficiency and functionality of IoT operations.[130] Additionally, the development of 5G-Advanced cellular networks promises to further elevate IoT performance, delivering faster, more reliable and energy-efficient connectivity.[131]

In the military domain, IoT adoption is expanding through advancements in drone technology, communication systems and increased reliance on satellite networks.[132] Nevertheless, cybersecurity remains a critical concern, with a continued push to implement robust security frameworks for IoMT devices, such as adopting the 'zero-trust' model,[133] to mitigate vulnerabilities and safeguard sensitive operations.

---

[124] Section 3.2 above provides a detailed analysis of sensors and the latest developments.

[125] Withrington (2023).

[126] Douglass (2022).

[127] Renals (2021).

[128] Section 5.2 below provides a detailed analysis of IoT applications and the latest developments.

[129] Section 5.1 below provides a detailed analysis of cellular technology and the latest developments.

[130] Gibson (2024).

[131] Ericsson (n.d.).

[132] Blair (2024).

[133] Mitchell (2024). Zero-trust model refers to a cybersecurity approach that mandates stringent verification processes for every user, device and application attempting to access resources, regardless of whether they are located inside or outside the network perimeter.

5.3. Satellite Communications

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

Satellite communications has witnessed significant developments by 2023, marked in particular by the rapid growth of low Earth orbit (LEO) satellite constellations such as SpaceX's Starlink system. These systems enhance global connectivity[134] and play an increasingly critical role in maintaining communication during conflicts.[135] In addition, progress in integrating quantum key distribution into satellite systems holds promise for heightened communication security.[136] Despite these advancements, satellite communication faces several security challenges, including potential cyber threats[137] and the persistent issue of space debris.[138] As military forces increasingly utilises commercial satellite technologies, concerns have arisen about differing incentives, operating principles and accountability mechanisms between public and private entities.[139]

Innovations in satellite technology in 2024 continue to offer advantages across civilian and military domains. LEO satellites remain pivotal in delivering high-speed data transmission and supporting applications such as missile warning and control systems.[140] Advances in laser technology also promise further improvements in communication efficiency through inter-satellite laser links (ISLLs), enabling high-speed data exchange between satellites and with ground stations. Space laser communication systems are expected to achieve data transfer speeds up to 100 times faster than traditional radio frequency systems.[141] In addition, AI is playing an increasingly central role in satellite communication innovations, including enhancing network management and optimising satellite operations.[142]

Moreover, the ongoing development of direct-to-cell satellite technology in the commercial sector aims to facilitate direct communication—text, voice and data—between satellites and mobile devices. By offering ubiquitous coverage and resilient connectivity, this capacity has the potential to transform existing military satellite communication systems.[143] As military reliance on commercial satellite services grows, cybersecurity remains a pressing concern.[144] Advances in QKD technology can help to achieve more robust and secure communication systems, although several technical challenges still need to be addressed.[145] Additionally, laser technology also offers enhanced security due to its point-to-point nature, which reduces the risks of jamming and interception.[146]

---

[134] Marquina (2022).

[135] Jayanti (2023).

[136] European Space Agency (2022).

[137] Menn (2023).

[138] Mukherjee (2021).

[139] Jayanti (2023).

[140] South (2024).

[141] Bernacchi (2024).

[142] Rainbow (2024).

[143] Erwin (2024c).

[144] Ibid.

[145] Swayne (2024a).

[146] Ruitenberg (2024).

6. Conclusion

In 2024, novel developments and applications across enabling technologies continue to deliver significant advantages in both civilian and military settings. Advances in material science, for instance, are enabling the production of smaller, more efficient components that offer higher performance for advanced applications, such as AI and quantum technologies. In addition, connectivity and system integration remain central to technological innovation. The development of 5G-Advanced, along with early-stage 6G research, signals a commitment to achieving faster, more reliable global communication. Meanwhile, enhanced IoT ecosystems, supported by AI and edge computing, are delivering real-time decision-making capabilities that are crucial in dynamic environments, including defence operations.

