Proceedings of 4th International Conference CNDCGS'2024
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / DOI 10.3849/cndcgs.2024.75

Quantum Technology and its Role (Not Only) in the Strategic Concepts of Central European States – Mapping Study

Oldřich KRULÍK[1], Irena TUŠER[2], Tomáš KOLOMAZNÍK[2]

[1] Department of Security Management, AMBIS University, Lindnerova 575/1, 180 00 Prague, Czech Republic
[2] Department of Law and Cyber Security, AMBIS University, Lindnerova 575/1, 180 00, Prague, Czech Republic

Correspondence: oldrich.krulik@ambis.cz

Abstract

Quantum technologies represent a new agenda that has the potential to fundamentally change the security environment on a global scale. Countries or groups of countries that adopt these technologies before others will be at an advantage. The aim of the authors was to provide an overview of the current status of creating conditions for the development of quantum technologies in selected Central European countries (Czech Republic, Slovakia, Austria, Hungary and Slovenia). The study maps the conceptual, organisational and technical situation in this area, focusing on the five North Atlantic Treaty Organisation member states and the European Union. As a result of the investigation, it is found that the complexity of quantum technologies requires cooperation at two levels. The first level is undoubtedly cooperation between the state sector, scientific organisations, the defence sector and multinational companies. The second level is cooperation between individual states or within international organisations. Regarding the security aspects of these technologies, cooperation based on North Atlantic Treaty Organisation and European Union is crucial. Ensuring technological superiority in the coming years is a big challenge for the United States of America, resp. North Atlantic Treaty Organisation and the European Union.

KEY WORDS: *Central European States, cryptography, education, European Union, North Atlantic Treaty Organization, military defence, public policy, quantum technology, security, threats*

Citation: Krulík, O., Irena Tušer, I., Kolomazník, T. (2024). Quantum Technology and its Role (Not Only) in the Strategic Concepts of Central European States – Mapping Study. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.75.

1. Introduction

The contribution is devoted to the emerging, but even more relevant, the strategic grasp of the quantum issue (including the North Atlantic Treaty Organization quantum strategy). The authors map the positives (added value) of the emphasis on this agenda and the weaknesses resulting from the delay in this issue. Attention will also be paid to the quantum capacities of the individual Central European countries, as Czech Republic, Slovakia, Hungary, Austria and Slovenia (including the relevant strategic documents and its possible personnel, organizational and financial coverage).

In relation to the issue, both the approach of individual countries and the priorities of relevant international organizations (especially North Atlantic Treaty Organization and European Union) are being monitored. In this context, is it possible to claim that the European Union focuses more on technology as such, with the security dimension of the topic being left behind?

In this context, the content and diction of existing strategic-conceptual documents will be monitored, as well as the related external constructive-critical comments, especially from the private sector environment.

The period after 2010 to the present is covered, with the fact that, in relation to all individual countries, as many identical variables as possible are monitored, which will enable a subsequent comparison.

In relation to the topics, open sources are used only. Although this aspect can be perceived as limiting, it is also a prerequisite for publishing a study in itself.

2. Quantum Technologies – Approaching the Topic

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

Quantum technologies are a broad and diverse category of technologies that use the phenomena of quantum physics [1].

In quantum computers, pulses do not play a key role, but subatomic particles such as electrons or photons.

A quantum bit, a qubit, is a quantum analogue of a classical information bit. While a classic bit can only take on the value 0 or 1, a qubit can represent multiple values or states at once. In other words, a quantum computer can perform multiple calculations simultaneously, not necessarily sequentially (like a traditional computer). Thus, quantum computing shows the potential to outperform traditional computers due to much higher computing speeds [2].

Quantum computers can also use entanglement, a phenomenon that binds two or more qubits together so that their states are correlated. Any quantum manipulation of one of the entangled qubits generates an immediate effect on the other entangled qubits, regardless of the distance or barriers between them [3].

Quantum technology will, with a high probability, become, next to artificial intelligence, the most important emerging technology for general use. Quantum computing can bring enormous progress in science, including currently unsolvable logistical or logical problems [3, 4].

3. Core categories of Quantum Technologies

Quantum technologies can be divided into several main categories. Each of these generates impacts on information, intelligence, surveillance, reconnaissance, and cyber operations relevant to security and defence. In general, it is possible to state that quantum technologies will not introduce fundamentally new weapons, as was the case with nuclear and laser technologies, but rather will improve current sensing, communication and computing capabilities [3]:

a) Quantum computing

This is the use of quantum systems to perform calculations based on quantum logic and algorithms. Quantum computers can perform parallel and probabilistic calculations that allow them to solve certain problems faster and more efficiently than classical computers. Despite the misconception that the exponential increase in processing speed will affect and take over all tasks intended for classical computers, quantum computers will be particularly effective at breakthroughs in certain highly complex and demanding computational problems. Examples of such problems are quantum crypto-analysis (breaking most asymmetric encryption schemes commonly used to encrypt e-mail, voice and video, data transmissions and remote access), faster search, faster solution of linear or differential equations, quantum optimization (logistics, investment portfolios, or new drug designs) and quantum machine learning. Quantum technology can help solve complex and large-scale optimization problems, including resource allocation and decision-making, which are important for planning and executing military operations [1].

b) Quantum networks and communications

Quantum networks and communications aim to transmit quantum information (qubits) across different channels, such as optical lines, or in free space [1, 3].

- Quantum communication may enable quantum cryptography. Quantum cryptography can provide a higher level of security and authenticity than conventional asymmetric encryption (public key cryptography) because it can detect and prevent any eavesdropping or tampering by exploiting the properties of quantum physics. Quantum communication can enable quantum key distribution, which is a protocol that allows two parties to share a secret key using quantum states and measurements and classical communication. This technology is already commercially available to some extent for use with optical fibers.
- Quantum communication may enable quantum digital signatures, which allow a message to be signed using quantum states and measurements.
- Quantum communication can improve metrology, i. e. measurement using quantum states, to achieve higher precision than classical methods.
- Quantum communications can help improve the collection, dissemination, and protection of sensitive and intelligence information, as well as its situational awareness and operational effectiveness.
- Quantum communications can enable remote sensing, which is the use of quantum systems and protocols to detect and measure physical properties and phenomena such as distance, temperature, pressure, or magnetic fields without disturbing the system or environment.
- Quantum communication can enable quantum teleportation, which is a protocol that allows two parties to transfer a quantum state from one place to another using entanglement and classical communication.
- Laser communication offers high-speed data transfer ensured by quantum communication.

A next-generation quantum network, called a quantum information network (QIN) or quantum internet, is distinguished by its ability to distribute entangled qubits. QIN will offer more security-related services such as secure identification, location verification, and distributed quantum computing. The biggest obstacle to QIN implementing is the

need for a reliable quantum memory to store quantum information for synchronization and distribution in a network with many intermediate nodes. In practice, the introduction of QIN can realistically be expected after 2030.

c) Quantum simulation

Quantum simulation is the use of quantum systems such as atoms, photons or electrons to simulate and model other quantum systems such as molecules, materials or fields. Quantum simulation can use quantum algorithms to perform calculations and measurements on quantum systems. Quantum simulation can be applied in various fields such as chemistry, physics, biology and engineering (simulating the behaviour of molecules for chemical and pharmaceutical research, development of new materials, etc.). It can help to understand and design complex and dynamic systems, such as molecular structures, chemical reactions, material properties and physical phenomena, which are relevant for research, development, testing and technology evaluation [1].

d) Quantum sensing (imaging)

This is a subfield of quantum optics that is active (a signal is emitted, and its reflection detected). The principle behind quantum sensing is the more precise measurement of various physical variables, such as magnetic or electric fields and biological magnetic signals, gravity gradients, rotation acceleration and time. Improved time measurements can be used for more accurate clocks (used by many current technologies), quantum inertial navigation, underground and undersea exploration, more efficient radio frequency communication, etc. This allows detection of metallic or other objects creating local magnetic anomalies, such as mines, improvised explosive devices, and camouflaged vehicles. This can also serve as an alternative method of underwater navigation (supposedly able to detect a submerged submarine from space). Quantum gravimeters are intended for underground surveillance systems and are being tested to detect underground structures such as caves, tunnels, bunkers or missile silos. Quantum imaging systems can be used in any weather, day or night. Quantum sensing can provide accurate and reliable information without relying on external signals such as GPS. Quantum sensing can also provide high-resolution images and provide detailed and accurate information about the composition, structure, and state of matter and energy of the monitored objects [3].

