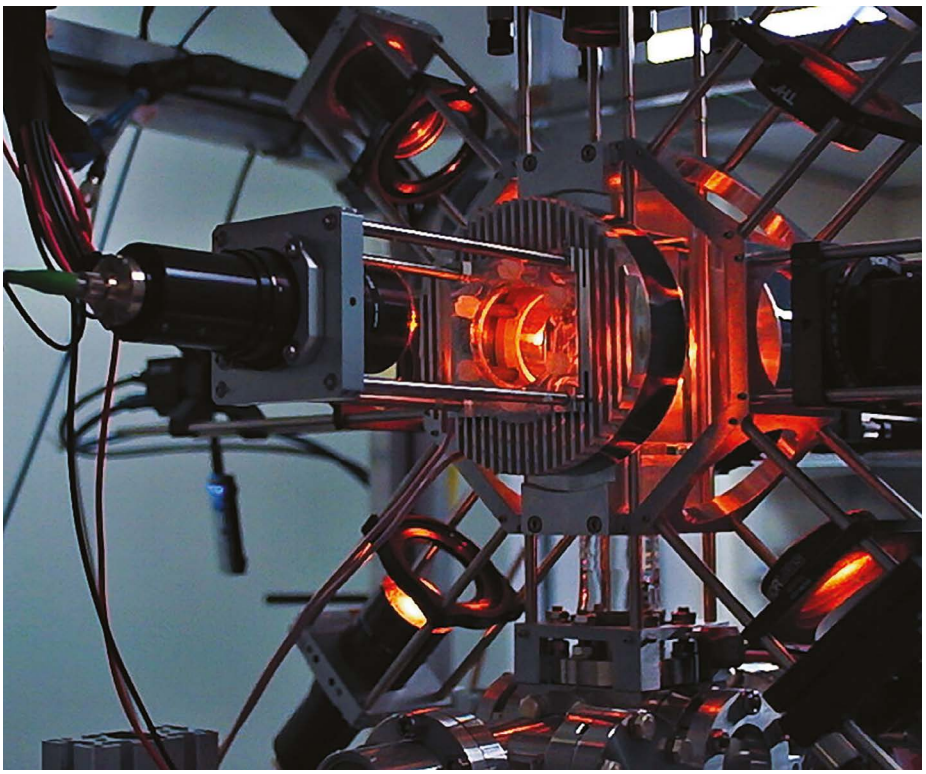
Comment

Consider the ethical impacts of quantum technologies in defence now

Mariarosaria Taddeo, Alexander Blanchard & Kate Pundyk

Quantum technologies can help to defend nations, but they also threaten human rights and values. Their design and development need ethical guidance, before it is too late.



ISABELLA MOORE/*THE NEW YORK TIMES*/REDUX/EYEVINE

A quantum sensor that measures local gravity using free-falling atoms.

Quantum technologies hold great promise for aiding national defence, by sharpening how countries collect data, analyse intelligence, communicate and develop materials and weapons. For instance, quantum sensors — which use quantum behaviours to measure forces and radiation — can detect objects with precision and sensitivity, even underground or underwater. Quantum communications systems that are resistant to jamming can revolutionize command and control.

Interest is growing globally. For example, in 2023, the US Department of Defense announced a US$45-million project to integrate quantum components into weapons systems to increase the precision of targeting. The nation also tested a quantum receiver for long-range radio communications. The UK Ministry of Defence (which funds some of our research) is investing in quantum sensors and clocks. Earlier this year, it tested a quantum-based navigation system that cannot be jammed. India's Ministry of Defence is investing in the use of quantum 'keys' to encrypt sensitive military data. China is also developing quantum capabilities for defence, including a quantum radar system that can overcome 'stealth' technology, which is designed to make aeroplanes or ships, for example, hard to detect using conventional radar.

However, as well as promises, these uses come with ethical risks[1,2] (see 'Key risks of using quantum technologies in defence'). For example, powerful quantum computers could enable the creation of new molecules and forms of chemical or biological weapons. They might break cryptographic measures that underpin secure online communications, with catastrophic consequences for digitally based societies. Quantum sensors could be used to enhance surveillance, breaching rights to privacy, anonymity and freedom of communication. Quantum algorithms can be difficult to reverse-engineer, which might make it difficult to ascribe responsibility for their outcomes (a 'responsibility gap').