AI's transformative impact is increasingly evident across nearly all categories of enabling technologies. It has accelerated innovation in fields such as semiconductors and nanotechnology, aiding in the creation of new materials with improved properties. The ongoing integration of AI capabilities into sensors, edge computing and wireless technology also marks a significant advancement, driving the development of smarter and more efficient systems. Furthermore, the large-scale data processing needs and specific demands of AI workloads are in turn spurring innovation in related hardware and infrastructure, including microchips and cloud infrastructure.

The integration of enabling technologies in military systems is accelerating their modernisation and enhancing capabilities such as situational awareness, data processing and precision targeting. However, the rapid deployment of enabling technologies could introduce new vulnerabilities and exacerbate existing ones, including risks related to supply chains and cybersecurity. Advances in these technologies also continue to intensify international technological competition, particularly in emerging fields such as quantum computing.[147] It is important to note that the resources and infrastructure needed to support the development and use of cutting-edge technologies are often concentrated in a small number of countries, as in the case of computing resources essential for running AI models and systems.[148] This disparity underscores the issue of inequalities in access and technological capabilities across regions, which could be compounded further by export control restrictions tied to technological competition and national security considerations.

Furthermore, ethical and legal challenges are increasingly evident in the potential military applications of technologies such as cloud and quantum computing, highlighting the urgent need for normative and governance frameworks to ensure their responsible development and use. Additionally, the private sector remains a critical driver of progress and innovation, delivering state-of-the-art and cost-effective services across sectors, including defence. However, growing reliance on private entities raises concerns, such as differing incentives with the public sector and the risk of service disruptions stemming from incidents affecting the broader infrastructure of private companies.

Advancements in enabling technologies will continue to have profound implications for

[147] Swayne (2024b).

[148] Lehdonvirta et al. (2024).

military practices and international security. This underscores the necessity of continuous horizon scanning to identify new and emerging weak signals and developments, as well as the need for further examination of potential governance frameworks to harness opportunities while mitigating risks. Moreover, the cross-cutting nature of these technologies—where advancements in one domain often drive or are driven by progress in another—must be carefully studied to fully understand their interconnected potential and broader implications.

References

Albon, Courtney. 2024. “Pentagon readies for 6G, the next of wave of wireless network tech”. Defense News. 13 September. https://www.defensenews.com/pentagon/2024/09/13/pentagon-readies-for-6g-the-next-of-wave-of-wireless-network-tech/

AMD. n.d. “AMD Instinct™ MI300 Series Accelerators”. https://www.amd.com/en/products/accelerators/instinct/mi300.html

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

Australian Government. 2024. “Australian Government Announces Top Secret Cloud”. 4 July. https://www.oni.gov.au/news/australian-government-announces-top-secret-cloud

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

Baker, Berenice. 2024. “Military-Grade Encryption Broken by Quantum Computer”. IoT World Today. 14 October. https://www.iotworldtoday.com/quantum/military-grade-encryption-broken-by-quantum-computer

Bernacchi, Giulia. 2024. “France Claims Word-First Satellite Communication Via Space Lasers”. The Defense Post. 25 September. https://thedefensepost.com/2024/09/25/france-satellite-communication-space-lasers/

Blair, Alex. 2024. “Will IoT in defence continue to grow amid cybersecurity concerns?”. Army Technology. 4 March. https://www.army-technology.com/features/will-iot-in-defence-continue-to-grow-amid-cybersecurity-concerns/

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

Cassella, Megan. 2024. “How a tiny town hit by Helene could upend the global semiconductor chip industry”. CNBC. 3 October. https://www.cnbc.com/2024/10/03/helene-quartz-mine-semiconductor-north-carolina.html

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

Chen, Stephen. 2024. “Chinese scientists produce powerful microwave chip for electronic warfare using diamond”. South China Morning Post. 22 February. https://www.scmp.com/news/china/science/article/3252815/chinese-scientists-produce-powerful-microwave-chip-electronic-warfare-using-diamond

