safeguarding science
SAFEGUARDING-SCIENCE.EU

ein Angebot vom
DLR Projektträger

Lists of critical and sensitive technologies - *scope, purpose and intended audience*

Jonathan Bernsdorf, Pablo Ramos Erpenbeck, Alice Wignjosaputro,
Laura Klueting, Gerold Heinrichs

DLR Projektträger

Imprint

Publisher
DLR Projektträger
Deutsches Zentrum für Luft- und Raumfahrt e.V. (German Aerospace Center)
Heinrich-Konen-Straße 1
53227 Bonn, Germany

DLR-PT.de

Editor
DLR Projektträger
European and International Cooperation Division
Asia, Oceania

Bonn, January 2026

ISBN 978-3-949245-33-6

Table of contents

Introduction

Scientific and technological progress is a key driver of security, prosperity, and efforts to address major societal and global challenges. Governments across the globe are developing strategic measures to accelerate research, strengthen innovation, and safeguard critical technologies.

Central to these strategies are critical technology lists. Such lists catalogue technologies of particular strategic importance, aiding policymaking, informing public discourse, and helping researchers understand the contextual relevance of their work.

This publication presents a structured and comprehensive overview of selected lists produced by Western governments and state actors, namely the EU, France, Canada, the Netherlands, Australia, and the United States. To provide context, the lists are presented alongside their strategic backgrounds and policy frameworks. Key information is summarised and organised under the categories "General Information", "Rationale", "Selection Criteria", and "Addressees". The publication concludes with a comparative Safeguarding-Science-Table of Critical Technologies (SGS-Table) that juxtaposes all six lists and situates them within the framework of the EUREKA Taxonomy of Technological Areas[1] in order to illustrate convergence and divergence in their thematic priorities.

The analysis was conducted in summer 2025. No claim to completeness is made. The selection presented here reflects a sample rather than the full set of existing critical or sensitive technology lists. It is intended as an initial overview that can be supplemented with documents from additional countries and actors as required.

DLR Projektträger has been providing comprehensive, knowledge-based services for the management of research, education and innovation for almost 50 years. Its clients include federal ministries, the European Commission, federal states, as well as universities, scientific organisations and associations. It advises on strategies and programmes, manages accompanying dialogue processes, plans and assumes the operational implementation of funding programmes, supports knowledge transfer, and evaluates the impact of the programmes and initiatives of its clients. It has developed expertise in the area of research security within the www.safeguarding-science.eu initiative and with a dedicated interdisciplinary team. DLR Projektträger is a central pillar of the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt or DLR) and complements its scientific orientation.

Key findings

A comparative analysis of critical and sensitive technology lists reveals both commonalities and significant differences. All lists acknowledge the strategic importance of specific technologies, but they vary in purpose, level of detail, and intended audience.

One key difference concerns terminology. While general discussions often refer to *sensitive* or *critical* technologies, each of the six selected lists uses slightly different terms: Critical Technology Areas (EU); Protected Scientific and Technical Sectors (France), Sensitive Technology Research Areas (Canada), Key Enabling Technologies (the Netherlands), Critical Technologies in the National Interest (Australia), Critical and Emerging Technologies (United States).

The purpose of the lists ranges from a protection and security-oriented approach to strategic economic assessments. While France, Canada, and the EU focus on leak prevention, control of affiliations, and collective risk assessment, the Netherlands and Australia emphasise economic competitiveness. The US approach combines both perspectives.

Another point of divergence concerns legal status. Some lists are legally binding, while others serve as guidance documents. The French and Canadian approaches include binding requirements for their intended addressees,

[1] https://www.eurekanetwork.org/programme-resources/taxonomy-of-technology-areas/

whereas the other lists provide policy direction. Canada's approach to reviewing the integrity of research funding and foreign influence is unique in this regard.

Despite substantial thematic overlap across all lists, France and the United States place greater emphasis on defence and military technologies (such as hypersonics, directed energy, and missiles). The US list is comparatively more extensive, as it includes most categories found in the other lists while adding more specific technology areas. The Dutch list differs slightly from the others by not only naming categories and corresponding technologies, but also indicating related technologies in a separate column. The French list stands out most clearly, presenting broad thematic areas rather than technology categories. As a result, many categories identified in other lists appear only as subcategories in the French approach.

The table below summarises key information on the six technology lists.

Country / Region	Name and link to list or strategy	Main purpose	Number of technologies (highest level categories)
European Union	Commission Recommendation (EU) 2023/2113 – Critical Technology Areas for Economic Security	Identify 10 critical technology areas relevant to the EU's economic security and provide a basis for coordinated risk assessments by Member States.	10 areas (with 4 flagged as priority)
France	Arrêté du 3 juillet 2012 (PPST), as amended (latest 1 Jan 2025) – Protected Scientific & Technical Sectors	Protect national scientific & technical potential; legally binding and primarily addressed to heads of research institutions.	9 sector headings (covering approximately 90 technologies)
Canada	Sensitive Technology Research Areas (STRA) Policy on Sensitive Technology Research and Affiliations of Concern (STRAC, 2024) Sensitive Technology List (STL, 2025)	Safeguard federally funded research by restricting affiliations with designated foreign organisations in sensitive technology areas.	11 categories
Netherlands	Nationale Technologiestrategie (National Technology Strategy, 2024)	Identify technologies where NL can lead by 2035; provide policy guidance.	10 categories
Australia	List of Critical Technologies in the National Interest Critical Technologies Statement	Identify technologies critical to economic prosperity, security & social cohesion; provide policy guidance.	7 broad domains
United States	Critical and Emerging Technologies (CET) List – 2024 Update	Provide a common reference framework for national security, R&D priorities, and interagency coordination; provide policy guidance.	18 areas (covering approximately 120 technologies)

We carried out a cursory search for similar "critical" technology lists, but did not include them in the analysis at this stage.

Country	Name of list	Main purpose	Number of top-level technologies
United Kingdom	UK Science & Technology Framework (DSIT/UKRI)	Focus public policy and investment on 5 technologies identified as central to the UK's strategic advantage.	5
South Korea	12 National Strategic Technologies (MSIT announcement)	Guide R&D and industrial policy by prioritising 12 strategic technology areas.	12
China	Made in China 2025 – 10 priority sectors (industrial strategy) (State	Strengthen manufacturing and technological leadership and support export	10

	Council/ Central People's Government of the PRC) Notice of the State Council on the Publication of "Made in China 2025"	control decisions for prohibited and restricted technologies.	
Germany	Hightech-Agenda Deutschland (Federal Govt., 2025)	Focus national efforts on six key technologies to enhance competitiveness and technological sovereignty.	6

Conclusion

Nature of "Critical Technology Lists"

We distinguish two types of lists: (1) Economically oriented industrial strategy lists, as used in the Netherlands, Australia and the European Union, which guide funding and policy decisions; and (2) Security and control lists, as used in Canada or France, which aim to protect research organisations, preserve national knowledge, and prevent information leakage. The US list, although not legally binding, covers both national assets and economic strategy.

One key advantage of these lists is that they provide a shared orientation for ministries and other national innovation stakeholders. Economically oriented lists signal to stakeholders, investors, and partners the strategic direction a country intends to pursue, thereby helping to concentrate resources. Security-oriented lists raise risk awareness and encourage the adoption of research security practices. The lists also serve as an important reference for the design of public funding programmes.

The breadth of technological areas covered across the lists varies, as does the specificity of individual technologies. Nevertheless, as noted above, a high degree of thematic overlap remains. One EUREKA technological area (biotechnology) appears in all lists, while five are included in five lists: (1) robotics/autonomous systems, (2) quantum technology, (3) AI, (4) industrial manufacture, and (5) energy technology.

One issue warrants further reflection: if different countries all prioritise the same topics, there is a risk that international cooperation in these areas may diminish entirely. Securitisation and nationalisation of research, particularly in areas of cross-cutting relevance for global civilian use, may not only hinder exchange among industrialised countries but also substantially limit access for researchers from other regions.

Furthermore, comparison of the lists shows that they are often thematically broad, rendering them somewhat vague. As a result, priorities may be diluted, and the lists become difficult to operationalise. A list is also always a snapshot in time: technology and threat landscapes change rapidly, and without regular updates, lists can quickly become outdated. Taken together, these factors contribute to the risk that such lists convey a false sense of certainty.

