Research Paper

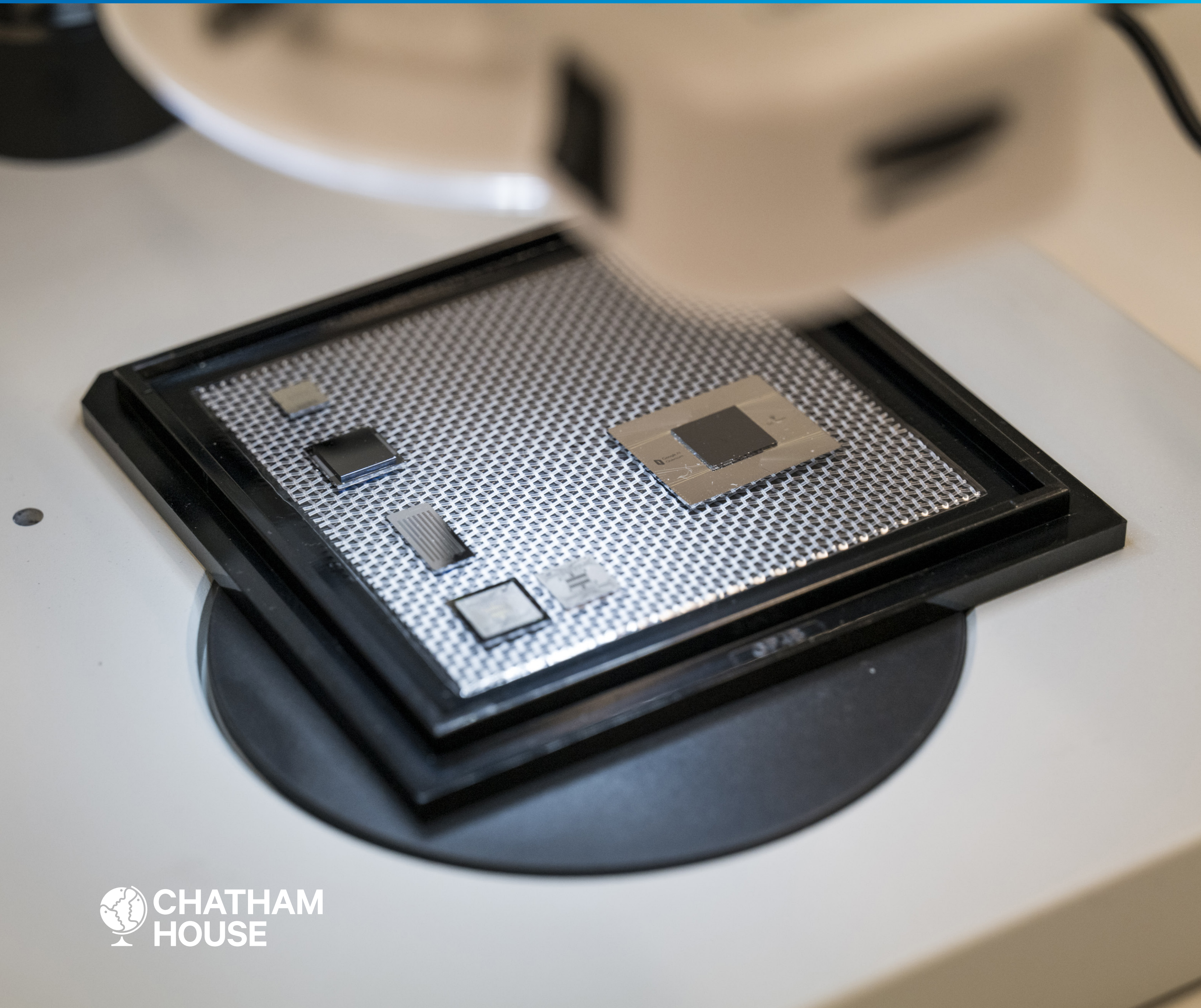
International Security Programme

January 2021

EU–US collaboration on quantum technologies

Emerging opportunities for research and standards-setting

Martin Everett



CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Summary

— While claims of 'quantum supremacy' – where a quantum computer outperforms a classical computer by orders of magnitude – continue to be contested, the security implications of such an achievement have adversely impacted the potential for future partnerships in the field.

— Quantum communications infrastructure continues to develop, though technological obstacles remain. The EU has linked development of quantum capacity and capability to its recovery following the COVID-19 pandemic and is expected to make rapid progress through its Quantum Communication Initiative.

— Existing dialogue between the EU and US highlights opportunities for collaboration on quantum technologies in the areas of basic scientific research and on communications standards. While the EU Quantum Flagship has already had limited engagement with the US on quantum technology collaboration, greater direct cooperation between EUPOPUSA and the Flagship would improve the prospects of both parties in this field.

— Additional support for EU-based researchers and start-ups should be provided where possible – for example, increasing funding for representatives from Europe to attend US-based conferences, while greater investment in EU-based quantum enterprises could mitigate potential 'brain drain'.

— Superconducting qubits remain the most likely basis for a quantum computer. Quantum computers composed of around 50 qubits, as well as a quantum cloud computing service using greater numbers of superconducting qubits, are anticipated to emerge in 2021.

Introduction

Quantum mechanics emerged as a branch of physics and mathematics over a century ago and many technologies, for example semiconductors and lasers, have developed from a growing understanding of quantum physics and its effects. These technologies harness many-body quantum effects, which manifest through macroscopic systems made up of a large number of particles. New and emerging technologies capitalizing on quantum physics at the single particle level – colloquially referred to as 'Quantum 2.0' – are set to have a strong impact on a number of sectors, in particular security, finance, communications, information science and manufacturing.

This research paper looks at the emerging opportunities for EU–US collaboration in the fast-developing field of quantum technologies. Several quantum technologies are already well established and are in the process of industrial and societal adoption. This paper does not examine these technologies in any depth, since they are well covered elsewhere – rather, it highlights possible new areas for potential EU–US cooperation in the near term.