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

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

Dailing, Paul. 2024. “Cracking the code: Researchers unlock a ‘new synthetic frontier’ for quantum dots”. Phys.org. 26 October. https://phys.org/news/2024-10-code-synthetic-frontier-quantum-dots.html

Dempsey, Harry and Edward White. 2024. “China’s export curbs on semiconductor materials stoke chip output fears”. Financial Times. 27 August. https://www.ft.com/content/9cd56880-4360-4e11-8c22-e810d3787e88

Dhull, Nidhi. 2024. “Why is Computer Modeling Important to Nanoscience Research?”. AZoNano. 17 April. https://www.azonano.com/article.aspx?ArticleID=6720

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). https://doi.org/10.1002/9781119892199.fmatter

Duranton, Sylvain. 2024. “Quantum Computing Takes Off With $55 Billion In Global Investments”. Forbes. 26 June. https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/

Easley, Mikayla. 2024a. “DIU launches new emerging tech portfolio, solicits industry for quantum sensing capabilities”. DefenseScoop. 9 May. https://defensescoop.com/2024/05/09/diu-transition-quantum-sensors-emerging-technologies-portfolio/

—. 2024b. “Army implements generative AI platform to cArmy cloud environment”. DefenseScoop. 10 September. https://defensescoop.com/2024/09/10/army-generative-ai-capability-carmy-cloud/

Ericsson. n.d. “5G Advanced”. https://www.ericsson.com/en/5g/5g-for-service-providers/5g-advanced

Erwin, Sandra. 2024a. “New direct-to-cell satellite tech could disrupt billion-dollar military satcom programs”. Space News. 10 June. https://spacenews.com/new-direct-to-cell-satellite-tech-could-disrupt-billion-dollar-military-satcom-programs/

—. 2024b. “Boeing to demonstrate air-space sensor fusion for U.S. military operations”. Space News. 18 September. https://spacenews.com/boeing-to-demonstrate-air-space-sensor-fusion-for-u-s-military-operations/

—. 2024c. “Northrop Grumman unveils flying data center for military intelligence”. Space News. 21 October. https://spacenews.com/northrop-grumman-unveils-flying-data-center-for-military-intelligence/

Etengoff, Aharon. 2024. “What to expect from 5G-Advanced”. 5G Technology World. 21 August. https://www.5gtechnologyworld.com/what-to-expect-from-5g-advanced/#

European Defence Agency. 2024. “‘Combat cloud’: EDA study shows benefits of cloud computing for EU militaries”. 25 January. https://eda.europa.eu/news-and-events/news/2024/01/25/combat-cloud-eda-study-shows-benefits-of-cloud-computing-for-eu-militaries

European Space Agency (ESA). 2022. “Quantum Encryption to Boost European Autonomy”. 22 September. 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. https://phys.org/news/2023-07-scaling-aligned-carbon-nanotube-transistors.html

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

Gelvanovska-Garcia, Natalija et al. 2024. “Bridging the digital divide: Harnessing data through cloud computing”. World Bank Blogs. 30 May. https://blogs.worldbank.org/en/digital-development/bridging-the-digital-divide--harnessing-data-through-cloud-compu

Georgia Institute of Technology. 2024. “Researchers Create First Functional Semiconductor Made From Graphene”. 4 January. https://research.gatech.edu/feature/researchers-create-first-functional-semiconductor-made-graphene

Gibson, Ryan. 2024. “The AIoT Revolution: How the Fusion of Artificial Intelligence and the Internet of Things is Shaping the Future”. WPN. 3 September. https://www.webpronews.com/the-aiot-revolution-how-the-fusion-of-artificial-intelligence-and-the-internet-of-things-is-shaping-the-future/

Gill, Jaspreet. 2022. “‘Disruptive impact’: India’s military starts investing in quantum key distribution”. Breaking Defense. 1 September. https://breakingdefense.com/2022/09/disruptive-impact-indias-military-starts-investing-in-quantum-key-distribution/