Implementation of the lists was not assessed as part of the analysis, as none of them included an easily accessible monitoring report. A future implementation assessment could draw on innovation funding data in the case of economically oriented lists, or on evidence such as rejected applications and changes in cooperation patterns for security-related lists.

Design principles for creating a "Critical Technology List"

By analysing the methodological and content-related approaches of the lists, it is possible to derive indications as to which aspects are relevant for the creation of such lists.

- **Objective:** It should be determined whether a list is intended to provide guidance for technology development or introduce specific security measures for technologies, or whether it pursues a dual objective by combining economic growth considerations with security concerns. The analysis suggests that these objectives are not always well aligned. Technologies requiring security-related risk assessment do not necessarily coincide with areas of economic strength or weakness. Developing two separate lists with clearly defined objectives and corresponding measures therefore seems preferable.
- **Scope and level of specificity:** Lists that are overly broad or rely on generic categories are difficult to operationalise and risk losing policy relevance. Conversely, overly specific lists cover only parts of the system and may create an impression of concreteness that likely cannot be sustained across many areas. If all lists mention largely the same technologies without differentiating national priorities, the selection may appear generic. The comparative analysis indicates that list-based interventions tend to focus on areas of particular strength or vulnerability, leaving a broader "middle section" of technologies to normal development. In the context of technology development, this implies reliance on international competition as the primary driver; in the context of technology security, it implies a conscious acceptance of certain risks. This leads to the observation that the number and specificity of the technologies included in a critical technology list may indicate how open or closed a country's research system is to international cooperation. Where many topics are included but defined only at a high level of aggregation, uncertainty for international collaboration increases. In such cases, responsibility for interpreting the scope and implications of the list shifts from policymakers to the scientific community, which has to plan and justify collaborations under conditions of heightened uncertainty.
- **Context considerations:** The design of technology lists depends on the size and structure of the national research and innovation (R&I) system. Large countries typically cover a wide range of technologies across research and industry, whereas smaller systems face stronger incentives to prioritise and consider complementarities with partners. In Europe in particular, this suggests that national approaches should be embedded in trust-based partnerships (within the EU and with Non-EU partners), and informed by a systematic mapping of technology overlaps.
- **Methodology:** Although the compilation methods of the analysed lists are rarely made explicit, methodological proposals can be derived from the comparative analysis. A two-step approach seems appropriate: An initial scan could establish a longlist of technologies based on defined economic, technological and scientific indicators, followed by a portfolio design that differentiates between priority levels with corresponding measures and monitoring requirements. Finally, the analysis highlights that the credibility and effectiveness of technology lists depends on clearly stated review periods, update rhythms, and monitoring indicators.

The SGS-Table: Proposal for the use by universities and research institutions

The comparative Safeguarding-Science-Table of Critical Technologies (SGS-Table) included in the final chapter brings together all six critical technology lists and maps them onto the EUREKA Taxonomy of Technological Areas. The table is intended as a starting point for a common reference framework for existing and future technology lists and may serve as an analytical tool to identify overlapping technological priorities. It can also be used as a baseline for tracing shifts in thematic focus over time, as additional lists are integrated.

Research organisations are increasingly required to develop risk assessment and risk management systems. In this context, the SGS-Table can support internal analysis by providing a structured overview of technology areas that are repeatedly identified as critical across different national lists.

Technology-oriented research institutions and universities may already be familiar with the EUREKA taxonomy, particularly where applied science is organised along these technology fields. Institutions could build on this by mapping their internal technology portfolios, respective units, industrial collaborations, and projects onto the

EUREKA taxonomy. In a subsequent step, technologies highlighted in the SGS-Table could be examined within this internal overview, for example by identifying areas that appear in the majority of the lists (see table below). This may constitute an initial input into an organisation's risk assessment process.

EUREKA Category/ Tech-Area	Number of mentions
Medicine, Human Health + Biology / Biotechnology	6
Automation, Robotics Control Systems	5
Quantum Informatics	5
Artificial Intelligence (AI)	5
Industrial Manufacture	5
Energy	5
Data Processing / Data Interchange, Middleware + Data Protection, Storage, Cryptography, Security	4
Telecommunications, Networking	4
Space Exploration and Technology	4
Sensor Technology related to measurements	4

From an institutional perspective, such an approach allows potential risk concentrations to be identified using a framework that reflects national and partner states' strategic priorities. It may also facilitate dialogue with international partners by providing a transparent basis for discussing technology-related risks.

Once relevant technology areas have been systematically identified, specific measures can be implemented to monitor or protect them as appropriate.

1. European Union

General information

In October 2023, the European Commission (EU Commission) presented the "Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States"[2] with a list of critical technologies in its annex as part of the EU's Economic Security Strategy[3]. The strategy builds on three pillars: (1) promotion of the EU's economic base, (2) protection against risks, and (3) partnerships with international actors. The list contains ten identified categories of critical technologies structured in numerical order according to their urgency and significance:

1. Advanced Semiconductors;
2. Artificial Intelligence;
3. Quantum Technologies;
4. Biotechnologies;
5. Advanced Connectivity, Navigation and Digital Technologies;
6. Advanced Sensing Technologies;
7. Space & Propulsion Technologies;
8. Energy Technologies;
9. Robotics and Autonomous Systems and
10. Advanced Materials, Manufacturing and Recycling Technologies.

The list also entails technologies related to the categories that "are a likely focal point for risk assessment", however, they are not exhaustive according to the EU Commission.

The four priority categories: Advanced Semiconductors, Artificial Intelligence, Quantum Technologies and Biotechnologies are considered as "highly likely to present the most sensitive and immediate risks related to technology security and technology leakage."

Rationale

In its Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, the EU Commission highlights rising geopolitical tensions coupled with advancing economic integration and technological innovations as the most significant developments in recent years that impose risks for the EU and its member states. Due to these dynamics the Commission is concerned that the economic security of the EU might be at risk.

The Commission adopted the "Joint Communication on European Economic Security Strategy" to support the development of a "comprehensive strategic approach to economic security". In the Strategy, four "broad and non-exhaustive categories of risks for further assessment" are identified: (1) Resilience of supply chains; (2) physical and cyber-security of critical infrastructure; (3) technology security and leakage as well as (4) weaponization of economic dependencies and economic coercion. On this basis, the EU Commission aimed to "assess the risks of technology security and leakage" and created the list of sensitive technologies as a foundation. Additionally,

[2] https://eur-lex.europa.eu/eli/reco/2023/2113/oj/eng
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020

the list reflects the EU’s intention to balance technological openness and innovation with protective measures, ensuring competitiveness while preventing technology leakage, misuse for military purposes, or human rights violations.

Selection criteria

In the Recommendation of the EU Commission three criteria are defined for the classification of a technology as ‘critical’:

1. **The enabling and transformative nature of the technology criterion**, which is further elaborated as evaluating "the technology's potential and relevance for driving significant increases of performance and efficiency and/or radical changes for sectors, capabilities, etc."
2. **The risk of civil and military fusion criterion**, that describes "the technology's relevance for both civil and military sectors and its potential to advance both domains, as well as risk of uses of certain technologies to undermine peace and security".
3. **The risk of misuse of the technology for human rights violations criterion,** that "looks at the technology's potential misuse in violation of human rights, including restricting fundamental freedoms."

Addressees

The list is directed at the EU member states encouraging them to conduct risk assessment on the identified critical technologies. In this regard, the recommendation states that further risk assessment will be discussed with the member states. The aforementioned four most important categories were part of a collaborative risk assessment with the member states until the end of 2023. The document is not binding legislation but rather a recommendation guiding Member States toward coordinated analysis and action, laying the foundation for future policy measures (promotion, partnership, or protection).

Requested actions are:

- Conduct a collective risk assessment of the four priority technology areas by the end of 2023.
- Engage in dialogue on scope, calendar, and methodology for assessing additional areas.
- Provide expert input, including from private sector actors, while ensuring confidentiality where requested.

Timeline: Explicitly, the collective assessment of the four priority technologies should be completed by the end of 2023. Broader dialogue and potential additional measures are foreseen by spring 2024.

Comment

At the time of this analysis in summer 2025, no public documents on the methodology, the actors or the results of the announced risk assessment were found in an online search. There are references to an initiated risk assessment process in individual documents of the Member States or the EU Commission.