Quantum radar is a quantum imaging system that works similarly to classical radar, but at the level of individual photons. The principles of quantum radar and quantum light detection (lidar) have already been successfully demonstrated in laboratories. However, the effectiveness of the solution as a whole is still very uncertain. Using a quantum sensor with a useful degree of accuracy is unlikely, as sufficient spatial resolution will result in insufficient sensitivity. On the other hand, some quantum sensors are expected to be tested in field conditions in the coming years, around 2028 [2, 3].

e) Post-quantum cryptography (PQC), also known as quantum-resistant cryptography

PQC is sometimes seen as a subcategory of quantum communication but is also often considered a separate category. Until now, information security was guaranteed by the mathematical complexity of encryption itself and the secure transmission of encryption keys. With the advent of quantum computers, the performance of which will make it possible to break encryption keys, it is necessary to find new ways of transmitting information that are resistant to cyber-attacks. The solution to such a problem is the transmission of encryption keys using quantum technologies. The concept itself is not necessarily related to quantum physics but is based on the development of contemporary asymmetric cryptography. This type of cryptography relies on more advanced mathematics that is more difficult to calculate, even for quantum computers. As such, the concept can be seen as a software/hardware upgrade of existing systems. Even this concept cannot be seen as completely secure, as new classical or quantum cryptanalytic attacks may occur. Nevertheless, tools falling under this definition will likely become available in the foreseeable future. [3, 5].

4. Unavailability of Quantum Solutions

All quantum systems are extremely fragile, and many can only be used at temperatures close to absolute zero (about -273°C). The slightest disturbance (heat, electromagnetic fields and moving air molecules) leads to loss of quantum information or sensitivity in quantum sensors. Some scientists predict that these obstacles will be overcome within the next 20 years. However, this speculative timeline is largely tied to the amount of financial and human resources allocated to this challenge. Quantum computers are likely to be too expensive to serve smaller groups of cybercriminals. Their pioneers will likely be large technology companies and research institutions – and variously motivated nation states [3, 4].

5. A New Concept of Deterrence? Rethinking Traditional Paradigms

Quantum technologies could have significant implications for nuclear deterrence, conventional forces, and cyber defence as they could create new vulnerabilities and asymmetries [1].

Some actors may gain access to quantum technology while others may not. This could create new challenges for the posture of the armed forces as well as for their strategic and operational capabilities. Quantum communications may also undermine existing norms and frameworks, such as the International Telecommunication Union and the Outer Space Treaty, which regulate the use of the electromagnetic spectrum and outer space. This could create new conflicts and require new agreements and regulations to ensure the peaceful and responsible use of quantum communication. Ensuring the security of information and communication is one of the key issues for the running of the state. A country is secure only if it can protect

information at the level of state institutions and its security forces, the health system, financial institutions, air traffic control, energy production and distribution, or transportation systems and logistics [5].

Anyone who assumes that the quantum threat is not a current challenge because quantum computing is not currently viable may be very wrong [4].

In October 2019, for example, Google announced the construction of a 53-qubit system, called Sycamore. He was able to calculate a proof in 3 minutes and 20 seconds confirming that the numbers generated by the random number generator are indeed random. The same task would take today's most powerful traditional computers about 10,000 years [2, 4, 6–8].

The People's Republic of China subsequently announced that it had a solution called Zuchongzhi with 66 qubits. In 2015, Prime Minister Xi Jinping explicitly designated quantum communication as a national strategic technological project where major breakthroughs to be achieved by 2030. Beijing is willing to allocate enormous resources to gain world leadership in quantum and other emerging technology fields. The total spending of the People's Republic of China on this agenda is estimated to be more than 2.5 billion USD per year after 2017, which is probably far more than the investment of the rest of the world combined [4, 9, 10].

This forced the Euro-Atlantic countries to take the subject seriously and invest accordingly. After all, history says that states capable of mastering the technology that gives them an edge in signal intelligence tend to be the winners in military conflicts as well. For example, the Allies were able to break the Enigma cipher that Nazi Germany relied on. London then kept its lead secret for decades to continue monitoring the communications of the Warsaw Pact countries [2, 11].

If anyone manages to build a fully functional quantum computer, much of conventional cryptography will fall apart. Quantum computing may disrupt some existing cryptographic systems being used to secure and encrypt data and communications. This could compromise the collection, dissemination and protection of sensitive and intelligence information.

As already stated in the text, quantum sensing can enable the discrete and remote detection and measurement of physical properties and phenomena such as temperature or magnetic fields. This could completely reshape the secrecy capabilities of any military and civilian activities. Military operations in all physical environments – on land, at sea, in the air, in space – rely on a variety of similar information technologies and networks that power the global economy. A systematic vulnerability in the cyber domain would become a systematic vulnerability in all domains. Classified information could be collected, changed or deleted. Personal, financial, legal, logistical and operational data could be manipulated to affect tactical and strategic operations. Malware could be installed at will to enable espionage or disrupt critical infrastructure.

With the prospect of a cryptographically significant quantum computer seemingly only a matter of time away, cybercriminals and geopolitical adversaries alike are rushing to obtain sensitive encrypted information that cannot be read today – so that it can be decoded once quantum computers become available.

Decrypting data encrypted by existing technologies will enable unprecedented visibility of highly valuable data. If the West were to lose the quantum computing race to rivals such as the People's Republic of China, the loss would be significant [4].

Cryptographic attacks can also negatively affect the economy and competitiveness. Quantum computers will increase the likelihood of intellectual property theft. Transport, energy distribution or communication systems will be particularly vulnerable. Disinformation could be spread from the secure accounts of senior officials, increasing the credibility of fraud efforts [8].

In relation to the issue, there is a very interesting mention of the creation of a new concept, which at the time of nuclear deterrence was called the **delicate balance of terror**. A new variant of the Cold War, apparently along the lines of the People's Republic of China versus the Euro-Atlantic states, may be based on the assumption that the mastery of quantum technology, capable of disrupting the functioning of an adversary's society, will be undesirable to the extent (assuming immediate retaliatory reaction) that the contending parties these eventualities they will really leave it as a weapon of the last judgment – and it will not be deployed.

The quantum threat to cyber security is an example of a self-fulfilling prophecy. The more convincing the prophecy of doom, the more determined its potential victims try to delay the disaster. In other words, states take this challenge so seriously that the most dangerous eventuality is unlikely to occur. So, there are reasons for cautious optimism that countermeasures are maturing faster than the threat. The quantum threat must be taken seriously, and that is precisely why it may never materialize. Given the pervasive importance of cyberspace, systematically compromising cybersecurity would be a strategic concern of the first order. History is full of expectations of technological transformation that never materialized. The race between offensive and defensive measures is as old as war itself. The balance between offense and defence at any given time depends on organizational and geostrategic context, not just technology. Scientific principles and technical feasibility limit the strategic and operational art of the possible. Technical trends set the boundary conditions for any potential **window of opportunity**. However, this window usually changes as individual actors start to create new weapons and to find new ways to use them [12].

A strategic swing would occur if one country acquired such a capability and kept this fact secret for several years or more. Other countries would not realize that everything, from their weapons systems to financial transactions, is vulnerable during this period – including historical records (encrypted communications collected by the adversaries and preserved in anticipation of obtaining this very capability). Attackers have an incentive to keep their progress secret because revealing it can prompt defenders to patch or reconfigure the respective systems. This represents a new “Sputnik moment”. Whoever acquires this technology first will also be able to cripple traditional defences and manipulate the global economy [12, 13].