—. 2024. "'JWCC 1 year in: Military branches test the waters as DoD envisions cloud service 2.0". Breaking Defense. 5 February. https://breakingdefense.com/2024/02/jwcc-1-year-in-military-branches-test-the-waters-as-dod-envsions-cloud-service-2-0/

Gu, Ronghui. 2024. "Decentralizing Cybersecurity: How Blockchain and Edge Computing Can Strengthen Data Security". The Fast Mode. https://www.thefastmode.com/expert-opinion/37666-decentralizing-cybersecurity-how-blockchain-and-edge-computing-can-strengthen-data-security

Hatt, Alison. 2024. "Groundbreaking Microcapacitors Could Power Chips of the Future". 6 May. https://newscenter.lbl.gov/2024/05/06/groundbreaking-microcapacitors-could-power-chips-of-the-future/

Hecht, Jeff. 2022. "Nanomaterials Pave the Way for the Next Computing Generation". *Nature*. 10 August. https://www.nature.com/articles/d41586-022-02147-3

Heckmann, Laura. 2024. "Military Struggles to Make Inroads With 5G Commercial Wireless Tech". National Defense. https://www.nationaldefensemagazine.org/articles/2024/8/5/military-struggles-to-make-inroads-with-5g-commercial-wireless-tech

Herr, Anna and Quentin Herr. 2024. "How to Put a Data Center in a Shoebox: Imec's plan to use superconductors to shrink computers". IEEE Spectrum. 15 May. https://spectrum.ieee.org/superconducting-computer

Horowitz, Jonathan. 2024. "One Click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict". *Chicago Journal of International Law*. Vol. 24 No. 2. https://cjil.uchicago.edu/print-archive/one-click-conflict-some-legal-considerations-related-technology-companies-providing

Howard, Nigel et al. 2024. "Quantum Computing: Developments in the UK and US". Inside Global Tech. 9 August. https://www.insideglobaltech.com/2024/08/09/quantum-computing-developments-in-the-uk-and-us/

Hurtado, Jorge. 2024. "Next-gen semiconductors: The 7-year roadmap to integrating 2D materials". July. https://www.prescouter.com/2024/07/roadmap-to-integrating-2d-materials/

IBM. 2024a. "IBM Quantum Roadmap". October. https://www.ibm.com/roadmaps/quantum.pdf

—. 2024b. "IBM Launches Its Most Advanced Quantum Computers, Fueling New Scientific Value and Progress towards Quantum Advantage". 13 November. https://newsroom.ibm.com/2024-11-13-ibm-launches-its-most-advanced-quantum-computers,-fueling-new-scientific-value-and-progress-towards-quantum-advantage

ICRC. 2023. "We call on States to stop turning a blind eye to the participation of civilian hackers in armed conflict". 14 December. https://www.icrc.org/en/statement-cyber-oewg-sixth-session

IEEE. 2024. "The Roadmap to 6G: AI Empowered Wireless Networks". 25 July. https://testbed.ieee.org/the-roadmap-to-6g-ai-empowered-wireless-networks/

Intel. n.d. "Intel Gaudi AI Accelerator: First Generation Deep Learning Training & Inference Processor". https://habana.ai/products/gaudi/

ITU. 2023. "ITU advances the development of IMT-2030 for 6G mobile technologies". 1 December. https://www.itu.int/en/mediacentre/Pages/PR-2023-12-01-IMT-2030-for-6G-mobile-technologies.aspx

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. https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

Johnson, Dexter. 2024. "Researchers Claim First Functioning Graphene-Based Chip". IEEE Spectrum. 18 January. https://spectrum.ieee.org/graphene-semiconductor

Johnston, Hamish. 2020. "Superconductivity endures to 15 °C in high-pressure material". Physics World. 14 October. https://physicsworld.com/a/superconductivity-endures-to-15-c-in-high-pressure-material/

Keller, John. 2024a. “Researchers approach industry to test and evaluate quantum computing for applications like machine learning”. Military Aerospace Electronics. 14 August. https://www.militaryaerospace.com/computers/article/55132726/quantum-computing-machine-learning-test-and-evaluate