List of 10 critical technology areas for the EU's economic security

Technology Area	Technologies
1. Advanced Semiconductors Technologies	- Microelectronics, including processors - Photonics (including high energy laser) technologies - High frequency chips - Semiconductor manufacturing equipment at very advanced node sizes
2. Artificial Intelligence Technologies	- High Performance Computing - Cloud and edge computing - Data analytics technologies - Computer vision - Language processing - Object recognition
3. Quantum Technologies	- Quantum computing - Quantum cryptography - Quantum communications - Quantum sensing and radar
4. Biotechnologies	- Techniques of genetic modification - New genomic techniques - Gene-drive - Synthetic biology
5. Advanced Connectivity, Navigation and Digital Technologies	- Secure digital communications and connectivity, such as RAN & Open RAN (Radio Access Network) and 6G - Cyber security technologies incl. cyber surveillance, security and intrusion systems, digital forensics - Internet of Things and Virtual Reality - Distributed ledger and digital identity technologies - Guidance, navigation and control technologies, including avionics and marine positioning
6. Advanced Sensing Technologies	- Electro-optical, radar, chemical, biological, radiation and distributed sensing - Magnetometers, magnetic gradiometers - Underwater electric field sensors - Gravity meters and gradiometers
7. Space & Propulsion Technologies	- Dedicated space-focused technologies, ranging from component to system level - Space surveillance and Earth observation technologies - Space positioning, navigation and timing (PNT) - Secure communications including Low Earth Orbit (LEO) connectivity - Propulsion technologies, including hypersonics and components for military use
8. Energy Technologies	- Nuclear fusion technologies, reactors and power generation, radiological conversion/enrichment/recycling technologies - Hydrogen and new fuels - Net-zero technologies, including photovoltaics - Smart grids and energy storage, batteries
9. Robotics and Autonomous Systems	- Drones and vehicles (air, land, surface and underwater) - Robots and robot-controlled precision systems - Exoskeletons - AI-enabled systems
10. Advanced Materials, Manufacturing and Recycling Technologies	- Technologies for nanomaterials, smart materials, advanced ceramic materials, stealth materials, safe and sustainable by design materials - Additive manufacturing, including in the field - Digital controlled micro-precision manufacturing and small-scale laser machining/welding - Technologies for extraction, processing and recycling of critical raw materials (including hydrometallurgical extraction, bioleaching, nanotechnology-based filtration, electrochemical processing and black mass)

Table 1: List of 10 critical technology areas for the EU's economic security. This table was created by the DLR Projektträger on the basis of the ANNEX to the EU Recommendation.

2. France

General information

On July 3rd 2012, the French "Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation"[4] ("Order on the protection of the nation's scientific and technical potential" (PPTS)) was passed. Since then, it has been updated on a yearly basis. The latest adjustment entered into force on the 1st of January 2025. Furthermore, an interministerial instruction dated 28 Apr 2025 updates how the regime is implemented[5]. Annex I of arrêté provides a national list of protected scientific and technical sectors, updated annually. Annex II details the categories of information to be transmitted to the competent "haut fonctionnaire de défense et de sécurité (HFDS)" (e.g., cooperation projects, unit creations/modifications, statistics) and the documents HFDS may review.

The "order" requires research bodies, universities, grandes écoles and companies to identify and secure "zones à régime restrictif (ZRR)" and "locaux sensibles", control access (including vetting, escorting and logging visits), and implement information-security measures. It also introduces tighter obligations concerning foreign links, internships, and prior review of certain international collaborations for "unités protégées". It lists protected scientific and technical sectors, divided into nine specialisations, each of which comprises several sub-categories.

The nine specialisations are the following:

- Biology, Medicine and Health;
- Chemistry; Mathematics;
- Physics, Agricultural and ecological sciences;
- Earth and Universe Sciences, Space;
- Applied mathematics, information and communication sciences and technologies;
- Engineering sciences;
- Humanities and social sciences.

Rationale

The list is part of a larger approach to ensure the security of French research and development. Its purpose is to identify public and private sectors, knowledge, expertise and technologies that are of particular importance to France and require special protection. The scope of the approach extends as far as establishing restricted zones in research facilities working on the listed topics.

Furthermore, it functions as a practical tool with direct implications for research management and research security: Heads of departments, organisations and companies operating in scientific and technical fields designated as protected on the list are granted the right to request additional information from prospective visitors. Such information includes e.g. information on marital status, professional or personal connections with a foreign state, a foreign or foreign-controlled company or organisation, a non-French nationality or professional activities on the national territory in connection with the main activity carried out within the restricted zone.

An annually updated catalogue allows the state to track technological shifts and newly exposed areas, align oversight (HFDS) and require proactive notifications on collaborations or structural changes. The 2024/2025

[4] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000026140136
[5] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050395110

reinforcement reflects a heightened risk environment (foreign influence, data exfiltration, cyber threats) and the need for coherent, enforceable protection measures across public and private research.

Selection criteria

The documents outline four overarching reasons or selection criteria for including a sector in the order. A sector may be included if the misappropriation or unduly transfer of knowledge could: (1) undermine the nation's economic interests, (2) weaken France's defense capabilities or strengthen foreign military arsenals; (3) contribute to the proliferation of weapons of mass destruction and their means of delivery; or (4) be used for terrorist purposes domestically or abroad.

The arrêté codifies a protected nomenclature that is reviewed yearly:

- Strategic relevance & systemic leverage (e.g. sectors that underpin multiple industries/capabilities: micro/nano-electronics, photonics, AI, data, quantum).
- Dual-use/defense sensitivity (e.g., missiles/arms, aerospace, cybersecurity, telecom networks).
- Risk of appropriation/misuse (e.g. rapid-diffusion digital tech; sensitive bio/health & agro-biotech; additive manufacturing).
- Critical enablers for future competitiveness (e.g. quantum technologies; AI/ML; data/big data).

The 2025-in-force Annex shows a targeted expansion around digital and frontier technology: explicit headings for "Technologies quantiques (46); Cybersécurité (78); Technologies de réseaux de télécommunications, internet des objets (79); Intelligence artificielle, apprentissage automatique (710), Sciences des données, données massives (712), and a defense line "Missiles, armes, sciences et techniques de défense (812)". This reveals emphasis on high-impact, high-leakage domains where knowledge flows (people, collaborations, data) and supply-chain chokepoints may create concrete security exposure.

Addressees

Overall, the PPST is a binding national protection framework aimed at preventing leakage/appropriation of sensitive know-how via governance of places, people and information across priority technology domains. The main addressees of the list are the heads of departments, organisations, or companies carrying out activities in the protected scientific and technical fields.

The arrêté requests the addressees to

- identify/delimit ZRRs; enforce access controls (e.g. authorisations, escorts, visit logs).
- maintain security policies and report major incidents; support evaluations; provide pre-scribed notifications (e.g. cooperations, unit changes, statistics).
- For "unités protégées", ensure stricter supervision (e.g., internships under named staff; prior HFDS/ministry review of certain international collaborations).

Further addressees might be visiting scientist, applicants or external providers, as the list is a legitimation to request further information from them that other facilities cannot. The order also gives an overview of which information is allowed to be requested from visitors.

French list of protected scientific and technological potential

Research Area	Technologies
1. Biology, Medicine And Health	- Molecular and cellular aspects of biology - Biomolecules, pharmacology, therapeutics - Physiology, biology of organisms, populations, interactions - Clinical research, technological innovation, epidemiology and public health - Biotechnology
2. Chemistry	- Chemistry of material - Organic, mineral and industrial chemistry - Theoretical, physical and analytical chemistry - Materials engineering - Chemistry of biomolecules and biological systems
3. Mathematics	- Mathematics and its interactions
4. Physics	- Elementary constituents and theoretical physics - Hot plasmas - Dense media, materials and components - Diluted media and fundamental optics - Nuclear physics - Quantum technologies
5. Agricultural And Ecological Sciences	- Environmental and population biology, ecology - Biology of organisms; animal, plant and microbial biotechnologies - Food biotechnology, food science
6. Earth And Universe Sciences, Space	- Astronomy, astrophysics - Solid and surface envelopes of the Earth and planets, critical zone - Fluid envelopes of the Earth and planets, oceans and atmosphere
7. Applied Mathematics, Information And Communication Sciences And Technologies	- Automation, production robotics - Signal and image processing - Electronics, microelectronics, nanoelectronics - Micro-nanosystems and sensors - Optical and photonic systems - Computer science and applications - Electromagnetism, microwaves, sources and antennas - Cyber security - Telecommunications network technologies, internet of things - Artificial intelligence, automatic learning - Applied mathematics - Data science, massive data
8. Engineering Sciences	- Process engineering - Cold plasmas - Power electronics - Electrical engineering - Acoustics - Bio-mechanics and biotechnologies - Energetics, thermics, combustion - Mechanics of fluid media - Civil engineering - Mechanical, production and transport engineering - Mechanics of solids, materials, structures and surfaces - Missiles, Weapons, Defence Sciences and Techniques - Additive manufacturing - Aeronautics and space
9. Humanities And Social Sciences	- Cognitive sciences and neurosciences - Language sciences (linguistics and general phonetics) - Psychology, clinical psychology, social psychology - Sciences and techniques of physical and sports activities - Ergonomics

Table 2: French list of protected scientific and technological potential. This table was created by the DLR Projektträger on the basis of the "Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation".