The first section of the paper looks at the likely developments in new quantum technologies over the next couple of years. The second section discusses general opportunities for EU–US collaboration on quantum technologies. The final section presents more detailed explanations of a selection of future quantum technologies and provides a brief note on some US quantum funding streams.

The observations in this paper were obtained through a combination of research into academic sources, press articles, business reports and interviews with research and business figures in the quantum technology sector.

Emerging quantum technologies

Researchers are on the cusp of solving some of the most difficult problems in quantum computing. A priority in this area is the current exploration of potential materials that can be used to create qubits (quantum bits) and utilized in information storage in quantum computing. Qubits are the quantum computing analogy to binary digits (bits) in classical binary computing, and they are the basis for communications, sensing and imaging. The major difference is that in binary computing the digits are either 0 or 1. In quantum computing, a qubit can be thought of as being in a state that is a combination of both 0 and 1. This is termed a superposition state, which can increase the computing power – and speed – for certain calculations by orders of magnitude.

A number of large projects across many countries are looking into suitable materials that can be used to create qubits. For example, within the EU's Quantum Flagship initiative, the OpenSuperQ project aims to create a quantum computer consisting of up to

100 superconducting qubits,[1] while the SQUARE[2] and MicroQC[3] projects use trapped ions as a basis for qubits. These projects, along with many others around the world,[4] are focused on building a quantum computing architecture that is scalable and integrable with existing and future communication networks. Related projects in the US, for example, include work on superconducting and diamond lattice point defect qubits sponsored by the National Science Federation (NSF),[5] and research into advanced microwave photonics at the National Institute of Science and Technology (NIST).[6] The US Department of Energy (DOE) is also funding research into different types of qubits, such as Majorana qubits,[7] where quantum information is encoded into the collective motions of electrons through nanowire structures.[8]

As with quantum computing, discussion and collaboration would help guide the EU and the US to a consensus on a standard infrastructure for quantum communications.

CEOs of quantum technology start-ups interviewed for this paper confidently anticipated progress on superconducting qubit and trapped ion qubit quantum computers (examples include the Quantum Flagship's OpenSuperQ and AQTION[9] projects). One CEO predicted the emergence of a quantum computer with a smaller number of qubits (approximately 10–20) but with high fidelity, as well as the option of connecting to it via a cloud service, by early 2021.[10] Several interviewees mentioned the work of Alpine Quantum Technologies (headquartered in Innsbruck, Austria), which is providing access to its trapped ion quantum computer via Cirq,[11] an open source cloud-based quantum computing

1 European Commission (n.d.), 'OpenSuperQ: A quantum computer based on superconducting integrated circuits', https://ec.europa.eu/digital-single-market/en/content/opensuperq-quantum-computer-based-superconducting-integrated-circuits.
2 European Commission (n.d.), 'SQUARE: Scalable Rare Earth Ion Quantum Computing Nodes', https://ec.europa.eu/digital-single-market/en/content/square-scalable-rare-earth-ion-quantum-computing-nodes.
3 European Commission (n.d.), 'MicroQC: Microwave-driven ion trap quantum computing', https://ec.europa.eu/digital-single-market/en/content/microqc-microwave-driven-ion-trap-quantum-computing; European Union, CORDIS (2018), 'Microwave driven ion trap quantum computing', https://cordis.europa.eu/project/id/820314.
4 For example, PsiQuantum silicon photonic quantum computers. See, Quantum Daily (2020), 'PsiQuantum Raises $215 Million with new $150m round led by Atomico', 7 April 2020, https://thequantumdaily.com/2020/04/07/psiquantum-quantum-computer-startup-raises-230-million-possibly-largest-qc-investment-to-date-2.
5 US National Science Foundation (2018), 'RAISE:TAQS: Materials spectroscopy for next generation superconducting qubits', 11 September 2018, https://www.nsf.gov/awardsearch/showAward?AWD_ID=1839199; US National Science Foundation (2018), 'RAISE:TAQS: Engineering high quality, practical qubits in diamond', 11 September 2018, https://www.nsf.gov/awardsearch/showAward?AWD_ID=1838976.
6 US National Institute of Standards and Technology (2020), 'Advanced Microwave Photonics', 28 February 2020, https://www.nist.gov/programs-projects/advanced-microwave-photonics.
7 Majorana qubits are quasiparticles – collective motions of electrons – that travel through nanowires. Quantum information may be encoded into pairs of these quasiparticles based on whether one has been moved relative to the other as they retain a 'memory' of being moved around. For additional information, see, Chen, S. (2018), 'The Hunt for the Elusive Majorana Qubit', *APS News*, 27(4), https://www.aps.org/publications/apsnews/201804/hunt.cfm.
8 US Department of Energy (2018), 'DE-SC0019275: Design, Control and Application of Next-Generation Qubits', https://pamspublic.science.energy.gov/WebPAMSExternal/Interface/Common/ViewPublicAbstract.aspx?rv=6bae49b0-8934-41cb-9c0a-566defa0c8a7&rtc=24&PRoleId=10.
9 European Commission (n.d.), 'AQTION: Advanced quantum computing with trapped ions', https://ec.europa.eu/digital-single-market/en/content/aqtion-advanced-quantum-computing-trapped-ions.
10 Private communication, 17 September 2019.
11 IDW (2019), 'Quantum computers by AQT and University of Innsbruck leverage Cirq for quantum algorithm development', IDW-Nachrichten, 16 September 2019, https://nachrichten.idw-online.de/2019/09/16/quantum-computers-by-aqt-and-university-of-innsbruck-leverage-cirq-for-quantum-algorithm-development.

framework created by Google.[12] Professor Dr Tommaso Calarco, coordinator of the EU's Quantum Flagship Coordination and Support Action, anticipated the emergence of prototypes of the first integrated multiqubit superconducting chips by early 2021. These would lead to systems of around 50 superconducting qubits by September 2021, when the ramp-up phase of the EU Quantum Flagship is scheduled to end.[13]