6. Approaches of Individual Monitored Actors to the Mentioned Agenda

In examining the varied approaches to this agenda, we observe distinctive strategies adopted by major entities such as the United States of America, the North Atlantic Treaty Organization (NATO), and the European Union.

6.1 United States of America and the North Atlantic Treaty Organization

When it comes to the activities of the North Atlantic Treaty Organization in the monitored area, it is crucial to see the pivotal role played by the United States of America in this regard:

- In 2016, the National Institute of Standards and Technology began the process of standardizing post-quantum cryptographic algorithms, aware of the rapid development of quantum computing and its potential impact on information security [56].
- In 2018, the White House released the National Strategic Review for Quantum Information Science. The National Office for Quantum Coordination, interconnecting 14 government agencies, was launched [14].
- In December 2019, the National Quantum Initiative Act passed, foreseeing an annual investment of at least 240 million USD in the development of quantum technologies [4].
- In 2022, the Quantum Cybersecurity Preparedness Act passed, setting the perspective for the migration of government information to post-quantum cryptography. The document envisages completion of the transition by 2035, ideally by 2030 for the most sensitive data [4, 15].
- In 2023, the National Cybersecurity Strategy identified protection against quantum cyber attacks as a national strategic goal [16].

North Atlantic Treaty Organization's nuclear deterrence is based on the principles of credibility and accountability. At the same time, it depends on safe and reliable command, control and communication systems, as well as on effective and resilient defence systems [1].

The Alliance also for this reason recognized the importance and potential of quantum technologies, and has taken some steps to address them, such as the Science for Peace and Security Programme, the Innovation Hub, and the Emerging and Disruptive Technologies Roadmap [17, 18, 19].

In February 2021, the defence ministers of the member states approved a strategy to promote a coherent approach to the development and deployment of dual-use technologies, with quantum-enabled technology being one of the nine technology areas promoted in the strategy. At the summit in 2021, a concept called the Defence Innovation Accelerator for the North Atlantic (DIANA) was introduced, also including the dimension of quantum technologies. DIANA consists of a network of test centres and accelerators across member states where innovators develop new technologies to address pressing security challenges. An example of such a workplace is the "Deep Tech Lab – Quantum" in Copenhagen, focusing on the financial return of quantum solutions [3, 20].

Secretary-General Jens STOLTENBERG called for the development of a transatlantic quantum community that harnesses the power of this critical technology for security. He emphasized the importance of closer cooperation between the public, private and academic sectors and the acceleration of responsible innovation. Speaking at the Copenhagen Quantum Conference 2023, STOLTENBERG said: "*NATO has always adapted and embraced new technologies to keep our people safe. With the rapid proliferation of disruptive technologies, we need to adapt further and faster than ever before, including in the quantum domain… We need to ensure that these technologies work for us – not against us… We need to ensure that the Alliance is "quantum ready" and "capable of integrating the right technologies into our capabilities and protecting against adversary use*" [20].

The North Atlantic Treaty Organization's Quantum Strategy, issued on November 28, 2023, states, among others, the following [21, 22]:

- Quantum technologies represent a potential revolution in the world of innovation and can be game changers in security, including warfare. It offers possibilities that far exceed the technologies that are currently available. It is necessary to ensure that the Alliance is prepared for this technological development.
- This topic needs to be closely monitored, along with other key trends represented by artificial intelligence, biotechnology and human enhancement,2 hypersonic technologies, energy and propulsion, new materials and next-generation communication networks.
- Many of these technologies are already partially used in the private sector and have become subject to strategic competition. The Alliance must therefore support and lead collaboration with industry in the development of a transatlantic quantum technology ecosystem.
- Mastering these technologies will represent a strategic advantage – and not mastering them a strategic weakness. It is necessary to prepare the Alliance and individual member states to defend against the use of quantum technologies by their adversaries and competitors. It is equally important to detect and block potential related incidents in cyberspace.

[2] The authors are preparing a separate study on the topic in the future [23].

- Innovations are expected to help advances in cryptography, develop high-speed lasers to improve satellite connectivity, and improved 3-D imaging sensors in underwater environments.
- This requires investment coherence, cooperation between allies in technology development opportunities, as well as the development and protection of a skilled workforce. It will also require the development and deployment of critical supportive technologies…
- Strategic competitors and potential adversaries can also take advantage of disinformation opportunities by creating public distrust in the use of quantum technologies – similar to what happened in the case of 5G networks (according to the motto, "if we can't do something technically ourselves, we will try to install in the adversary's public that their homegrown advanced technologies are more harmful than beneficial…"). Allies will seek to pre-empt and counter any such efforts through strategic communications [24].

Some other recommendations and proposals of the Alliance for quantum technologies are, for example [1, 3]:

- Establishing a dedicated quantum technology office to coordinate and oversee all quantum activities and initiatives within the Alliance and among its allies and partners.
- Investing in research and finding opportunities to accelerate development and reduce related costs.
- Developing a quantum technology roadmap that would outline the vision, goals and priorities of the Alliance and allies and partners regarding quantum technologies.
- Enhancing its own quantum technology capabilities by investing in quantum research and development and deploying quantum technologies within its missions and operations.
- Enhancing technology education and training through the development and implementation of quantum technology curricula and courses and technology workshops and seminars for its employees and partners.
- Ensuring the development and implementation of quantum technology standards and regulations.
- Establishing and enforcing quantum technology rules for communication, information, and cyber systems.
- Ensuring quantum technology ethics and responsibility by developing and implementing quantum technology principles and guidelines, including the establishment and application of technology oversight and review mechanisms.
- Establishing goals and standards to support development and ensure interoperability.

6.2 European Union

For the European Union to thrive as a global competitor in quantum technology, it must protect access to sensitive government or personal data, or any data relevant to its technological and economic growth. The efforts that need to be made in this area go beyond the individual investment and research capacities of member states, and therefore there is a need to combine efforts and collaborate [25, 26].

To a certain extent, the European Union rather follows up and responds to the initiative steps of the United States of America (which it elaborates or adapts to the European environment). Union standardization processes follow the processes formulated by the National Institute of Standards and Technology. The whole concept is often mentioned as the connection of four levels [27]:

- Ultra Secure Connectivity Program from 2022 [20].
- Union scientific research initiative European Union Quantum Flagship; EUQF [28].
- Research projects within Horizon Europe [29].
- European quantum communication infrastructure (EuroQCI), an initiative that aims to build a secure quantum communication infrastructure that will span the entire space of the European Union member states. Quantum key transfer requires a very specific quantum communication infrastructure, which member states have committed to build within the EuroQCI initiative. EuroQCI is the Union's flagship project, with the aim of ensuring secure communication until 2027. All member states are signatories to this project, which in 2021 recorded the first interstate quantum-secure communication (100.5 km) between Trieste, Ljubljana and Zagreb. The EuroQCI concept, consists of several phases [1, 8, 30]:
    - Test phase, where there is an effort to operate various quantum lines via optical cables and ideally also with quantum satellites. This is a task for universities and other research platforms.
    - Educational phase, when possible, users will be introduced to the possibilities and functioning of quantum technologies.
    - Real deployment of quantum networks (assuming operation up to the SECRET level). This is the task of state agencies, or some certified operators and companies.

At the same time, coordinated prevention of "harvesting attacks" (theft of data for later decryption) is necessary. To support and expand the geographical scope of EuroQCI, the European Union approved the Union Secure Connectivity Program in 2022, concerning the development of the space segment for EuroQCI, the IRIS2 space constellation, built on the GOVSATCOM infrastructure. When completed, IRIS2 could become the flagship of the space program, along with the Copernicus and Galileo projects. In November 2019, member countries of the European Space Agency pledged to support the Space Systems for Safety and Security program, including a quantum component [31, 7, 32, 33].

However, according to critics, the EuroQCI concept distracts policy makers from paying attention to the fundamental challenges in relation to cyber security. The EuroQCI concept is intended to secure government communications and critical infrastructure but does not necessarily prevent incidents that disrupt other areas of cybersecurity, such as private supply chains [14, 8].