3. Canada

General information

Canada's Science.gc.ca site[6] publishes a Policy on Sensitive Technology Research and Affiliations of Concern[7] (STRAC) under the umbrella of Canada´s "Safeguarding Your Research"-Initiative. The STRAC policy consists of two lists: "Sensitive Technology Research Areas" and the List of Named Research Organizations[8]. Under this policy, federal research grant applications with research proposals that aim to advance sensitive technology areas included on said list must contain an attestation: that none of the named researchers are currently affiliated with or receiving support from a Named Research Organization (NRO) — a list of institutions considered risky due to links to military, defense, or security entities. The policy is designed to integrate into Canada's federal funding system, making the attestation requirement part of the grant/funding application process. It also links with the National Security Guidelines for Research Partnerships[9] (NSGRP), requiring that research partnerships (especially international ones) consider security implications.

The NRO and STRA lists are marked as reviewed regularly and updated to reflect evolving technology landscapes. In February 2025, Canada released a Sensitive Technology List (STL), intended to inform export controls, foreign investment review, and cross-departmental policy. The STL uses the same 11 categories as STRA, with more technical detail. The STL does not replace STRA, but complements it. Thus, the Canadian framework couples a technology classification system (STRA/STL) with a grant-level risk attestation policy (STRAC) targeted at safe-guarding research from foreign influence or leakage of sensitive know-how.

The Canadian government published an overview of Sensitive Technology Research Areas on 16 January 2024. The list was last revised in May 2025 and is scheduled for regular updates. In its latest version, the overview consists of eleven categories, with varying numbers of subcategories:

- Advanced Digital Infrastructure;
- Advanced Energy Technology;
- Advanced Materials and Manufacturing;
- Advanced Sensing and Surveillance;
- Advanced Weapons;
- Aerospace, Space and Satellite Technology;
- Artificial Intelligence and Data Technology;
- Human-Machine Integration;
- Life Science Technology;
- Quantum Science and Technology;
- Robotics and Autonomous Systems.

The subcategories represent different fields of application and are intended to provide the researchers with greater specificity regarding the primary areas of concern. Additionally, the list provides detailed explanations to the subcategories in order to avoid misunderstandings regarding the technologies. There is a category weapon-related technologies, but no further details on subcategories or specific technologies within this category 'Advanced Weapons' is given. The overview also covers various stages of research development. Technologies that are already "ubiquitous in the course of a research project" are not subject to oversight by the Canadian

[6] https://science.gc.ca/site/science/en
[7] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern
[8] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/named-research-organizations
[9] https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships

government. Instead "the advancement of a technology during the course of research" is considered of particular concern.

Rationale

The "List of Sensitive Technology Areas" contains "advanced and emerging technologies that are important to Canadian research and development, but may also be of interest to foreign state, state-sponsored, and non-state actors, seeking to misappropriate Canada's technological advantages to our detriment" and should therefore be particularly well protected.

By mandating attestation and screening of researcher affiliations, Canada seeks to guard against foreign influence in R&D while preserving collaboration with trusted partners.

Selection criteria

The Canadian STRA framework uses a conceptual-criteria approach to describe and update the categories:

- Emerging & enabling potential: The list focuses on technologies not just in use but evolving, transformative, or with frontier potential (e.g. quantum, human-machine integration).
- Dual-use/defense relevance: Many listed areas overlap civilian and military domains (e.g. sensors, aerospace, surveillance). The concern is the possible misapplication in defense or intelligence contexts.
- Value to foreign/special actors: The document frames the list as capturing areas "of interest to foreign state, state-sponsored, and non-state actors" seeking to exploit Canada's technological advantages.
- Strategic leverage & systemic importance: The categories chosen tend to be cross-cutting, foundational or backbone technologies (digital infrastructure, materials, energy, AI) whose control or leakage would have disproportionate ripple effects.
- Adaptivity & reviewability: The list is explicitly stated to be reviewed and updated as technologies evolve or new threats emerge. Thus, while the selection is not via a rigid numerical scoring rubric in public view, it is grounded in sensitivity, futurity, dual-use risk, and strategic impact, maintained through periodic expert review.

Addressees

Main addressees are researchers (applicants, co-applicants, collaborators with named roles) seeking federal funding (NSERC, CIHR, SSHRC, CFI) for projects advancing sensitive technology areas and their research institutions/organizations administering or hosting such funded projects. The second addressees are funding agencies and their evaluation systems as well as the broader international research community.

Researchers must determine whether their grant proposal advances one of the STRA sub-areas. And if yes, they must complete and submit an attestation that they are not currently affiliated with, nor receiving funding/in-kind support from any NRO. Funding agencies will validate attestation accuracy.

The STRAC policy is binding for federal funding opportunities that are declared in scope.

Canadian List of Sensitive Technology Research Areas

Research Area	Technology
1. Advanced Digital Infrastructure Technology	- Advanced communications technology - Advanced computing technology - Cryptography - Cyber Security technology - Data store technology - Distributed ledger technology - Microelectronics - Next-generation network technology
2. Advanced Energy Technology	- Advanced energy storage technology - Advanced nuclear generation technology - Wireless power transfer technology
3. Advanced Materials And Manufacturing	- Augmented conventional materials - Auxetic materials - High-entropy materials - Metamaterials - Multifunctional/smart materials - Nanomaterials - Powder materials for additive manufacturing - Superconducting materials - Two-dimensional (2D) materials - Additive manufacturing - Advanced semiconductor manufacturing - Critical materials manufacturing - Four-dimensional (4D) manufacturing - Nano-manufacturing - Two-dimensional (2D) materials manufacturing
4. Advanced Sensing And Surveillance	- Advanced biometric recognition technologies - Advanced radar technologies - Atomic interferometer sensors - Cross-cueing sensors - Electric field sensors - Imaging and optical devices and optical devices and sensors - Magnetic field sensors (or magnometers) - Micro (or nano) electro-mechanical systems (M/NEMS) - Position, navigation and timing (PNT) technology - Side scan sonar - Synthetic aperture sonar (SAS) - Underwater (wireless) sensor network
5. Advanced Weapons	
6. Aerospace, Space And Satellite Technology	- Advanced wind tunnels - On-orbit servicing, assembly and manufacturing systems - Payloads - Propulsion technologies - Satellites - Space-based positioning, navigation and timing technology - Space stations - Zero-emission/fuel aircraft
7. Artificial Intelligence And Big Data Technology	- AI chipsets - Computer vision - Data science and big data technology - Digital twin technology - Machine Learning (ML) - Natural language processing
8. Human-Machine Integration	- Brain-computer interfaces - Exoskeletons - Neuroprosthetic/cybernetic devices

	- Virtual/augmented/mixed reality - Wearable technology
9. Life Science Technology	- Biomanufacturing - Genomic sequencing and genetic engineering - Proteomics - Synthetic biology - Chemical, biological, radiological and nuclear (CBRN) medical countermeasures - Gene therapy - Nano medicine - Tissue engineering and regenerative medicine
10. Quantum Science And Technology	- Quantum communications - Quantum computing - Quantum materials - Quantum sensing - Quantum software
11. Robotics And Autonomous Systems	- Molecular (or nano) robotics - (Semi-) autonomous/uncrewed aerial/ground/marine vehicles - Service robots - Space robotics

Table 3: Canadian "List of Sensitive Technology Research Areas". This table is created by the DLR Projektträger on the basis of the .