Predictions about the development of quantum technologies are also made in the commercial sphere. For example, a 2018 Deloitte report on quantum technology forecast that the market for quantum computers would perform comparably to other specialized computer markets (such as supercomputers) until at least the 2030s.[14] (The report also noted the short-term value of Noisy Intermediate-Scale Quantum (NISQ) computers for a variety of sectors, such as finance and logistics.[15]) It recommended that governments and companies take immediate action to ensure their encryption is not vulnerable to attack by quantum computers in the future as their capabilities develop.[16]

To date, claims of 'quantum supremacy' have been contested and even the term is not consistently defined in the sector. A typical definition is 'the use of a quantum computer to solve *some* well-defined set of problems that would take orders of magnitude longer to solve with any currently known algorithms running on existing classical computers'.[17] The term is strongly criticized, however, by many researchers and experts, who advise that quantum computers should be judged on their ability to complete tasks that only these computers can handle – preferring instead the terms 'quantum advantage' or 'quantum ascendancy'.[18]

In 2017, Jay Gambetta of IBM Research recommended treating quantum supremacy achievements as a useful benchmark in quantum technology[19] – in much the same way as achieving a 100-qubit quantum computer is often considered a significant step in quantum development.[20] This approach, however, relies on using classical computing to benchmark quantum computing, which is radically different. Additionally, even after achieving such milestones, substantial research would still need to be dedicated to improving other parameters of these devices, such as maintaining high qubit fidelity to minimize errors in the results produced by such computers.[21]

---

12 Google AI Blog (2018), 'Announcing Cirq: An Open Source Framework for NISQ Algorithms', 18 July 2018, https://ai.googleblog.com/2018/07/announcing-cirq-open-source-framework.html.
13 Private communication with Tommaso Calarco, 17 September 2019; Quantum Flagship (2018), 'The launch of the Quantum Flagship', 29 October 2018, https://qt.eu/newsroom/quantum-flagship-launch-press-release/#targetText=The%2520first%25203-year%2520phase,field%2520to%2520its%2520farthest%2520frontiers.
14 Ibid., p. 97.
15 Ibid., p. 97, p. 102.
16 Ibid., p. 102.
17 Aaronson, S. (2019), 'Scott's Supreme Quantum Supremacy FAQ!', *Shtetl-Optimized blog*, https://www.scottaaronson.com/blog/?p=4317.
18 Giles, M. and Knight, W. (2018), 'Google thinks it's close to "quantum supremacy." Here's what that really means', *MIT Technology Review*, 9 March 2018, https://www.technologyreview.com/2018/03/09/144805/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means.
19 Ball, P. (2017), 'Race for quantum supremacy hits theoretical quagmire', *Nature*, 13 November 2017, doi:10.1038/nature.2017.22993.
20 Lindström, T., Weides, M., Ginossar, E., Hartmann, M., Brierley, S. and Pashkin, Y. (2018), 'Opportunities for superconducting quantum technology in the UK', National Physical Laboratory, Report TQE 13, October 2018: p. 1, https://www.npl.co.uk/special-pages/documents/quantum-metrology-institute/qmi-superconducting-quantum-computing-report.
21 Johnston, H. (2019), 'Silicon two-qubit gate achieves 98% fidelity', *Physics World*, 13 May 2019, https://physicsworld.com/a/silicon-two-qubit-gate-achieves-98-fidelity.

On 14 September 2019, a draft of a Google AI Quantum paper was accidentally posted to the NASA Technical Reports Server before being taken offline. The paper claimed that the Sycamore quantum computer comprised of 53 superconducting qubits sampled the output of a pseudo-random quantum circuit in 200 seconds. It was estimated that the same calculation, if performed on a number of classical computers, such as an IBM Summit supercomputer and Google Cloud servers, would take 10,000 years. As a result of this experiment, the paper claimed that Sycamore had achieved quantum supremacy.[22]

In response, a number of IBM researchers including Gambetta wrote that a better optimized simulation of the experiment could be performed on a Summit supercomputer in a mere two and a half days. They also disputed that Google's result demonstrated quantum supremacy, claiming that the original meaning of the term was intended to describe quantum computers performing tasks that classical computers could not.[23]

Indeed, according to Professor Calarco:

> At this stage, the race is really open, and there is no evidence that Europe is losing out in any of the fields. The only evidence of a clear advance in the US relative to EU is in superconducting quantum computing. The stated goal of the EU Quantum Flagship is to reach a comparable level of functionality as Google's quantum supremacy result in the next two years. Obviously Google and other American researchers will advance further in this time as well. It's possible to catch up, but equally development of quantum technology is non-linear – Google originally predicted they would achieve this quantum supremacy result in 2017.[24]

European Quantum Communication Infrastructure

Quantum communication is a fast-growing, exciting approach to more secure communications, including quantum key distribution (QKD) and other related protocols, quantum networking, quantum internet and the use of the principle of quantum entanglement (see below for more details). In April 2019, a technical agreement was signed to foster collaboration on a European Quantum Communication Infrastructure (QCI). The agreement states the intention of preparing, between 2019 and 2020, plans for secure communication via QKD, with implementation beginning from 2021.[25] Several EU member states have since signed up to the QCI,[26] and an important technological step was taken in September 2019 with the launch of OPENQKD, a multidisciplinary programme for developing the first test bed for QKD.[27]

22 The initial draft of the paper, and some commentary on it, can be found at: Inverse (2019), 'Here's Google "Quantum Supremacy" paper it pulled from NASA's website', 23 September 2019, https://www.inverse.com/article/59507-full-quantum-supremacy-paper.
23 Pednault, E., Gunnels, J., Maslov, D. and Gambetta, J. (2019), 'On "Quantum Supremacy"', IBM Research Blog, 21 October 2019, https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy.
24 Private communication with Tommaso Calarco, 29 January 2020.
25 European Commission (2019), 'Working arrangement between: the European Commission's Directorate General for Communications Networks, Content and Technology (DG CNECT) and the European Space Agency's Directorate for Telecommunications and Integrated Applications', 9 April 2019, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58568.
26 European Commission (2019), 'The future is quantum: EU countries plan ultra-secure communication network', 18 July 2019, https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network; European Commission (2019), 'Hungary, Portugal and Poland sign up to EU quantum communication infrastructure initiative', 19 July 2019, https://ec.europa.eu/digital-single-market/en/news/hungary-portugal-and-poland-sign-eu-quantum-communication-infrastructure-initiative.
27 European Union, CORDIS (2019), 'Open European Quantum Key Distribution Testbed', https://cordis.europa.eu/project/id/857156.