"The goal is not to curb innovation, but to control and shape it as it develops."

Some of these risks are similar to those associated with the use of artificial intelligence (AI), which is also being used for defence purposes. This is good news, because it enables us to tackle the risks by building on existing research and lessons learnt from AI ethics. However, although the risks might be similar, their drivers, likelihoods and impacts differ and depend on the unique characteristics of quantum technologies.

That is why it is crucial to develop ethical governance that is focused specifically on quantum technologies. So far, defence organizations have remarked on this need — for example, in the Quantum Technologies Strategy

from the North Atlantic Treaty Organization (NATO) and the 2020 US National Defense Authorization Act. Yet, little work has been done to develop an ethical approach to governance of quantum applications in defence[1,3].

Here we begin to fill this gap, and set out six principles for responsible design and development of quantum technologies for defence. We propose an 'anticipatory ethical governance approach' – that is, to consider the ethical risks and opportunities that might arise as decisions are made, from the design and development stages to end use. This approach will allow defence organizations to put in place measures to mitigate ethical risks early, rather than paying high costs later.

Start now

The lack of research on ethical governance of quantum technologies in defence stems from these being emergent technologies with varying levels of maturity. Quantum sensors, for example, are already on the market, but other applications, such as quantum computers, are only now transitioning from the laboratory or are at an embryonic stage.

It is still unclear whether quantum technologies, once they are mature, will be small, light and power-efficient enough to meet requirements for defence use. Many such technologies require sophisticated cooling systems, and these are bulky. For example, IBM's Goldeneye cryostat – a prototype 'superfridge' designed to cool quantum computers to temperatures colder than outer space – weighs more than 6 tonnes, has a volume of almost 2 cubic metres and requires vacuum pumps and helium isotopes to run.

Thus, defence organizations are either cautious about investing in ethical analyses of technologies that are still at an early stage and might not come to fruition, or they view such efforts as premature, unnecessary and impractical. The former approach is sensible – governance should evolve with the technologies. The latter approach is dangerous and conceptually mistaken.

It rests on the 'neutrality thesis', the idea that technology itself is ethically neutral and that implications emerge only with its use, implying that no ethical governance of quantum tech is needed before it is used. This is wrong – the ethical implications of any technology emerge at the design and development stages, which are informed by ethically loaded choices[4].

For example, design and development decisions dictate whether AI models are more or less interpretable[5] or subject to bias[6]. AI governance has lagged behind the rate of development of those technologies, raising a host of issues that policymakers are only just beginning to grapple with, from who has access to codes to how much energy AI systems use.

As scholars and policymakers have become more aware of the real risks and potential that AI systems pose, most now agree that ethical analyses ought to inform the entire AI life cycle. Those eyeing quantum technologies, especially in defence, should heed those lessons and start to weigh the ethical risks now.

Successful governance hinges on getting the time right for policy interventions. This is often portrayed as a dilemma: if governance comes too soon, it might hinder innovation; if it comes too late, risks and harms might be hard to mitigate[7]. But this binary view is also mistaken. The timing of tech governance is analogue, not binary. Governance should accompany each moment of the innovation life cycle, with measures that are designed to support it and that are proportionate to the risks each moment poses.

"We recommend setting up an independent oversight body for quantum technologies in defence."

The goal is not to curb innovation, but to control and shape it as it develops, to elicit its good potential while ensuring that this does not come at the cost of the values underpinning our societies.

Here, we outline six principles for responsible design and development of quantum technologies in defence. The principles build on those outlined in the literature for responsible innovation of quantum technologies[1,2], human rights and democratic values, ethical conduct in war (just war theory) and lessons learnt from AI governance.

Develop a model for categorizing risks

Any defence organization that funds, procures or develops quantum technologies should build a model for categorizing risks posed by these technologies. This will be difficult owing to the dearth of information around the risk types, drivers and uses of quantum tech[8].

Thus, for now, we suggest categorizing risks on a simple scale, from more to less predictable – as 'known knowns', 'known unknowns' or 'unknown unknowns'. Defence organizations can use these to prioritize risks to address and build strategies for mitigating them. The costs of ethical governance would thus be proportionate to the risks and to the level of maturity of innovation, and justifiable.