4. The Netherlands

General information

In June 2024, the Dutch government published its "Nationale Technologie Strategie" (National Technology Strategy, NTS)[10]". The strategy contains ten priority or "key enabling" technologies where the Netherlands possesses or can build competitive strength, to be the focus of public-private mobilization, investment, infrastructure, talent, and coordination. The NTS is positioned as a tool to respond to global competition, resource constraints (energy, materials, space, human capital), and geopolitical dependencies. The ten priority technologies are further divided into subcategories. A third column further identifies related and impacted technologies for each category, offering an overview of potential interconnections and dependencies between the key technologies and other fields of technology.

The ten listed key enabling technologies are:

- Optical Systems and Integrated Photonics;
- Quantum Technologies;
- Process Technology, including Process Intensification;
- Biomolecular and Cell Technologies;
- Imaging Technologies;
- Mechatronics and Optomechatronics;
- Artificial Intelligence and Data;
- Energy Materials;
- Semiconductor Technologies;
- Cybersecurity Technologies.

For each technology, the NTS outlines an ambition towards 2035, describes the technology landscape, potential application domains, and hurdles to scaling up. The long-term-goals are described based on the following questions: "(1) Which position do we wish the Netherlands to have acquired by 2035 for each key enabling technology, and (2) what is needed to achieve that objective?" Afterwards, each section assesses the policy context in which the NTS and its technologies can be integrated. Overall, the NTS is not a regulatory text but a strategic, guiding policy document explicitly intended to guide investment, coordination, prioritization, and ecosystem development.

Rationale

The NTS describes that the strong position in research of the Netherlands is increasingly challenged by global dynamics, including rising geopolitical tensions and Europe's growing lag behind China and the USA in research and development. Furthermore, the Netherlands faces intensifying international competition in technology, strategic dependencies (on foreign supply chains), and constraints in energy, materials, space, and talent. Taken together, these developments prompted the creation of the NTS, which sets out measures both to address this gap and to safeguard the Dutch research environment. The government sees that it cannot lead in every domain, so it must make targeted choices. The list of priority technologies provides focus: to channel public/private resources, to drive coordinated ecosystem building, to reduce vulnerabilities, and to maximize the impact of investments.

The NTS is the last step of a Strategic Technology Policy. This policy includes three parts:

- Broad base: Focus on the development, application and upscaling of technology with innovation policy, enterprise policy, industrial policy and digitalisation policy.
- Specific focus: Focus on 44 key enabling technologies through the mission-driven innovation policy

[10] https://hollandhightech.nl/_asset/_public/__site_4/257-034_Nationale_Technologie_Strategie-EN_met_agenda.pdf

- Strategic priorities: Strategic focus on priority key enabling technologies – specifically the niches in markets and control points in value chains with the greatest opportunities for the Netherlands.

Selection criteria

The selection of key technologies from the longer list was carried out based on various indicators, with the goal of identifying technologies, "that have the greatest potential for the Netherlands”. Dutch authorities consider key technologies as "technological domains where the Netherlands has a strong scientific position and that are expected to have a major social and economic impact in the coming years".

Experts from each technology field participated in discussions on the key technologies, during which the following questions were addressed:

- Contribution to national earning capacity / economic value: Which key enabling technologies make an important contribution to the current and/or future economic earning potential of the Netherlands?
- Societal challenges: Which technologies are essential to address the challenges faced by our society?
- National security: Which key enabling technologies contribute to our national security?
- Existing Dutch strengths / comparative advantage: Which key enabling technologies build on the Netherlands' existing strengths in science and technology, R&D and ecosystems?

In addition, the feasibility of scaling was considered as well as an international context, dependencies, and the need to avoid over-reliance on external actors. The annex mentions that the selection used a qualitative and quantitative analysis, as well as consultations with around 60 experts.

Addressees

Addressees are mainly Ministries (especially Economic Affairs & Climate, Innovation, Research), Regional governments, knowledge institutions (universities, research institutes), industry stakeholders, public-private consortia etc. They are requested to align investment, programmes, and infrastructure with the ten key enabling technologies. In addition, action agendas should be developed for each technology, and public funding should be allocated accordingly.

The NTS is a non-binding strategic guidance.

Comments

The Dutch National Technology Strategy has been published in an English and a Dutch version. The Dutch version is authoritative. Our analysis is based on the translated and streamlines English version. It conveys the same core content (ten priority technologies, ambitions, agenda) but with less Dutch administrative detail and fewer footnotes to legal/institutional context.

Dutch National Technology Strategy

Technology Area	Technology	Related and affected technologies
1. Optical Systems and Integrated Photonics	- Encompasses the technology behind optical systems - Wireless optical technology for laser communications - Systems that refract, reflect or manipulate light to fulfil various optical functions - Information carriers for communications - Photonic Integrated Circuit - Systems integration - Transceivers for telecommunications and data communications (generic) and biosensors for the agrifood sector (specific)	- Lithography systems - Freeform mirrors and lenses - Wireless optical communications - Lighting - Metamaterials, particularly optical metamaterials - Mechatronics and optomechatronics - Semiconductor technologies - Functional devices and structures (at nanoscale) - Quantum communications - Quantum sensing - Quantum computing - Discrete resistors - Coatings, including nanoscale coatings - Quantum applications such as internet, sensing and computing applications.
2. Quantum Technologies	- Quantum Computing - Quantum Communications - Quantum Sensing - Quantum Chips - Quantum Systems - System engineering	- Semiconductor technologies - Optical systems and integrated photonics - Nanotechnology - Functional devices and structures - Nanomanufacturing
3. Process Technology, including Process Intensification	- Transition from fossil to sustainable feedstocks - Plastic waste streams - First- and second-generation sustainable biofuels - Optimal, stable and safe design of chemical production processes - Scalability - Heat integration - Optimal downstreaming processing - Use of space and cost efficiency - Conversion technology	- Catalysis - Separation technology - Biomanufacturing and bioprocessing - Advanced reactor engineering - Electricity-driven chemical reaction technologies - Artificial Intelligence
4. Biomolecular and Cell Technologies	- Analysing, measuring and using molecules such as DNA, RNA and proteins/metabolites - Omics - Gene editing - Stem cell technology - Synthetic cell technology	- Biosystems and organoids - Bio-informatics - Data science - Artificial Intelligence - Biomanufacturing - Bioprocessing
5. Imaging Technologies	- Analysis, generation and duplication of images (e.g. used in the medical sector, the semiconductor industry, the security domain, agriculture, industry, traffic and spaceflight) - Hardware - Sensors - Data collection (electronics/optics) - Software - Analysing and processing - Visualization	- Data sciences - Data analytics - Data spaces - Artificial Intelligence - Mechatronics and optomechatronics - Photonic/optical systems and integrated photonics - Systems Engineering - Energy materials - Quantum technologies - Semiconductor technologies
6. Mechatronics and Optomechatronics	- Complex electromechanical systems and control	- Production of semiconductors - 3D-printing

	- Automation technology (Used for semiconductor machinery building, medical equipment, components for the automotive and aviation industries, spaceflight applications, equipment for manufacturing semiconductors, food processing, agriculture and logistical processes) - Systems engineering - Development of mechanical systems and associated control and automation systems - Mechanical engineering - Physics - Electrical engineering - ICT - Integration of optical technology into mechatronic systems	- Medical equipment - Spaceflight (including laser satellite communications) - Robotics - Optical systems and integrated photonics - Imaging technologies and sensor and actuator technologies - Digital manufacturing technologies - Artificial Intelligence - Data Spaces
7. Artificial Intelligence and Data	- Supervised machine learning - Unsupervised machine learning - Reinforcement learning - Deep learning - Data science - Data analytics - Data spaces	- Cyber security technologies - Software technologies and computing - Digital connectivity technologies - Digital twinning - Immersive technologies - Neuromorphic technologies - Imaging technologies - Bio-informatics - Digital manufacturing - Robotics - Quantum technology - Optical systems and integrated photonics - Sensor and actuator technology - Systems engineering
8. Energy Materials	- Materials that make it possible to capture, store and transport energy	- Nanomanufacturing - Process technology, including process intensification - Thin films and coatings - Electricity-driven chemical reaction technologies - Photovoltaics - Digital connectivity technologies - Biomanufacturing - Bioprocessing - Catalysis
9. Semiconductor Technologies	- Semiconductor technologies are used in the automotive industry, the computer industry, the communication sector, for medical equipment and play a major role in energy transition and digitalisation - Further applications are defence applications - Encompassing of semiconductor components and/or highly miniaturised electronic subsystems and their integration into larger products and systems - Manufacturing (including metrology and characterisation) - Design, packaging and testing of semiconductor components	- Sensor and actuator technologies - Robotics - Digital manufacturing technologies - Imaging technologies - Digital and information technologies - AI - Data processing - Optical systems and integrated photonics - Mechatronics and optomechatronics - Quantum technologies - Integrated photonics

	- Microscale systems that integrate multiple functions on a chip - Development and construction of machines to carry out these services	
10. Cybersecurity Technologies	- Digital technical applications designed to mitigate relevant digital risk - Preventing Cyber incidents	- AI - Quantum computing - Data - Software technologies - Computing - Digital connectivity technologies - Digital twinning - Immersive technologies - Neuromorphic technologies - Digital manufacturing technologies - Microelectronics - Systems engineering - Sensor and actuator technologies - Imaging technologies - Additive manufacturing - Robotics

This table is created by the DLR Projektträger on the basis of the "Nationale Technologie Strategie".