Experts anticipate significant developments in quantum communications and networking within Europe over the next 18 months, particularly in the work of QCI, although they acknowledge that additional technological work would be needed before a quantum internet could materialize. The EU's plans for economic recovery from the COVID-19 pandemic explicitly referenced development of quantum digital capacity and capability.[28]

In discussions between the EU Quantum Flagship and White House agencies there has been some buy-in predominantly on the level of basic scientific research.

The European Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT) issued a call for tenders in September 2020 for a 15-month detailed systems study for QCI.[29] Included within the requirements of the study are a detailed implementation roadmap, which indicates efforts towards the tangible realization of this infrastructure in the coming 10 years. Some areas of focus of the eventual QCI include quantum repeaters, amplifiers, and improved single-photon detection – all of which are required for a quantum internet.[30]

Several EU Quantum Flagship projects are already investigating quantum networking devices – the QIA project seeks to connect several quantum network nodes together, as well as build improved quantum repeaters –[31] that extend the range and reliability of quantum communication by teleportation of qubit information to intermediate stages en route, rather than sending the information in one jump and mitigating potential signal loss. The UNIQORN project is developing mass-market quantum communication devices.[32] QMiCS (Quantitative Microwave Communication and Sensing) is developing microwave-based quantum local area networks,[33] and QRANGE is focusing on well-established quantum random number generators (QRNGs) – truly random sources that are already being incorporated into existing devices and will be useful in both quantum simulation and for strengthening quantum key exchange.[34]

28 European Commission (2020), 'Europe's moment: Repair and Prepare for the Next Generation', https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0456&from=EN.
29 European Commission Directorate-General for Communications, Networks, Content and Technology (2020), 'Detailed system study for a Quantum Communication Infrastructure Competitive Procedure with Negotiation', https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69304.
30 Private communications, 17 September 2019.
31 European Commission (n.d.), 'QIA: Bringing the Quantum Internet to Europe', https://ec.europa.eu/digital-single-market/en/content/qia-bringing-quantum-internet-europe.
32 European Commission (n.d.), 'UNIQORN: Affordable quantum communication for everyone', https://ec.europa.eu/digital-single-market/en/content/uniqorn-affordable-quantum-communication-everyone.
33 European Commission (n.d.), 'QMiCS: Quantum Microwave Communication and Sensing', https://ec.europa.eu/digital-single-market/en/content/uniqorn-affordable-quantum-communication-everyone.
34 European Commission (n.d.), 'QRANGE: Quantum Random Number Generators: cheaper, faster and more secure', https://ec.europa.eu/digital-single-market/en/content/qrange-quantum-random-number-generators-cheaper-faster-and-more-secure; Stipčević, M. (2011), 'Quantum random number generators and their use in cryptography', *2011 Proceedings of the 34th International Convention MIPRO*, pp. 1474–1479, Opatija, 29 July 2011, https://ieeexplore.ieee.org/document/5967293.

As with quantum computing, discussion and collaboration would help guide the EU and the US to a consensus on a standard infrastructure for quantum communications. Work on common standards and common infrastructure for QKD is progressing through the International Telecommunication Union (ITU, a specialized UN agency) and the European Telecommunications Standards Institute (ETSI), which could help establish that the EU and the US could convert research into commercially competitive products in the global market – leading to faster rates of progress and increased economic efficiencies. Likewise, multi-stakeholder discussions between members of the US and EU research and industrial communities and the relevant national and supranational authorities are necessary to decide the future trajectory of encryption standards in the quantum era, given the potential impacts of quantum computing and quantum communications. A common EU–US quantum communications standard is important as the creators of such standards will gain important competitive advantages. These common standards are also a necessary condition for industrial collaboration between entities that adopt them.[35]

Quantum sensing

Quantum sensing encompasses an increasingly well-developed set of technologies. Quantum imaging – using states of light and new detection methods that conventional imaging devices cannot achieve – is already having a significant impact in industry. Other applications for quantum sensing include medical scanners, underground mapping and new accurate timing capabilities.

On the horizon, new approaches include the experimental demonstration of quantum radar by researchers at the Institute of Science and Technology Austria.[36] Quantum radar utilizes a split beam of entangled photons to irradiate the target, and the reflected signal is compared with the other half of the unaltered signal. This process is much more effective than classical radar at picking up low-reflective objects in noisy environments.[37]

This demonstration has made somewhat of a splash, as it is being reported as the first experimental demonstration of a quantum radar capability[38] – although official Chinese media claimed in 2016 that the country had already developed such systems.[39] However, speculation in the press suggests that intentional decoherence of a quantum radar beam may be researched as a possible countermeasure.[40]

35 Private communication with Tommaso Calarco, 29 January 2020.
36 Barzanjeh, S., Pirandola, S., Vitali, D. and Fink, J. M. (2019), 'Microwave quantum illumination using a digital receiver', arXiv, https://arxiv.org/abs/1908.03058.
37 Barzenjeh, S., Guha, S., Weedbrook, C., Vitali, D., Shapiro, J. H. and Pirandola, S. (2015), 'Microwave Quantum Illumination', *Physical Review Letters,* 114(8): p. 080503, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.114.080503.
38 *MIT Technology Review* (2019), 'Quantum radar has been demonstrated for the first time', 23 August 2019, https://www.technologyreview.com/2019/08/23/75512/quantum-radar-has-been-demonstrated-for-the-first-time.
39 *Global Times* (2016), 'China successfully develops quantum radar system', 9 September 2016, https://www.globaltimes.cn/content/1005525.shtml.
40 Chan, D. M. (2019), 'Stealth killer: Quantum radar actually works', *Asia Times*, 7 September 2019, https://asiatimes.com/2019/09/stealth-killer-quantum-radar-actually-works.

