European Commission

JRC TECHNICAL REPORT

Quantum as a disruptive technology in Hybrid Threats

Evaldas Bruze, L3CE

R. Andrew Paskauskas, L3CE

Edmundas Piesarskas, L3CE

Tomas Krilavicius, L3CE

Egidija Versinskiene, L3CE

Sigute Stankeviciute, L3CE

Dominykas Versinskas, L3CE

Monica Cardarilli, JRC (Ed.)

2021

Joint Research Centre

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information
Name: Georgios GIANNOPOULOS
Address: Via E. Fermi 2749, 21027, Ispra (VA), Italy
Email: georgios.giannopoulos@ec.europa.eu
Tel.: +39 0332786211

EU Science Hub
https://ec.europa.eu/jrc

JRC126379

Ispra: European Commission, 2021

Contents

Abstract

Hybrid warfare/conflict is nothing new in essence. However, technological trends suggest that the portfolio of hybrid hazards will rapidly expand. With their disruptive potential, they open up new avenues for undermining democracies.

New technologies create windows of opportunity for adversaries to launch hybrid attacks that can inflict significant damage, while the attacked party contemplates in uncertainty, trying to understand what is happening, and what is an appropriate response.

Today, innovative technologies provide a means of achieving political goals in the grey area at the interface between war and peace, for example, especially during periods of peace. At the same time, however, new technological developments may offer options to better identify, understand, defend against and counter hybrid attacks. Therefore, it is important for political, civilian, military leaders and decision makers, as well as industry and academia, to develop a comprehensive understanding of the implications of innovative technologies in a hybrid warfare/conflict context.

This paper discusses the significance of disruptive technologies and the need for viable strategies to counter hybrid threat onslaughts. Analysis of the disruptive potential of quantum computing serves as a practical case, highlighting how the hybrid community may contribute to the process of making our countries more resilient.

Acknowledgements

This research was financially supported by the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883054 (project EU-HYBNET).

The completion of this paper could not have been possible without the participation and assistance of so many people and security practitioners whose names may not all be enumerated. Their contributions are sincerely appreciated and gratefully acknowledged.
In addition, we would like to express our deep appreciation and indebtedness particularly to the following:
Mr. Tomas Tauginas for his endless support, understanding and deep professional insights during the preparation and writing phases of this report.
Mrs. Päivi Mattila for her painstaking efforts to meet deadlines.
To all relatives, friends and others who in one way or another offered their support, either morally or physically.

The authors also want to acknowledge the contribution of the two reviewers, among them *Mr. Martino TRAVAGNIN,* from the Joint Research Centre (JRC) of the European Commission, Ispra, Italy, who have provided their valuable comments and suggestions for improving the overall quality of this report.

Authors

Evaldas Bruze, L3CE
R. Andrew Paskauskas, L3CE
Edmundas Piesarskas, L3CE
Tomas Krilavicius, L3CE
Egidija Versinskiene, L3CE
Sigute Stankeviciute, L3CE
Dominykas Versinskas, L3CE

Lithuanian Cybercrime Centre of Excellence for Training, Research and Education (L3CE), Didlaukio str. 55, Vilnius LT-08329, Lithuania

Editor

Monica Cardarilli, Joint Research Centre (JRC), Via E. Fermi 2749, I-21027 Ispra (VA), Italy

1 Research Methodology

Different research methods were used while conducting research for this paper. We undertook a review of the relevant scientific literature and conducted interviews of experts. The collected data were analysed and processed using the following theoretical methods: systematic, historical and comparative analyses.

The research is based on several sources:

1. Papers found using keywords such as quantum strategy, quantum computation, quantum supremacy, quantum security, quantum race, hybrid threats, post-quantum, etc., within the following databases: Google Scholar, Crossref, Microsoft Academic, Scopus, Web of Science.
2. NATO STO (science and technology) studies.
3. Relevant projects.
4. Interviews with individual experts and practitioners.

The review of the scientific literature revealed the views of researchers in the EU and other countries, particularly in areas of forecasting and predicting technological developments and disruptive effects on security and defence domains in relation to hybrid threats. An analysis of the scientific literature also helped to explain why security and defence agencies should raise awareness to better direct, strategically align and synchronize policy development to benefit from technological advances and better prepare for future evolving threats.

Due to the rapid development of cyberspace technology, legal regulation in this dynamic field is influenced by powerful companies (Facebook, Google, Apple, IBM etc.). The paper analyses global trends and the monitoring method disclosed pertinent information that allowed for the prediction of future changes or the need for those changes. The sources employed in the monitoring process were global newspapers and various portals such as NATO international press, Gartner, Financial Times, The Economist, The Guardian, Reuters, and MIT Technology Review.

Unstructured interviews were conducted with experts having different levels of experience on a particular research topic. Due to sensitivity issues, experts had the opportunity to remain anonymous and the detailed content was not disclosed. All experts were asked different questions in accordance with their expertise. (This paper is based on non-confidential information only.)

The varied factors influencing the execution of hybrid threats in relation to quantum technologies (QT) (differing national legal regulations, strategies, political factors, the role of technological companies) presupposed that a systematic approach to the object of research was needed.

First, a method of systematic analysis was applied. Next, the method of historical research helped to determine the doctrinal basis of hybrid threats, the evolution of quantum technologies and the factors influencing their interrelation. The various sections of this paper are also arranged in thematic order, for example, from cryptographic technology to related domains, such as AI.

2 Window of Opportunity for Hybrid Threats

2.1 Hybrid Threats conceptual model

This section is dedicated to providing a short description of the Hybrid Threats. This description allows the reader to link QT (described in the following section) to the Hybrid Threats phenomena and significance of timing.

A definition and conceptual model of Hybrid Threats phenomena is elaborated in numerous sources. But the most in depth and reflective European approach is provided by the Joint Research Centre of the European Commission (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) [1]. It does not aim to provide a universal definition of Hybrid Threats, but rather provides the conceptual model enabling one to arrive at a common understanding among the various stakeholders of the concept of Hybrid Threats.