5. Australia

General information

The Australian government published their "List of Critical Technologies in the National Interest[11]" in May 2023 with updates planned in a two year cycle. The pending 2025 update has not yet (Oct. 2025) been published. The publication replaced the previous list and consists of seven critical technologies categories. The earlier versions from 2022 included 63 specific technologies grouped under headings. An evaluation report[12] commissioned by the government in 2022 suggested a prioritization. The current list reflects a narrowing and focusing process that considers strategic weight, systemic leverage, stakeholder input, and evolving threat vectors. The current list forms part of a broader initiative by the Australian government to strengthen research security and is intended to be read in parallel with the Critical Technologies Statement | Department of Industry Science and Resources[13]. The Statement explains "how the Australian Government is supporting critical technologies" and provides further guidance on how to distinguish critical technologies.

The seven categories are:

- Advanced Manufacturing and Material Technologies;
- AI Technologies;
- Advanced Information and Communication Technologies;
- Quantum Technologies;
- Autonomous Systems, Robotics, Positioning, Timing and Sensing;
- Biotechnologies;
- Clear Energy Generation and Storing Technology.

Each category is accompanied by a dedicated website outlining example applications, global research trends and rankings, commercialisation, the development of the Australian industry, international cooperation, and future outlooks. It is pointed out by the Australian government that the list "has been developed through an extensive public consultation process" and was revised based on the feedback. As a result, the seven categories represent the technology fields with high impact on Australia's national interests.

Australia´s government explains this framework as foundational: future interventions, funding, regulation, standards, and policies in technology will be guided by the balancing of economic, security, and social dimensions. The documents provide a strategic orientation: identify key technology domains of national interest, highlight the dual nature of opportunities and threats, and set a policy lens by which future government action should proceed.

Rationale

The "critical technologies" are considered essential for Australian "economic prosperity, social cohesion and national security" and are endangered due to the rising geopolitical tensions. The list was created as one of several measures to "align Australia's critical ecosystem" and to "support consistency and coordination across related government activity". The list of measures presented by the Australian government to attain this goal includes:

- Developing solutions to key challenges with supporting a thriving ecosystem;
- Improving the technology investment environment by enhancing Australia as a destination for investments through identifying priority fields;
- Informing other priority setting mechanisms to provide guidance for the development of investment mandates and co-investment plans for the National Reconstruction Fund;
- Being more attractive to students and skilled workers to attract and retain talent;

[11] https://www.industry.gov.au/publications/list-critical-technologies-national-interest
[12] https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1500/RRA1534-1/RAND_RRA1534-1.pdf
[13] https://www.industry.gov.au/publications/critical-technologies-statement

- Focussing international partnerships by clearly indicating Australia's priority critical technology fields and thus underpinning international engagement.

Since options and actions regarding "critical technologies" will be developed through a dedicated framework based on the list, it also carries practical implications for Australian policy decisions. The framework takes four considerations into account: (1) whether the technology is listed as critical, (2) whether the technology aligns with government priorities or strategic needs, (3) the assessment of options and actions through a national interest lens and (4) strategies to secure Australia's ability to capture economic opportunities.

Selection criteria

The public documents do not provide a formula for selection. However, the "critical technologies" were selected for their high impact on Australian national interests:

- Strategic impact / national interest alignment: Technologies were chosen for their capacity to influence Australia's economic prosperity, national security, and social cohesion.
- Cross-sectoral or enabling nature: The fields selected are enablers: they underpin a broad set of industries, not just specialized niches (e.g. AI, advanced materials, communications).
- Emerging or future relevance and technological momentum: The list considers technologies not only already important, but "could become critical within the next 10 years".
- Risk exposure and vulnerability: History of leakage, cyber risk, supply chain dependency, or foreign strategic competition are part of the rationale.
- Consultative input and review: The government engaged in a public consultation process before adopting the list.
- Practical tractability & coherence: Rather than many specific technologies, the list is grouped into seven broad domains to make the policy manageable.

In addition, these technologies are strategically important, meaning that they provide opportunities and significant benefits for the growth of the Australian economy, hold the opportunity to provide well-paying jobs and improve the lives of the Australian people.

Addressees

The main addressees are the Australian Government departments and agencies (especially those in industry, science, defense, innovation), the research institutions, universities, industry actors, investors working in the identified fields, policy makers involved in standardization, procurement, regulation, and security as well as foreign investment/immigration control bodies.

The addressees should use the list as a guiding reference for research funding, support programmes, infrastructure investment, industrial policy, standards development and procurement decisions. Furthermore, they should balance opportunity and risk when dealing with critical technologies.

The documents are policy statements to give strategy guidance, rather than legislative mandates. They are not binding laws. However, the definition of "critical technology" is used in regulatory instruments[14].

[14] https://www.homeaffairs.gov.au/nat-security/Pages/critical-technology.aspx

Australian List of Critical Technologies in the National Interest

Technology Area	Technology
1. Advanced Manufacturing and Material Technologies	- Additive manufacturing, including 3D printing - Critical minerals extraction and processing - Advanced composite materials - High specification machining processes - Semiconductors and advanced integrated circuit design and manufacture
2. AI Technologies	- Machine learning, including neural networks and deep learning - AI algorithms and hardware accelerators - Natural language processing, including speech and text recognition, analysis and generation
3. Advanced Information and Communication Technologies	- Advanced data analytics - Advanced optical communications - Advanced radiofrequency communications, including 5G and 6G - High-performance computing - Protective cyber security technologies - Virtual worlds
4. Quantum Technologies	- Quantum computing - Post-quantum cryptography - Quantum communications - Quantum sensors
5. Autonomous Systems, Robotics, Positioning, Timing and Sensing	- Advanced robotics - Autonomous systems operation technology - Drones, swarming and collaborative robots - Advanced imaging technology - Advanced sensor technologies - Satellite and positioning technologies - Advanced aerospace technologies, including propulsion, hypersonics and guidance systems - Nuclear technologies, including for submarine propulsion and waste management
6. Biotechnologies	- Synthetic biology, including biological manufacturing - Neural engineering and brain computer interfaces - Genome and genetic sequencing and analysis - Vaccines and medical countermeasures - Novel medicines, including nuclear, antiviral and antibiotic
7. Clean Energy Generation and Storage Technologies	- Emissions reduction technologies - Advanced energy storage technologies - Directed-energy technologies - Large-scale renewable energy generation - Low-emission alternative fuels, including biofuels - Small-scale distributed energy harvesting

This table is created by the DLR Projektträger on the basis of the "List of Critical Technologies in the National Interest".

6. United States of America

General information

In February 2024, the Critical and Emerging Technologies List Update[15] was published by the White House's Office of Science and Technology Policy (OSTP), through by the Fast Track Subcommittee on Critical and Emerging Technologies (CET). This Subcommittee was founded in 2020 as part of the National Science and Technology Council (NSTC). The main goal of the Council is to "ensure that science and technology policy decisions and programs are consistent with the President's stated goals".

When this analysis was done in summer 2025 it was unclear whether the NSTC is still active as its last documents predate the new Trump administration and President Trump announced the creation of the President's Council of Advisors on Science and Technology in January 2025. The President's Council of Advisors on Science and Technology has not published a newer list since then, meaning the 2024 updated list on Critical and Emerging Technologies remains the most recent publication.