For example, quantum sensing poses known known risks for privacy and mass surveillance, which can be tackled now. Defence organizations might consider when and where these risks might occur, and the magnitude of their impact. Criteria might be set in the next few years for the design, development and use of these technologies to ensure that any privacy breaches remain necessary and proportionate. For example, access to them might be tracked or restricted for states that are known to violate human-rights laws.

At the same time, an organization might begin focusing on harder-to-assess known unknown risks for more immature technologies. Risks concerning the supply chain for quantum technology are one example. Such technologies require specific materials, such as high-purity helium-3, superconducting metals and rare-earth elements, which are limited in availability and often sourced from geopolitically sensitive regions. Risks concern access to these resources and the environmental impacts of their extraction, as well as strategic autonomy, should the supply chain be disrupted because of political instability, export restrictions or supply-chain breakdowns.

Mitigating these risks might require redesigning the supply chain and allocations of crucial resources, as well as finding sustainable solutions for mining and processing. Governments' geopolitical postures should account for these needs and avoid disrupting commercial relations with strategically important partners. Implementing these measures will take time and effort, underscoring the need to address the ethics of quantum technologies now, rather than later.

By their nature, the unknown unknown risks are difficult to predict, but might become clear as quantum technologies mature and the ethical, legal and social implications become evident. The main idea of our approach is to act on them as early as possible.

Defence organizations should not run risk-categorization models by themselves[9]. Experts and other parties with relevant interests should be involved, to ensure that the scope of modelling is broad and information is accurate and timely. The process should include physicists and engineers familiar with how quantum technologies work, as well as national defence and security practitioners. It should also encompass specialists in international humanitarian law, human rights, ethics of technology and war, and risk assessment.

Counter authoritarian and unjust uses

Malicious uses of quantum technologies pose threats, which need to be identified and mitigated. Their uses need oversight, and a compelling and democratic vision for innovation and adoption of these technologies should be developed.

For example, some state actors might use quantum computing to break encryption standards for repressive purposes, such as monitoring and surveillance, or to increase the destructive power of weapons systems. The combination of quantum technologies and AI also needs particular attention. Quantum computing could enhance the performance

KEY RISKS OF USING QUANTUM TECHNOLOGIES IN DEFENCE

Type	Risk	Example
Known knowns	Privacy	Quantum computers could break encryption standards, resulting in unauthorized access to sensitive data.
	Security	Breaking of encryption standards could reveal government secrets, with national security implications.
	Oversight	Quantum algorithms could be difficult to reverse-engineer, hindering transparency and auditing.
	Sustainability	Energy-intensive computing will have a negative impact on the environment.
Known unknowns	Just war	The synthesis of new molecules might create chemical or biological weaponry that could breach just-war requirements.
	Compound risks	Quantum tools will exist in an ecosystem with other technologies, such as artificial intelligence, compounding the risks posed by those technologies (including undue discrimination, responsibility gap and limited transparency).
	Strategic autonomy	Quantum tools will rely on specific materials and hardware that might not be available domestically. This could create a dependence on exports from another country, undermining strategic autonomy.
	Security	Quantum sensors could undermine the invulnerability of submarines and weaken nuclear-deterrence regimes.

of AI, exacerbating its existing ethical risks, such as bias, lack of transparency and problems with the attribution of responsibility. At the same time, AI can help to detect patterns in data collected through quantum sensors, increasing the risks of privacy breaches and mass surveillance.

Implementing this principle means considering strategies to limit the access of authoritarian governments to quantum technologies. This would be consistent with existing regulations for the export of technologies used for surveillance, such as the EU's Dual-Use Regulation Recast.

Ensure securitization is justified and balanced

Development of defence and security technologies takes place in a geopolitically competitive environment in which states, particularly adversarial ones, try to outcompete each other for strategic advantage. There might be benefits to global competition if it drives innovation. But as quantum technologies are increasingly 'securitized' — identified as a national security priority — states might limit access to relevant research and technologies.