—. 2024b. “RTX Raytheon to upgrade forward-looking infrared (FLIR) targeting sensors aboard armored combat vehicles”. Military Aerospace Electronics. 6 November. https://www.militaryaerospace.com/sensors/article/55240736/raytheon-technologies-corp-forward-looking-infrared-flir-armored-combat-vehicles-targeting

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

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

Larsson, Daniel Chen. 2024. “6G standardization – an overview of timeline and high-level technology principles”. Ericsson. 22 March. https://www.ericsson.com/en/blog/2024/3/6g-standardization-timeline-and-technology-principles

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

Lehdonvirta, Vili et al. 2024. “Compute North vs. Compute South: The Uneven Possibilities of Compute-based AI Governance Around the Globe”. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 7(1), 828-838. https://doi.org/10.1609/aies.v7i1.31683

Ling, Xin. 2024. “Chinese team makes quantum leap in chip design with new light source”. South China Morning Post. 20 April. https://www.scmp.com/news/china/science/article/3259756/chinese-team-makes-quantum-leap-chip-design-new-light-source

Linthicum, David. 2024. “The rise of specialized private clouds”. InfoWorld. 11 November. https://www.infoworld.com/article/3602661/the-rise-of-specialized-private-clouds.html

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

Marr, Bernard. 2024. “The 7 Revolutionary Cloud Computing Trends That Will Define Business Success In 2025”. Forbes. 4 November. https://www.forbes.com/sites/bernardmarr/2024/11/04/the-7-revolutionary-cloud-computing-trends-that-will-define-business-success-in-2025/

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

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

Merle, Quentin. 2024. “Chips Supply Chain: Bifurcation and Localization”. ETH Zurich. https://css.ethz.ch/en/center/CSS-news/2024/07/chips-supply-chain-bifurcation-and-localization.html

Miller, Kyle and Andrew Lohn. 2023. “Onboard AI: Constraints and Limitations”. Center for Security and Emerging Technology (CSET). August. 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. https://wp.technologyreview.com/wp-content/uploads/2023/03/Synopsys-Report-v6.pdf

—. 2024. “Advancing to adaptive cloud”. 8 August. https://www.technologyreview.com/2024/08/08/1095619/advancing-to-adaptive-cloud/

Mitchell, Billy. 2024. “Senate NDAA calls for guidance to apply zero trust to ‘internet of military things’ devices”. Defense Scoop. 10 July. https://defensescoop.com/2024/07/10/senate-2025-ndaa-zero-trust-internet-of-military-things-devices/

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

Nature Nanotechnology. 2024. “Reimagining computing with 2D semiconductors”. 18 July. https://doi.org/10.1038/s41565-024-01743-w

NEXTDC. 2024. “The Rise of Hybrid and Multi-Cloud Computing Architecture”. 15 February. https://www.nextdc.com/blog/the-rise-of-hybrid-and-multi-cloud-computing-architecture

Nokia. n.d. “5G-Advanced explained”. https://www.nokia.com/about-us/newsroom/articles/5g-advanced-explained/

NVIDIA. n.d. “NVIDIA Blackwell Architecture”. https://www.nvidia.com/en-us/data-center/technologies/blackwell-architecture/

—. 2024. “NVIDIA Accelerates Google Quantum AI Processor Design With Simulation of Quantum Device Physics”. 18 November. https://nvidianews.nvidia.com/news/nvidia-supercharges-google-quantum-processor-design-with-simulation-of-quantum-device-physics

O’Donnell, James. 2024. “What’s next in chips”. MIT Technology Review. 13 May. https://www.technologyreview.com/2024/05/13/1092319/whats-next-in-chips/

Oehme, Sven. 2024. “AI Is Accelerating the Demand for Cloud, But Which Type?”. Forbes. 17 June. https://www.forbes.com/councils/forbestechcouncil/2024/06/17/ai-is-accelerating-the-demand-for-cloud-but-which-type/

