Walker-Munro *EPJ Quantum Technology* (2025) 12:136
https://doi.org/10.1140/epjqt/s40507-025-00448-w

EPJ.org

EPJ Quantum Technology

RESEARCH Open Access

Moving beyond "dual use": quantum technologies and the need for new research security paradigms

Brendan Walker-Munro[1,2*]

*Correspondence:
brendan.walker-munro@scu.edu.au
[1]Faculty of Business, Law & The Arts, Southern Cross University, Coolangatta, Australia
[2]National Security College, Australian National University, Canberra, Australia

Abstract

The development of quantum technologies has been labelled the next revolution in human scientific and industrial endeavour. Because quantum technologies have potential military, defence, intelligence and law enforcement applications, there has been a great deal written about quantum as a dual-use technology; however, most of the research on quantum technologies is performed in higher education environments that lack robust security cultures. This theoretical paper generates a basic overview of the impact that quantum technologies are having, and could have, on how technologies are secured in university and higher education settings ("research security"). This paper then analyses the implications of quantum technology from the perspective of research security, arguing that a new paradigm is needed that moves beyond the dual-use binary. Specific applications of quantum technology are used as examples of challenges to the definitions and explanations of dual-use, and several alternatives are proposed and summarised.

Keywords: Dual-use technology; Quantum technology; Quantum security; Research security; National security; Higher education

1 Introduction

Technology is a key enabler of political, military, and economic power [1], and as such is being pursued by both established hegemons such as the United States and China as well as the so-called middle powers like India, Japan, Brazil and Australia. To protect their foreign policy, national security and economic interests in technology, these (and other) nation-States have been employing a wide variety of legal and policy responses to discourage illicit or malign use or diversion of critical tech. This has spurred debate about the notion of technologies carrying both military and civilian end-uses, and their definition as so-called "dual-use technologies" [2–5].

One of the most predominant emerging technologies to have assigned the dual-use moniker has been quantum technology: those technologies arising from the second quantum revolution and involving the manipulation of individual quanta to achieve mathematical, measurement, cryptographic, sensing or computational power that has not previously

Springer

been observed in human advancement [6]. Unlike the technologies of the first quantum revolution – which commenced with splitting the atom and resulted in nuclear power, lasers, and semiconductors (all of which remain dual-use technologies) [7] – new quantum technologies are not strictly new capabilities in or of themselves but have a fundamentally disruptive capacity that transform existing capabilities; see, for example, [2, 4, 5].

Most quantum research worldwide is conducted in higher education environments [8] (though there are some domains where the private sector has outpaced both scale of investment and number of researchers involved [9]). These institutions usually do not culturally prioritise or embed strong security practices. That is a significant problem, given that countries are more likely to use illicit and quasi-licit strategies like espionage and intellectual property theft to advance their research and economic competitiveness, especially in relation to dual-use technologies [10, 11]. In response, most nation-States have domestically enacted measures to protect academic research from national security threat ("research security"), but as an academic discipline, much remains unsaid about what research security is or how it is best pursued. With potential applications for quantum technology in military, defence, and security contexts [6], quantum is a domain ripe for the exploration of research security paradigms.

This paper uses quantum technology as a case study to argue that dual-use as a terminology lacks utility in protecting academic research. I propose, and defend, a move beyond that term, especially in the context of research security. Given that every sub-field of quantum technology has a potential intelligence, security or defence utility, discussing regulatory policy is impossible using the dual-use technology lens. Theoretically, taxonomic lists which rely on distinguishable criteria (defining what *is* or *is not* "dual-use") should enable participating nation-States to execute a flawless, contiguous and unbroken regulatory framework around such technologies. In practice this is not the case. Quantum technology as a case study thus exposes long-standing structural problems with the definition of "dual-use technology". Consequently, I argue that research security responses that prioritise dual-use technology – whether in respect of quantum or elsewhere – lack nuance, efficacy and efficiency.

It is not intended that this paper present a fully developed and robust replacement, but instead to show the benefits of some proposals which move beyond dual-use as a policy framework. To that end, three proposals are presented here in the alternative, to assist in moving debates beyond the dual-use dichotomy, and how research security practices might apply to an amended framework. It is also not intended that this paper form a holistic assessment of the current state of quantum technology research and possible outcomes. That has been done elsewhere; see, for example [6, 12, 13].

This paper comprises six sections. Section 2 introduces necessary terms used throughout the paper, before Sect. 3 introduces four core technological groupings in which quantum advancements are challenging dual-use technology classifications. Section 4 builds on Sect. 3, identifying the implications of quantum technology for research security and how dual-use technology remains an unhelpful term for assessing technological research and development in quantum. In Sect. 5, some potential alternatives to dual-use technology are presented from the literature, including some areas for potential future research that could yield benefits for research security practitioners as well as academics in quantum research settings. Section 6 concludes.

2 Definitions

Quantum technology is a large and ever-expanding field, but for the purposes of this paper it is defined as follows [6]:

> *Quantum technology* (QT) is an emerging field of physics and engineering based on quantum-mechanical properties – especially quantum entanglement, quantum superposition and quantum tunnelling – applied to individual quantum systems, and their utilisation for practical applications.

QT is about *application*; it is an umbrella term for a variety of technologies in different stages of development, though its boundaries are mostly vague and sometimes arbitrary. QT can also be an enabler of other forms of technology, where it does not specifically create new types of functions or capabilities but expands and improves existing capabilities by orders of magnitude (one can readily see this from the appendage of the prefix "quantum" to a wide array of existing technologies; see, for example [6, 10, 13–15]). It is important to note that most QT is still at a fundamental stage of research and development, with a substantial portion of public reporting adding to hype and sensationalism which has overplayed some capabilities and overshadowed others [12]. That said, if even some of the theorised capabilities are realised, they could potentially be disruptive to existing means, methods and mechanisms of warfare, intelligence, peacekeeping and law enforcement.

> *Dual-use technology* refers to fields of research and development with potential to generate knowledge or technology that has the potential to be exploited to purposely cause harm and threaten public health or national security, although the research itself is conducted for beneficial purposes [16].