The challenges posed by quantum computers to European cyber security may seem distant, but the European Union's ability to detect, protect, defend and recover from them in the future starts with taking the necessary mitigation measures now. Therefore, a quantum cyber security program is essential for Europe's economic security in a rapidly evolving geopolitical environment and it is in the Union's interest to act swiftly [8].

In July 2021, for example, the European Union published a proposal for new anti-money laundering rules. They also include the creation of a new platform (Anti-Money Laundering Authority, AMLA), based on the cooperation and mutual support of the financial analytical units, as well as new requirements for cryptocurrency transfers. A separate problem that concerns all digital services is the long-term security of electronic communication between clients and banking entities. A possible risk comes from the introduction of quantum computers that can break current encryption methods. New technologies can be used/abused in stock market trading. This will probably happen as early as 2026 [34, 35].

The recommendations for the European Union, which result from the above statements, can be summarized as follows [8]:

- Create a quantum transition action plan that outlines clear goals and timeframes and monitors the implementation of national post-quantum encryption transition plans.
- Establish a new expert group within the European Union Agency for Cybersecurity (ENISA) with seconded national experts to exchange best practices and identify obstacles to transition to post-quantum encryption [14].
- Assist in prioritizing the transition to post-quantum encryption to respond to emerging vulnerabilities. Some – but not all – Member States are already taking steps to combat these emerging threats using available tools.
- Facilitate political coordination between the European Commission, and individual member states, national agencies for cyber security and the European Union Agency for Cybersecurity, with the aim of determining related technological priorities.
- Facilitate technical coordination at Union level, with the aim of addressing research gaps in quantum-safe technologies.

7. Individual Member States of the European Union

National quantum strategies are usually documents that define strategic goals in the field of quantum technologies, both security and economic. They usually include aspects such as the support and growth of a national quantum ecosystem, self-independence/self-sufficiency for specific technologies (for example, the establishment of a national quantum computer) and security strategic goals, where the transition to quantum-resistant encryption or quantum key distribution can be defined [36].

At least 12 Member States present national quantum strategies in the form of direct state-led science and research programmes. However, as of 2023, only a few member states have published plans to combat emerging quantum threats, and even fewer have initiated steps to mitigate them, such as Germany [37]. The cyber security budget and the number of specialists available allow only limited expectations regarding the mitigation of emerging threats [80].

Croatia, Cyprus, Greece, France, Lithuania, Slovakia, Slovenia, Sweden and Finland have agreed to cooperate with the other member states of the European Union to develop a quantum communication infrastructure (QCI) in Europe. In June 2019, the representatives of the mentioned states signed the initiated declaration of cooperation. The signatories, together with the European Commission and with the support of the European Space Agency, are going to explore the development and deployment of the European QCI over the coming years. Ultimately, it would connect sensitive public and private communication assets across the European Union [7].

Several countries, including **Austria** and **Slovenia**, participated in the project within the **European Defense Agency**, which is focused on the military use of quantum technologies. The project was led by France and focused on the following areas [38]:

- Fully autonomous positioning and timing for military platforms.
- Secure communication for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR).
- Quantum network of sensors for synergic connection.

7. Case Studies Concerning Selected Member States of the European Union

In relation to the countries monitored in more detail, there is an effort to at least indicatively mention key milestones, related strategic documents and the most relevant workplaces in relation to the monitored area. If possible, mention will be made regarding practical results, with an emphasis on the area of defence.

7.1 Czech Republic

The Czech Republic conducts remarkable research in a number of areas related to quantum technologies, but the connection between research and practice shows shortcomings. The fact that basic research is dominant here is related to funding opportunities, i.e. mainly from the Grant Agency or various infrastructure projects [39].

The Tensor Ventures fund has invested about a million dollars in the American start-up QC82, which develops quantum technology. In the future, however, they may be beneficial in the discovery of new drugs, materials, and help in energy savings or emission reduction [40].

The LUMI-Q project of the IT4Innovation company (national quantum computer) [41, 42] should be mentioned. The transfer of quantum keys between individual cities has also already taken place in the Czech Republic. The transfer was successful between Ostrava, where the academic organization CESNET and IT4Innovations computer centre joined the event, and Těšín. It is envisaged to build another quantum infrastructure with connections to Austria, Poland, Slovakia and Germany [9, 43, 44].

In February 2022, the Czech Technical University announced cooperation on projects dedicated to artificial intelligence, quantum technologies and other fields, with other platforms, including parts of the North Atlantic Alliance (DefSec Innovation Hub, Supreme Allied Commander Transformation). In doing so, a project mapping the physiological effects of methods of cognitive (**disinformation**) influence on individuals was explicitly mentioned [45, 17, 46].

Applied research mainly in quantum communications is reported by the University of Technology in Brno (NESPOQ project) [47].

In the field of education, there is an inter-faculty field at the Czech Technical University [48].

However, despite the mentioned activity, the **quantum ecosystem is a relative weakness of the state**. There are few start-ups in the country, among which Quantum Phi is the most visible, whose main content is consulting and advisory activities [39, 49].

The Quantum Day event was dedicated to efforts to link capacities in this scientific field, but the related results are ambiguous [50].

Transnational players such as IBM, Microsoft or Tensor Ventures are also active in the Czech Republic. However, most of the activities of the domestic academic sphere are apparently concentrated in the area of basic and not applied research (Palacký University). For the purpose of coordinating the involvement of domestic actors in national and international quantum projects, the National Initiative for Quantum Technologies was established, but its activities apparently stagnated around 2020. The initiative is linked to a roadmap that describes activities at individual workplaces. Some plans look promising, but many have not been translated into applied form, let alone commercially successful results [9, 51–53].

The vision of the reform of the transfer of knowledge and technology, mentioned in the text of the Program Statement of the current government, is related to the topic. According to the prime minister, the country must try to gain a strategic advantage in many relevant fields, since quantum technologies are not explicitly mentioned [54, 55].

The National Office for Cyber and Information Security resisted the task in the mentioned area for about a year, until the government assigned it to it through an official resolution. However, the state lacks experts in this field anyway [56–59].

When **Minister of Defence** Jana ČERNOCHOVÁ presented the priorities of the Ministry of Defense of the Czech Republic for the year 2022, the key word was modernization. "*We want to complete key modernization projects. Autonomous combat systems, **quantum technology**, biotechnology and artificial intelligence must be key for us"* [60].

7.2 Slovakia

The Government of Slovakia in collaboration with private sectors and academic institutions, has initiated several projects aimed at developing quantum computing, sensing, and cryptography solutions [61, 62]. These efforts are supported by strategic partnerships within the European Union, notably participating in the European Union Quantum Technologies Flagship program [28], which facilitates the development of quantum technologies across the Europe.

The main coordinator of the project is the Institute of Physics of the Slovak Academy of Sciences, which plans to build the southern and northern branches of the national quantum communication layer in the coming years. Other involved institutions are the Comenius University in Bratislava; Department of Electrical Engineering of the Slovak Academy of Sciences; Institute of Experimental Physics of the Slovak Academy of Sciences and the International Laser Centre [5].

Slovakia used the experience of the recent quantum transmission of encryption keys between Vienna and Bratislava as well as cooperation with various European research institutions. Slovakia received funds from the Digital Europe program, launched by the European Commission at the end of 2021. This is how part of the supporting quantum communication layer of the future European quantum internet was built. The project is part of the innovation plan under the auspices of the Ministry of Investments, Regional Development and Informatization of the Slovak Republic. The uniqueness of the proposed approach is also the creation of own experimental-technological expertise in the field of quantum technologies in the direct involvement of national scientific teams, students and private companies [63, 64].

In January 2023, the Slovak Quantum Communication Infrastructure (skQCI) European Union project was launched. Its main goal is to build a quantum communication infrastructure that will connect 12 academic institutions from

across the country. In addition, connections with neighbouring countries or quantum transmission of encryption keys using satellites arise. The creation of a highly efficient photon detector is planned, to be tested in the created communication infrastructure with a wide spectrum of use, practically in every field of quantum technologies [5].