The concept of Hybrid threats, described in the document, can be summarised as follows: a hostile actor deliberately combines and synchronizes action, specifically targeting the systemic vulnerabilities in democratic societies, in ways that have roots in tactics with which authoritarian states, revisionist powers, rogue states and non-state networks that are seeking to undermine democratic state system have been trying to maintain their power, exert control and weaken opponents [1]. The concept also emphasises a malign intent behind the action, that can be characterized by the following:

- Using multiple synchronized tools (in principle, non-military) both linear and non-linear effects;
- Creating ambiguity (covert and plausible deniability) and hiding the real intent;
- Exhibiting deliberate threshold manipulation when it comes to detection and response;
- Exploiting the seams of democratic society as well as between different jurisdictions;
- Often including a distraction element, such as action in one place, and a target somewhere else [1].

The concept describes Hybrid Threats from the perspective of democratic states.

For a better understanding of the concept, it is further divided into four main pillars: Actors (and their strategic objectives); Tools applied by the actor; Domains that are targeted, and Phases (including the types of activity observed in each phase).

The basic structure/visualization of the analytical framework of the conceptual model is introduced further which captures the above-mentioned pillars and demonstrates their links in a dynamic way. At this stage relevance of QT to identified pillars is to be elaborated.

State and non-State actors are both relevant in light of quantum computing development. Most likely quantum abilities will be developed at the state level.

At the tools level, Quantum Computing (QC) may have a profound impact on cybersecurity, communication and other cyber-related areas. Some of the tools with military applications will be discussed in the article.

Domain wise, the article will discuss the very direct link of Quantum to Cyber domain and Military/Defence, but those may have significant impact to other domains as well. Quantum Computing would be exploitable in all stages of Phase pillar (Activities component).

The next section provides structured description of the Quantum Computing. Having both descriptions – Hybrid Threats and Quantum computing – will allow us to link those phenomena, being a key task of this paper.

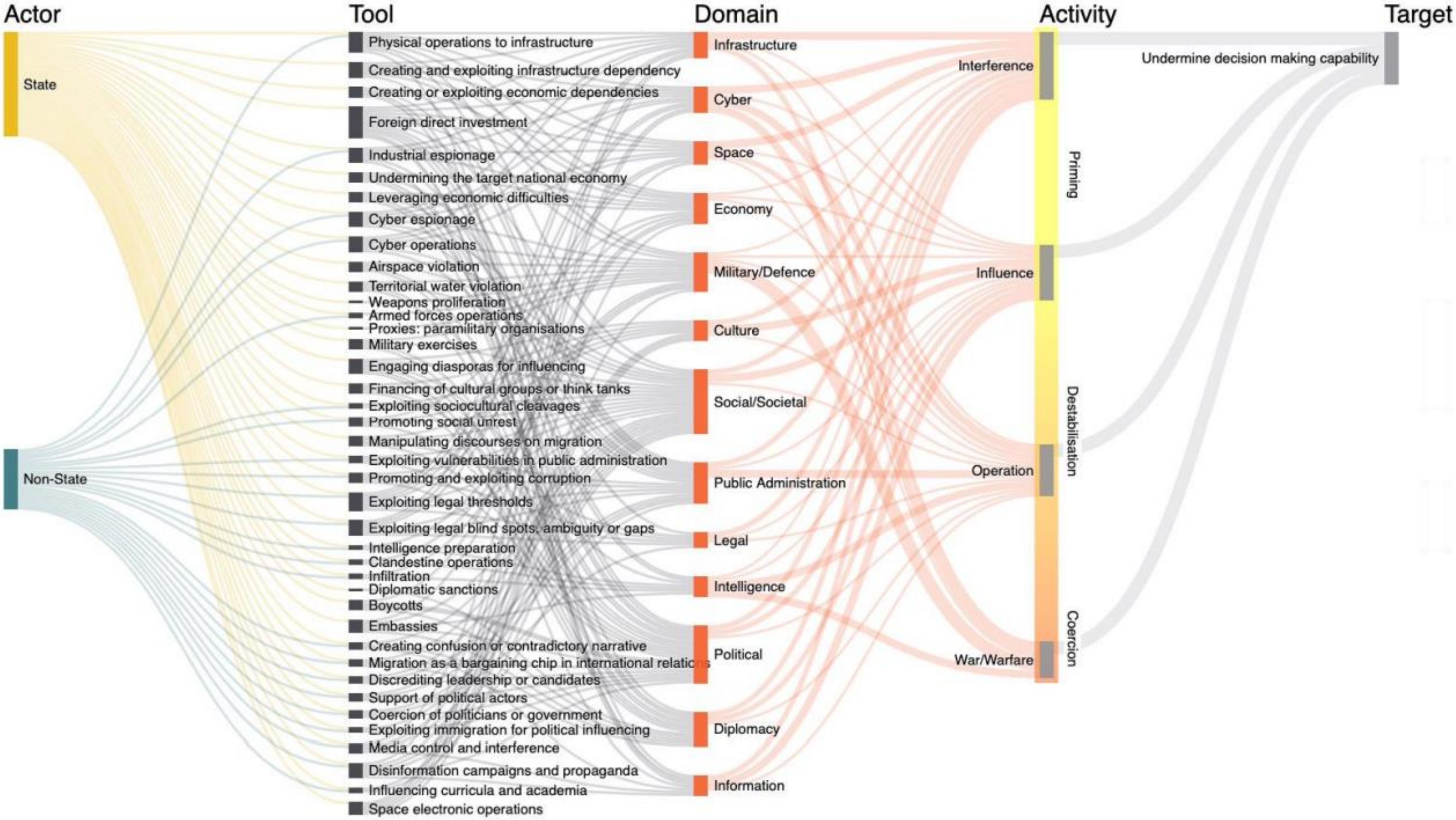
Actor
Tool
Domain
Activity
Target
State
Non-State
Physical operations to infrastructure
Creating and exploiting infrastructure dependency
Creating or exploiting economic dependencies
Foreign direct investment
Industrial espionage
Undermining the target national economy
Leveraging economic difficulties
Cyber espionage
Cyber operations
Airspace violation
Territorial water violation
Weapons proliferation
Armed forces operations
Proxies: paramilitary organisations
Military exercises
Engaging diasporas for influencing
Financing of cultural groups or think tanks
Exploiting sociocultural cleavages
Promoting social unrest
Manipulating discourses on migration
Exploiting vulnerabilities in public administration
Promoting and exploiting corruption
Exploiting legal thresholds
Exploiting legal blind spots, ambiguity or gaps
Intelligence preparation
Clandestine operations
Infiltration
Diplomatic sanctions
Boycotts
Embassies
Creating confusion or contradictory narrative
Migration as a bargaining chip in international relations
Discrediting leadership or candidates
Support of political actors
Coercion of politicians or government
Exploiting immigration for political influencing
Media control and interference
Disinformation campaigns and propaganda
Influencing curricula and academia
Space electronic operations
Infrastructure
Cyber
Space
Economy
Military/Defence
Culture
Social/Societal
Public Administration
Legal
Intelligence
Political
Diplomacy
Information
Interference
Influence
Operation
War/Warfare
Priming
Destabilisation
Coercion
Undermine decision making capability