As the name suggests, the 2024 list is an update of a previous critical technologies list that was created in 2022. It includes 18 categories of CET with each category containing several subcategories and technologies. Overall, around 120 technologies are listed with varying levels of detail.

The listed categories are:

- Advanced Computing;
- Advanced Engineering Materials;
- Advanced Gas Turbine Engine Technologies;
- Advanced and Networked Sensing and Signature Management;
- Advanced Manufacturing;
- Artificial Intelligence (AI);
- Biotechnologies;
- Clean Energy Generation and Storage;
- Data Privacy, Data Security, and Cybersecurity Technologies;
- Directed Energy;
- Highly Automated, Autonomous and Uncrewed Systems (Uxs), and Robotics;
- Human-Machine Interfaces;
- Hypersonics;
- Integrated Communication and Networking Technologies;
- Positioning, Navigation, and Timing Technologies (PNT);
- Quantum Information and Enabling Technologies;
- Semiconductors and Microelectronics;
- Space Technologies and Systems.

Rationale

The list is a tool to identify security relevant technologies in the USA and to "inform government-wide and agency-specific efforts concerning U.S. technological competitiveness and national security"[16].

Yet the authors of the list point out that the list should not be interpreted as a priority list for either policy development or funding but as an instrument to (1) "inform future efforts that promote U.S. technological leadership; (2) cooperate with allies and partners to advance and maintain shared technological advantages; (3)

[15] https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf
[16] https://www.arnoldporter.com/en/perspectives/advisories/2024/02/updated-critical-and-emerging-technologies-list

develop, design, govern, and use CETs that yield tangible benefits for society and are aligned with democratic values; and (4) develop U.S. Government measures that respond to threats against U.S. security".

Selection criteria

The 2024 CET update does not publish a selection methodology or a scoring model for the selected technologies. However, it describes an interagency process and reasoning and commentaries exist. The following criteria can be elaborated:

- National security relevance: Technologies must pose significant implications for U.S. national security, defense, or strategic advantage (e.g. adversarial capabilities, defense systems, military applications).
- Transformative potential and enabling nature: Advanced technologies with breakthrough or enabling capabilities (e.g. AI, advanced computing, materials).
- Dual-Use: Many CETs can be used for civilian and military purposes.
- Interagency Coordination: The update was produced by subject matter experts across departments and agencies, reflecting broad consultation.
- Subfield Identification: The process sought to refine and reorganize subfields from previous lists (e.g. pulling out data privacy, cybersecurity) to make the list more coherent.

The document explicitly cautions that inclusion in the CET list does not equate to immediate prioritization or guaranteed funding; it should not be interpreted as a rigid ranking. The list is an expert-driven roadmap for strategic alignment.

Addressees

The main addressees are U.S. federal departments and agencies, departments involved in R&D, defense, intelligence, and technology (e.g. DoD, NSA, DARPA, DOE, NSF) as well as research institutions, universities, industry, and corporate actors. In addition, policy makers, regulators and standards bodies.

They should use the CET list as a framework for planning, evaluating, and coordinating R&D, defense, innovation, procurement, export controls, and regulation, and align interagency and departmental efforts to support U.S. leadership in areas on the list.

The CET list is non-binding. Its role is guidance, coordination, intelligence orientation, and strategic prioritization within the executive branch. Agencies may use it to design policies or funding programmes, but it does not impose direct obligations on private actors. The 2024 list update builds on the 2022 version and the 2020 original list. An update is expected no less than every two years.

US List of Critical and Emerging Technologies

Technology Areas	Technologies
1. Advanced Computing	- Advanced supercomputing, including for AI applications - Edge computing and devices - Advanced cloud services - High-performance data storage and data centers - Advanced computing architectures - Advanced modelling and simulation - Data processing and analysis techniques - Spatial computing
2. Advanced Engineering Materials	- Materials by design and material genomics - Materials with novel properties to include substantial improvements to existing properties - Novel and emerging techniques for material property characterization and lifecycle assessment
3. Advanced Gas Turbine Engine Technologies	- Aerospace, maritime, and industrial development and production technologies - Full-authority digital engine control, hot-section manufacturing, and associated technologies
4. Advanced and Networked Sensing and Signature Management	- Payloads, sensors, and instruments - Sensor processing and data fusion - Adaptive optics - Remote sensing of the Earth - Geophysical sensing - Signature management - Detection and characterization of pathogens and of chemical, biological, radiological and nuclear weapons and materials - Transportation-sector sensing - Security-sector sensing - Health-sector sensing - Energy-sector sensing - Manufacturing-sector sensing - Building-sector sensing - Environmental-sector sensing
5. Advanced Manufacturing	- Advanced additive manufacturing - Advanced manufacturing technologies and techniques including those supporting clean, sustainable, and smart manufacturing, nanomanufacturing, lightweight metal manufacturing, and product and material recovery
6. Artificial Intelligence (AI)	- Machine learning - Deep learning - Reinforcement learning - Sensory perception and recognition - AI assurance and assessment techniques - Foundation models - Generative AI systems, multimodal and large language models - Synthetic data approaches for training, tuning, and testing - Planning, reasoning, and decision making - Technologies for improving AI safety, trust, security, and responsible use
7. Biotechnologies	- Novel synthetic biology including acid, genome, epigenome, and protein synthesis and engineering, including design tools - Multi-omics and other biometrology, bioinformatics, computational biology, predictive

	modelling, and analytical tools for functional phenotypes - Engineering of sub-cellular, multicellular and multi-scale systems - Cell-free systems and technologies - Engineering of viral and viral delivery systems - Biotic/abiotic interfaces - Biomanufacturing and bioprocessing technologies
8. Clean Energy Generation and Storage	- Renewable generation - Renewable and sustainable chemistries, fuels, and feedstocks - Nuclear energy systems - Fusion energy - Energy storage - Electric and hybrid engines - Batteries - Grid integration technologies - Energy-efficiency technologies - Carbon management technologies
9. Data Privacy, Data Security, and Cybersecurity Technologies	- Distributed ledger technologies - Digital assets - Digital payment technologies - Digital identity technologies, biometrics, and associated infrastructure - Communications and network security - Privacy-enhancing technologies - Technologies for data fusion and improving data interoperability, privacy, and security - Distributed confidential computing - Computing supply chain security - Security and privacy technologies in augmented reality/virtual reality
10. Directed Energy	- Lasers - High-power microwaves - Particle beams
11. Highly Automated, Autonomous, and Uncrewed Systems (Uxs), And Robotics	- Surface - Air - Maritime - Space - Supporting digital infrastructure, including High Definition (HD) maps - Autonomous command and control
12. Human-Machine Interfaces	- Augmented reality - Virtual reality - Human-machine teaming - Neurotechnology
13. Hypersonics	- Propulsion - Aerodynamics and control - Materials, structures, and manufacturing - Detection, tracking, characterization, and defence - Testing
14. Integrated Communication and Networking Technologies	- Radio-frequency (RF) and mixed-signal circuits, antennas, filters, and components - Spectrum management and sensing technologies - Future generation wireless networks - Optical links and fibre technologies - Terrestrial/undersea cables - Satellite-based and stratospheric communications - Delay-tolerant networking - Mesh networks/infrastructure independent communication technologies

	- Software-defined networking and radios - Modern data exchange techniques - Adaptive network controls - Resilient and adaptive waveforms
15. Positioning, Navigation, and Timing (PNT) Technologies	- Diversified PNT-enabling technologies for users and systems in airborne, space-based, terrestrial, subterranean, and underwater settings - Interference, jamming, and spoofing detection technologies, algorithms, analytics, and networked monitoring systems - Disruption/denial-resisting and hardening technologies
16. Quantum Information and Enabling Technologies	- Quantum computing - Materials, isotopes, and fabrication techniques for quantum devices - Quantum sensing - Quantum communications and networking - Supporting systems
17. Semiconductors and Microelectronics	- Design and electronic design automation tools - Manufacturing process technologies and manufacturing equipment - Beyond complementary metal-oxide-semiconductor (CMOS) technology - Heterogeneous integration and advanced packaging - Specialized/tailored hardware components for artificial intelligence, natural and hostile radiation environments, RF and optical components, high-power devices, and other critical applications - Novel materials for advanced microelectronics - Microelectromechanical systems (MEMS) and Nanoelectromechanical systems (NEMS) - Novel architectures for non-Von Neumann computing
18. Space Technologies and Systems	- In-space servicing, assembly, and manufacturing as well as enabling technologies - Technology enablers for cost-effective on-demand, and reusable space launch systems - Technologies that enable access to and use of cislunar space and/or novel orbits - Sensors and data analysis tools for space-based observations - Space propulsion - Advanced space vehicle power generation - Novel space vehicle thermal management - Crewed spaceflight enablers - Resilient and path-diverse space communication systems, networks, and ground stations - Space launch, range, and safety technologies

This list is created by the DLR Projektträger on the basis of the "List of Critical Technologies in the National Interest".