The very definition of dual-use technology remains highly contested and includes realms of research and development linked to military or defence capability, illicit proliferation of arms or nuclear weapons, the development or design of Weapons of Mass Destruction (WMD), or the interference with internationally recognised human rights [2–5, 17]. Equally, acceptance of and adherence to dual-use definitions varies substantially depending on the source of the definition's production, whether it be multilateral arms control agreements (Wassenaar Arrangement, Missile Technology Control Regime (MTCR), Australia Group, etc.), international legal instruments (i.e., UN General Resolution 1540 (2004), Arms Trade Treaty, Biological Weapons Convention) or domestic or municipal arms control laws (US International Trafficking in Arms Regulation (ITAR), EU Regulation 428/2009) [2, 17, 18].

At the same time, dual-use is a definition with a problem, being the ever-diminishing gap between military and civilian end-uses posed by an enabling technology like QT [19]. There have been attempts to narrow down the application of dual-use so that it does not capture every conceivable application in each field, but these are equally imperfect. For example, dual-use research of concern (DURC) has emerged in relation to the life, biological and medical sciences to describe a subsection of research involving conferring microbes and pathogens with characteristics (such as enhanced transmission or increased viral reproduction) which do not occur normally and could pose risks relating to the proliferation of biological weapons [20]. However, DURC suffers from a similar lack of consensus over meaning [14], as well as a body of researchers who fundamentally disagree on both the threshold at which DURC should apply, and the regulatory controls that should be imposed on research which finds itself classified as such [21–23].

> *Research security* refers to a set of actions taken by governments or other public or funding bodies, usually in collaboration with academia and research institutes, to safeguard against the risk of undesired technology transfers, interference in or misuse of research, and threats to research integrity [18].

The definition of research security is like dual-use, highly contested, and its relative level of acceptance to any given field of research depends entirely on its originating source. The European Commission references technology transfer and malign influence on research but also touches on acts which suppress or infringe rights conferred by other EU treaties (which are absent from other jurisdictions) [24]. The US and Canadian definitions, promulgated by the National Science Foundation [25] and Public Safety Canada [17] respectively, are more unilateral and reflect nation-State concerns around the protection of not just national security, but also economic competitiveness and foreign policy. In the QT space, the high watermark in research security appears to be the establishment of specific law enforcement entities to protect QT investment, such as the FBI's Quantum Information Science Counterintelligence Protection Team (QISCPT) [26] or Australia's Technology Foreign Interference Taskforce (TFIT) [27].

Problematically, research security also faces challenges imposed by their cleavage to nation-State narratives. For example, the Netherlands government is currently courting controversy by proposing a background screening regime that would apply to every foreign-born researcher working on sensitive technologies (including QT) [28]. In France, the "Protecting the Nation's Scientific and Technical Potential" (PPST) policy has been a strong feature of French law since 2012 but is even now needing to be updated to meet the obligations imposed by the European Commission [29].

3 Current quantum technologies; or, why dual-use doesn't work

The fundamental prospects (and hazards) of QT arise because they involve manipulation of the most basic level of subatomic construction, such as quantum and qubits [12]. The established properties of quantum mechanics observable in real-world particles and their various interactions have given rise to a host of new concepts in QT [13, 30, 31]:

- **State**: refers to any "possible state that a quantum mechanical system may exist, which contains all the information of the system" (such as energy, spin or polarization) at a point in time [31].
- **Superposition**: describes that a quantum system exists in any state as a superposition of different eigenstates, until the quantum system is measured (popular culture has seized upon the thought experiment used to explain superposition of Schrodinger's Cat, the ill-fated feline sealed in a box with a poison flask who is both alive and dead until the box is opened [32]).
- **Entanglement**: the establishment of a connection between two or more particles in a quantum system, such that manipulation of the state of one will affect all the others in the connection, irrespective of the distance or barriers between them.
- **Collapse**: As a corollary of the above two concepts, observing either a superpositioned quantum system or an entangled pair will fundamentally alter its quantum state (i.e., the system or pair's energy, spin or polarization) and can potentially result in the collapse of the system or pair [13].

These fundamental concepts of QT can present unique ways of observing, storing, communicating, transmitting or receiving, and processing information. Thus, it exposes the

first challenge to dual-use technology regulation – that of barriers to entry. When dual-use technology was first conceptualised, it was in the domain of countering nuclear weapons proliferation and applied usually to uranium enrichment and reprocessing [14]. These technologies could only be useably deployed by highly qualified individuals with significant financial backing, required highly protected 'precursor' materials (i.e., both nuclear fuel in the form of uranium or plutonium as well as shaped explosives to commence the nuclear reaction), and needed advanced computing power to calculate highly complex equations. Of course, technological innovation often involves 'trickle down' effects where the novel and world-changing eventually becomes run-of-the-mill [14] – but this does not mean that today nuclear weapons can be manufactured in backyard laboratories. QT does not specifically engage with barriers to entry; quantum states exist everywhere, so any nation-State with a sufficiently resourced physics laboratory can undertake QT research and development. One need only examine the scope and scale of investment in quantum research around the globe to be convinced of its ubiquitousness [8, 33].

The second limitation of dual-use in respect to QT flows from analysis of export controls, i.e., those laws that were enacted to prevent proliferation of nuclear weapons post-World War II [14, 34]. Though export controls clearly limited that weapon development to a handful of nation-States (and a counterproliferation effort, especially in relation to Iran, continues today [35]), export controls did nothing to limit countries that *already had* nuclear weapons technology. In effect, export controls protected the monopoly of nuclear-enabled States, keeping those technologies to themselves and out of the hands of geostrategic competitors [34]. In other words, the notion of what is a given dual-use technology could just as easily be described as 'whatever technology the State that owns it wants to call dual-use'. Diffusion of QT around the globe has eroded any notion of a strategic monopoly by a handful of nation-States that might use the term "dual-use" to protect competitive advantage [8, 33].

Like many other forms of technological-based research, QT invokes issues of research security. This is because the requirement to protect research that has dimensions of national security and competitiveness (especially in a higher education setting, which lacks a robust security culture) comes into tension with the international academic community's standards of open publication, freedoms of speech and expression, and collaboration without borders [18, 36–40]. The emergence of new applications for (and indeed highly theoretical conjecture around) technologies like QT can also outstrip the efforts of regulators to subject them to legal constraint, forcing regulators to make limited attempts at challenging malicious behaviour [3, 41–44].

