COI STRATEGY & DEFENCE

Hybrid CoE Working Paper 7

MARCH 2020

Quantum sciences – A disruptive innovation in hybrid warfare

RALPH THIELE

Hybrid CoE

Hybrid CoE Working Paper 7

Quantum sciences – A disruptive innovation in hybrid warfare

RALPH THIELE

Hybrid CoE Working Papers are medium-length papers covering work in progress. The aim of these publications is to share ideas and thoughts, as well as to present an analysis of events that are important from the point of view of hybrid threats. Some papers issue recommendations. They cover a wide range of important topics relating to our constantly evolving security environment. Working papers are not peer reviewed.

COI Strategy & Defence is focusing on hybrid warfare, related strategies and resulting implications for security policy, military and defence. It aims at discovering the essence and nature of hybrid warfare as well as the logic and pattern of hybrid strategies in order to develop an analytical framework for the assessment of current and future hybrid warfare situations and their practical implication. COI S&D follows an interdisciplinary academic based approach, hereby combining empirical evidence with the theory of war and strategy. Overarching objective is to contribute to the education of common and comprehensive judgment of Participants, EU and NATO as a precondition for joint and comprehensive action in defense and response.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-32-8
ISSN 2670-160X

March 2020

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

Preface

> *"It is imperative to keep an eye on new technologies and their potential for future development and disruption, and to analyse these developments with regard to their relevance in a hybrid warfare context. Their relationships must be understood before their implications become manifest in the context of hybrid warfare. In this regard, the technological revolution requires orchestration. This should not be left primarily to potential hybrid challengers."*[1]

Hybrid warfare/conflict is nothing new in essence. However, technological trends suggest that the portfolio of hybrid hazards will rapidly expand.[2] With their disruptive potential, they open up new avenues for violence, as well as for the use of force in a hybrid warfare/conflict environment.[3] New technologies have a catalytic effect on hybrid methods and tools. They improve the starting conditions for hybrid action, expand the arsenal of hybrid players and thus help to increase the reach of their activities as well as their prospects of success. Today, new technologies provide a way to achieve political goals in the grey area of various interfaces, such as between war and 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 and military leaders and decision-makers, as well as industry and academia, to develop a comprehensive understanding of the implications of new technologies in a hybrid warfare/conflict context.

With this in mind, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and its Community of Interest for Strategy and Defence (COI S&D) have initiated the **Hybrid Warfare: Future & Technologies (HYFUTEC)** project, aimed at assessing and enhancing understanding of the disruptive potential of new technologies in the context of hybrid warfare/conflict. Within its broad future & technology horizon scanning, the project has identified 19 technological trends with urgent and profound implications in the context of hybrid scenarios.[4]

HYFUTEC Technology Papers are designed to provide insights into selected technological trends and to improve understanding of their implications for hybrid warfare/conflict. In this vein, the papers intend to raise awareness, inform debate and contribute to the education of judgment within participating states, the EU and NATO in order to identify ways to deal with resulting threats and challenges effectively. This **HYFUTEC Technology Paper No. 2** concentrates on **quantum sciences** as a game-changing paradigm and **disruptive innovation in hybrid warfare**.

Johann Schmid
Director, Community of Interest for Strategy and Defence

Community of Interest Strategy & Defence (COI S&D)
HYFUTEC Hybrid Warfare: Future & Technologies

1 Johann Schmid and Ralph Thiele, "Hybrid Warfare – Orchestrating the Technology Revolution". In Robert Ondrejcsak & Tyler H. Lippert (Eds.), *STRATPOL. NATO at 70: Outline of the Alliance today and tomorrow*. Special Edition of Panorama of Global Security Environment 2019, Bratislava December 2019, 211–225, https://www.stratpol.sk/wp-content/uploads/2019/12/panorama_2019_ebook.pdf.
2 Ibid.
3 For a conceptual understanding of hybrid warfare, see Schmid, J. COI S&D Conception Paper: Hybrid warfare – a very short introduction (Helsinki, May 2019), ISBN: 978-952-7282-20-5.
4 See Thiele, R. HYFUTEC Inspiration Paper No. 2 (updated): Hybrid Warfare – Future & Technologies Horizon Scan & Assessment (Sept 2019).

A new computing paradigm

While most institutions, organizations and companies are still struggling with digitization, **a new computing paradigm is emerging**.[5] Together with the general theory of relativity, quantum physics research has turned the established notions of nature's basic laws upside down.