Figure 1. Conceptual framework for Hybrid Threats (source: [1])

2.2 Timing of Hybrid Threats

It is important to emphasize, that Hybrid Threats is not a static model. Timing is of key importance for planners of hybrid attacks.
The conceptual model [1] illustrates phases of Hybrid Threats in the following figure.

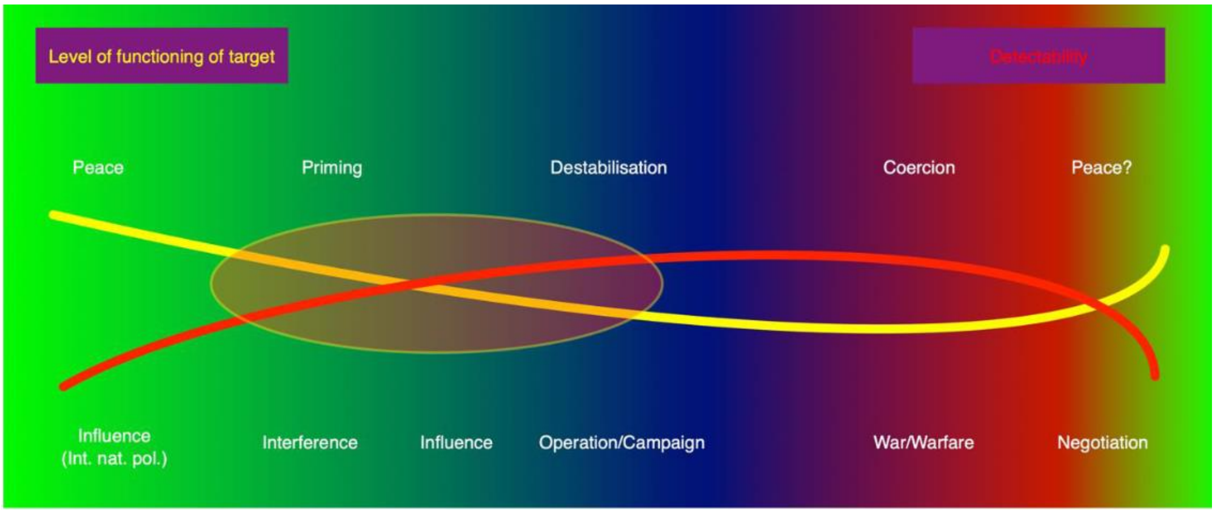

Figure 2. Phases of Hybrid Threats phenomenon (source: [1])

The step when an adversary shifts from the Priming stage to Destabilization depends on many aspects. Deadlines may be important in the adversary's plans.
But it is commonly observed that an adversary is very keen to use events beyond their own control (such as the COVID pandemic), as the moment for destabilizing, increasing influence, etc. Such leverage of natural opportunities provides a framework for deniability and an opportunity to increase the level of hostile activities while still staying below the radar. There is a smaller probability of response, as attacked governments are under the stress of management of the natural events.

Disruptive technological change may create specifically tempting opportunities for an adversary to launch an attack. Asymmetric advantages that the adversary may gain provide huge incentives to launch both targeted and opportunistic attacks. Motivations grow if they are deniable and/or the chance of a symmetric response is minimal.
It is quite usual, that any technological advantage diminishes in time, and some kind of equilibrium sets. The advantage can only be sustained with very high asymmetrical investments, which very rarely is sustainable. But that temporary advantage may provide additional motivation for adversary to use it.
Advancement in quantum technologies may become one such disruptive technological change. Analysis of the phenomenon and its possible impacts in the hybrid threats space may be instrumental in better understanding risks of the disruptive technological change and how to be prepared for them.

3 Quantum Technologies

The purpose of this article is to introduce the distinctive, disruptive characteristics of Quantum Technologies in general and focus on the potential consequences of its application as a platform for hybrid attacks.
Together with the general theory of relativity, quantum physics research has turned the established notions of nature's basic laws upside down. In this context, a new computing paradigm is emerging – Quantum Computing.

Quantum Technology

Next-generation quantum technologies exploit quantum physics and associated phenomena at the atomic and sub-atomic scale – specifically, superposition and entanglement. Superposition is an ability of the particle to exist in two or more possible states at the same time. Quantum entanglement refers to sharing the state across two or more particles such that observing one particle collapses it to one of possible state, and simultaneously collapses the state of the entangled particle into a correlated state, however far apart they are.
These effects support significant technological advancements primarily in cryptography; computation; precision navigation and timing; sensing and imaging; communications; and materials.

The increase of computing power since the invention of the microprocessor was fast, but incremental, as outlined in Moore's Law, which states that the number of transistors on a microchip doubles every two years, at the same time, the cost of it halves. This trend cannot continue indefinitely, because it is not possible to make transistors with fewer than one atom. An engineering or economic limit may be reached well before the single-atom level Quantum Computing is an alternative paradigm, in which information is represented in quantum states, and which promises a continued increase in computing power after Moore's law no longer holds. For suitable workloads the efficiency gains would be drastic.

Quantum computing will likely evolve as an accelerator of other technologies such as nano, bio, IT, and neuro, and consequently strengthen hybrid threat actors engaged in grey zone activities. We will see vastly improved capabilities in computing, communication, cryptography, navigation, and sensing that will enable hybrid threat actors to push the envelope of hybrid aggression.
Progress in quantum computing is difficult to assess as deployable systems range from nearly ready to hard-to-predict. The timeframe for an industry-ready Quantum Computer is 5–20 years, depending on usage scenarios, a wide range of architectural and technical factors, while the timeframe for deployment of adversarial countermeasures is much shorter, likely 10 years. In view of this, there is a massive rush to invest in the classical and quantum hardware and software, if not entirely in Europe, certainly in China, Russia, and the USA.