The national strategic research agenda for quantum technology [65] is being shaped by Slovak National Centre for Quantum Technologies (QUTE). QUTE long-term strategic vision is to prepare Slovakia for the quantum industry. The QUTE Centre has been instrumental in establishing an environment that boosts Slovakia's capacity for competitive and excellent research and innovation in quantum technology. As a contributing member of the QUTE Centre, the Slovak Academy of Sciences is involved in several key initiatives: [66, 5]

- Developing an educational program [66] and founding eduQUTE, an international training centre.
- Establishing iQUTE, a virtual institute of quantum technologies that consolidates various research teams.
- Building the quantum communication infrastructure, netQUTE, as part of the EuroQCI European initiative, and developing a single-photon detector tailored for netQUTE's requirements [67].

In addition to local research hubs, Slovakia benefits from its collaborations with international entities and neighbouring countries. These partnerships help in sharing knowledge, joint research initiatives, and in securing funding for expansive projects that further the defence-oriented quantum research [68, 69].

One of the most compelling applications of quantum technology in defence is in the realm of quantum cryptography. Slovakia is involved in the development of quantum key distribution systems (QKD), which provide theoretically unbreakable encryption for secure military communications [65].

Another significant area is quantum sensing, where research teams are working on quantum radar and other sensing technologies that could potentially detect objects invisible to conventional radar systems. These technologies are crucial for surveillance and reconnaissance missions, providing a tactical advantage in defence operations.

Despite the promising developments, the road ahead for quantum technology in Slovakia's defence sector faces several challenges. These include high investment costs, the need for specialized human capital, and the rapid pace of global quantum technology advancements, which Slovakia must keep up with. Furthermore, ethical considerations and international regulations on quantum technologies in warfare need continuous attention [70, 71].

7.3 Austria

Austria is one of the countries where quantum research is developing the most. Success in this field is evidenced by the fact that Austrian quantum physicist Anton ZEILINGER received the 2022 Nobel Prize in Physics. Rainer BLATT founded the Institute for Quantum Optics and Quantum Information in Innsbruck already in 2003 [72].

Important activities in this field in recent years include, for example, The Austrian Quantum Technology Initiative in 2016. Austria launches the national research ad development funding programme for quantum research and technology with a budget of 32,7 million EUR over 2017-2021 [73].

In 2021, Austria launched the Quantum Austria research campaign. This is an initiative of the Federal Ministry for Education, Science and Research. Austria is investing 107 million EUR into expanding quantum research and technologies using the Next Generation European Union recovery and resilience plan funds [74, 75].

Other important documents in this area include Austrian Research Infrastructure Action Plan 2030, which focuses on expanding research infrastructure and participating in European and international large-scale research infrastructure. The strategy is to strengthen Austria's international position in this area [76].

In Austria, several institutions are devoted to quantum technology. The Vienna Centre for Quantum Science and Technology (VCQ) undoubtedly belongs to the essential institutions in Austria, and it is one of the largest quantum hubs in Europe. There are integrated 31 research groups from the University of Vienna, the Technical University Wien, the Austrian Academy of Sciences, and the Institute of Science and Technology Austria [77].

In December 2023, Austria’s cluster of excellence for quantum sciences was launched. It comprises more than sixty research groups in Innsbruck, Vienna, Linz, and Klosterneuburg [78].

The QCI-CAT consortium is building the Austrian national project of the European Commission initiative EuroQCI. It is a team made up of scientists from five universities, major industrial partners and with the support of relevant ministries. The consortium brings together a mature ecosystem of technology suppliers, integrators and operators, and finally end users, which will enable the project to carry out its activities as close as possible to the actual operation of secure quantum communication networks. The project aims to adopt modern encryption technology for highly secure communication between public authorities. In addition, new technological approaches, such as the combination of post-quantum encryption, are being researched 79–81].

The association Quantum Society Austria was founded in 2022 in Vienna, Austria. A platform brings together experts of various levels in the field of research and practice [42].

Austrian Institute of Technology is part of the QUARTZ consortium, which is developing the quantum key distribution satellite system and service architecture. This includes the service, underlying technologies, and ground-based end-to-end testing. The technologies will also be used in security and the military. Other international institutions from Germany or the Czech Republic participate in the project. The Austrian Armed Forces are also involved in this project, with aim to use quantum technologies, especially in cyber defence, digitalization and autonomous systems [82].

Austria is cooperating with People’s Republic of China on quantum technologies even though, for example, the United States of America are trying to eliminate China's approaches to these technologies. In 2017, Austrian and Chinese

scientists created a quantum communication link between Beijing and Vienna using the Mozi satellite. This satellite was also used to connect People's Republic of China and Russian Federation in 2023 [83].

7.4 Hungary

Hungary has been among the first European countries with a programme for quantum technology. The first flagship programme was Hungary Quantum Technology – HunQuTech (2017-2021). Hungary also became a member of the European Union's Quantum Flagship, a large-scale initiative launched in 2018 that involves developing quantum technologies across Europe over a ten-year period (funded under Horizon Europe) [84, 85, 28].

In 2020, Hungary launched the National Laboratories programme [86]. National Laboratories are conceived as knowledge centres and scientific hubs in areas with high potential for the national economy. National Laboratories are dynamic, institutionalised, collaboration-based arenas of discovery and experimental research that open up new, international dimensions and enable the social, economic and environmental utilisation of research results. As a key vehicle for international collaboration in quantum technologies in Hungary, QuantERA plays a crucial role in coordinating and funding research projects that span various aspects of quantum technologies, including quantum communication, quantum simulation, quantum computation, and quantum sensing. QuantERA not only amplifies Hungary's presence in the global quantum technology scene but also aligns with the country's broader goals of enhancing its scientific and technological infrastructure [67].

The Quantum Communication Infrastructure (QCI Hungary) project, officially known as the Deploy Advanced Quantum Communication Infrastructure in Hungary, is a significant initiative under the European Union's Digital Europe Programme, aimed at establishing a robust quantum communication infrastructure across Hungary. The overarching goal of this project is to integrate Hungary into a larger pan-European quantum network, enhancing the country's technological infrastructure and its position within the European Union's strategic communications framework. QCI Hungary seeks to connect Budapest, with three other major cities (Győr, Nagykanizsa, and Szeged) laying the groundwork for potential future expansions into neighbouring countries (Austria, Slovakia, Slovenia, Croatia, and Romania). The infrastructure within Budapest will include a metropolitan quantum network designed to serve multiple applications, supported by commercially available quantum key distribution (QKD) systems [68].

Through these efforts, QCI Hungary aims not only to advance quantum communication technology but also to secure a leading role for Hungary in the European quantum landscape, enhancing both national security and technological prowess.

7.5 Slovenia

The Ministry of Public Administration of Slovenia promotes the concept that the European Union must remain a global superpower when it comes to investing in quantum technologies. The country declares an effort to make new technology to be safe and serve society as a whole, both in space and on Earth [60].

One of Slovenia's key strategic documents is the Digital Slovenia 2030 Strategy, which is devoted to developing quantum technologies [87].

In 2019, Slovenia signed the Declaration on Cooperation Framework on Quantum Communication Infrastructure [88].

In 2021, Slovenia, together with other countries, signed the Quantum Future Declaration. This initiative aims to achieve the same level of quantum technology cooperation as developed Western European countries by fostering cooperation on these technologies between countries that have not yet made significant progress in this area [89].

In 2021, a demonstration of quantum communication between three countries took place: Italy, Slovenia and Croatia. It was Encrypted audio-video communication among Trieste, Ljubljana and Rijeka [90].

In May 2023, Google launched quantum tech centre in Ljubljana. The centre is devoted to research, but also educational activities. For example, students can carry out their PhD research in the most advanced quantum laboratories, mostly across Europe [91, 92].