Quantum sciences deal with emerging technologies, harnessing the properties of quantum physics to enable new capabilities. These technologies will enable the performance of electronics to increase beyond Moore's Law, which already states that we can expect the speed and capability of our computers to increase every couple of years, and we will pay less for them.[6] On the one hand, quantum sciences create qualitatively new capabilities. On the other hand, for example by using quantum computers, the functionalities of already existing conventional technologies can be significantly improved in terms of sensitivity, accuracy, speed or user-friendliness.[7] Quantum will likely evolve as an accelerator of other technologies such as nano, bio, IT, and neuro, and consequently strengthen hybrid actors significantly in their grey zone activities. In particular, we will see vastly improved *computing*, *communication*, *cryptography*, *navigation*, and *sensing* capabilities that will enable hybrid actors to push the envelope of hybrid aggression.[8]

The progress is hardly calculable as deployable systems range from nearly ready to hard-to-predict. The timeframe for **usable QC** is **5–20 years,** depending on applications. The timeframe for **deployment of countermeasures** is much shorter, namely **up to 10 years**. In view of this, there is a massive rush to invest in the respective hardware and software for these multiple technologies, namely in China, Russia and the USA.

> *Quantum technology is an emerging field of physics and engineering; it uses the properties of quantum effects – the interactions of molecules, atoms, and even smaller particles, known as quantum objects – to create practical applications in many different fields.*

Quantum sciences will enable powerful networks of sensors and shooters to rapidly accelerate the process of detecting, evaluating, targeting, and delivering effects in both the virtual and the physical domain. They will enable hybrid actors to engage in stealthy operations, such as clandestine operations to influence, coerce, sabotage or communicate in the electromagnetic spectrum. At the same time, they may enable aggressors to unveil the stealth technologies of NATO and the EU, to bypass network security in real time and take over critical infrastructures.

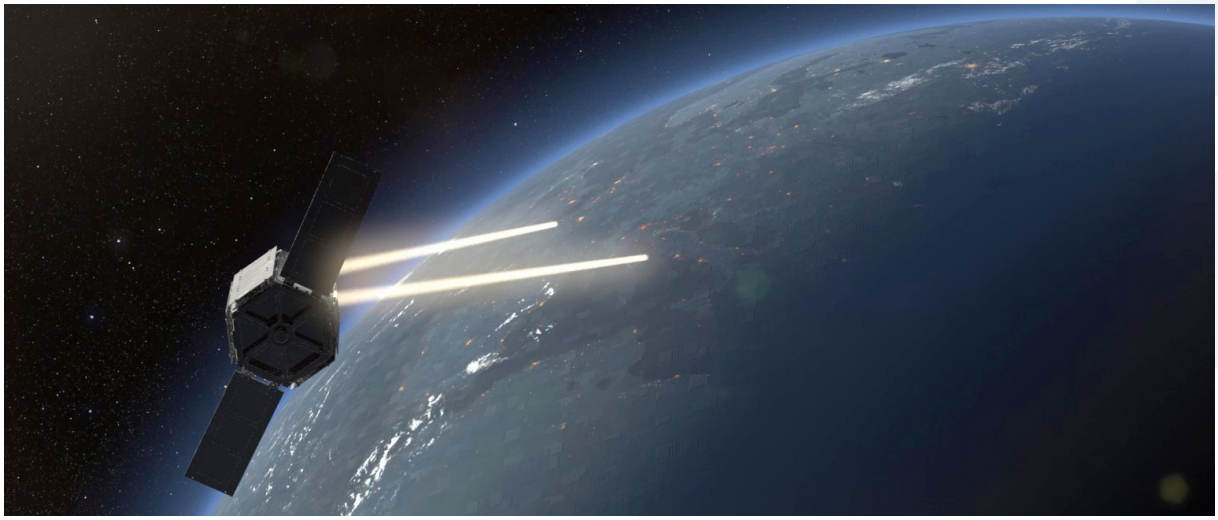
In light of this, NATO, the EU, and their member states run the risk of:

- loss of technological leadership;
- loss of cryptographic infrastructure;
- loss of signals intelligence (SIGINT);
- a silent takeover of civilian and military critical infrastructure.[9]

Disruptive effects

The quantum world is bizarre. It does not adequately accord with our own experiences in our social and professional lives; this dissonance will complicate competent governance. Quantum particles can be in two places at the same time. They can pass through walls. They master teleportation. They are highly sensitive. Even the slightest contact with the outside world is enough for them to collapse. This is the challenge for the construction of the quantum computer: protecting quantum states and simultaneously controlling and manipulating them. Researchers all over the world are working on this, and they are making promising progress. For decision-makers, it will be quite a challenge to

5 Philip Inglesant, Marina Jirotka and Mark Hartswood, "Responsible Innovation in Quantum Technologies applied to Defence and National Security", Oxford 2016, https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2018-11/Responsible%20Innovation%20in%20Quantum%20Technologies%20applied%20to%20Defence%20and%20National%20Security%20PDFNov18.pdf.
6 European Commission, "Quantum Technologies Flagship", Brussels, October 2018, https://ec.europa.eu/digital-single-market/en/quantum-technologies.
7 Inglesant, Jirotka and Hartswood, "Responsible Innovation".
8 Cf. https://en.wikipedia.org/wiki/Quantum_technology and https://ec.europa.eu/digital-single-market/en/blogposts/europes-future-quantum.
9 Dr. Christoph Marquardt, HYFUTEC study input.