3.1 Quantum Computing Challenges Cybersecurity

One of the most visible and practical threats that QC poses in cybersecurity is the projected capability, of the Shor algorithm [2] to break asymmetric cryptographic algorithms which empower a very significant part of current internet security. Essentially all asymmetric algorithms: RSA (algorithm is standard in conventional banking systems to send encrypted information), ECC and Diffie-Hellman algorithms, are considered to be vulnerable.
Though perfectly practical quantum computers have yet to be built, and preparations for a quantum-resistant world is still underway, the threat that QC poses remains a present-day concern.

Currently harvested and stored encrypted communications and data may be decrypted years later, when QC becomes available. So, scenarios should be considered where communication and data stored by an adversary might be used in the future. And the only way to protect from these threats is do it now.
As quantum-vulnerable algorithms are so widely used, huge infrastructure vulnerabilities will have to be dealt with in preparing for the era of quantum-vulnerability. Quantum resilient cryptographical methods are being developed and coming to market, and this will imply the necessity for the application of relevant upgrades. But full infrastructure upgrades will require extensive time and coordinated effort. Moreover, since there is no consensus on what the most promising technologies are, the best investment strategy is uncertain. Most devices used on a daily basis are not designed to allow such upgrades and will require replacement. This includes all peripheral devices, digital locks, routers, simple digital keys, etc.

Therefore, the highest risk for Post Quantum security is related to public and private infrastructures, that – if attacked, can cause significant damage to societal trust, privacy, and the financial domain.
Further development of quantum key distribution (QKD) and post-quantum encryption options will provide superior encryption capabilities. In general, as far as standards and cybersecurity are concerned, most of the research and development efforts on the part of the key players are focused on the level of algorithms; whereas the leading-edge thinking suggests that overall security of cyber systems, whether classical or quantum, needs to be considered right from the beginning of the design and development phases, taking into account the overall architecture of the system of systems, as it was, so that the ultimate implementations of future technologies are cyber-secure ready [3].
In any case, a sample of some of the important work at the algorithmic level that has been achieved thus far includes: NIST's Post-Quantum Cryptography project which aims to provide a new standard that will specify one or more quantum-resistant algorithms each for digital signatures, public-key encryption, and the generation of cryptographic keys, augmenting previous efforts in these areas. Significantly, it plans to release the initial standard for quantum-resistant cryptography in 2022 [4].

The NIST paper entitled, 'Getting Ready for Post-Quantum Cryptography' explores the challenges associated with adoption and use of post-quantum cryptographic algorithms [5], once the standardization process is completed. It also identifies the planning requirements necessary for migration to post-quantum cryptography and concludes with recommended next steps for successful migration.
Aforementioned efforts aim to develop state-of-the-art quantum safe algorithms, like Quantum Key Distribution, but sceptical views do exist. Weighing costs and benefits, French *Agence Nationale de la Sécurité des Systèmes d'Information* states "The constraints inherent in QKD make it impossible to envisage a massive deployment that would offer high security guarantees in practice. The future of secure communications can be assured over time without the need to use the QKD. Thus, while this technology may be called upon to play a role in niche applications, it does not constitute the natural path of evolution of secure communications. The security guarantees provided in principle by the QKD come at the cost of heavy use constraints that reduce the scope of the services offered and compromise the level of security that can be achieved in practice" [6].

German BSI Bundesamt für Sicherheit in der Informationstechnik in statement of March & August 2020 [7] [8], USAF Scientific Advisory Board concluded [4], UK National Cyber Security Centre statement, 24/03/2020 [9], USA National Security Agency statement, 26/10/2020 [10] all indicate complexity of required infrastructure, limited usage scenarios and lack of market readiness among other factors, to be cautious about QKD.
Symmetric encryption algorithms are considered to be quantum resistant and available now. Naturally, they do pose other set of security threats, but we are much more accustomed to those. Thus, some authors argue, that at least in a number of scenarios, conscious planning of use of cryptography protocols can reduce quantum vulnerabilities now, just by leveraging currently existing and widely available symmetric algorithms.
When put in the perspective, it is important to note, that we are living in cyber-insecure world. Communications currently are vulnerable to both penetrable loopholes in technology and social engineering exploits. Critical infrastructures are consistently and successfully targeted, fake news has already had a huge impact on the societal landscape.

Concluding this chapter we should recognize, that considering billions of quantum vulnerable devices functioning worldwide, reaching the quantum secure infrastructure milestone seems very unlikely. Thus, functional QC promises to introduce large scale disruption. A significant part of currently used encryption which secures communications and infrastructures might become instantly penetrable. This predicament is qualitatively different from the usually encountered vulnerabilities (like the discovery of significant vulnerabilities in operating systems). First, the scale of it promises to be immense. Second, it is very probable, that there will be no "quick fix" solution, no patch that would eliminate the vulnerability at the same massive scale.

3.2 Quantum Safe Communications

While previous chapter discusses how quantum computing enables breaking encrypted communication and may render current and future communication channels insecure, in this chapter we discuss development of the ultra-secure communication channels leveraging quantum physics.

Three underlying quantum concepts give reason to believe of “unbreakable” qualities of quantum safe communications. One, the quantum no-cloning theorem states, that an unknown quantum state cannot be cloned. Two, a quantum system can be prepared in such a way that any observation made without a suitable a priori knowledge about its possible states will unavoidably and irreversibly perturb it. A quantum message that is intercepted and read by an eavesdropper will become garbled and useless to the recipient of the message. Three, the effects produced by measuring a quantum property are irreversible, which means the eavesdropper cannot put a quantum message back into its original state [5].

Quantum communications capability for ultra-security channels is an important research area, driven primarily by public sector/defence interests. Use of near-term QT may enable the detection of an eavesdropper on a communication channel. Further development of quantum key distribution (QKD) and post-quantum encryption options would enable quantum-safe encryption capabilities.