Important research centres in quantum technologies include the Jozef Stefan Institute, Faculty of Mathematics and Physics, University of Ljubljana. The Institute mainly deal with quantum-enhanced devices and their applications in quantum computing, quantum simulations, quantum communication, and quantum metrology [93].

University of Ljubljana in general is working on a project called the Slovenian Quantum Communication Infrastructure Demonstration. The project addresses the implementation of a quantum network between research and government organizations in Slovenia. In addition to the technological focus, the project also focuses on preparing experts and training key personnel [94].

8. Results of the Investigation

The topic of quantum technologies may very soon represent a nemesis for modern civilization. It is in the interest of the Euro-Atlantic states not to fall behind in this area, including related military use. Any recommendations in the monitored area imply the need to invest considerable resources and acquire qualified personnel, which is very difficult at a time when there are a number of parallel social ties.

The complexity and comprehensiveness of quantum technologies require cooperation on two levels. The first level is undoubtedly the cooperation of the state sector, scientific organizations, defence and multinational companies. Without the connection of these entities, it isn't easy to imagine achieving positive results. As we have already shown in the mapping of the individual states of Central Europe, cooperation is already intensively underway. The second level is cooperation between individual states, resp. cooperation within international organizations. With regard to the security aspects of these technologies, cooperation based on North Atlantic Treaty Organisation, or the European Union is crucial. Ensuring technological superiority in the coming years is a big challenge for the United States, resp. North Atlantic Treaty Organisation and the European Union.

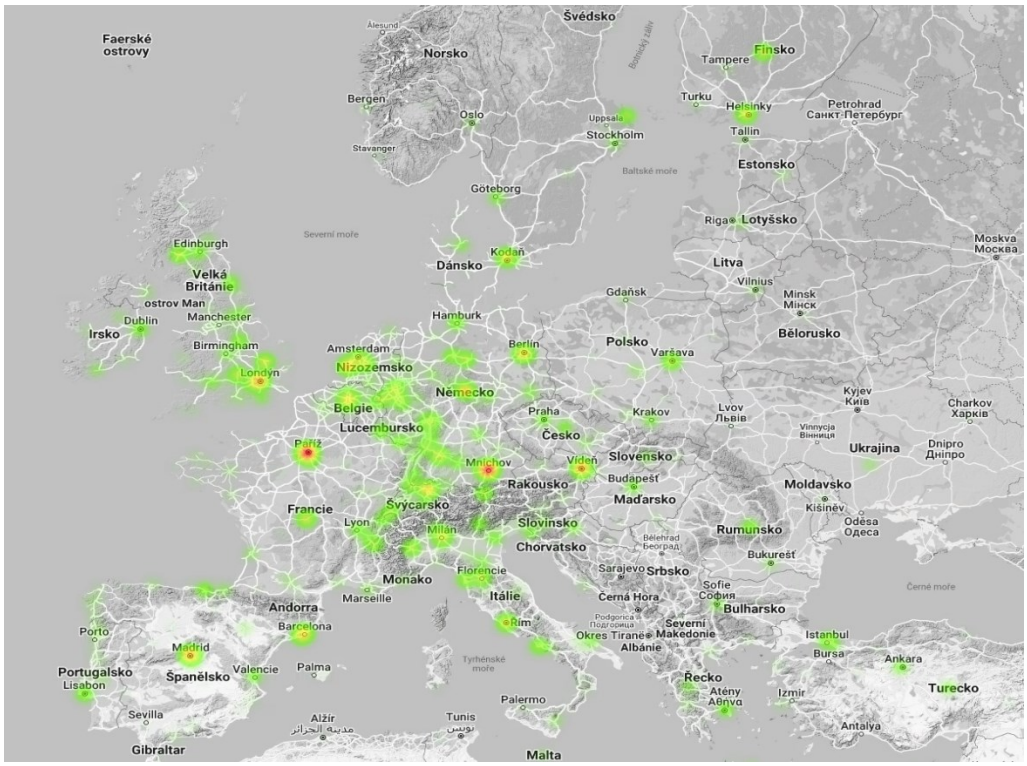

Fig. 1. Gradually focused heat map regarding the distribution of capacities for solving tasks related to quantum technology according to the European Union Quantum Flagship platform [94].

Fig. 2. Gradually focused heat map regarding the distribution of capacities for solving tasks related to quantum technology according to the European Union Quantum Flagship platform [94].

On the other hand, the effort to join forces within international organizations is reaching its limits, when some member states of the European Union and the North Atlantic Treaty Organization on the other side even today see the potential for cooperation with the People's Republic of China or even the Russian Federation in the field of quantum technologies. In several places, there is mention of the phenomenon of disinformation, for which quantum technologies represent a much greater opportunity – regarding its creation, dissemination and targeting, than for its suppression. Separately, the topic of quantum technologies is mentioned regarding the development of new drugs or in estimating the development of the economy (stock prices), which are again agendas with a high degree of potential abuse. In this respect, quantum technologies also bring many societal risks and will gradually become a significant topic.

Gradually focused heat map regarding the distribution of capacities for solving tasks related to quantum technology according to the European Union Quantum Flagship platform [94] is presented in Fig. 1. and Fig. 2. It is obvious that the observed five countries are in this respect, with the exception of Vienna, rather peripheral [95].

9. Conclusions

Quantum technology represents a relatively new solution, the anchoring of which at the level of states and relevant international organizations represents a very pressing challenge, especially in light of the sharp deterioration of the international security situation. Central European countries are significantly involved in this area and are achieving interesting results in it. Mastering the issue can thus be a decisive advantage in the event of a possible conflict, or rather play a role in the related deterrence. On the contrary, failure to master the topic can become a significant weakness, degrading the potential of a certain actor's security system.

Acknowledgements.

The paper was prepared on behalf of AMBIS University, to whom the authors thank for the support.

References

1. **Holitschke S.** Quantum Technologies and NATO's Deterrence and Defense Posture: Opportunities, Risks, and Implications. LinkedIn, 11 December 2023. Available online: https://www.linkedin.com/pulse/quantum-technologies-natos-deterrence-defense-posture-holitschke-nhjde.
2. **Zhou, Q.** The Subatomic Arms Race: Mutually Assured Development. Harvard International Review. Vol. 42, No. 2, Spring 2021, pp. 15-19. Available online: https://www.jstor.org/stable/27275694.
3. **Křelina M., Dúbravčík D.** Quantum Technology for Defence: What to Expect for the Air and Space Domains. Journal of Joint Air Power Competence Centre, February 2023. Available online: https://www.japcc.org/articles/quantum-technology-for-defence/.
4. **Grobman, S.** Quantum Computing's Cyber-Threat to National Security. Prism, 2020, Vol. 9, No. 1, pp. 52-67. Available online: https://www.jstor.org/stable/10.2307/26940159.
5. **The Quantum Era Begins in Slovakia.** Slovak Academy of Sciences, 31 January 2023. Available online: https://www.sav.sk/?lang=en&doc=services-news&source_no=20&news_no=11001.
6. **Dargan J.** Quantum Journey from the Search Engine to Google Sycamore. Quantum Insider, Available online: 14 July 2022. https://thequantuminsider.com/2022/07/14/google-sycamore/.
7. **Nine More Countries Join Initiative to Explore Quantum Communication for Europe.** European Commission; Digital Strategy, 28 November 2019. Available online: https://digital-trategy.ec.europa.eu/nl/node/1305/printable/pdf.
8. **RodriguezA., G.** A Quantum Cybersecurity Agenda for Europe: Governing the Transition to Post-Quantum Cryptography. Europe's Political Economy Programme, Discussion Paper, 17 July 2023. Available online: https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf
9. **Sedlák J.** The Czech Republic has succeeded in quantum data transfer and is in the process of building a quantum network. Ekonom, 29 July 2021. In Czech available online: https://ekonom.cz/c1-66956300-cesku-se-povedl-kvantovy-prenos-dat-a-resi-vystavbu-kvantove-site.
10. **Němečková K.** Czech scientists underestimate the risks of cooperation with China. Czech Press Office, 23 November 2022. In Czech available online: https://www.ceskenoviny.cz/tiskove/zpravy/cesti-vedci-podcenuji-rizika-spoluprace-s-cinou/2289252.
11. **China Electronic Technology Group Corporation.** Available online: http://www.cetcei.com.
12. **Lindsay, J., R.** Surviving the Quantum Cryptocalypse. Strategic Studies Quarterly, Vol. 14, No. 2, Summer 2020, pp. 49-73. Available online: https://www.jstor.org/stable/10.2307/26915277.
13. **Schroeder, P.** Historical Reality vs. Neo-Realist Theory. International Security, 1994, vol. 19, No. 1 (Summer), pp. 108-148. Available online: https://www.jstor.org/stable/2539150?origin=crossref.
14. **Post-Quantum Cryptography: Anticipating Threats and Preparing the Future.** European Union Agency for Cybersecurity, 19 October 2022. Available online: https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future.