© ESA

think through, judge and orchestrate the development of this new ecosystem.

In past decades, quantum technologies of the First Quantum Revolution, such as smartphones or the internet, have been used in everyday life. All microelectronics are based on chips, inside which quantum physical processes are used. Lasers emit light quanta with a very specific energy. Now, with the Second Quantum Revolution, a new technological performance class is emerging, offering the potential for game-changing new products for business and industry, as well as for government and defence applications. While economic applications are still years away, there will clearly be a **disruptive effect**.[10]

Quantum Computing (QC) will enable unprecedented processing power, duly allowing for the processing of volumes of data, resolving classes of problems that far exceed the capacity of classic computers. QC will likely be used to either speed up computations deep inside current machine learning, or deep learning algorithms, or to provide for completely different and much more efficient algorithms. There are already known quantum algorithms that would break existing forms of internet encryption. Several countries have begun to collect encrypted foreign communications with the expectation that they will be able to decode these within the next decade. In response, researchers are developing 'post-quantum' or quantum-safe cryptography, which uses classic mechanisms to replace the current public key schemes.

Encryption with quantum physical properties guarantees absolute security during data transmission. The respective protection of critical infrastructures would gain enormously because manipulation or external control, for example of autonomous systems, nuclear power plants or power grids, would no longer be possible. Quantum communication technologies enable new forms of secure communications, such as **Quantum Key Distribution** (QKD)-enabled cryptography. QKD already works.[11]

Quantum metrology and sensing promises unprecedented levels of resolution, sensitivity and accuracy. High-precision gravitational sensors will be capable of detecting hidden objects or cavities behind buildings, underground, underwater, or in the air, such as submarines or stealth aircraft. The high sensitivity and precision of inertial measurements, even during acceleration and rotation, provides for accurate and non-manipulable navigation systems, which can be used in aviation, space travel and shipping, as well as for autonomous driving, and even for navigation inside houses. High-precision clocks can be used to syn-

10 IISS, The Military Balance 2019, "Quantum computing and Defence", February 2019, 18–20, https://www.iiss.org/publications/the-military-balance/the-military-balance-2019/quantum-computing-and-defence.
11 ESA, "Space Photons Bring a new Dimension to Cryptography", 5 May 2018, https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Space_photons_bring_a_new_dimension_to_cryptography.

chronize large data networks or radio telescopes, to improve time scales and for global satellite navigation. Quantum Imaging will be capable of detecting gases, and of detecting objects around corners, through buildings, fog, smoke, or dust; it will also be able to build images under conditions of very low light.

Game-changing capabilities

Defence and national security are likely to be among the first domains to adopt emerging quantum technologies, particularly quantum-enabled clocks, quantum navigators, quantum gravity sensors and quantum imaging. This technological leap is expected to have far-reaching effects for military forces, intelligence services and law-enforcement agencies.

Fully capable quantum computing is still some years away, but early forms of quantum computing and quantum simulation are already available. **Specific benefits for hybrid contingencies** include artificial intelligence algorithms, highly secure encryption for communications satellites – that is, QKD – and accurate navigation that does not require GPS signals. Cyber actors can hardly expect the ability to use quantum computers to hack into encrypted military servers and into the servers controlling the national infrastructure systems of opponents unchecked.

For aircraft and spacecraft design and operation, it could lead to dramatic improvements in stealth and agility, both in the aerobatic sense and in the sense of mission versatility. The speed of data computation and processing, which quantum systems will significantly improve, will affect the work of unmanned and autonomous military platforms, enabling decisions to be taken more swiftly, making work more accurate, and allowing for multiple targets to be engaged with at once.

Also from a Russian and Chinese perspective, quantum computers will make it possible to grasp multi-domain situation developments much better than before.[12] Intelligence communities can employ such technologies for information superiority, collating public and secret information to automatically discover when adversarial entities have both the intention and resources to engage offensively.

The quantum race

A number of nations are currently investing heavily in quantum research in order to derive economic and military benefits.