7. The comparative SGS-Table of critical technologies

Background information

While compiling the overview of critical technology lists, it became apparent that there are substantial overlaps and similarities in the topics and categories covered. However, differences in how these topics are structured across the lists make it difficult to identify common themes, even when comparing the lists side by side. This observation led to the development of the comparative Safeguarding-Science-Table of Critical Technologies (SGS-Table) that juxtaposes and reorganises the individual lists to align them thematically and improve clarity and comparability.

After comparing various FOS (Fields of Science) and technology taxonomies, the EUREKA Taxonomy of Technological Areas[17] was chosen as a systematic framework for the comparative analysis. The EUREKA taxonomy was developed by the EUREKA network in close coordination with European technology fields and industry needs. It shows a high degree of thematic consistency with the technology lists under consideration, offers an appropriate level of detail without being too granular, and has a hierarchically organised structure.

The EUREKA Taxonomy of Technological Areas is organized in three levels that we labelled as (1) Main Category; (2) Subcategory and (3) Technology Area.

Table Design

The SGS-Table is divided into two sections. On the left-hand side, the three levels of the EUREKA taxonomy are shown: the main category on the far left, the subcategory in the middle, and the technology area on the right. Each level represents a subgroup of the one preceding it.

On the right-hand side, topics from the critical technology lists are matched to the corresponding rows of the respective EUREKA technology areas. Some topics could not be assigned to the third level of the EUREKA taxonomy because they cover a broader scope. In such cases, the topics were assigned to the corresponding first or second level of the EUREKA taxonomy. This is indicated by a blank field in the lower-level rows.

In other cases, topics from the critical technology lists corresponded to more than one EUREKA category. Where this occurred, related EUREKA categories were either merged into a single row or the topic was assigned to multiple rows. This was done in two ways: (1) when the topic name in a critical technology list explicitly matched the EUREKA category, the topic was written in black font; (2) If the topic name did not explicitly match a EUREKA category, but underlying individual technologies did, the topic was written in grey font.

Only explicitly matching topics are counted towards the total number of topic mentions (labelled: "Sum") in the final row. This approach allows the table to capture technological areas referenced in the critical technology lists both at the topic level and at the level of underlying individual technologies.

This classification was carried out with great care, but does not claim complete accuracy. It should be understood as a best-effort approach to support work with critical technology lists.

The SGS-Table presents only the topic names from the respective critical technology lists. A more detailed version containing all individual technologies is available and used for DLR-PT risk assessment services[18].

[17] https://www.eurekanetwork.org/wp-content/uploads/2025/08/Taxonomy-of-technological-areas.pdf
[18] https://www.safeguarding-science.eu/contact/

EUREKA: Field	EUREKA: Sub-field	EUREKA: Tech-Area	USA	EU	France	Canada	Australia	Netherlands	Sum
ELECTRONICS, IT AND TELECOMMS	Electronics, Microelectronics	Automation, Robotics Control Systems	11. Highly Automated, Autonomous, and Uncrewed Systems (UxS), and Robotics	9. Robotics and Autonomous Systems	7. Applied Mathematics, Information and Communication Sciences and Technologies	11. Robotics and Autonomous Systems	5. Autonomous Systems, Robotics, Positioning, Timing and Sensing	6. Mechatronics and Opto-mechatronics	5
	Electronic circuits, components and equipment	Quantum Informatics	16. Quantum Information and Enabling Technologies	3. Quantum Technologies	4. Physics	10. Quantum Science and Technology	4. Quantum Technologies	2. Quantum Technologies	5
		Semiconductors	17. Semiconductors and Microelectronics	1. Advanced Semiconductors Technologies	7. Applied Mathematics, Information and Communication Sciences and Technologies			9. Semiconductor Technologies	3
	Information Processing & Systems, Workflow	Data Processing/ Data Interchange, Middleware + Data Protection, Storage, Cryptography, Security	9. Data Privacy, Data Security, and Cybersecurity Technologies	2. Artificial Intelligence Technologies	7. Applied Mathematics, Information and Communication Sciences and Technologies	1. Advanced Digital Infrastructure Technology	3. Advanced Information and Communication Technologies	10. Cybersecurity Technologies	4
		Artificial Intelligence (AI)	6. Artificial Intelligence (AI)	2. Artificial Intelligence Technologies	7. Applied Mathematics, Information and Communication Sciences and Technologies	7. Artificial Intelligence and Big Data Technology	2. AI Technologies	7. Artificial Intelligence and Data	5
		User Interfaces, Usability	12. Human-Machine Interfaces			8. Human-Machine Integration			2
		Computer Technology/ Graphics, Meta Computing	1. Advanced Computing	2. Artificial Intelligence Technologies		1. Advanced Digital Infrastructure Technology			1
		Imaging, Image Processing, Pattern Recognition					5. Autonomous systems, robotics, positioning, timing and sensing	5. Imaging Technologies	1
	Telecommunications, Networking		14. Integrated Communication and Networking Technologies	5. Advanced Connectivity, Navigation and Digital Technologies	7. Applied Mathematics, Information and Communication Sciences and Technologies	1. Advanced Digital Infrastructure Technology	3. Advanced Information and Communication Technologies		3
		Satellite Technology/ Positioning/ Communication in GPS	15. Positioning, Navigation, and Timing (PNT) Technologies	5. Advanced Connectivity, Navigation and Digital Technologies			5. Autonomous systems, robotics, positioning, timing and sensing		2
INDUSTRIAL MANUFACTURING, MATERIAL AND TRANSPORT	Industrial Manufacture		5. Advanced Manufacturing	10. Advanced Materials, Manufacturing and Recycling Technologies	8. Engineering Sciences	3. Advanced Materials and Manufacturing	1. Advanced manufacturing and material technologies	3. Process technology, including process intensification	5
	Materials Technology		2. Advanced Engineering Materials	10. Advanced Materials, Manufacturing and Recycling Technologies	2. Chemistry	3. Advanced Materials and Manufacturing	1. Advanced manufacturing and material technologies		4
	Aerospace Technology	Space Exploration and Technology	18. Space Technologies and Systems	7. Space & Propulsion Technologies	6. Earth and Universe Sciences, Space	6. Aerospace, Space and Satellite Technology	5. Autonomous systems, robotics, positioning, timing and sensing		4
		Propulsion	13. Hypersonics			6. Aerospace, Space and Satellite Technology	5. Autonomous systems, robotics, positioning, timing and sensing		1
			3. Advanced Gas Turbine Engine Technologies						1
ENERGY			8. Clean Energy Generation and Storage	8. Energy Technologies	8. Engineering Sciences	2. Advanced Energy Technology	7. Clean energy generation and storage technologies	8. Energy Materials	5
BIOLOGICAL SCIENCES	Medicine, Human Health + Biology / Biotechnology		7. Biotechnologies	4. Biotechnologies	1. Biology, Medicine and Health	9. Life Science Technology	6. Biotechnologies	4. Biomolecular and Cell Technologies	6
MEASUREMENTS AND STANDARDS	Measurement Tools	Sensor Technology related to measurements	4. Advanced and Networked Sensing and Signature Management	6. Advanced Sensing Technologies		4. Advanced Sensing and Surveillance	5. Autonomous Systems, Robotics, Positioning, Timing and Sensing		4
PHYSICAL AND EXACT SCIENCES	Chemistry				2. Chemistry				1
	Physics				4. Physics				1
		Optics	10. Directed Energy					1. Optical Systems and Integrated Photonics	2
AGRICULTURE AND MARINE RESOURCES	Agriculture				5. Agricultural and Ecological Sciences				1
OTHER	Humanities				9. Humanities and Social Sciences				1
	Mathematics				3. Mathematics				1
	Engineering				8. Engineering Sciences				1
	Weapons				8. Engineering Sciences	5. Advanced Weapons			1