15. **Quantum Computing Cybersecurity Preparedness Act.** United States Congress, 21 December 2022. Available online: https://www.congress.gov/bill/117th-congress/house-bill/7535.
16. **National Cybersecurity Strategy.** White House, 1 March 2023. Available online: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
17. **DefSec Innovation Hub.** Available online: http://www.dsih.org/index.php/en/.
18. **Emerging and Disruptive Technologies.** North Atlantic Treaty Organization, 15 April 2024. Available online: https://www.nato.int/cps/en/natohq/topics_184303.htm.
19. **Science for Peace and Security Programme.** North Atlantic Treaty Organization, 17 April 2023. Available online: https://www.nato.int/cps/en/natohq/topics_85373.htm.
20. **Musil M.** Stoltenberg calls for a transatlantic quantum community and welcomes Danish leadership. Army Mag, 1 October 2023. In Czech available online: https://www.armymag.cz/2023/10/stoltenberg-vyzyva-k-vytvoreni-transatlantickeho-kvantoveho-spolecenstvi-a-vita-vedeni-danska/.
21. **NATO Releases First Ever Quantum Strategy.** North Atlantic Treaty Organization, 17 January 2024. Available online: https://www.nato.int/cps/en/natohq/news_221601.htm.
22. **Summary of NATO's Quantum Technologies Strategy.** North Atlantic Treaty Organization, 16 January 2024. Available online: https://www.nato.int/cps/en/natohq/official_texts_221777.htm.
23. **Summary of NATO's Biotechnology and Human Enhancement Technologies Strategy.** North Atlantic Treaty Organization, 12 April 2024. Available online: https://www.nato.int/cps/en/natohq/official_texts_224669.htm.
24. **Hoyle A., Šlerka J.** Cause for Concern: The Continuing Success and Impact of Kremlin Disinformation Campaigns; Working Paper 29. The European Centre of Excellence for Countering Hybrid Threats. Helsinki, March 2024. ISBN 978-952-7472-94-1. Available online: https://www.hybridcoe.fi/wp-content/uploads/2024/03/20240306-Hybrid-CoE-Working-Paper-29-The-impact-of-Kremlin-disinformation-WEB.pdf.
25. **Quantum threat and quantum-resistant cryptography.** National Office for Cyber and Information Security Czech Republic, 1 July 2023. In Czech available online: https://1url.cz/RuyPh.
26. **Questions & Answers: Connectivity Package.** European Commission, 21 February 2024. Available online: https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_942.
27. **European Union Secure Connectivity Programme 2023-2027.** European Parliament. 2022; 2023. Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729442/EPRS_BRI(2022)729442_EN.pdf.
28. **Quantum Technologies Flagship.** European Commission, 2023. Available online: https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship.
29. **Quantum: Digital and Emerging Technologies For Competitiveness and Fit for the Green Deal.** National Information Centre For European Research; Technology Centre Prague. Available online: https://www.horizontevropa.cz/en/calls/yiifchallenges/177.
30. **European quantum communication infrastructure (EuroQCI).** Evropská komise. Available online: https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci.
31. **GOVSATCOM, the European Union Secure Satcom Service Hub.** European Union Agency for the Space Programme, 27 February 2024. Available online: https://www.euspa.europa.eu/newsroom-events/news/govsatcom-eu-secure-satcom-service-hub.
32. **Space Systems for Safety and Security.** Connectivity and Secure Communication; European Space Agency. Available online: https://connectivity.esa.int/space-systems-safety-and-security-4s.
33. **Taking Climate Monitoring into the Future with Quantum.** European Space Agency, 26 May 2022. Available online: https://www.esa.int/Applications/Observing_the_Earth/FutureEO/Taking_climate_monitoring_into_the_future_with_quantum.
34. **Juřík P.** Customer identification in "new clothes". Biometrics as the optimal way? Hospodářské noviny, 11 November 2021. In Czech available online: https://HN.HN.CZ/c1-66998520-identifikace-zakazniku-v-bdquo-novem-havu-ldquo-biometrie-jako-optimalni-cesta.
35. **Quantum Computing.** Anti-Money Laundering. Available online: https://anti-money-laundering.eu/quantum-computing/.
36. **Křelina M.** Czech National Quantum Strategy. Qubits.cz, 5 July 2023 (2023a). In Czech available online: https://qubits.cz/clanky/nazor-ceska-narodni-kvantova-strategie/.
37. **Quantentechnologien in Deutschland.** Bundesministerium für Bildung und Forschung. Available online: https://www.quantentechnologien.de/qt-in-deutschland.html.
38. **QuantaQuest Project Explores Application of Quantum Technologies in Defence.** European Defence Agency, 19 January 2024. Available online: https://eda.europa.eu/news-and-events/news/2024/01/19/quantaquest-project-explores-application-of-quantum-technologies-in-defence.
39. **Call 2021 – 39 European Excellent Projects Awarded Funding.** Quantera. Available online: https://quantera.eu/quantera-call-2021-39-european-excellent-projects-awarded-funding/.
40. **ICT Network News.** Czech fund Tensor Ventures invested 23 mil. CZK in a start-up in quantum technology. Czech Press Office. 28 April 2022. In Czech available online: https://cz.ict-nn.com/cesky-fond-tensor-ventures-vlozil-23-mil-kc-do-start-upu-v-kvantove-technologii/.