3.3 Quantum enabled AI

Significantly, up to now, AI-related hybrid threats [11] [12] [13] [14, 15, 16, 17, 18, 19] and the impact of Quantum Computing have been subjected to thorough analyses. Combinations of AI and QC are often considered as means to achieve supremacy on the battlefield, whether physical, virtual or information related [20] [21]. T. Gabor et al. go further by taking into account the synergetic connection between quantum computing and artificial intelligence. The authors relate quantum artificial intelligence to a formal model for machine learning processes, and deduce four major challenges for the future of quantum artificial intelligence: (i) Replace iterative training with faster quantum algorithms, (ii) distil the experience of larger amounts of data into the training process, (iii) allow quantum and classical components to be easily combined and exchanged, and (iv) build tools to thoroughly analyse whether observed benefits really stem from quantum properties of the algorithm [21] . Still, others predict a slowdown of AI progress, increases in the costs of AI research (which has represented the status quo up to now) and development of new AI algorithms demanding fewer resources. The AI and QC combination is discussed in a number of papers, e.g. quantum algorithms for supervised and unsupervised machine learning [22]; and M. Schuld et al. take advantage of the fact that for certain tasks, quantum computing outperforms classical computing; hence, a growing number of contributions try to use this advantage in order to improve or extend classical machine learning algorithms by methods of quantum information theory [23].

AI-related hybrid threats can be made more effective by combining with QC in the following ways:

- Quantum computing potentially allows for faster training of AI algorithms; and more advanced AI models can lead to faster analysis of big data sets using particular classes of algorithms. If an adversary, for example, has access to such technologies, several attack vectors are possible such as:
  information attacks by employing better bots to generate specific content, e.g., fake news, deep
fakes (38), production of high-quality targeted complex fakes (videos, audio, text).
- More advanced, more effective phishing tools using text and image generation.
- Simulation of different attack scenarios, e.g., using reinforcement learning, would allow adversaries to prepare attacks more effectively.
- Coordination and execution of complex (dis)information campaigns in the information space, potentially combined with cyber and kinetic attacks.

3.4 Quantum Technology Trends in Defence and Security Domains

The following provides a summary of key EDT areas critical for the evolution of a sustainable defence sector. Again, our intention is not to discuss in depth the technical side of developments, but rather illuminate the possible impact of such developments. In short, the promise of quantum technologies in defence and security domains is impressive:

- **Quantum enabled Sensing:** Progress with quantum sensing is currently quite significant. In the future, advanced QT will evolve with extended capability for the detection of gravitational and magnetic anomalies that will enable georeferenced mapping with precision that is significantly higher than current capability levels.
- **Positioning, Navigation and Timing (PNT):** There are two fundamentally different approaches to PNT: one involving the transmission and receipt of external signals, such as GNSS/Galileo, and the others relying on the self-contained sensing of motion, such as provided by inertial systems. Investment in QT will enhance resilience to jamming, spoofing and GNSS/Galileo denied environmental vulnerabilities. Quantum technologies are expected to support the combination of ultra-precise time measurements with ultra-precise acceleration and angular rotation measurements (each of which uses a different quantum technology), to provide ultra-precise inertial navigation (and timing), which will be needed as GNSS/Galileo and other signal dependent means become unavailable due to countermeasures. With continuous investments in the mid and long term, the systems are expected to decrease in size, weight, power, and cost and ultimately provide higher quality navigation performance capabilities than are currently offered by GNSS/Galileo, with greatly reduced reliance on external references.
- **Quantum Remote Sensing (QRS)**: Quantum radar, a form of QRS, has the potential to obsolesce stealth technologies, provide more accurate target identification, and allow detection of covert surveillance operations. There are two known approaches to Quantum-enhanced remote sensing: either by using quantum interferometry or by using quantum illumination. These sensors will enable much more accurate and sensitive measurement and the use of much lower power, for applications such as the detection and tracking of small, stealth targets.
- **Magnetic and Gravity Sensing**: Precise measurement of the magnetic field is used by maritime patrol aircraft for the localization of submarines, using MAD (magnetic anomaly detection) sensors. Current sensors are not suitable for use on small UAVs, due to size-weight-power constraints, but emerging quantum technologies may provide a solution. There are also special applications of gravity sensing that could be enabled by quantum technology, for specialized mobile surveillance applications such as underground structure detection (tunnels, bunkers) from an airborne platform. Modelling and simulation (M&S) for defence problems may be applied to special and limited BDAA problems. Considering that these methods are a basis for all machine learning, matching, filtering, and profiling algorithms, quantum enablement, if applied in big data analytics and OSINT fields, can revolutionize efficiency and accuracy, at the same time creating near to real time micro-targeting.
- **Materials:** Quantum simulations which accurately model quantum many-body systems, offer the promise of predicting the behaviour of new materials. This capability will allow the explicit design and creation of new materials with specific desirable physical properties such as ultra-hard armour, superconductivity, high-temperature tolerance, etc.

How do these trends relate to hybrid domain? There is a line of thought, that if an adversary succeeds in acquiring significant advantage in these fields, it may significantly decrease military superiority of democratic bloc of countries. It is very unlikely that such a change would be significant enough to initiate military conflict. But it may provide motivation for an adversary to take riskier and more aggressive actions in hybrid space.

4 Developing a strategic response to Quantum-related challenges

As discussed previously, advancement in quantum computing and other quantum-related areas may prove to be highly disruptive. Most countries which are advanced in QC, first to build quantum secure infrastructures and develop QC capacities enabling breaking of existing cryptography, may find themselves in a highly superior position. Authoritarian regimes with such capabilities may find motivation to use the opportunity. So, the quantum race is not only about who "wins" it, but about who "loses" it and for how long this gap will remain.

4.1 The Quantum Race

Several nations are currently investing heavily in quantum research to derive economic and military benefits.

China's attempt to become a quantum powerhouse is strategically driven by three fundamental factors [24]: (i) information security – a need to protect communications from foreign adversary spying, sabotage, and influence; (ii) economic competition – belief that, due to the disruptive nature of the technology, current US advantage may not be transferable to the quantum field. So, given its manufacturing and human capital potential, China may be able to turn a market advantage into sustained global technological leadership in the quantum field; (iii) military competition – advances in quantum technologies may disrupt current military paradigms, where the US presently holds a distinct advantage.