Individual forms of QT also challenge the dichotomous nature of dual-use, not just because of QT's clear national security implications, but also for other reasons deeply connected with the legal and policy motivations behind technology regulation. As an enabling technology that is increasingly democratized, for every conceivable benign use of QT, there is a malign use that could be exploited by nation-States or non-State groups to cause harm, damage property, and threaten the lives or safety of the broader public [12, 33]. As Johnson [45] makes irresistibly clear: "[e]ach application of quantum technologies has dual-use characteristics, contemplating both socially beneficial and nefarious uses grounded in the same technological platform". QT may be "inherently neutral in design but acquire distinct characteristics based on their application. . . the same technolo-

gies that drive economic and social progress can also enable conflict, destabilization, and human rights violations" [3].

Also, because much of the forecasted utility of QT remains hypothetical or experimental, it is nearly impossible to determine whether a national security use-case for any given capability is based on hyperbole versus verifiable science. Existing export controls that apply to QT limit technologies based on suggested characteristics or metrics that are either arbitrary, ill-suited, or otherwise capture capabilities which existing technologies do not have (and which are by all accounts "impossible" at our currently technology level [46]). That said, the aggression with which nation-States are pursuing military or intelligence applications of QT [6, 12, 13] suggest that these States do not foresee any shortcomings in the utility of that technology. A State that perfects a given QT offering a military or intelligence advantage is unlikely to squander that opportunity simply because of pragmatic concerns around deploying it; the State will merely get on with the job of getting that technology in the field as fast as possible. Indeed, the Russian invasion of the Ukraine – featuring near-daily unconceivable instances of militarisation of off-the-shelf technologies – stands as testament to the inventiveness of armed forces given an incentive to overcome the technological supremacy of an opponent [47].

3.1 Quantum communication and cryptography

The principles of quantum entanglement and collapsing quantum states led to a branch of QT aligned with improving or enhancing the security of communications; and conversely, with the interception and decryption of such communications. Indeed, scholars have begun warning about the imminence of "Q-Day" – being the day on which quantum computing is capable of breaking RSA-2048, the most widely used cryptographic cypher [6] – with some suggesting that Q-Day could be upon us in as little as two years [48]. At the same time, QT offers the possibility that encryption could be 'uncrackable', or at least 'perfected', because any attempts to observe or interfere with information stored in a quantum state results in its collapse and reveals the intrusion attempt [12].

Unsurprisingly, the application of QT to cryptography has substantial national security implications, when everything from State secrets to banking information could become compromised [6, 12]. Governments have already begun to test, verify and implement 'post-quantum cryptography', algorithms suggested to be resistant to quantum computing [49, 50]. Suggestions that Q-Day could be sooner than anticipated fuelled speculation that global governments would 'harvest now and decrypt later' when Q-Day arrives [50], whilst protecting their own secrets in traditional storage means (i.e., paper files, air-gapped servers) to prevent quantum decryption [51].

Further, because quantum entanglement seemingly disregards both distance and barriers, QT has the potential revolutionize communications technologies (including for military and intelligence purposes). China has successfully tested quantum exchanges from Beijing using a satellite network to communicate with Shanghai, Vienna and Stellenbosch (South Africa) [10, 52]. Although current QT involves communication of quantum states using photons in fibre-optic cables, future mechanisms for quantum communication are unlikely to rely on cables to transmit quantum states. QT also permits communication with objects underwater (at great depth and largely undetectably) and in environments degraded by electromagnetic phenomena, a significant benefit for numerous military capabilities [6, 12, 13].

Dual-use technology breaks down as a useful dichotomy for quantum communication and cryptography because cryptography will always be a feature of regulated trade between nation-States: whether this is because of the ubiquitousness of information technology, the need to protect national security information whilst degrading the capability of others to do the same, or the need to protect the wealth of personal and sensitive data that modern society transfers across digital networks [2]. Further, the power in describing dual-use technologies arguably comes from the ability to distinguish between (and therefore proscribe) which technologies should be subject to more intrusive oversight and scrutiny. After all, research and development into technologies which are *not* dual-use are usually subject to much lower (if any) regulatory standards [2, 14, 16, 18]. Because QT enables both *anticipatory* responses (i.e., harvesting information ahead of Q-Day/moving information to offline storage methods) as well as *reactive* responses (i.e., post-quantum cryptography), it will inherently *always* be a dual-use technology and labelling it as such produces no tangible benefits.

3.2 Quantum computing and simulation

The development of semiconductors led to the computing revolution of the late twentieth and early twenty-first century, where computing operations wholly depended on the state of 'bits', i.e., a binary representation of either 0 or 1. However, because of quantum superpositioning, a quantum state can exist in every possible state simultaneously, leading to both an exponential increase in standard computing power [6] as well as the contemplation of types or classes of calculations currently impossible by even the most modern computers [12]. As an example, Shor's algorithm is widely used as a test of quantum computing power because it would take 100 ordinary computers around 10,000 years to solve a similar mathematical problem [53] and is suggested to demonstrate when the technology has reached 'quantum supremacy', i.e., solving a problem infeasible for a normal computer [6].

Quantum computing displays potential to reform and enhance every aspect of computing in society, including in military, security and intelligence fields [6, 12, 45]. As Krelina observes, quantum computing could allow for "computational advantages for processing complex intelligence data… [and] enhance sensor fusion, target identification and decision making at speeds and scales not currently achievable with classical systems" [13]. Equally, Johnson [45] states that quantum computing could threaten computer and communications security, accelerated forms of surveillance, or even tools of censorship or repression in the name of "national security".

However, quantum computers suffer from substantial challenges in deployability not presently relevant to their ordinary counterparts – qubits 'decohere' (i.e., lose their information state) faster [10], whilst quantum computers themselves usually require massive cooling apparatus or complex support infrastructure like lasers or magnetometers [13], and can be thrown off by environmental interferences like vibrations or temperature [54]. Error accumulation, a phenomenon easily corrected in ordinary computers, also becomes significantly more complex to avoid collapsing quantum states [10]. Further, the actual integration of quantum computers into a militarily relevant platform is yet to be realised.

This has led to developments in quantum computing such as hybridised computing structures, where classical or ordinary semiconductor computers are employed in conjunction or tandem with quantum computers [15]. Essentially a 'best-of-both-worlds' so-

lution, a quantum computer would thus perform tasks amenable to high power and repetitive iteration, whilst the classical computer would ameliorate issues such as error detection and decoherence of qubits. However, doubling the computing capability does not just double the infrastructure and resource cost – it increases it by orders of magnitude [50, 54]. There are also suggestions that because ordinary and quantum computers operate on such fundamentally different operating premises (i.e., bits vs qubits), that there will be a gulf formed between the two systems of calculations which one computer simply cannot communicate to the other [12, 50].

Where then does the notion of dual-use technology apply in the realm of quantum computing and simulation? Many of the same criticisms for applying dual-use technology in quantum communication will apply here, so rather than repeating them it is more useful to consider potential *outcomes* of the use of QT in computing and simulation domains. For example, the use of a quantum computer to calculate missile flight paths or troop or submarine deployments [13] is very clearly of greater national security implication than one simulating weather patterns for flood or fire risk, or optimizing financial models for investments in the stock market [54]. Nonetheless, countries (including the EU) have rushed to prohibit or regulate the export of quantum computers that notionally would be capable of achieving calculation or processing speeds which are currently impossible to realise and may never actually be achievable in reality [46].

Yet again, we can see how the idea of regulating or scrutinizing dual-use technology falls apart in the domain of QT. Firstly, having the kind of fidelity to know the precise outcomes for which any given quantum computing system is being deployed is beyond the surveillance capabilities of most governments [55], and demanding transparency of research could potentially trigger intellectual property and commercial confidence concerns [56]. Secondly, there are use cases for QT in simulation where the differentiation between benign and malign use is razor thin – one State's use of quantum to predict molecular structures for antibiotics or drugs is another State's way to develop chemical or biological weapons [6, 12, 32].

3.3 Quantum sensing and metrology

QT also has applications in the fields of sensing and metrology, where the measurement of physical characteristics such as electromagnetic radiation or magnetic anomalies – radio transmissions, and hidden or stealth targets (such as fighters or submarines) – is military useful [13]. One such example is the quantum radar, which is suggested to use entangled photons to annul stealth technologies whilst also avoiding electromagnetic jammers [6]. However, both empirical and theoretical technical assessments suggest that quantum radar will remain the domain of science fiction for the foreseeable future [57]. QT is also suggested to render some existing technologies in this domain obsolete. Quantum clocks will eventually replace digital variants, enabling greater precision in military and intelligence operations, whilst quantum navigation is suggested to eventually replace reliance on the Global Positioning System, which requires both satellite networks and an uncontested electromagnetic environment to function [10, 12].

There are also more sceptical views of the national security implications arising from deployment of QT which are yet to be fully explored. As one such example, surveillance technologies supplemented by QT are more likely to be capable of decrypting and interpreting current events protected by standard forms of encryption, increasing the change

of a phenomenon known as 'turnkey tyranny' (involving a potential future where an autocratic or despotic ruler maliciously uses the surveillance environment established, for all good intents and purposes, by a previously elected democratic institution: see [55]).

From that perspective, there are several aspects of quantum sensing and metrology that will challenge the paradigm of dual-use technology. Given that QT in sensing and metrology has already entered the market – atomic clocks have been around for at least half a century, and the 1964 Mariner IV mission to Mars carried a quantum sensor [33] – this branch of QT is widely predicted to have the most immediate impacts on national security [58]. However, it does so at a time when most nation-States lack domestic regulatory frameworks for QT [8], and an international treaty or binding agreement through consensus appears incredibly unlikely [41, 59]. Further, the precise nature of national security implications which might otherwise trigger a dual-use technology classification may be absent from current deployments. The impending Q-Day for cryptography [48, 51] and "quantum supremacy" for quantum computing [6] demonstrate similar challenges for dual-use as a concept in QT; effectively, crystallisation or realisation of the threat to national security occasioned by the dual-use technology comes too late to be of any protective utility.

3.4 Quantum materials and metamaterials

The final category of QT which poses national security challenges – whilst also challenging the dichotomous nature of dual-use technologies – can be seen in recent advances in materials processing and metamaterials development. QT offers the ability to confer unique properties to standard materials, or to create entirely bespoke materials with no natural analogues [60]. This research has led to suggestions that traditional materials could be given incredible capabilities such as invisibility to traditional detection methods or ultra-high tolerance [6], integrated information storage [61], through to the development of largely unspecified 'exotic weapons' [62].

QT has the potential to comprehensively shift our understanding of how matter is (and might be) ordered and composed – and for more than just national security reasons – because all materials must be explained by quantum mechanics. For example, the US Defense Advanced Research Projects Agency commenced the Electronics Resurgence Initiative in 2021, aimed to use quantum materials to displace US reliance on Chinese rare earths and critical minerals in the technology sector [62]. Materials science may move from the predominantly silicon-based (i.e., semiconductors) industry of the past fifty years, to one where carbon nano-materials take prominence [63]. The national security implications of QT in this domain are not difficult to identify – in fact one of the earliest incidents of university-based espionage involved the alleged theft by Chinese doctoral student Ruopeng Liu of metamaterials research from the laboratory of Professor David Smith at Duke University in 2009 [64].

The challenge to dual-use technology definitions in relation to quantum materials becomes even more complicated because the very definitional frame of 'what' a technology is or does in relation to quantum materials begins to break down completely. Quantum metamaterials have suggested capabilities far beyond ordinary materials, such as invisibility from traditional sensing [60] or harvesting energy from surrounding quanta [63]. Is a piece of fabric that can detect hidden soldiers on the battlefield [65] a sensing technology, a military garment, both or neither? What about a paperweight that can detect the miniscule perturbations in the Earth's magnetic field produced by ballistic missile submarines [65]?

Blending of existing technologies – such as 'cyberbiosecurity' to describe converging lines of research in cybersecurity, biological and life sciences [66], or the slightly preposterous-sounding 'bio-nano-cyborg' [67] – may also soon seen the appendage of 'quantum' to their name, making the parameters of what the technology does even more nebulous and difficult to define with precision [6, 12, 13, 50].

Given the above considerations, I argue that we have reached a technological plateau where the appellation of "dual-use" to QT is in fact pointless – where even a toaster can have a dual-use potential [68, 69] – such that in order to fulsomely protect emerging technologies like QT whilst sustaining innovation, a new viewpoint is needed.

4 Quantum implications in research security; or, why dual-use still doesn't work

The precise parameters by which QT will disrupt research security is not yet fully known; however, it is reasonable to assume that QT will occupy the same space as other forms of disruptive technologies with national security dimensions such as DURC [14, 20], artificial intelligence [39] and hypersonics [40]. Current literature around research security suggests that the dual-use paradigm remains a common touchstone for both institutional- and national-level governance frameworks [18, 39, 70–72], even though the challenges to the dual-use paradigm are well documented [2, 50, 73, 74]. The following sections will again demonstrate the lack of utility of the dual-use technology paradigm for QT, this time from the perspective of research security measures as functions of export control, economic competitiveness and foreign policy.

4.1 Quantum, research security and export controls

In the space of managing national security risks to higher education research, export controls (usually constituted by governmental screening of proposed exports of military-related technologies and equipment) have long played a significant role [1, 34, 71, 75]. Although there have been developments in domestic laws designed to exempt 'fundamental' research from usually draconian arms proliferation prohibitions, even the precise parameters of what research ought to be considered fundamental remains contested [39, 76]. Loopholes in even most carefully crafted of research security regimes also exist, such as the 50% corporate ownership threshold for the US Bureau of Industry and Security which is currently being circumvented and subverted by Chinese tech companies [77]. Further, export controls are increasingly being mobilised to protect economic interests and incentivise domestic producers, often to the detriment of foreign competitors and research participants (this overlap will also be dealt with in the next section); see, for example [78, 79].

Export control regimes routinely incorporate dual-use technology as a relevant metric for the application or capture by laws designed to limit arms proliferation. For example, the EU [2, 72, 80–82], US [39, 80], Canada [17, 81, 83], Australia [18, 76], New Zealand [84, 85], and Japan [75, 85, 86] all use different definitions of dual-use and do not specifically meet with agreement on any one particular element (save for general proscription of military use and/or breaches of international law such as war crimes, arms proliferation or terrorism). The implication for a lack of consensus for dual-use technology means that different jurisdictions will have different regulatory thresholds, reporting obligations, compliance/permit processes, and enforcement priorities, that is domestically protective but globally patchy. The sole exemplar here is the US ITAR, which for decades has been

derided for being strongly enforced by US Customs and Commerce agents even in foreign sovereignties where US law does not apply (but the re-export provisions of the ITAR notionally ground sufficient US 'subject matter jurisdiction' for prosecution); see, for example [87–89].

Another problem facing the dichotomy of dual-use technology is the rise of certain externalities which impact the higher education environment, unfairly preferencing the role of government in regulating academic research [90]. Such externalities are broadly suggested to include the emergence of 'grey-zone' or 'influence' operations falling below thresholds for international action [66], the enrolment of military technologies in counterintelligence and law enforcement [26, 27, 33], and the mobilisation of higher education to take roles in domestic security initiatives [39, 91, 92]. The result is a system of regulation where it is 'increasingly difficult to disentangle the relative contributions made by researchers undertaking basic studies in traditional universities from those made by researchers working in projects specifically organized or funded by military or defense sources… [which] can often obscure rather than clarify which particular uses of science and technology are potentially problematic or objectionable' [90].

4.2 Quantum, research security and economic competitiveness

As has already been covered above, export controls have been increasingly militarised to protect domestic manufacturing and economic competitiveness for nation-States that possess a specific technological or research advantage. For example, the US CHIPS and Science Act of 2022 not only banned sales of semiconductor chips to entities in China (and their proxies), but it also incentivized domestic semiconductor manufacture through direct funding and tax relief in a way that had not been seen in five decades [78]. The Act also prioritised the position of research security as a tool of geopolitical competition, firmly fixing it to the notion that the US (and not China) should remain a pre-eminent technological global leader [79].

Export controls are not the only tool of research security which has been invoked in the name of economic security. Rules and prohibitions on foreign direct investment (FDI) continues to preoccupy discourse around university and higher education research, in large part because FDI restrictions have implications for research funding through the award of strategic grants, international and transnational funding bodies, and philanthropy from private sector actors [93–96]. Several divestment and blocking orders have been issued to UK universities seeking to commercialised technologies with a national security dimension [93], whilst increased tech spending by China is causing an uptick in FDI scrutiny and enforcement in the US [94] and EU [96]. The lack of synchronicity between FDI scrutiny and export control lists identified in the literature [5, 93, 97–99] also means that newly emerging dual-use technologies might be considered controlled by one regime but exempted by another. FDI systems also share little common regulatory DNA – the US [98], Australia [93] and Canada [99] all use centralised legal structures for FDI regulation, whilst the EU is forced by its nature to adopt a decentralised system [81, 98]. On top of that, no nation-State in the world (save perhaps for China [94, 96, 100]) can possibly match the FDI regulatory system of the US given the system's broad 'reliance on the broader economic and political power that the US wields' [98].

4.3 Quantum, research security and foreign policy

The final area in which the dual-use technology paradigm fails to yield tangible benefits for research security in relation to QT is in foreign policy. A fulsome academic exploration of what is meant by 'foreign policy' is beyond the scope of this paper; instead, it will be sufficient to observe this section deals with the leftover rump of research security controls being marshalled to protect emerging technologies (such as QT) outside of either export controls or economic competitiveness. This section will cover three such examples: the creation and enforcement of 'banned' or 'sanctioned' entity lists with whom trade is restricted or prohibited (falling outside the usual parameters of export control), funding restrictions on international collaboration efforts (such as 'foreign malign talent recruitment programs'), and increased visibility of international research arrangements.

Numerous nation-States deploy 'banned' or 'sanctioned' entity lists including the US, Canada, Japan, Australia and the EU [17, 18, 22, 25, 36, 72]; however, the most widely recognised and of greatest import in both research security and QT discourse is the US Entity List circulated as Supplement No. 4 to 15 CFR §744 [101]. The Entity List provides a comprehensive database of parties that are prohibited from receiving numerous U.S.-origin technologies because of engagement in activities contrary to US national security or foreign policy interests; perhaps unsurprisingly given such a focus, Chinese entities feature heavily [101]. However, dual-use features neither in the US Entity List nor in similar global analogues; instead, the foreign entity is itself 'sanctioned' and unable to participate in trade with the relevant sanctioning nation-State [17, 18, 72]. In effect, the regulatory focus is on the proposed recipient of *any* technology, rather than the national security implications of the technology sought to be provided to them. In this way, 'banned' or 'sanctioned' entity lists represent a significant departure from existing export control regimes and structures, and assist in demonstrating the utility of moving beyond the dichotomy of dual-use technologies (especially in relation to QT).

The second area of implication for research security and QT is 'foreign malign talent recruitment programs' and is another area where the US sets a strident regulatory position. These types of programs – typified by the Thousand Talents Program and the 111 Project [100] – involve forms of payment, compensation, honours or awards for academic researchers willing to provide details of their research to, or conduct their research in collaboration with, a foreign country. They often incorporate elements requiring deception of the domestic nation-State as to the true nature of the agreement and can also facilitate potential acts of fraud perpetrated on domestic funding body/ies [100]. In the US for example, the NSF 'Proposal and Awards Policies and Procedures Guide (PAPPG)' reflects the *CHIPS and Science Act of 2022* in requiring projects receiving US funding to annually declare they are not participating in a foreign malign talent recruitment program [25]. Failures to properly disclose or obfuscate such reporting obligations has led to at least one American scholar being criminally convicted [102]. Again, concepts of dual-use technology (and specifically QT) do not feature in the research security obligations arising under such funding programs. This has led to some scholars hypothesising that funding agencies could leverage a stronger compliance result from higher education researchers by tying national security obligations to receipt of public grant funding, rather than nebulous definition of dual-use [18, 39, 73, 103].

The final research security control in this domain increased visibility of international research arrangements. Australia [18] and the UK [104, 105] have pioneered legislative

development in this particular space, creating publicly-searchable registers of collaborative agreements with foreign entities in the name of countering foreign interference (including interference in university research agendas). However, these lists have also been bedevilled with problems; the UK register overlapped significantly with other forms of national security control such as the National Security and Investment Act and the Academic Technology Approval Scheme [105], whilst Australia's regime was the subject of a scathing Parliamentary review in 2024 which concluded the scheme was confusing, poorly designed, under-enforced and not meeting its statutory objectives [18]. Again, dual-use technologies matter little to controls where the focus is on the nature of the arrangements between individual entities or the entities themselves.

5 Moving beyond dual-use as a metric

This paper has argued that a common understanding of the dual-use technology concept is irrelevant, because the very notion of dual-use technology – especially with respect to its origin as a control of nuclear weapons proliferation – is well and truly beyond its "sell-by date". Put another way, the proliferation of alternative definitions of dual-use technologies globally (and explored here through the lens of QT) suggest the problem is not one of unification of standards and 'the same reasoning may be applied to justify the uselessness of to a homogeneous and global implementation of dual-use export controls. Inevitably, different interpretations, investigation and enforcement structures, borderline cases, end-user concerns, and levels of information or intelligence among states lead to different export control decisions' [2]. Similarly, even making minor or aesthetical changes to dual-use regulation can undermine the entire policy or principle behind the proscription of that form of technology [106].

That raises the question of what regime or framework might be elucidated or explored by scholars (and thence applied by practitioners) to more adequately discuss, describe and protect the trajectory of emerging and critical technologies like QT, and especially in higher education settings [8] and for research security purposes [18]. The focus here remains on higher education, because security controls in the private sector – such as non-disclosure agreements, intellectual property, commercial-in-confidence, internal security programs and the like – are both better received and more easily justifiable than in universities, where research is conducted "for the public good" and where publication is an expectation [107, 108]. Absent an international consensus or legally binding international instrument [41, 59], there are several alternatives worth exploration.

5.1 What are the other alternatives?

Proposal 1 *Dual-use technology should be replaced with a multi-variate measure of risk*.

Export controls which particularise or rely upon dual-use technologies have been widely criticised by academics and practitioners [73, 80–82, 98, 109], opening the door for potential alternatives that might replace dual-use as an export control criterion. Some scholars have suggested more specific multi-variate domains of research would benefit, such as identifying technologies that have an easily articulable political, security, intelligence, and military (PSIM) end-use [90]. However, the exact parameters of PSIM requires more specifics about how those fields, i.e., 'political', 'security', etc. are themselves defined, as current definitional frames linking dual-use technology to either investment or research

Table 1 How Technology Shapes Information Constraints on Cooperation [111]

		Distinguishability	
		High	*Low*
Integration	*Low*	Permissive zone (best prospects—H1) • Minimal detection or disclosure constraints • Additional monitoring not necessary to detect military violations from civilian uses • Monitoring less likely to disclose damaging information • Dual use nature of technology does not itself narrow range of viable arms control options	Detection constraint (modest prospects—H3) • Severe but surmountable detection constraint • More information needed to verify compliance • Niche technology creates fewer security risks from information disclosure • Dual use nature of technology leads states to pursue intrusive inspections over narrow technology subset
	High	Disclosure constraint (modest prospects—H4) • Severe but manageable disclosure constraint • Military violations easy to distinguish from permitted civilian uses • Integration creates high security risks from monitoring • Dual use nature of technology leads states to limit damage from monitoring via unilateral collection or restricted inspections	Dead zone (worst prospects—H2) • Severe detection and disclosure constraints • Greater monitoring measures needed to verify compliance • But high integration increases the potential damage from monitoring • Dual use nature of technology creates a dead zone for cooperation where states reject most arms control options

to a vaguely articulated 'defence sector' are already of no use. Put another way, toasters are still a potential PSIM technology [68, 69].

Others have suggested that dual-use controls should be applied to the *outcomes* of research (and the potential implications of those outcomes for national security) rather than nebulous components of a framework referring to 'things', 'items' or 'goods' [2, 73, 81, 82]. Forge for example suggests that 'knowledge' contributes differentially to 'research outcomes' such as technologies and artifacts, such that a technology is dual-use 'if there is a (sufficiently high) risk that it can be used to design or produce a weapon, or if there is a (sufficiently great) threat that it can be used in an improvised weapon, where in neither case is weapons development the intended or primary purpose' [110]. However, that definition is problematic because it requires connection of the technology to a 'weapon', which does not adequately reflect emerging nation-State concerns surrounding factors relevant to human security (i.e., EU dual-use applying to human rights violations, and US dual-use incorporating war crimes and terrorism) [2].

Vaynman and Volpe [111] describe how dual-use technologies constrain cooperation between States as geopolitical competitors. Their framework (Table 1) examines all possible technologies (i.e., those capable of operating as either a *weapon* or *weapon system*) to identify two dual-use dimensions: "the ease of distinguishing military from civilian uses" and the "degree of integration within military enterprises and the civilian economy". Technologies where military and civilian uses are indistinguishable will require greater resources to monitor for potential unethical uses or misuse of the technology; whilst on the other hand, highly integrated technologies will result in sharper costs to the owning State that discloses its existence or capabilities [111]. This framework demonstrates a substantial improvement over dual-use, especially in QT. Rather than merely recognising QT is "dual-use", this framework offers specific responses to how a given QT moves through each of the quadrants in Table 1.

For example, let us consider quantum computing. Given that the distinguishability of malign and benign use cases for this form of technology is very low (i.e., a quantum computer could act in both capacities interchangeably), regulatory controls need to focus on keeping the *integration* of that QT into military componentry low. Table 1 suggests a stricter monitoring and oversight framework rather than one of direct intervention, and that disclosure of information around the technology – such as via publication or academic collaboration – is less likely to cause security risks (and so can occur more or less without restriction or interference).

Proposal 2 *Dual-use controls should be replaced with a risk response spectrum.*

Given that the significance of criticisms for dual-use technology as a criterion for considering the application of potential other forms of legal regulation, there is an emerging suggestion in the literature that dual-use should be a criterion of risk response and not a classification of 'things', 'items' or 'goods' [68]. One example of that strategy has been the development by Massachusetts Institute of Technology (MIT) of a Dual-Use Readiness Level™ under the ambit of their Mission Innovation X portfolio [112]. Rather than produce one Technical Readiness Level (TRLs, which largely measures the maturity of the technology to be presented to market: [6, 12]), MIT's framework examines four additional elements on top of TRLs to generate a more cohesive risk picture: commercial funding readiness, mission funding readiness, commercial customer readiness, and mission customer readiness [112]. Holistically, MIT's model presents a more cogent and granular view of the wide array of risks posed by dual-use technology than is presently considered. However, the MIT framework is largely in its infancy and empirical studies of its applicability to more adequately protecting emerging or disruptive technologies are non-existent.

In a different vein, Mahfoud et al. [90] suggest that self-regulation by universities and higher education institutions is a possible alternative, but note that 'their capacity to actually shape, let alone terminate, lines of research that raise fundamental ethical and social issues has not been demonstrated'. But that may no longer be the case. Germany has embarked on a historic effort to change various lines of their foreign policy in response to the 'turning point' of Russia's invasion of the Ukraine (*Zeitenwende*; see, for example [113]). An emerging theme of research from that pivot about the role of "committees for ethics in security-relevant research" (*Kommissionen für Ethik sicherheitsrelevanter Forschung*; "Security Committees") suggests that academics are capable of self-regulatory efforts where national security implications are raised [114, 115]. The specific definitions for Germany's Security Committees are instructive (even though the foundational document still refers to dual-use: [114]). 'Security-relevant research' includes all 'scientific work that has the potential to produce knowledge, products or technologies that can be misused by third parties to harm human dignity, life, health, freedom, property, the environment or peaceful coexistence' [114], blending both traditional constructions of national security with emerging human security principles from across the EU. Research may then be escalated to being 'of concern' to either the institution or broader society if it meets the characteristics of having a 'misuse [that] can be immediate', and/or where 'the potential damage is significant' [114].

By taking a stronger role in research ethics, institution "scrutiny committees" can not only contribute to education and security-minded culture-building but also allows the embedding of civil society and the reflections of popular norms in the conduct of academic

research [116]. It also allows academics to communicate with academics about research security risks (i.e., between members of a scrutiny committee and a research team) with a shared language that both understand. Members of intelligence agencies or the government may even be appointed to such scrutiny committees, either on a standing or an *ad hoc* basis. This gives government an access point to assist them in the formulation of research security policy. What is yet to be fulsomely demonstrated is the empirical utility of scrutiny committees: though Security Committees are already embedded into the research precautions of Germany [115], no studies have yet been done about the broader applicability of such committees in other jurisdictions to address research security risks.

Proposal 3 *There should be a greater role for international standards bodies.*

Dual-use technologies already challenge existing frameworks of law and regulation, but this is particularly evident at the international and transnational level and at the intersection of export controls, non-proliferation, and the countering of WMDs. Almost all (if not all) emerging, critical or disruptive technologies has a civilian utility that can be repurposed for military, security, intelligence or law enforcement functions. Current legal frameworks (especially consensus-based frameworks) cannot fully account for rapid emergence, evolution and dissemination of such technologies.

In many ways, regulation of QT – as an enabling technology – bears hallmarks like debates around generative artificial intelligence (AI), large language models and machine learning algorithms [106]. Such technologies are themselves also dual-use and also enabling (in that they permit existing technologies to be enhanced or uplifted at scales and speeds previously impossible). Like QT, crystallisation of harms may not arrive until well after the technology has been released, and even in circumstances where those harms were not adequately apparent to the developers or designers [116]. In both cases of QT and AI, export controls are considered useful in restricting the most obvious dangers of dual-use technologies but are inappropriate levers for the more nuanced regulation that dual-use requires [81, 82, 116–119].

It is in this space that international regulatory bodies – preferably ones that bring together researchers, institutions, governments and funding agencies – have been suggested as having utility in dual-use technology regulation [116, 120, 121]. The role of funders is especially crucial, because these bodies can make fundamental decisions tied to which research receives funding or is prioritised, sending regulatory signals to researchers about which areas or domains of technology use are considered too high-risk for exploration. Whilst such an approach might be considered manipulative (i.e., by implicitly nudging researchers to only research 'acceptable' topics), or an interference with academic freedom (i.e., to research any topic, no matter how controversial, for the good of the public) [117, 118], such interference is justified (some might say necessary) to avoid potential downstream implications from dual-use technology [18, 90, 101, 103, 122].