Pendleton, John and Ariel Levite. 2024. “Our Lives Depend on the Cloud. Now What?”. Just Security. 6 August. https://www.justsecurity.org/98445/our-lives-depend-on-cloud/

Pennsylvania State University. 2024. “Combining materials may support unique superconductivity for quantum computing”. Phys.org. 8 February. https://phys.org/news/2024-02-combining-materials-unique-superconductivity-quantum.html

Perrigo, Billy. 2024. “Exclusive: Google Contract Shows Deal With Israel Defense Ministry”. Time. 12 April. https://time.com/6966102/google-contract-israel-defense-ministry-gaza-war/

Qiu, Hao et al. 2024. “Two-dimensional materials for future information technology: status and prospects”. *Science China Information Sciences* 67, 160400 (2024). https://doi.org/10.1007/s11432-024-4033-8

Rainbow, Jason. 2024. “Improving Space AI: Ground-to-orbit efforts aim to advance satellite intelligence”. Space News. 12 November. https://spacenews.com/improving-space-ai-ground-orbit-efforts-aim-advance-satellite-intelligence/

Renals, Pete. 2021. “Future Developments in Military Cyber Operations and Their Impact on the Risk of Civilian Harm”. ICRC Humanitarian Law & Policy. 24 June. 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. https://nationalinterest.org/feature/have-we-created-philosopher%E2%80%99s-stone-policymakers-should-care-about-room-temperature

Rodgers, Lucy et al. 2024. “Inside the miracle of modern chip manufacturing”. Financial Times. 28 February. https://ig.ft.com/microchips/

Royal Navy. 2024. “Royal Navy successfully tests quantum-sensing technology”. 31 October. https://www.royalnavy.mod.uk/news/2024/october/31/20241101-royal-navy-successfully-tests-quantum-sensing-technology

Ruitenberg, Rudy. 2024. “France tests space lasers for secure satellite downlink in world first”. Defense News. 13 September. https://www.defensenews.com/global/europe/2024/09/13/france-tests-space-lasers-for-secure-satellite-downlink-in-world-first/

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

Samsung. 2023. “Samsung Electronics Unveils Foundry Vision in the AI Era at Samsung Foundry Forum 2023”. https://news.samsung.com/global/samsung-electronics-unveils-foundry-vision-in-the-ai-era-at-samsung-foundry-forum-2023

Seoul National University College of Engineering. 2024. “Novel visible light communication encryption technology uses chiral nanoparticles”. Phys.org. 10 October. https://phys.org/news/2024-10-visible-communication-encryption-technology-chiral.html

Sharma, Alkesh. 2024. “Oracle founder Larry Ellison says AI-powered cloud systems will thwart cyber attacks”. The National. 11 September. https://www.thenationalnews.com/future/technology/2024/09/10/oracle-founder-larry-ellison-says-ai-powered-cloud-systems-will-thwart-cyber-attacks/

Śliwa, Joanna and Marek Suchański, 2022. “Security threats and countermeasures in military 5G systems”. *2022 24th International Microwave and Radar Conference (MIKON), Gdansk, Poland*. https://ieeexplore.ieee.org/document/9924818

Starr, Michelle. 2024. “Superconductor Feature Seen Operating at Temperatures Once Thought Impossible”. ScienceAlert. https://www.sciencealert.com/superconductor-feature-seen-operating-at-temperatures-once-thought-impossible

Songshan Lake Materials Laboratory. 2024. “Coupling quantum mechanical simulations and AI paves way for screening new superconductors”. Phys.org. 16 May. https://phys.org/news/2024-05-coupling-quantum-mechanical-simulations-ai.html

South, Todd. 2024. “Hundreds of satellites to give military faster tactical comms and data”. Defense News. 10 April. https://www.defensenews.com/news/your-marine-corps/2024/04/10/hundreds-of-satellites-to-give-military-faster-tactical-comms-and-data/