China has already registered more patents than the USA in the fields of quantum communication and cryptography. Chinese researchers are very successful in basic research and in the development of quantum technologies. These include quantum cryptography, communications, and quantum computing, as well as quantum radar, sensor technology, imaging, metrology, and navigation. China has managed to cultivate close working relationships between government research institutes, universities, and companies like China Shipbuilding Industry Corporation (CSIC) and China Electronics Technology Group (CETC).

China launched the world's first quantum satellite which successfully completed links with ground stations and teleportation optical links. This progress, as well as several quantum communication networks at various levels, is built on the ground of steady strategic investment and sustained attention towards quantum technology development. Overview of the Economist article [25] shows a clear tendency, that by 2015 China was a strong leader in patents on Quantum cryptography. While quantum key distribution was led by US in the first decade of the century, China became clear leader in the second decade.

Russia is also investing in quantum technologies. It has created a dedicated Russian quantum centre but is lagging China and the USA. However, President Vladimir Putin is said to have increased the budget for research and development (R&D) by around USD 3 billion, some of which can certainly be channelled towards the quantum technologies sector.

Since 2016, the US government has sponsored over USD 200 million in quantum research, and in 2018 the Department of Energy and the National Science Foundation committed another USD 250 million to support quantum sensing, computing, and communications through two to five-year grant awards. The US Army Research Office funds extensive research in the field of quantum informatics. The US Air Force considers quantum technology to be a game changer in the context of information and space warfare.

The private sector, sometimes facilitated by public funding, should not be underestimated. Global companies like Google, IBM, Intel, and Microsoft have been conducting quantum research for almost a decade. Together with the Canadian company DWave Systems, they lead the West in the development of quantum computers. Google, IBM and Intel make substantial progress. But progress is not limited to big established names, vibrant start-up scene is undoubtfully contributing to the development of technologies.

The European Union has a good starting position for the development of quantum technologies. Europe is the world leader in quantum physics – with around 50 per cent of all scientific publications and almost 40 per cent of all researchers in this field. At the same time, EU established around 10 quantum focused labs. However, some of these are running on US and China infrastructures, which creates serious vulnerabilities for the autonomy of EU's innovation ecosystem and competitiveness in the fields related to quantum. In October 2018, the European Commission launched the Quantum Technology Flagship initiative, which is designed to support over 5,000 of Europe's leading researchers in the field of quantum technology over the next ten years. The programme aims to develop a "quantum network" in Europe, in which quantum computers, simulators and sensors are interconnected via quantum communication networks. This is intended to kickstart a competitive European quantum industry, with research results becoming available as commercial applications.

4.2 Quantum Technology policies in the EU

In 2016 the European Commission (EC) published the Commission Staff Working Document on Quantum Technologies and the European Cloud Initiative – Building a competitive data and knowledge economy in Europe [26]. The Working Document summarizes the application of quantum technologies, potential markets and proposes preliminary pathways for EU regarding quantum technologies. In the section on 'Future and Emerging Products and Markets', the Working Document identifies devices and systems that exploit fundamental quantum effects and groups them along the following lines:

- Quantum Sensing, Metrology, and Imaging Systems;
- Quantum Communication;
- Quantum Computation and Simulation.

Furthermore, the EC had set up a financial support plan to foster the development of quantum computing in the EU. According to the Working Document "after almost 20 years of investment of around ~550M€ in EU funding, Europe has a well acknowledged world-class scientific and technical expertise in Quantum Technologies". Thus, in 2016, it was well-positioned to take advantage of the quantum technology science-base which had been built up under the Framework Programmes, up to Horizon 2020, Future and Emerging Technologies (FET), European Research Council (ERC) and Marie Skłodowska-Curie Actions (MSCA) [26]. Furthermore, pre-commercial procurement, public procurement of innovation and projects funded by the European Fund for Strategic Investment (EFSI) were identified as useful instruments to drive quantum technology forward [26].
To achieve global European industrial leadership in Quantum Technologies, the EU must embark upon an "ambitious coordinated strategy to support joint science, engineering and application work, including IPR, standardisation, market development, training and public procurement" [26].

The EC also initiated dialogues with European industry and other stakeholders to foster interest and investment in quantum [26]. As a result, a "Quantum Manifesto" was signed by numerous EU universities and research organizations, industry, public bodies, and funding agencies [27]. It expressed the need for an all-inclusive strategy for Europe to sustain a position at the forefront of the second Quantum Revolution. Short- and long-term goals regarding quantum technologies as well as a need for a €1 billion flagship scale initiative in Quantum Technology were identified [28].
The Quantum Technologies Flagship embodies the European Commission's principal objective in relation to its strategic direction for quantum computing over the next decade: to establish a world-leading European quantum technology ecosystem by 2030 [29] [30].
The Flagship's Strategic Advisory Board has compiled a series of key performance indicators (KPIs) and recommendations that include monitoring and evaluating the development of quantum technologies in Europe. These KPIs consist of the following technological and topical pillars: Ecosystem, Quantum Communication, Quantum Computing, Simulation, Quantum Sensing and Metrology, as well as Education, Training, Diversity and Equity [30].
The Flagship will run for ten years, with an expected budget of €1 billion. In its ramp-up phase (October 2018 - September 2021), the New Strategic Research Agenda on Quantum Technologies [31] includes provision of €132 million for an array of 20 quantum-related projects which include:

- Implementation of leading-edge Quantum Communications networks using single photons, which will be impossible to intercept by adversaries without detection;
- Development of quantum-enhanced physical layer security services combined with modern cryptographic techniques;
- Revolutionizing the Quantum Ecosystem from fabrication to application;
- Quantum Sensing and Metrology projects that will focus on sophisticated medical and imaging applications;

- Quantum Computing initiatives to realise a scalable European quantum computer based on the manipulation of single-charged atoms;
- Various Quantum Simulation platforms that will address scientific and engineering applications, and a wide range of Basic Science related projects.

A second important EU policy concerns building a quantum communications infrastructure (QCI). All EU Member States have signed the Euro QCI declaration of cooperation [32] and have agreed to cooperate in exploring capabilities of quantum communication infrastructure across the EU within 10 years. The developed infrastructure has to be created in a way that would enable information to be transmitted and stored ultra-securely, and that would link communication assets over the whole of EU [33]. The long-term plan involves EuroQCI becoming the cornerstone of a quantum internet in Europe [34].