41. **Křelina, M.** Czech Republic one step closer to the first quantum computer. Qubits, 28 June 2023 (2023c). Available online: https://qubits.cz/tiskovky/ceska-republika-o-krok-blize-k-prvnimu-kvantovemu-pocitaci/.
42. **Quantum Society Austria.** Available online: https://www.quantumsocietyaustria.com.
43. **Open QKD.** Available online: https://openqkd.eu/.
44. **Quantum Computing Lab.** IT4Innovations. Available online: https://www.it4i.cz/en/research/research-laboratories/quantum-computing-lab.
45. **Czech Technical University in Prague will cooperate with NATO.** Czech Press Office, 23 February 2023. In Czech available online: https://denikn.cz/minuta/1087915/.
46. **Hack the Mind.** DefSec Innovation Hub. Available online: http://www.dsih.org/index.php/en/events/hack-the-mind.
47. **NESPOQ project.** Brno University of Technology – Crypto/AXE Team. Available online: https://www.nespoq.cz.
48. **Czech Technical University.** It will be possible to study quantum informatics at the Czech Technical University. 1 November 2022. In Czech available online: https://aktualne.cvut.cz/stalo-se/20221101-na-cvut-bude-mozne-studovat-kvantovou-informatiku.
49. **Quantum Phi.** Available online: https://www.quantumphi.com.
50. **Louda J.** The first Quantum Day was far from the last. LinkedIn, 30 June 2023. In Czech available online: https://www.linkedin.com/pulse/prvn%C3%AD-quantum-day-nebyl-zdaleka-posledn%C3%ADm-jan-louda/.
51. **Křelina M.** The Czech Republic has no quantum companies or applied research, or concerns about the national quantum strategy. Lupa, 13 July 2023 (2023b). In Czech available online: https://www.lupa.cz/clanky/cesko-nema-kvantove-firmy-ani-aplikovany-vyzkum-aneb-obavy-z-narodni-kvantove-strategie/.
52. **National Quantum Technology Initiative.** In Czech available online: https://nikt.cz/.
53. **Quantum Technologies in Czechia Roadmap.** National Quantum Technology Initiative, 29 May 2017. In Czech available online: https://nikt.cz/files/roadmap-QT-CZ-v3.pdf.
54. **Government of the Czech Republic**. The reform should deepen the link between research and the private sphere. Czech Press Office, 25 January 2024. In Czech available online: https://vlada.gov.cz/cz/media-centrum/aktualne/reformu-provedeme-ve-spolupraci-s-vysokymi-skolami-93037/.
55. **Government of the Czech Republic.** Government Programme Statement. 1 March 2023. In Czech available online: https://vlada.gov.cz/cz/programove-prohlaseni-vlady-193547/.
56. **Langšádlová H.** Minister for Science, Research and Innovation. We need a stronger education for entrepreneurship, which includes the ability to take risks, to have ambitious plans. 7 October 2023. In Czech available online: https://vlada.gov.cz/scripts/detail.php?pgid=1062.
57. **Czech Technical University.** The USA wants to make the Czech Republic a centre for quantum computers. But the state is not ready yet. 8 June 2023. In Czech available online: https://aktualne.cvut.cz/zpravy-z-medii/20230608-usa-chteji-z-ceska-udelat-centrum-pro-kvantove-pocitace-stat-ale-zatim-neni.
58. **Bekesiene S., Meidute-Kavaliauskiene I., Hoskova-Mayerova S.** Military leader behavior formation for sustainable country security. Sustainability, 2021, 13(8), 4521. doi:10.3390/su13084521.
59. **Nikitin A, Bekešienė S, Hošková-Mayerová Š, Krasiuk B.** Multidimensional Model of Information Struggle with Impulse Perturbation in Terms of Levy Approximation. *Mathematics*. 2024; 12(8):1263. https://doi.org/10.3390/math12081263.
60. **Černochová J.** Department of Defense. The army wants people who can shoot and know their way around a map10 January 2022. In Czech available online: https://www.idnes.cz/zpravy/domaci/cernochova-obrana-nato- priority-ministerstvo-rusko-zbrane.A220110_085510_domaci_remy.
61. **Centre of Scientific and Technical Information of the Slovak Republic.** Available online: https://www.cvtisr.sk/.
62. **QWorld Association Estonia.** Available online: https://qworld.net/.
63. **Slovak Quantum Communication Infrastructure.** Available online: http://skqci.qute.sk/.
64. **Centre for Scientific and Technical Information of the Slovak Republic.** Available online: https://www.cvtisr.sk/.
65. **Ziman M.; Grajcar M.; Samuely T.; Gmitra M.** Platform Action Plan QUTE.SK. Slovak National Quantum Center for Quantum Technologies, November 2018. Available online: http://www.qute.sk/wp-content/uploads/2023/11/qutesk_akcny_plan.pdf.
66. **Slovak National Center for Quantum Technologies.** Available online: http://www.qute.sk.
67. **Vagaská A., Račková P., Jekl J.** Key dimensions of an innovative approach to the teaching of mathematics at technical universities (in SK and CZ). In: ICERI2021 Proceedings. Online Conference: IATED, 2021, vol. 14, p. 9995-10002. ISSN 2340-1095. ISBN 978-84-09-34549-6. doi:10.21125/iceri.2021.2374.
68. **QuantERA.** Available online: https://quantera.eu.
69. **Quantum Communication Infrastructure in Hungary.** Available online: https://qcihungary.hu/en/home/.
70. **Cortez K.; Bambauer, E.; Bambauer, Y.; Jane, R.; Guha, S.; Fleming, S.** A Quantum Policy and Ethics Roadmap. Social Science Research Network – Elsevier, United States, 2023. http://dx.doi.org/10.2139/ssrn.4507090.
71. **How, M.-L.; Cheah, S.-M.** Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era. Businesses 2023, No. 3, pp. 585-605. https://doi.org/10.3390/businesses3040036.
72. **Quantum Technology is Developing at a Rapid Pace.** Society of German Natural Scientists and Physicians. Available online: https://www.gdnae.de/en/rainer-blatt-quantum-technology-is-developing-at-a-rapid-pace/.

73. **Quantum Technologies and Space.** European Patent Office. Munich, 2021. Available online: https://www.espi.or.at/wp-content/uploads/2021/11/Quantum-Technologies-and-Space-Collaborative-Study.pdf.
74. **Austria Launches Quantum Austria Research Campaign.** Austrian Research Promotion Agency; Quantum Austria, 25 Noveber 2021. Available online: https://www.ffg.at/en/press/austria-launches-quantum-austria-research-campaign.
75. **Quantum Austria.** Available online: https://www.ffg.at.
76. **Forschungs Infrastruktur Datenbank.** Federal Ministry of Education, Science and Research. Available online: https://forschungsinfrastruktur.bmbwf.gv.at/en.
77. **Vienna Center for Quantum Science and Technology.** Available online: https://vcq.quantum.at/.
78. **Austria's Cluster of Excellence for Quantum Sciences Launched.** Wiley Industry News, 1 December 2023. Available online: https://www.wileyindustrynews.com/en/news/aus-tri-cluster-excellence-quantum-sciences-launched.
79. **Alpine Quantum Technologies.** Available online: https://www.aqt.eu/.
80. **Making Austria Quantum Secure.** QCI-CAT. Available online: https://qci-cat.at/.
81. **Quantum Technology Laboratories.** Available online: https://www.qtlabs.at/.
82. **Austrian Institute of Technology.** Available online: https://www.ait.ac.at.
83. **Weber V.** The New Quantum Technology Race. International Politik Quarterly, 2024, No. 2. 22 March 2024. Available online: https://ip-quarterly.com/en/new-quantum-technology-race.
84. **HunQuTech; National Quantum Technology Program.** Available online: https://wigner.hu/quantumtechnology/en/node/1.
85. **National Research, Development and Innovation Office.** Available online: https://nkfih.gov.hu/about-the-office.
86. **Quantum Information National Laboratory.** Available online: https://qi.nemzetilabor.hu/.
87. **Digital Slovenia 2030 Strategy.** National Interoperability Framework. Available online: https://nio.gov.si/nio/asset/strategija+digitalna+slovenija+2030?lang=en.
88. **Future Is Quantum: European Union Countries Plan Ultra-Secure Communication Network.** European Commision, 13 June 2019. Available online: https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.
89. **Dargan J**. 11 CEE Countries Intent On A Quantum Future. Quantum Insider, 2 May 2021. Available online: https://thequantuminsider.com/2021/05/02/11-cee-countries-intent-on-a-quantum-future/.
90. **First Demonstration of Quantum Communication among Three States.** Ministry of Science and Education, 5 August 2021. Available online: https://mzo.gov.hr/news/first-demonstration-of-quantum-communication-among-three-states/4489.
91. **Google Launching Quantum Tech Centre in Ljubljana.** Slovenska tiskovna agencija, 30 May 2023. Available online: https://english.sta.si/3176623/google-launching-quantum-tech-centre-in-ljubljana.
92. **QT Future.** Nanocenter. Available online: https://www.nanocenter.si/qt-future/.
93. **Physics of Quantum Technologies.** Jozef Stefan Institute; Faculty of Mathematics and Physics, University of Ljubljana. Available online: http://qt.ijs.si/.
94. **SiQUID – Slovenian Quantum Coomunication Infrastructure Demonstration.** Fakulteta za matematiko in fiziko; Univerza v Ljubljani, 2023. Available online: https://www.fmf.uni-lj.si/sl/raziskave/mednarodni/siquid/.
95. **Where to Find Quantum Flagship Members.** European Union Quantum Flagship. Available online: https://qt.eu/.