A related technology is the development of a quantum 'compass' – inertial navigation sensors that use quantum states of matter to create guidance systems that retain accuracy while not relying on satellites.[41] Previous work in this field focused on the creation of quantum magnetometers for measuring local variations in the Earth's magnetic field (so they can be used as a navigational reference point), as well as working on a quantum gyroscope.[42] (It must be noted, too, that more sensitive magnetometers are better at detecting submarines,[43] which could undermine strategic military systems.)

EU–US quantum collaboration

Opportunities facilitated by the EU Quantum Flagship

The EU Quantum Flagship is supporting some important areas that could form the basis of further EU–US quantum collaboration. Both parties discussed priority research topics of mutual EU–US interest in Washington DC in September 2019, including enabling the development of quantum hardware, algorithms and control methods.[44] In the longer term, they also discussed the possibility of a secure quantum transatlantic connection.[45] As noted in the first section of this paper, this would entail considerable new research on additional quantum devices, such as repeaters. So far in discussions between the EU Quantum Flagship and White House agencies, such as the Office of Science and Technology Policy, there has been some buy-in predominantly on the level of basic scientific research. US scientists have also signalled a potential interest in topics related to industry policy, such as standardization for quantum communications.[46]

The Quantum Flagship Coordination and Support Action has been given a mandate by Mariya Gabriel, European Commissioner for Innovation, Research, Culture, Education and Youth, to explore opportunities for collaboration *limited* to the scientific field.[47] This would indicate a degree of tentativeness at the highest levels of the EU at this point as regards pursuing quantum collaboration with the US beyond fundamental scientific research. According to Calarco:

> Cooperation is a good thing that can lead to a win-win situation. This win-win can occur if there is no ambiguity on mutual interest and cooperation. This is the case with science and scientific cooperation – there is an exchange of knowledge involved, that can benefit

41 MuQuans (n.d.), 'Absolute Quantum Gravimeter', https://www.muquans.com/product/absolute-quantum-gravimeter; Dunning, H., Angus, T. and Sayers, M. (2018), 'Quantum 'compass' could allow navigation without relying on satellites', Imperial College London, 9 November 2018, https://www.imperial.ac.uk/news/188973/quantum-compass-could-allow-navigation-without.
42 Chen, S. (2018), 'Quantum Physicists Found a New, Safer Way to Navigate', *Wired*, 1 November 2018, https://www.wired.com/story/quantum-physicists-found-a-new-safer-way-to-navigate.
43 Chen, S. (2017), 'Has China developed the world's most powerful submarine detector?', *South China Morning Post*, 24 June 2017, https://www.scmp.com/news/china/society/article/2099640/has-china-developed-worlds-most-powerful-submarine-detector.
44 Private communication with Tommaso Calarco, 17 September 2019.
45 Ibid.
46 Ibid.
47 Private communication with Tommaso Calarco, 29 January 2020.

> both sides. What is not so established, and requires deeper reflection at a policy level, is whether the same holds on the industrial side. [The] US has a stronger involvement in the quantum technology industry – there is an asymmetry here between the US and the EU.[48]

Future meetings on joint EU–US quantum cooperation are scheduled to take place. Here, quantum cooperation opportunities could be explored between scientists, social scientists, industry representatives and policymakers, with a view to creating openings for joint publications, intellectual property, patents and commercial opportunities.

Funding and security challenges around quantum collaboration

Interviews with CEOs of quantum technology start-ups highlighted a number of challenges confronting quantum research and development in Europe. One of these issues is that in the now global race for technology and talent, Europe risks losing out to other parts of the world that are investing heavily in these new opportunities.[49] This new 'brain drain' may be exacerbated by US companies acquiring some European start-ups.[50] While they acknowledged the value of programmes such as the EU Quantum Flagship for increasing funding for quantum research, some of the CEOs interviewed emphasized that there were challenges inherent in developing a quantum start-up in Europe, due to differences in available funding levels compared to the US.[51] While there are likely to be stronger funding opportunities in the US, especially in terms of venture capital, additional EU funding could at least begin to mitigate this scenario.

However, there is also a growing sense within the scientific and technical community that international collaboration on quantum research and development is becoming increasingly challenging as quantum technology is seen more widely as not only commercially valuable, but also significant from a national security perspective.[52] As outlined in the detailed technological explanations in the final section of this paper, many quantum technologies could have security implications. Quantum computing can make existing encryption standards easier to crack and are incentivizing the creation of stronger classical encryption standards; strenuous efforts are being made to develop new 'post-quantum' or 'quantum-resistant' algorithms.[53] Quantum key exchange can be used to create stronger encryption standards that are less vulnerable to eavesdropping. Finally, quantum sensing may result in more sensitive radars and more accurate navigation and guidance systems for military vehicles and weapons that are not reliant on satellites. The perceived unique properties and potential civil

48 Ibid.
49 European Quantum Flagship (2016), 'Quantum Manifesto: A New Era of Technology', *qt.eu*, May 2016, https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf.
50 Laurent, L. (2019), 'Google and Facebook Are Sucking the Brains Out of Europe', *Bloomberg*, 1 July 2019, https://www.bloomberg.com/opinion/articles/2019-07-01/google-and-facebook-are-sucking-the-ai-brains-out-of-europe.
51 Private communication, 17 September 2019.
52 Biamonte, J. D., Dorozhkin, P. and Zacharov, I. (2019), 'Keep quantum computing global and open', *Nature*, 11 September 2019, https://www.nature.com/articles/d41586-019-02675-5.
53 US National Institute of Standards and Technology (2019), 'NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'', 30 January 2019, https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals.

and military uses of these technologies may be leading to an increased securitization of the field of quantum research, with less state funding available to finance international collaborations on quantum technologies due to national security concerns.

As a result, there are fears that the US might impose export controls on quantum technology,[54] and there have been reports that the US government is already considering introducing similar restrictions, in particular on quantum computers, encryption and sensing,[55] which may well further deter overseas researchers (including those from EU member states) from working in the US.[56] Developing and broadening schemes for conference sponsorship for start-ups and hosting larger networking events could encourage cooperation once the COVID-19 pandemic declines – although costs can be prohibitive for start-ups to afford to attend these events, despite their value in developing vital business and research connections.[57] In this context, organizers could hold a short, three-to-five-day, retreat and sponsor the attendance of 10 quantum researchers and start-up representatives from both the EU and the US. At such a retreat the researchers could present their research findings and proposals, receive coaching and participate in workshops on building research collaborations and business links between the EU and US.

It is to be expected that advanced countries and alliances will compete for peak position in the research and development of quantum technologies. Given the security implications in this area, it is natural that some wariness will exist regarding collaboration.[58] However, common standards, transparency, the freedom of research-related information as well as the exchange of research personnel would allow the EU and US to maximize their competitiveness in the field of quantum information science, while strengthening their bilateral collaborative relationship.

Maintaining a competitive edge is important, given that funding of quantum research is increasing in other countries, for example, China. The securitization of quantum technologies, to the extent that deeper collaboration is inhibited, should be limited in order to enable competition. It is important to note, however, that there is some debate over the precise level of Chinese investment in its domestic research on quantum information science. According to Calarco:

> We have no evidence that China is investing more than Europe or the US in this field. What we know is they declare they are doing so. But whenever we speak to colleagues there, we hear that those public numbers do not correspond to reality, and in practice are an order of magnitude lower.

54 Private communication, 17 September 2019.
55 Federal Register (2018), 'Review of Controls for Certain Emerging Technologies', 19 November 2018, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.
56 Waddell, K. (2018), 'Trump administration's proposed export controls could hinder tech research', *Axios*, 28 November 2018, https://www.axios.com/trump-export-controls-harm-tech-research-national-security-9561b8a4-7f74-45dd-8162-2807fa7d8ed1.html.
57 Private communication, 17 September 2019.
58 Farrell, H. and Newman, A. L. (2019), 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', *International Security*, 44(1): pp. 42–79, doi:10.1162/isec_a_00351.

> I can see scenarios in which this might lead to stronger ties. I can also see scenarios in which this rhetoric exacerbates the whole discourse in the political arena, in such a way to make any move problematic. We have done all we can to decouple this discourse from conflict with China, including to avoid escalating it to the political level, which would do our cause a disservice. This includes not riding the wave of anti-China rhetoric.[59]

To summarize, this paper notes that the most attainable prospects for quantum collaboration between the EU and US at present are in basic scientific research, with interest shown towards a policy of mutual industry standardization for quantum communications. There are ways to facilitate EU scientific and business involvement with the wider field of quantum technology that could be arranged more unilaterally – for example, increasing sponsorship of conferencing and networking events for academics and start-ups. This could be done on a small scale to begin with, with the sponsoring of retreats for a select, limited number of EU and US quantum researchers and industry representatives.

Of greater concern is the perception that the window for collaboration is at present limited, if not shrinking, due to an increased securitization of quantum technologies, which may close off future collaboration opportunities as sought by the EU. China is competing with the EU and US for technological successes and investment in quantum technologies. While it is understandable that security concerns can inhibit collaboration, overcoming these inhibitions will strengthen both the EU–US relationship and the quality of their quantum research. Taking a more pessimistic view, failure to collaborate risks leaving both the EU and US playing 'catch-up' with China's quantum technology research.

As a starting point, in order to reduce the impact of this dynamic and facilitate additional trust and confidence-building towards further collaborations, the EU could pursue the available short-term opportunities for quantum collaboration in the areas of basic scientific research and aim to achieve a set of EU–US standards for quantum communications as a minimum. This would constitute a significant joint project that would also broaden the potential extent of EU–US quantum collaboration. Beyond that, the main priority is to keep as open as possible the opportunities for the exchange of information and personnel researching quantum technologies.

Future quantum technologies and US funding streams

Quantum computing: algorithms and simulations

The fundamental unit of information processing and storage in classical computers is the binary digit, or 'bit', where information is represented as either 0 or 1. However, if one uses quantum objects as a basis for information processing, this permits the formation of quantum bits or 'qubits'. The closest analogy is that a qubit can be said to be in a state that is a combination of both 0 and 1 (a superposition state). Considerable

59 Private communication with Tommaso Calarco, 29 January 2020.

advantage is gained from swapping classical bits (0 or 1) for quantum bits (superposition of 0 and 1) so that certain calculations can be performed significantly faster. However, depending on what calculation is being performed, this could lead to a sudden reduction in effectiveness of important security protocols.

The best-known example of this is the problem of integer factorization. Public-private key encryption is asymmetric – that is, it can be relatively straightforward to encrypt information, but far more difficult to decrypt the information. These protocols typically rely on the multiplication of two large prime integers (the public and private keys) to create an encryption key – a trivial task in comparison with factorizing the product of those two numbers back into the public and private key. With classical factorization algorithms, the problem becomes practically unsolvable for sufficiently large keys due to the length of computation time it would take to discover the factors. However, by implementing a *quantum* factorization algorithm (e.g. Shor's algorithm)[60] on a quantum computer with an adequate number of qubits, the time required for breaking the same strength of public key encryption shortens drastically.[61] The core concern of this technology is a possible 'Enigma moment' where a sufficiently capable quantum computer is used to start breaking information encrypted with asymmetric public-private key encryption.

This would have an impact on a number of sectors, as public key encryption authenticates users of the Transport Layer Security (TLS) protocol used to secure data in HTTP connections, which is utilized for online banking, sales and telephone calls.[62] Many cryptocurrency wallets secure the bearer's currency by means of public key encryption, implying that quantum attacks on those wallets may allow the attacker to 'pickpocket' them.[63] Nor is it just public-private key encryption that is potentially vulnerable to a quantum attack – research is being conducted into the application of Shor's algorithm to other forms of asymmetric encryption.[64] Although symmetric encryption is less vulnerable to quantum attack, the Grover quantum search algorithm can find items in a list of size N (for example, a specific decryption key within a particular key space) in $\sqrt{N}$ attempts as opposed to $N/2$ attempts on a classical computer.[65]

However, quantum computers are not yet sufficiently complex to accomplish this sort of significant breach of public key encryption. This is a fair comment when one considers the physics involved – qubits, as with any quantum superposition, are quite fragile, with vibrations, heating and electromagnetic disturbances potentially causing the superposition to break down (in effect, the simultaneous 0 and 1 of the qubit suddenly

60 MinutePhysics (2019), *How Quantum Computers Break Encryption: Shor's Algorithm Explained*, 30 April 2019, https://www.youtube.com/watch?v=lvTqbM5Dq4Q.
61 Shor, P. (1997), 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *J.Sci.Statist.Comput.,* 26(5): pp. 1484–1512, https://doi.org/10.1137/S0097539795293172.
62 Holmes, D. (2017), 'How Quantum Computing Will Change Browser Encryption', F5 Labs, 13 July 2017, https://www.f5.com/labs/articles/threat-intelligence/how-quantum-computing-will-change-browser-encryption.
63 Rafaeli, R. (2018), 'How quantum computing could wreak havoc on cryptocurrency', The Next Web, 14 April 2018, https://thenextweb.com/contributors/2018/04/14/quantum-computing-wreak-havoc-cryptocurrency.
64 Mavroeidis, V., Vishi, J., Zych, M. D. and Jøsang, A. (2018), 'The Impact of Quantum Computing on Present Cryptography', *International Journal of Advanced Computer Science and Applications*, 9(3): pp. 1–10.
65 Grover, L. K. (1996), 'A fast quantum mechanical algorithm for database search', arXiv, 19 November 1996, https://arxiv.org/abs/quant-ph/9605043.

snaps back to either 0 or 1, and it functions essentially like a classical bit). There are means of compensating for this problem of *decoherence*, such as quantum error correction, which encodes the same information into multiple qubits to minimize information loss via decoherence. It should be noted that this requires the construction of a quantum computer that contains even more functional qubits, which increases the scale of the technical challenge at this stage.[66]

The core concern of this technology is a possible 'Enigma moment' where a sufficiently capable quantum computer is used to start breaking information encrypted with asymmetric public-private key encryption.

While sufficiently complex quantum computers capable of cracking widely used encryption protocols do not yet exist, the belief that quantum computers are coming has securitized the issue. Already, major national signals intelligence agencies – such as the US National Security Agency and the British GCHQ – are publicly expressing concern about the development of quantum computers and their effect on cryptographic security. There is also a growth of classical 'quantum-resistant' encryption protocols, which are believed to be less vulnerable to quantum decryption algorithms.[67] Symmetric encryption standards, such as the Advanced Encryption Standard (AES) can be strengthened against the Grover quantum search algorithm by increasing the key length. Thus, even if quantum computers may be stuck in a semi-permanent state of being 'just five years away', the fear of their emergence is already having a reinforcing impact on encryption by spawning a diversification of encryption protocols.

New quantum communication: encryption and networking

Quantum communication relies on many of the same principles and apparatus as quantum computing. A qubit can be described as a single particle functioning as a mixture or superposition of 0 and 1 simultaneously. A superposition of a system of multiple particles – where the state of one particle intrinsically depends on the state of another particle – is referred to as *entanglement*.

Two qubits, when entangled, allow the result of the measurement of one qubit to provide information about the state of the other qubit. An extension of this principle allows for the teleportation of a quantum object's state from one location to another. Entangling two qubits together permits the state of a third qubit to be teleported between them. This is not 'faster-than-the-speed-of-light' communication – necessary

66 Bassan, T. (2018), 'Decoherence: Quantum Computer's Greatest Obstacle', Hackernoon, 1 June 2018, https://hackernoon.com/decoherence-quantum-computers-greatest-obstacle-67c74ae962b6.
67 US National Security Agency, Central Security Service (2016), 'Commercial National Security Algorithm Suite and Quantum Computing FAQ', Cryptome, January 2016, https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf; UK Government, National Cyber Security Centre (2016), 'Quantum-safe cryptography', 30 November 2016, https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography.

measurements performed on the system as part of the communications protocol are limited to the speed of light – nor is it the physical teleportation of objects. In quantum communication, 'teleportation' enables the state of a qubit to be transferred to another site; it also allows for a transfer of information without needing to physically transport that information. Experiments in this field are pushing the boundaries of entangled communication, a successful Chinese quantum communication test via satellite (claimed in 2017) is a notable example.[68]

It is also possible to use quantum entanglement in a protocol for encryption key exchange. As the entangled system cannot be measured without altering it, this protocol also has enhanced resistance to interception, where the error rate in the protocol may be indicative that the communications channel has been compromised. This holds for all QKD protocols, not only those that utilize entanglement.[69]

These principles facilitate quantum networking, a fundamental part of any future quantum information infrastructure. Limiting factors on the development of these technologies are similar to those for quantum computing – maintaining entanglement over large distances and durations. New quantum encryption protocols will have an impact on international security, in particular by being inherently more resistant to interception. Furthermore, given that quantum key exchange techniques can be developed using a similar technological base to quantum computers – which may facilitate the breaking of existing classical encryption protocols – these technologies, when combined, could put substantial stress on existing communication standards and security. However, such technologies would also enable both the US and EU to create secure quantum information networks of their own.

The US quantum funding stream

In December 2018, the National Quantum Initiative (NQI) Act came into force in the US. The act incorporates research from NIST, DOE and NSF, and funds the NQI. In addition, NIST, DOE and NSF regularly fund quantum research.[70] The NQI Act explicitly encourages collaboration between a number of bodies mentioned therein, and their international partners; the National Science and Technology Council's Subcommittee on Quantum Information Science and the NQI Advisory Committee are given responsibility for determining opportunities for international cooperation with strategic allies.[71] The NQI was initially advocated by the National Photonics Initiative, which noted that the US lacked a large, centralized quantum research project equivalent in scope to the

68 Liao S.-K. et al. (2017), 'Satellite-to-ground quantum key distribution', *Nature*, 549: pp. 43–47, https://www.nature.com/articles/nature23655.
69 Ekert, A. K. (1991), 'Quantum Cryptography Based on Bell's Theorem', *Physical Review Letters*, 67(6): pp. 661–663.
70 US National Institute of Science and Technology (n.d.), 'Projects/Programs: Quantum Information Science', https://www.nist.gov/laboratories/projects-programs?k=&a%5B%5D=248311&a%5B%5D=249246&tag=; US Department of Energy (2018), 'Department of Energy Announced $218 Million for Quantum Information Science', 24 September 2018, https://www.energy.gov/articles/department-energy-announces-218-million-quantum-information-science; US National Science Foundation (2018), 'NSF announces new awards for quantum research, technologies', 24 September 2018, https://www.nsf.gov/news/news_summ.jsp?cntn_id=296699.
71 US Congress (2018), 'H.R.6227 – National Quantum Initiative Act', 3 January 2018, https://www.congress.gov/bill/115th-congress/house-bill/6227/text#HDEB502BED9CC4603A0E5F21C179960E7.

EU's Quantum Flagship, or to China's large-scale investment programmes.[72] The NQI Advisory Committee was officially established by President Donald Trump on 30 August 2019.[73] The Subcommittee on Quantum Information Science, in its strategic overview document published in September 2018, encouraged collaboration with like-minded governments and espoused a science-first approach that welcomes fundamental quantum science research.[74] More detailed information about the US programme, from the perspective of the UK Knowledge Transfer Network, was collated during a Global Expert Mission to the US in November 2019[75] and was published in *Quantum Technologies in the USA 2019*.[76]

Conclusions and recommendations

The short-term technological predictions of the sources consulted for this research paper primarily converged around the emergence of superconducting qubits as an established basis for a quantum computer. The debate on the emergence of some kind of 'quantum supremacy' moment continues to rage fiercely with a lack of a clear resolution in sight. As mentioned in the first section of this paper, Google posited such a claim in September 2019, which IBM later challenged.[77] This paper recommends that subject-matter experts continue both to monitor the technological developments in the field of superconducting quantum computing – as well as the debate surrounding it – and to scrutinize how 'quantum supremacy' is being defined.

European quantum communications infrastructure developments should continue to be observed, as progress is expected in 2021, though technological obstacles still remain (improving quantum repeaters, amplifiers and single-photon detection). Progress in quantum computing and communication will present an increasing challenge for the secure encryption of sensitive information, which may necessitate a shift towards a classical computing-based 'quantum-resistant' encryption, or possibly even secure communication through quantum key distribution.

The main focus in the short term for quantum technology collaboration between the EU and the US is likely to be confined primarily to basic scientific research, which could be improved by increasing funding for quantum start-up representatives to attend

---

72 US National Photonics Initiative (2018), 'National Quantum Initiative – Action Plan', 3 April 2018, https://www.lightourfuture.org/getattachment/85484dca-465a-46f4-8c8c-090aeb845d09/FINAL-Action-Plan-for-a-NQI-Apr-3-2018.pdf; US National Photonics Initiative (2017), 'Call for a National Quantum Initiative', 22 June 2017, https://www.lightourfuture.org/getattachment/Home/About-NPI/Resources/NPI-Recommendations-to-HSC-for-National-Quantum-Initiative-062217.pdf.
73 The White House (2019), 'Executive Order on Establishing the National Quantum Initiative Advisory Committee', 30 August 2019, https://www.whitehouse.gov/presidential-actions/executive-order-establishing-national-quantum-initiative-advisory-committee.
74 The White House, Subcommittee on Quantum Information Science (2018), 'National Strategic Overview for Quantum Information Science', September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf.
75 UK Knowledge Transfer Network (2019), *Quantum Technologies US Global Expert Mission, November 2019,* https://www.slideshare.net/KTNUK/quantum-technologies-global-expert-mission-dissemination-workshop.
76 Innovate UK (2019), *Quantum Technologies in the USA 2019, Innovate UK Global Expert Mission,* https://admin.ktn-uk.co.uk/app/uploads/2020/03/0183_KTN_USA-QuantumTechnologiesReport_v4.pdf.
77 Inverse (2019), 'Here's Google "Quantum Supremacy" paper it pulled from NASA's website'.

conferences in the US. While there is also the possibility of some collaboration on quantum communications standards, growing securitization of the field is increasingly inhibiting this direction. It is vital that all opportunities for cooperation are maximized in order to increase industrial collaboration. On the European side, this paper strongly recommends closer liaison between the EU Policy and Outreach Partnership in the USA (EUPOPUSA) and the EU Quantum Flagship, which has already engaged in consultation with the US administration on collaboration opportunities.

About the author

Martin Everett is a graduate of the Science and Security Programme at Kings College London. Originally trained in physics at the University of St Andrews, Martin specialized in quantum optical physics in postgraduate studies at Imperial College London. He has performed open-source research at Ridgeway Information, and worked on the application of open-source methods in human rights abuse cases. He has previously published articles on anti-hypersonic missile defences and strategic stability.

Acknowledgments

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the author and can in no way be taken to reflect the views of the European Union.

Chatham House is part of a consortium, coordinated by B&S Europe, implementing the EU Policy & Outreach Partnership in the United States.

The author would like to thank EUPOPUSA for the provision of financial support and advice. The author would also like to express appreciation to the interviewees who provided valuable contributions – Professor Calarco, in particular, was a patient and helpful interlocutor during the writing of this paper. Thanks also to the anonymous peer reviewers for their comments and suggestions on earlier drafts of this paper. The author is particularly grateful to the International Security Programme at Chatham House, in particular to Patricia Lewis for her advice and feedback on earlier drafts and to Calum Inverarity for his support throughout the project. Finally, the author thanks Vera Chapman and Michael Tsang for their many valuable corrections and refinements during editing.

Cover image: Superconducting quantum processors sit on display during a Google AI event in San Francisco on 28 January 2020.
Photo credit: Copyright © David Paul Morris/Bloomberg/Getty Images

ISBN 978 1 78413 421 1

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

CHATHAM HOUSE

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223