For our purposes, the KPIs that stand out revolve around connecting all countries in Europe to a quantum communication network that is safe and functional and that combines "Post Quantum Cryptography and QKD, for IoT, 5G, SDN, and critical infrastructure, as well as quantum internet applications exploiting long-range entanglement between remote quantum processors, clocks and sensors" [30].

5 Discussion on What the Hybrid Threats Community may add on Quantum Technologies

We have discussed above in some detail, how quantum technology development can bring disruptive technological changes.

As discussed in Sub-section 4.1 The Quantum Race, it seems major powers do recognize the potential of disruptive change and invest heavily in building capacities and technologies for quantum computing. Threats that QC poses to cybersecurity and secure communications are understood, and new encryption methods are being developed.

What does it leave Hybrid Threat community? Can it find a voice to deliver a message that would add substance beyond "watch out, there is a threat!"? We believe it does.

The following disruptive effects in relation to hybrid threats have been identified by interviewed experts, which in most aspects relate to the direct impact of quantum technology developments:

- loss of technological leadership;
- new and changed positions in technological supremacy;
- disruption of the world order;
- new economical dependencies;
- development of new areas of stealthy influence and manipulation;
- new ways and areas for civil disruption having massive cascading effects on trust and stability;
- loss of cryptographic infrastructure;
- loss of signals intelligence (SIGINT);
- a silent takeover of civilian and military critical infrastructure;
- new types of crimes and criminal instruments;
- loss of strategic autonomy.

The hybrid threats field is related to the wider impact on democratic societies and their fabric of trust. The discussed vulnerabilities may have not only direct risks but may also accumulate cascading effects of significant scale. Complex and interrelated links transpose quantum technologies via tools – impacts – activities to possible target. So, analysis from the quantum technology point of view would not cover all the complexity of phenomena.

Hybrid threats point of view can be instrumental. Importantly, a hybrid threats approach should not aim to contribute to technical understanding of the phenomena, as we have significant research and practitioners' communities specializing in the respective fields. Hybrid threats communities rely on their deep knowledge and on their day-to-day work mitigating the risks.

Hybrid threats communities can contribute value in illuminating higher level, longer perspective, interconnected risks, and their scenarios.

Thus, from the Hybrid threats perspective, we suggest classifying hybrid threats into several main categories in terms of risks that:

- The application of quantum sensing, and positioning/navigation/timing technologies may significantly diminish military superiority of NATO/democratic countries, and this may motivate adversaries to launch more aggressive hybrid attacks.
- For a significant period, critical infrastructure will become massively vulnerable to attacks by adversaries in possession of QC tools.
- Secure communications channels will become accessible to adversaries in possession of QC tools.
- Through employment of QC increased computing capabilities, a greater number of sophisticated manipulations via microtargeting, and deep fake production, will be enabled.
- An adversary will be able to create the appearance of possessing powerful quantum tools and would be able to exert influence without actual application of quantum technologies.

There may be significant benefits to be attained by an adversarial country, which would provide the greatest opportunities for increased attacks based on innovative technologies, even though these could only be sustained for a brief period.

In the future, we should expect that a post-quantum equilibrium will be reached, as the quantum secure technologies are developed and deployed. Thus, the motivation to leverage this opportunity for the adversary in such a limited time span could be very tempting.

6 Recommendations

It is of utmost importance to ensure that democracies do invest in leading edge quantum computing technologies to retain a strategic advantage. Even if adversaries achieve temporary advantage, a state of preparedness must warrant that the quantum-vulnerability period is at a minimum by:

- investing in quantum technologies with the aim of achieving and maintaining quantum leadership;
- deploying quantum-secure communication infrastructures EU wide;
- developing guidelines for quantum-upgradable infrastructures and applying these accordingly;
- ensuring infrastructures are ready for upgrades when quantum-secure technologies become available.

Equally important, the hybrid threats domain may not be overlooked. While the hybrid threats community does not participate directly in quantum research and/or development, its involvement in understanding the capabilities of the associated technologies, as well as their use and potential impact, is important:

- increasing investments in the hybrid threats domain to ensure that methods and technologies for increasing resilience of the population are adequately developed.
- establish permanent links between the hybrid threats community and the quantum computing community (EU-HYBNET project[1] may be instrumental here);
- invest in enhancing knowledge of the hybrid community in the intricacies of quantum computing;
- demand from hybrid threats community to develop risk scenarios and response scenarios to induced disruptions, based on quantum technologies.

The hybrid threat community should engage in "soul searching" for formulating how best it can direct its efforts for recognition and preparation for emerging threats:

- **Firstly**, given the growing recognition among policymakers and practitioners, that hybrid threats are real threats which make tangible and lasting damage to societies, find ways to recognize them and develop capacities to build robust responses. So, the role of hybrid threat community is to facilitate understanding of policymakers how technical developments may eventually pave the way for attacks of high impact. So, the direct risks would be mitigated.
- **Secondly**, define specific aspects of vulnerabilities which may have extremely high impact to undermine democracies. From the technical subject matter these aspects may not necessarily be so visible. Scenarios of pure "influence" attacks should be explored, e.g., discussing the impact of the credible evidence that adversary does possess QC capability (though it may not).
- **Thirdly,** develop contingency and resilience improvement plans for the events when major disruptive events will occur. Scenario analysis, development and training, overall have a potential to augment capabilities of awareness and response. For this, realistic scenarios must be developed, based on technically probable developments, capabilities tested, and lessons learned.

[1] https://euhybnet.eu/

Bibliography

[1] H. S. M. T. G. Giannopoulos, “The landscape of Hybrid Threats: A conceptual model,” 5 February 2021. [Online]. Available: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

[2] P. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc*, 1994.

[3] O. Zendra and B. Coppens, “Cybersecurity Must Come to IT Systems Now,” 2021. [Online]. Available: https://zenodo.org/record/4719394#.YW6PFxxRXb0.

[4] "Scientificadvisoryboard," 10 10 2021. [Online]. Available: https://www.scientificadvisoryboard.af.mil/Portals/73/Documents/Abstract/Abstract%202015/Final%20UQS%20Abstract%20(Approved%20for%20Public%20Release).pdf?ver=w3TGFs59Sipu5fbKulUM7g%3D%3D.