China is positioning itself as a powerhouse in quantum science.[13] For example, it has already registered more patents than the USA in the fields of quantum communication and cryptography. Chinese researchers are extremely 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.[14]

"Already in 2016, Beijing launched the world's first quantum satellite, which teleported a photon to Earth in 2017. … The planned USD 10 billion National Laboratory for Quantum Information Sciences in Hefei, Anhui province, will lead the nation's drive for quantum computing and sensing."[15] Obviously, 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).

Russia is also investing in quantum technologies. It has created a dedicated Russian quantum centre, but is lagging behind 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 attributed to the quantum technologies sector.[16]

12 Sputnik, "Quantum Computing Arms Race Takes Shape as China, US, Russia Vie for Supremacy", 11.05.2017, https://sputniknews.com/military/201705111053523495-quantum-computing-military-applications-analysis/.
13 Elas B. Kania, John Castello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership", Center for a New American Security, September 12, 2018, https://www.cnas.org/publications/reports/quantum-hegemony.
14 Martin Giles, "The US and China are in a quantum arms race that will transform warfare", MIT Technology Review, January 3, 2019, https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/.
15 IISS, The Military Balance 2019, "Quantum computing and Defence".
16 Ibid.

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 for the Army 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.[17]

The private sector should not be underestimated. Companies like Google, IBM, Intel and Microsoft have been conducting quantum research for almost a decade. Together with the Canadian company D-Wave Systems, they lead the West in the development of quantum computers.

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. In October 2018, the European Commission launched the Quantum Technology Flagship Programme, 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 kick-start a competitive European quantum industry, with research results becoming available as commercial applications.[18]

This is imperative as, in contrast to the situation in China and the US, industrial actors in Europe are not yet participating in the quantum race. There are hardly any companies that invest in hardware or offer components. Early involvement would be preferable. For example, the 5G networks currently being developed need to be quantum-resistant and quantum-capable from the outset, otherwise they may be out-of-date in ten to fifteen years.[19] This would entail the rapid destruction and replacement of very expensive infrastructure, such as fibre optic networks. Even today, encryption methods should be able to withstand the potentiality of quantum technologies.

17 European Commission, "Quantum technologies flagship kicks off with first 20 projects", October 29, 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6205.
18 IISS, The Military Balance 2019, "Quantum computing and Defence".
19 Arthur Herman, "How America Can Still Win The Battle For 5G", Forbes, https://www.forbes.com/sites/arthurherman/2019/03/26/how-america-can-still-win-the-battle-for-5g/#16dd3cf066ed.

Quantum takeaways

- *Enables game-changing capabilities in computing, communication, cryptography, navigation, and sensing, thus enhancing the spectrum and reach of hybrid threats.*
- *Accelerates other technologies, including Cyber, AI, and XR, thus expanding hybrid warfare effects in offence and defence.*
- *Defence and national security are likely to adopt emerging quantum technologies, particularly quantum-enabled clocks, quantum navigators, quantum gravity sensors and quantum imaging, for example.*
- *Specific benefits for hybrid contingencies include artificial intelligence algorithms, highly secure encryption for communications satellites – that is, QKD – and accurate navigation that does not require GPS signals.*
- *Industrial actors in Europe are not yet participating in the quantum race.*
- *Technological leadership of opponents may lead to unforeseen hybrid warfare capabilities.*
- *Risk of loss of technological leadership, of cryptographic infrastructure andof signals intelligence (SIGINT).*
- *Protection of critical infrastructure and long-term secrets is time-critical. Up to 10 years left for deployment of countermeasures.*
- *Worst case: Silent takeover of critical infrastructure (civilian and military).*

Recommendations

- **Strengthen core research programmes.**
- **Identify, prioritize, and coordinate investment in both fundamental and applied challenges.**
- Push Quantum Key Distribution to support own operations.
- Develop a quantum-smart workforce capable of dealing with evolving quantum-related hybrid threats.
- Foster convergent, trans-sector approaches.
- Deepen governmental engagement with the quantum industry.
- Increase investment in joint quantum-technology research centres through partnerships between industry, academia, and government to accelerate pre-competitive quantum research and development.
- Identify critically needed infrastructure.
- Establish end-user testbed facilities along with training and engagement.
- Seek to increase international cooperation with like-minded industry and governments.
- Monitor international actors' strengths and focus areas, to identify gaps and opportunities.

Author
Colonel (R) Ralph D. Thiele is Managing Director of StratByrd Consulting, Chairman Political-Military Society, Berlin, and President EuroDefense – Germany. StratByrd Consulting, founded in 2013 in Germany, advises and implements solutions to strategy and digital transformation issues of networked security at the interface between industry and government against the backdrop of hybrid challenges. StratByrd is a freelance consulting company with a large network of science and politics, business and society, which configures itself flexibly and task oriented.


Hybrid CoE