Where possible, such measures ought to be balanced with, and not undercut, the potential global benefits of quantum technologies. This means recognizing that, although the securitization of certain technologies is a regrettable but necessary response to geopolitical dynamics in some cases, it is not always necessary.

Policymakers should be mindful of the possible negative consequences of a securitization approach to quantum tech, learning from the securitization of AI. For example, the development of AI technologies has been played out as a race. As AI has matured, race dynamics and isolated and protectionist policies adopted by countries such as the United States and China have proved to be detrimental to AI's development, adoption and mitigation of risks.

Particularly in defence, it has become clear that leveraging the full potential of AI requires sharing capabilities — fostering interoperability, shared standards and testing systems in alliances, for example. This is why, in 2022, NATO established the Data and Artificial Intelligence Review Board to develop for its allies "a common baseline to help create quality controls, mitigate risks and adopt trustworthy and interoperable AI systems". Similar connections will be needed should quantum technologies become securitized, as seems likely.

Build in multilateral collaboration and oversight

Defence organizations ought to continue to work with, in and through international forums and organizations to establish multilateral regulatory frameworks and guidelines to govern quantum technologies. Because the harmful effects potentially arising from such technologies will cross borders, states should not govern them in isolation.

We recommend setting up an independent oversight body for quantum technologies in the defence domain, similar to the International Atomic Energy Agency. As with AI, such measures need to be taken well before the widespread adoption of quantum technologies.

Put information security at the centre

Defence organizations should seek to reduce the risks of information leaks surrounding sensitive quantum technologies. This means emphasizing information security throughout the quantum technology life cycle. This must be done before the technologies mature, to mitigate the risks of cyberattacks that aim to 'harvest now, decrypt later'.

Promote development strategies for societal benefit

As for nuclear power and AI, quantum technologies are dual-use. The defence establishment should develop strategies to support civilian applications of quantum technologies to address global challenges in areas such as health care, agriculture and climate change.

This is another lesson from AI. China's successful harnessing of AI has been driven in part by a 'fusion' development strategy, in which cooperation between civilian research organizations and defence allows the pooling of resources[10]. At the same time, collaboration with civil society can help to demystify quantum tech, fostering trust between the public and national defence and security organizations as innovation progresses.

The anticipatory ethical governance we propose here demands investments in time, funding and human resources. These are key to steering the quantum transformation of defence in line with societal values. Ignoring the need for ethical governance now to sidestep these costs is a path to failure — addressing harms, correcting mistakes and reclaiming missed opportunities later on will be much more costly.

The authors

Mariarosaria Taddeo is professor of digital ethics and defence technologies at the Oxford Internet Institute, University of Oxford, UK, a DSTL ethics fellow at the Alan Turing Institute, London, UK, and a member of the AI Ethics Advisory Panel to the UK Ministry of Defence. **Alexander Blanchard** is senior researcher at the Stockholm International Peace Research Institute, Sweden. **Kate Pundyk** is research assistant at the Oxford Internet Institute, University of Oxford, UK.
e-mail: mariarosaria.taddeo@oii.ox.ac.uk

1. Kop, M. *et al. Quantum Sci. Technol.* **9**, 035013 (2024).
2. Gasser, U., De Jong, E. & Kop, M. *Nature Phys.* **20**, 525–527 (2024).
3. Krelina, M. *EPJ Quantum Technol.* **8**, 24 (2021).
4. Floridi, L. *Philos. Technol.* **36**, 60 (2023).
5. Rudin, C. *Nature Mach. Intell.* **1**, 206–215 (2019).
6. Tsamados, A. *et al. AI Soc.* **37**, 215–230 (2022).
7. Collingridge, D. & Reeve, C. *Science Speaks to Power: The Role of Experts in Policy Making* (Pinter, 1986).
8. McDowell, I. *J. Public Health* **30**, 219–223 (2008).
9. Taddeo, M., Blanchard, A. & Thomas, C. *Philos. Technol.* **37**, 42 (2024).
10. Roberts, H. *et al. Inf. Soc.* **39**, 79–97 (2023).

M.T. declares competing interests; see go.nature.com/4f8vs9n for details.

Disclaimer: the views expressed here are those of the authors and not of the UK Ministry of Defence or the UK government (see Supplementary information at go.nature.com/4f8vs9n for full disclosure statements).