[5] B. Auburn, “Quantum Encryption–A Means to Perfect Security. SANS White Paper.,” [Online]. Available: https://www.sans.org/white-papers/1477/ . [Accessed 10 10 2021].

[6] [Online]. Available: https://www.ssi.gouv.fr/agence/publication/lavenir-des-communications-securisees-passe-t-il-par-la-distribution-quantique-de-cles/.

[7] [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html;jsessionid=BF1370FFEC09BFE2771B2C5A7A7C207C.inte.

[8] [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Quantenkryptografie/quantenkryptografie.html.

[9] [Online]. Available: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

[10] [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[11] Thorisson, H., Baiardi, F., Angeler, D. G., Taveter, K., Vasheasta, A., Rowe, P. D., ... & Linkov, I. Resilience of critical infrastructure systems to hybrid threats with information disruption. Resilience and Hybrid Threats: Security and Integrit, “Resilience of critical infrastructure systems to hybrid threats with information disruption. Resilience and Hybrid Threats: Security and Integrity for the Digital World,” 2020.

[12] Thiele, R. D., & Schmid, J., “Hybrid Warfare–Orchestrating the Technology Revolution,” 2020.

[13] N. Masuhr, “AI in Military Enabling Applications. CSS Analyses in Security Policy, 251,” 2019.

[14] A. Antinori, “Terrorism and DeepFake: From hybrid warfare to post-truth warfare in a hybrid world. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics (p. 23),” 2019, October.

[15] A. Antinori, "Terrorism and DeepFake: From hybrid warfare to post-truth warfare in a hybrid world. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics (p. 23).," 2019, October.

[16] R. Kumar, "Potential impact of Artificial Intelligence on future strategies.," [Online]. Available: https://www.researchgate.net/publication/350022050_Potential_impact_of_Artificial_Intelligence_on_future_strategies. [Accessed 10 10 2021].

[17] R. Thiele, ""Hybrid Warfare - Future & Technologies" (HYFUTEC). Inspiration," vol. Paper No. 2, May14, 2019.

[18] B. Theile, ""Hybrid Warfare in the 21st Century. Information and Communications Technology as Key Enabler"," May 22, 2019.

[19] J. Schmid, ""Hybrid Warfare – a very short introduction"," May 2019.

[20] S. Ali, "Coming to a Battlefield near You: Quantum Computing, Artificial Intelligence, & Machine Learning's Impact on Proportionality.," 2020.

[21] Gabor, T., Sünkel, L., Ritz, F., Phan, T., Belzner, L., Roch, C., ... & Linnhoff-Popien, C., "The Holy Grail of Quantum Artificial Intelligence: Major Challenges in Accelerating the Machine Learning Pipeline.," 2020, June.

[22] Tadashi Kadowaki and Hidetoshi Nishimori., "Quantum annealing in the transverse Ising model.," Vols. Physical Review E 58, 5 (1998), 5355., 1998.

[23] C. C. McGeoch., "Adiabatic quantum computation and quantum annealing: Theory and practice.," Vols. Synthesis Lectures on Quantum Computing 5, 2(2014), 1–93., 2014.

[24] J. Costello, 16 March 2017. [Online]. Available: https://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony_Final2.pdf.

[25] M. Travagnin, "Patent Analysis of Selected Quantum Technologies," no. EUR 29614 , 2019.

[26] [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/commission-staff-working-document-quantum-technologies. [Accessed 9 2021].

[27] [Online]. Available: http://qurope.eu/manifesto/endorsers?order=organization_type&sort=asc. [Accessed 20 10 2021].

[28] [Online]. Available: http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf. [Accessed 20 10 2021].

[29] "Shaping Europe's digital future," [Online]. Available: https://digital-strategy.ec.europa.eu/en.

[30] [Online]. Available: https://ec.europa.eu/digital-single-market/en/blogposts/quantum-technologies-flagship-story-so-far-and-quantum-future-ahead . [Accessed 20 10 2021].

[31] [Online]. Available: https://ec.europa.eu/digital-single-market/en/eu-funded-projects-quantum-technology. [Accessed 21 10 2021].

[32] [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/estonia-latest-country-sign-euroqci-initiative. [Accessed 21 10 2021].

[33] [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network. [Accessed 21 10 2021].

[34] [Online]. Available: https://www.airbus.com/newsroom/press-releases/en/2021/05/a-consortium-of-european-digital-players-to-design-the-future-eu-quantum-internet.html. [Accessed 21 10 2021].

[35] The Economist, "Here, There and Everywhere," 2017. [Online]. Available: https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own.

[36] ""Quantum computing and Defence".," The Military Balance, 2019.

List of Abbreviations

5G	The fifth-generation technology standard for broadband cellular networks
AI	Artificial Intelligence
BDAA	Big Data and Advanced Analytics
CETC	China Electronics Technology Group
CSIC	China Shipbuilding Industry Corporation
EC	European Commission
EDT	Emerging Disruptive Technologies
ETSI	European Telecommunications Standards Institute
EU MS	European Union Member State
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPU	Graphics Processing Unit
HiPEAC	European Network on High-performance Embedded Architecture and Compilation
HPC	High Performance Computing
ICT	Information and Communications Technology
IMINT	Imagery intelligence
IoT	The Internet of Things
IPR	Intellectual Property Rights
JRC	Joint Research Centre
KPI	Key Performance Indicator
L3CE	Lithuanian Cybercrime Center of Excellence for Training, Research and Education
M&S	Modelling and Simulation
MAD	Magnetic Anomaly Detection
MIT	Massachusetts Technology Institute
NATO	The North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OSINT	Open Sources Intelligence
PNT	Positioning, Navigation and Timing
PQC	Post-Quantum Cryptography
PQS	Post Quantum Security
QAQA	Quantum Approximate Optimization Algorithm
QC	Quantum Computing, Quantum Computer
QCI	Quantum Communication Infrastructure
QKD	Quantum Key Distribution
QRL	Quantum Resistant Ledger
QRS	Quantum remote sensing
QT	Quantum technologies
QUBO	Quadratic Unconstrained Binary Optimization

R&D	Research and Development
SDN	Software-defined networking
SIGINT	Signals Intelligence
STO	Science and Technology Organization
SVM	Support Vector Machines
TPU	Tensor Processing Unit
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
XMSS	Extended Merkle Signature Scheme

List of Figures

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office
of the European Union