Swayne, Matt. 2024. “Germany’s QUBE CubeSat Explores Quantum Key Distribution in Space on SpaceX Mission”. Quantum Insider. 20 August. https://thequantuminsider.com/2024/08/20/germanys-qube-cubesat-explores-quantum-key-distribution-in-space-on-spacex-mission/

—. 2024. “U.S. Restricts Quantum Tech Investments in China, Citing National Security Risks”. Quantum Insider. 29 October. https://thequantuminsider.com/2024/10/29/u-s-restricts-quantum-tech-investments-in-china-citing-national-security-risks/

Taddeo, Mariarosaria et al. 2024. “Consider the ethical impacts of quantum technologies in defence – before it’s too late”. *Nature*. October, 634(8035):779-781. https://www.nature.com/articles/d41586-024-03376-4

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

Toskala, Antti. 2024. “First 5G-Advanced specification is ready for implementation”. Nokia. 21 June. https://www.nokia.com/blog/first-5g-advanced-specification-is-ready-for-implementation/

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

United Nations General Assembly. 2024. “Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts”. UN document A/79/224, 23 July.

University of Oxford. 2024. “Breakthrough promises secure quantum computing at home”. 11 April. https://www.ox.ac.uk/news/2024-04-11-breakthrough-promises-secure-quantum-computing-home-0

University of Tokyo. 2024. “Sound Science: How Phononic Crystals are Shaping Quantum Computing”. SciTechDaily. 5 July. https://scitechdaily.com/sound-science-how-phononic-crystals-are-shaping-quantum-computing/

US Congressional Research Service. 2024. “Defense Primer: Quantum Technology”. 4 November. https://crsreports.congress.gov/product/pdf/IF/IF11836

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

Vijayabaskar, Santhosh. 2024. “Scaling Small Language Models (SLMs) For Edge Devices: A New Frontier In AI”. Forbes. 15 November. https://www.forbes.com/councils/forbestechcouncil/2024/11/15/scaling-small-language-models-slms-for-edge-devices-a-new-frontier-in-ai/

Welch, Carley. 2024. “Google Cloud unveils new appliance to bring cloud, AI to ‘tactical edge’”. Breaking Defense. 17 July. https://breakingdefense.com/2024/07/google-cloud-unveils-new-appliance-to-bring-cloud-ai-to-tactical-edge/

Whitney, Jamie. 2024. “The next generation in digital sensor and signal processing”. Military Aerospace Electronics. 17 April. https://www.militaryaerospace.com/computers/article/14310053/digital-sensor-signal-processing-embedded-computing-artificial-intelligence-ai

Winn, Zach. 2024. “Startup accelerates progress toward light-speed computing”. MIT News. 1 March. https://news.mit.edu/2024/startup-lightmatter-accelerates-progress-toward-light-speed-computing-0301

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

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

Zhang, Tong. 2023. “Revolutionising the semiconductor industry: Chinese scientists unveil 12-inch wafer with groundbreaking 2D materials”. South China Morning Post. 28 August. https://www.scmp.com/news/china/science/article/3232116/revolutionising-semiconductor-industry-chinese-scientists-unveil-12-inch-wafer-groundbreaking-2d

—. 2024. “Could this way of making ultra-thin semiconductors lead to faster microchips?”. South China Morning Post. 23 July. https://www.scmp.com/news/china/science/article/3271376/chinese-method-making-ultra-thin-semiconductors-could-lead-faster-microchips

Zhao, Weiwei and Changjin Zhang. 2024. “New superconducting material discovered in transition-metal dichalcogenides materials”. Phys.org. 19 January. https://phys.org/news/2024-01-superconducting-material-transition-metal-dichalcogenides.html#google_vignette

Zsombor, Peter. 2024. “Malaysia’s chip industry falls in crosshairs of US sanctions on Russia”. Al Jazeera. 3 June. https://www.aljazeera.com/economy/2024/6/3/malaysias-chip-industry-falls-in-the-crosshairs-of-us-sanctions-on-russia

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais des Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG