European Journal of Risk Regulation (2023), **14**, 476–483
doi:10.1017/err.2023.44

CAMBRIDGE UNIVERSITY PRESS

SYMPOSIUM ON CLIMATE, AI & QUANTUM

Quantum Computing: Bridging the National Security–Digital Sovereignty Divide

Anders Liman[1] and Kate Weber[2]

[1]Duke University, Durham, NC, USA and [2]Google, Inc., Mountain View, CA, USA
Corresponding author: Anders Liman; Email: anders.liman@duke.edu

Abstract

Quantum computing research and development efforts have grown dramatically over the past decades, led in part by initiatives from governments around the world. Government quantum computing investments are often driven by national security or digital sovereignty concerns, with the language used depending on the geography involved. For example, a focus on "national security" and quantum computing is prominent in the USA, while European countries regularly focus on "digital sovereignty". These phrases are often loosely defined and open to interpretation, and they share some common motivations and characteristics (but also have important differences). This paper identifies specific governmental entities typifying the national security/digital sovereignty perspectives, along with these organisations' respective roles within national and international policy engagement in quantum computing. It analyses governmental structures, historical developments and cultural characteristics that contributed to this national security–digital sovereignty divide. Building on this analysis, we use the history of other technologies to illustrate how we might adapt tested policy approaches to modern political dynamics and to quantum computing specifically. We frame these policy approaches so that they do not overemphasise "digital sovereignty" or "national security", but rather address interests shared across both concepts, with a view to facilitating international collaboration.

Keywords: Digital sovereignty; international collaboration; national security; quantum computing

I. The divide

The United States Government (USG) and European governments have been investing in quantum technologies research for decades, but governments on both sides of the Atlantic recently focused these efforts around national/regional initiatives. The language describing these initiatives illustrates the USA's focus on quantum computing (QC) through a national security lens and the European focus on digital sovereignty.[1]

On 21 December 2018, the bipartisan US National Quantum Initiative (NQI) Act was signed into law "to accelerate quantum research and development (R&D) for the *economic and national security* of the US" (emphasis added).[2] With more than $1.2 billion in authorised funding over five years, the NQI Act tasks the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF) and the Department of

[1] Cf T Roberson, J Leach and S Raman, "Talking about public good for the second quantum revolution: analysing quantum technology narratives in the context of national strategies" (2021) 6(2) Quantum Science and Technology 025001.

[2] National Quantum Initiative Act 2018.

Energy (DOE) with strengthening quantum information science (QIS) programmes, centres and consortia. The NQI Act also calls for a coordination of R&D efforts through an NQI Advisory Committee (NQIAC) and three National Science and Technology Council (NSTC) subcommittees, including one that is specifically focused on security concerns: the Subcommittee on the Economic and Security Implications of Quantum Science (ESIX). ESIX is co-chaired by the Office of Science and Technology Policy (OSTP), DOE, Department of Defense (DOD) and National Security Agency (NSA), and these national security-focused agencies are also responsible for the majority of US R&D funding for QC (eg via DOE national laboratories and the Defense/Intelligence Advanced Research Projects Agencies, DARPA and IARPA). The US focus on the defence/security implications of QC is also evident in the focus on QIS in the National Defense Authorization Act (NDAA) – yearly legislation to authorise US defence activities.[3] NDAA quantum provisions have asked the DOD to increase the technology-readiness level of QIS in the USA, support the development of a QIS workforce and enhance awareness of QIS.

Also in 2018, across the Atlantic, the European Union (EU) launched the Quantum Flagship with a €1 billion investment in EU quantum R&D over ten years.[4] The Quantum Flagship's goal is to "consolidate and expand European scientific leadership and excellence" in QIS technologies and to "make Europe a dynamic and attractive region for innovative research, business and investments in this field".[5] While this language does not mention digital/technological sovereignty specifically, it does allude to the competitive lens through which the EU views QC – and this perspective is further reflected in the implementation of EU research funding, which has excluded traditional partners from collaborations in "strategic research" under the broader Horizon Europe umbrella, including quantum research.

The focus on sovereignty is more pronounced in several EU Member States. For example, around the same time as the Quantum Flagship was introduced, the German government announced a €650 million investment in quantum R&D, a combined effort of the Ministry of Education and Research (BMBF), Ministry of Economic Affairs and Climate Actions (BMWK), Ministry of the Interior and Community and Ministry of Defense (BMVg).[6] In addition to "expanding the research landscape of quantum technologies", the programme seeks to "*ensure technological sovereignty*" (emphasis added) and "take the people of our country with us".[7] In 2020, the German government announced an additional nearly €2 billion investment in QC by BMBF and BMWK.[8] According to the Minister of Education and Research, the goal of the QC investment is to "increase our prosperity, *strengthen our technological sovereignty*, and help technology made in Germany to take a real leap" (emphasis added).[9] In 2021, IBM and Fraunhofer-Gesellschaft announced a partnership to develop and deploy a quantum computer *on German soil*.[10] The president of Fraunhofer-Gesellschaft called the launch an "important milestone on the path to

[3] John S. McCain National Defense Authorization Act for Fiscal Year 2019.

[4] European Commission, "Introduction to the Quantum Flagship" (*Quantum Technology*, 2020) <https://qt.eu/about-quantum-flagship/introduction-to-the-quantum-flagship/> (last accessed 31 August 2022).

[5] ibid.

[6] A Thoss, "€650 million for quantum research in Germany" (*Laser Focus World*, 2018) <www.laserfocusworld.com/lasers-sources/article/16571451/650-million-for-quantum-research-in-germany/> (last accessed 31 August 2022).

[7] ibid.

[8] É Kelly, "Germany to invest €2B in quantum technologies" (*Science Business*, 2021) <https://sciencebusiness.net/news/germany-invest-eu2b-quantum-technologies/> (last accessed 31 August 2022).

[9] ibid.

[10] O Noyan, "Germany launches Europe's first 'revolutionary' quantum computer" (*Euractiv*, 2021) <www.euractiv.com/section/digital/news/germany-launches-europes-first-revolutionary-quantum-computer/> (last accessed 31 August 2022).

https://doi.org/10.1017/err.2023.44 Published online by Cambridge University Press

Germany's *technological sovereignty*" (emphasis added).[11] Chancellor Angela Merkel said the new quantum computer "promises tremendous innovative achievements" and referred to its "*key role for digital and technological sovereignty*" (emphasis added).[12] And the Minister of Education and Research said "building up this ecosystem is *a very important question for security and sovereignty*" (emphasis added, and one of the few references we see to "security" in a European context).[13]

Similarly, in January 2021, French President Emmanuel Macron presented the nation's €1 billion quantum plan over five years.[14] Aiming to "preserve *national sovereignty*, especially with regard to the United States and China … as well as (US) tech giants" (emphasis added), the plan rests on two main axes.[15] "The first is global and integrated technological development", said Macron, and "the second is the *strengthening of the French innovation ecosystem* in its European environment" (emphasis added).[16] In June 2021, during European Commission's President Ursula von der Leyen's visit to French quantum facilities, Secretary of State for European Affairs Clément Beaune noted that QC "represents a share of European *technological sovereignty*" (emphasis added), further confirming the nation's strategic plan.[17]

II. The definitions

What do countries mean by "national security" and "digital sovereignty"? How are they similar and different?

While several US agencies often discuss the importance of QC for national security, they do not always mean the same thing. The notion of national security is more helpful when broken down into physical security, economic security, energy security, cybersecurity, environmental security, infrastructure security and political security. Of these, the first four are especially relevant to QC. Physical security is often seen among defence- and intelligence-focused agencies (eg DOD, DARPA, Office of the Director of National Intelligence (ODNI), IARPA, NSA, Department of Homeland Security (DHS)), and it is the concept that most distinguishes the US from the European rhetoric and focus on QC. Economic security is more prominent among economic agencies (eg NIST, Bureau of Industry and Security (BIS), ESIX). Likewise, energy-focused agencies emphasise energy security (eg DOE). And virtually all agencies are concerned with cybersecurity in the context of QC.

Digital sovereignty, while also ambiguous at times, generally denotes a nation state's independence in relation to other states (ie external sovereignty) and its supreme authority to govern within its territory (ie internal sovereignty) in the digital space. Oftentimes, this translates to owning and/or independently operating certain digital technologies. This also often purports to storing digital data within jurisdictional boundaries.

[11] ibid.

[12] ibid.

[13] C Goujard, "Germany unveils powerful quantum computer to keep Europe in global tech race" (*Politico*, 2021) <www.politico.eu/article/germany-unveils-europes-first-quantum-computer/> (last accessed 31 August 2022).

[14] S Felix, "French research at the heart of the Quantum Plan" (*CNRS News*, 2021) <https://news.cnrs.fr/articles/french-research-at-the-heart-of-the-quantum-plan/> (last accessed 31 August 2022).

[15] ibid.

[16] A-F Pelé, "French President Details €1.8b Quantum Plan" (*EE Times*, 2021) <www.eetimes.eu/french-president-details-e1-8b-quantum-plan/> (last accessed 31 August 2022).

[17] V Booth, "Eason. Quantum computer, a sovereignty issue for France and the European Union" (*Tech News Insight*, 2021) <https://technewsinsight.com/eason-quantum-computer-a-sovereignty-issue-for-france-and-the-european-union/> (last accessed 31 August 2022).

https://doi.org/10.1017/err.2023.44 Published online by Cambridge University Press

While distinct, national security and digital sovereignty are certainly interconnected and at times mutually reinforcing. National security ordinarily seeks to maintain a nation's safety and stability regarding inside and outside threats, thereby affirming the nation's sovereignty, including in the digital spheres. Conversely, a drive for digital sovereignty is often motivated by some of the aspects of national security we outline above, though usually with more of an emphasis on economic security (note references in the above section to increasing prosperity) and comparatively less on physical security.

III. The history

How did we get to the current state, with a US emphasis on national security and an EU emphasis on digital sovereignty? It is no secret that national security is a significant emphasis in USG policy far beyond QC. This is evident in the scale of US defence investments and development. In 2021, US military expenditure amounted to $801 billion – almost 40% of the total military expenditure of the world, and nearly three times as much as that of China, who was in second place.[18] This emphasis also extends beyond military and traditional defence spheres (ie weapons and combat technologies). Intelligence and defence agencies in the USG have long been involved in (non-military) science innovation. This involvement was crystallised and catalysed in the founding of the (Defense) Advanced Research Projects Agency (ARPA) in 1958, now known as DARPA. The agency's mission is "to make pivotal investments in breakthrough technologies for national security".[19] Originally created as a response to the Soviet launching of Sputnik 1, DARPA forms and executes R&D projects in collaboration with academia, industry and government partners to expand the frontiers of technology and science far beyond immediate military requirements. From weather satellites to GPS, from drones to the recent COVID-19 vaccine, the list of science innovations in which DARPA has been involved is impressive.

In the early 1960s, computer scientist Joseph Carl Robnett Licklider was appointed as the head of the Information Processing Techniques Office (IPTO) at ARPA. During his tenure at the IPTO, it is estimated that 70% of all US computer science research was funded by ARPA.[20] (Some speculate that this was due to Cold War fears.) In an internal memorandum, Licklider outlined the challenges of establishing a time-sharing network among ARPA computers to more effectively facilitate research efforts.[21] Succeeding Licklider and building on his vision, Bob Taylor convinced the head of ARPA at the time to reallocate $1 million from a ballistic missile defence programme to fund the development of the Advanced Research Projects Agency Network (ARPANET).[22] The ARPANET became one of the first packet-switched networks implementing the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Packet-switching and TCP/IP, along with the development and expansion of the ARPANET, eventually helped realise the modern Internet.

While similarly prominent in the EU, digital sovereignty does not share a similar, long-standing government investment tradition. The political concept of sovereignty, understood as a state's exclusive and ultimate power to govern within its territory, is

[18] DL da Silva et al, "Trends in World Military Expenditure, 2021" (*Stockholm International Peace Research Institute*, 2021) <www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf> (last accessed 31 August 2022).

[19] "About DARPA" (*Defense Advanced Research Project Agency*, 2023) <www.darpa.mil/about-us/about-darpa> (last accessed 31 August 2022).

[20] K Featherly, "ARPANET: United States defense program" (*Britannica*, 2022) <www.britannica.com/topic/ARPANET> (last accessed 31 August 2022).

[21] JCR Licklider, "Memorandum for Members and Affiliates of the Intergalactic Computer Network" (1963).

[22] J Markoff, "Robert Taylor, Innovator Who Shaped Modern Computing, Dies at 85" (*The New York Times*, 2017) <www.nytimes.com/2017/04/14/technology/robert-taylor-innovator-who-shaped-modern-computing-dies-at-85.html> (last accessed 31 August 2022).

https://doi.org/10.1017/err.2023.44 Published online by Cambridge University Press

of course not novel. However, it had been of much less concern in the relatively stable post-World War era – until the rise of the Internet. The inherent interconnectedness of the Internet presented a modern need for multi-stakeholder governance.[23] The blurring of state borders in the digital space and the dominance of US companies in this space revived conversations around political sovereignty.

To be clear, digital sovereignty is not only an EU focus. For example, India has banned WeChat and Baidu over sovereignty and integrity concerns. The EU, however, emphasises it to a greater extent. While there are several factors that may have contributed to this emphasis, many attribute it to two main considerations: (1) 92% of data from the West is hosted in the USA;[24] and (2) there are no European companies in the Fortune list of Top 20 global technology companies.[25]

Citing these concerns, the German and French governments launched project Gaia-X in 2019. The project aims to establish a federated ecosystem of EU cloud providers that respects freedom, transparency and sovereignty, hoping to help Europe regain its digital sovereignty. However, by 2022, the project was considered by some to be "stuck in the concept stage" and "turning into a cautionary tale about the EU's tech ambitions".[26] Meanwhile, Amazon, Google and Microsoft continue to dominate the EU cloud computing market.[27] While some believe the project is an unfortunate misstep resulting from inflated expectations, others claim it demonstrates the impossibility of achieving complete sovereignty in the digital space.

Nevertheless, EU member governments continue to champion and fight for digital sovereignty. "Now is the time for Europe to be digitally sovereign", stated the chancellor of Germany and prime ministers of Denmark, Estonia and Finland, jointly calling for the EU to accelerate its efforts to strengthen digital sovereignty.[28]

IV. The antidote

Many existing technologies have national security and digital sovereignty impacts. For some of these – often those with important military applications – governments take more nationalistic approaches. For example, nation states usually develop their own satellites, missiles, nuclear technologies and some chemical/material tools. For others, governments are more ready and willing to foster international collaboration. For example, the International Space Station (ISS) is an international, collaborative project that has

[23] J Pohle and T Thiel, "Digital sovereignty" (2020) 9(4) Internet Policy Review <https://policyreview.info/concepts/digital-sovereignty/> (last accessed 31 August 2022).

[24] E Amiot et al, "European Digital Sovereignty: Syncing values and value" (*Oliver Wyman*, 2020) <www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf> (last accessed 31 August 2022).

[25] Fortune, "Global 500" (2022) <https://fortune.com/ranking/global500/2021/search/?sector=Technology> (last accessed 31 August 2022).

[26] H Vaske, "European cloud project Gaia-X is stuck in the concept stage" (*CIO*, 2022) <www.cio.com/article/308818/european-cloud-project-gaia-x-is-stuck-in-the-concept-stage.html> (last accessed 31 August 2022); C Goujard and L Cerulus, "Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project" (*Politico*, 2021) <www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/> (last accessed 31 August 2022).

[27] Synergy Research Group, "European Cloud Providers Double in Size but Lose Market Share" (2021) <www.srgresearch.com/articles/european-cloud-providers-double-in-size-but-lose-market-share> (last accessed 31 August 2022).

[28] H Wright, "Estonia, EU countries propose faster 'European digital sovereignty'" (*ERR News*, 2021) <https://news.err.ee/1608127618/estonia-eu-countries-propose-faster-european-digital-sovereignty> (last accessed 31 August 2022).

https://doi.org/10.1017/err.2023.44 Published online by Cambridge University Press

arguably provided greater benefit than the sum of its participating agencies.[29] Notably, the ISS relies on similar capabilities of satellite technologies but is underpinned by a much more collaborative approach. The Human Genome Project was another international, collaborative project to identify, map and sequence all of the genes in the human genome.[30]

A more recent example that falls somewhere in the middle of the spectrum between nationalistic and collaborative policy approaches is governments' approaches to addressing the COVID-19 pandemic. The virus is of at least some national security concern due to its ability to effectively imperil citizen health and thereby to compromise infrastructure and economic stability. This is the reason homeland security and border control agencies were among the earliest policy responders regarding COVID-19. Countries also have focused on technological sovereignty in vaccine and treatment development.

On the other hand, the pandemic did generate an increased level of international academic collaboration regarding COVID-19, which helped facilitate the rapid development of vaccines.[31] More academics also openly shared the results of their research through pre-prints, which helped scientists around the world accelerate their work – but also led to challenges in terms of scientific integrity.[32]

This academic collaboration did, however, drop rather rapidly. Despite the early hike, international collaboration rates around COVID-19 in 2020 were comparable to those of all research.[33] Nations also began to re-prioritise collaboration partners in light of national security concerns. The USA, for example, increased its collaboration with the UK and decreased its collaboration with China around COVID-19. The World Health Organization (WHO) noted that the rising politicisation of pandemic responses, vaccine nationalism and Member States' reluctance to trust one another greatly impeded the WHO's global response to the virus.[34]

Ultimately, COVID-19 and the additional examples described here show that nation states can indeed strategically collaborate on technologies that have great national security and sovereignty implications – and when they do, they often end up in better positions. Some researchers have shown that extreme border control policies are often unnecessary and show non-positive effects.[35] Nations that refused to cooperate with supranational efforts also seem to have fared poorly against the pandemic.[36] However, these examples also show that such collaborations are most successful when they are clearly scoped and focused on a specific goal (eg developing a vaccine, building and running a space station, sequencing the human genome) rather than a broader set of

[29] NASA, "International Cooperation" (*Nasa.gov*) <www.nasa.gov/mission_pages/station/cooperation/index.html> (last accessed 31 August 2022).

[30] National Human Genome Research Institute, "The Human Genome Project" (*Genome.gov*) <www.genome.gov/human-genome-project> (last accessed 31 August 2022).

[31] LC Druedahl, T Minssen and WN Price, "Collaboration in times of crisis: A study on COVID-19 vaccine R&D partnerships" (2021) 39(42) Vaccine 6291.

[32] C Watson, "Rise of the preprint: how rapid data sharing during COVID-19 has changed science forever" (2022) 28 Nature Medicine 2.

[33] B Maher and R Van Noorden, "How the COVID pandemic is changing global science collaborations" (*Nature*, 2021) <www.nature.com/articles/d41586-021-01570-2> (last accessed 31 August 2022).

[34] JB Bump, P Friberg and D Harper, "International collaboration and Covid-19: what are we doing and where are we going?" (2021) 372 BMJ 180.

[35] P Zhu and X Tan, "Evaluating the effectiveness of Hong Kong's border restriction policy in reducing COVID-19 infections" (2022) 22 BMC Public Health 803; Z Zhu et al, "Sustainable border control policy in the COVID-19 pandemic: A math modeling study" (2021) 41 Travel Medicine and Infectious Disease 102044.

[36] Associated Press, "WHO: Omicron makes China's 'zero-COVID' policy unsustainable" (*AP News*, 2022) <https://apnews.com/article/covid-health-china-pandemics-united-nations-c2b99ca8ce5f99f0d2b60aa6dcb8c2d5> (last accessed 31 August 2022).

https://doi.org/10.1017/err.2023.44 Published online by Cambridge University Press

policy challenges (eg harmonised COVID-19 policies, space orbit technologies, genetics research writ large).

V. The future

The development of QC will probably affect global geopolitics in significant measure.[37] So how can we apply these lessons from other fields to nascent collaboration efforts in QC, particularly transatlantic efforts? The key is understanding where US national security and EU digital sovereignty approaches can align around specific goals. Often these projects will create common, non-competitive resources that can be used equally by all countries involved (such as the sequence of the human genome and the ISS). Some ideas for such collaborations include the following.

1. A common US–EU testbed facility to validate the performance of quantum computing components

The COVID-19 pandemic has highlighted the risk of brittle supply chains. Because of QC industry being in its the early stages, its supply chain is especially underdeveloped, and often QC hardware makers must invest significant amounts of time and resources with specific component vendors in order to acquire parts that meet their needs. Many of these vendors and hardware makers are based in the USA and Europe. The US and European governments could cooperate to establish a joint testbed facility for the central validation and testing of hardware components, which would help both vendors and suppliers on both sides of the Atlantic.

2. Workforce development and exchange programmes

The USA and European countries could jointly identify specific QC workforce needs (eg electronics control engineers, cleanroom technicians, etc.) and universities/companies in the USA and Europe with outsized expertise in these fields. They could then establish a programme whereby scientists and engineers would spend one to two years working with top experts on the other side of the Atlantic, facilitated by expedited visa processing. This would not only help address specific workforce issues, but also would strengthen the web of ties between the US and European QC communities, which would probably lead to additional benefits.

3. Grand challenges

Although we can predict some of the probable application areas of QC, we do not yet have a clear idea of its most impactful specific applications. As these applications become more clear, it may make sense for governments to jointly establish international research groups focused on solving specific problems that are of general scientific interest for all countries – for example, joint databases of molecular structures or reactions modelled using quantum computers.

[37] C Ten Holter, P Inglesant, R Srivatava and M Jirotka, "Bridging the quantum divides: a chance to repair classic(al) mistakes?" (2022) 7(4) Quantum Science and Technology 044006.

https://doi.org/10.1017/err.2023.44 Published online by Cambridge University Press

VI. Conclusion

While QC is not of global health concern, it has seen similar political tensions to the COVID-19 pandemic. National security concerns have led to stricter visa policies around Chinese nationals studying QC in the USA. Chinese scientist Jian Wei Pan had to miss two conferences in the USA, including one in which he was to receive the Newcomb Cleveland Prize, due to visa issues.[38] Some believe that if such visa issues continue, Chinese scientists will prioritise their collaboration with Europe and eventually break ties with the USA. Digital sovereignty concerns have similarly led to several EU countries being hesitant to collaborate with US QC companies. Some governments will only fund and partner with homegrown QC startups. Some believe that if this reluctance to collaborate continues, EU Member States will end up with a dozen subpar QC platforms instead of a few exceptional ones. While the Member States will be sovereign over these technology solutions, they will end up worse off than if they had collaborated to generate better outcomes.

As such, QC engagement and governance present critical opportunities for governments on both sides of the Atlantic to foster constructive collaborations and accentuate shared visions, thereby bridging the national security and digital sovereignty divide.

Competing interests. The authors declare none.

[38] A Silver, J Tollefson and E Gibney, "How US–China political tensions are affecting science" (2019) 568 Nature 443.

Cite this article: A Liman and K Weber (2023). "Quantum Computing: Bridging the National Security–Digital Sovereignty Divide". *European Journal of Risk Regulation* **14**, 476–483. https://doi.org/10.1017/err.2023.44

https://doi.org/10.1017/err.2023.44 Published online by Cambridge University Press