One of the challenges in relying on international bodies to do this work will likely be the lack of rigid enforcement. Export controls, especially in the US, are strongly enforced – in large part, this contributes to their regulatory character [72, 80]. Lifting dual-use technology regulation out of national structures and to a transnational level requires tangible punishments for the very small selection of actors who pursue dual-use technology research for malign ends [5]. When technologies like are democratised, highly internationalised, and have low barriers to entry, regulations that lack 'teeth' are highly unlikely

Table 2 Summary of the new proposals of "beyond dual-use"

Dual-use technology should be replaced with a multi-variate measure of risk.	Rather than focus on "dual-use" appellations, the focus should be on: • The "ease of distinguishing military from civilian uses" and • The "degree of integration within military enterprises and the civilian economy".
Dual-use should be replaced with a risk response spectrum	Universities should focus on "getting to yes", i.e., encouraging research but subject to conditions, monitoring, or oversight, to ensure that both ease of distinguishing military uses and degree of integration can be properly accounted for.
There should be a greater role for international standards bodies	Rather than international treaty or national legislation, a supra- or transnational body could articulate standards that encourage or "nudge" nation-States into minimum standards or norms of behaviour.

to shift or moderate behaviour [116, 118]. Further, States are less likely to enforce – either on themselves or their geopolitical allies – regulations that conflict with their national interests [3, 111]. As an example, the US has vociferously fought against international legal instruments that could constrain the use of 'cyber-weapons' (i.e., weaponized computer viruses and malicious code: [123]) and espionage [124] because this would infringe on or inhibit US intelligence operations abroad.

This leads on to another challenge in the regulation of dual-use technologies by international bodies: asymmetry of regulation. Such asymmetry arises from nation-States pressing for regulatory agendas that more broadly reflect their domestic priorities and national interests [111]. For example, in the realm of international trade law, whilst many nations may publicly defend free trade agreements, such defence is more aggressive in areas where their exports are competitive, whilst nationalistically defending domestic markets from competitive imports [125]. Nation-States may also have other agendas for rejecting international moves to regulate or "crackdown" on particular dual-use technologies that are not always apparent. Again, the motivation behind the reluctance of the US to limit cyber-weapons development in the 2010s was not immediately apparent until their role (alongside Israel) in developing the Stuxnet virus was revealed in 2007 [123].

Table 2 summarises the above propositions.

5.2 Further research

This paper has argued throughout that the nomenclature for dual-use technology is reaching the end of its usable life. Although innumerable scholars have (as I have done) used dual-use technologies as a lens for teasing out the research security challenges from emerging developments like QT, dual-use technology remains as difficult to define as it ever was. There are therefore three specific observations I wish to make about future research in this space.

The first is that, as a discipline, research security remains crucially under-theorised, and empirical data about research security is difficult to obtain. Beyond splashy reports in media or public court proceedings, most research security incidents remain classified or secret to avoid compromising domestic intelligence, or confidential to research institutions keen to avoid the reputational damage of public scandals. More work is clearly needed, perhaps in the vein of assessments of the ill-fated US 'China Initiative' (the FBI's operation to investigate and prosecute cases of IP theft by predominantly Chinese scholars: [126]) or Australia's recent *Cost of Espionage* report [127].

Second, alternative frameworks for dual-use technologies such as those explored here [90, 99, 111] need further elucidation. One could pose research questions about whether

Table 3 How new measures might contribute to more robust security cultures at higher education environments

Dual-use technology should be replaced with a multi-variate measure of risk.	Stronger focus on what the risk is, to whom the risk is posed, and how that risk should be measured or quantified. Individual institutions faced with the same level of risk retain the flexibility of response, i.e., determining how *they* want to respond to that risk.
Dual-use should be replaced with a risk response spectrum	These measures would permit a more graduated response than just the "ban" / "allow" dichotomy present in current export controls. Enables flexibility for approaches to be tailored domestically (i.e., intra-State) and internationally (i.e., inter-State).
There should be a greater role for international standards bodies	The most collaborative approach, this could bring together the widest possible list of academic and industrial contributors. There is a likelihood of more academic "buy-in" of standards formulated by a panel of experts than government, i.e., IEEE, ISO, etc.

frameworks should prioritise competitive effectiveness or economic security, or merely stick to matters solely relevant to a narrowly-defined "national security". Others might suggest closer working connections between export control frameworks and FDI initiatives, such that the gaps for dual-use technologies to escape through become minimised. Yet more questions could be asked about whether a focus on dual-use technologies a definition actually *harms* cooperation and collaboration, breeding distrust and paranoia in university research sectors that is anathematic to good progress. Table 3 summarizes some of the required work.

Thirdly – and what I believe is most important of all – is further establishing work on scrutiny committees *a la* Germany's Security Committees [114, 115]. Given the need for strict legal regulation of dual-use technologies to be supplemented by a 'web of prevention' [106, 120, 121, 128] amongst researchers, institutions, funders and professional associations, the emergence of Security Committees seems timely. The benefits of such committees appear numerous, including being able to maintain a careful balance of the necessary levels of academic freedom and implications for career development alongside potential reputational damage, legal obligations, and/or harm to the broader public that may arise from unregulated dual-use research. But questions remain: what role should government play? Are there circumstances where they should intervene, or should the academy have the final say about publication? How will scrutiny committees deal with – should the issue arise – classified information[1]? Studies could also focus on whether the Security Committees, embedded within the research architecture of Germany, could be (or indeed should be) transplanted into domestic legal structures of other nations.

6 Conclusion

There can be no doubt that QT will drive fundamental changes to the existing technological landscape and challenge the existing economic and national interests of every nation on earth. By manipulating or interfering with the very building blocks of matter, it is difficult to consider any application of QT (whether carrying direct national security risk or not) that will not cause disruptions to the existing *status quo*. Although many QT remain either on the drawing board or at a low technological readiness level [MIT], the sheer pace of development and innovation in this domain will see new capabilities emerging on an ever-increasing time scale.

[1] In the United States, this also extends to the quixotically-termed "Controlled Unclassified Information".

This paper has argued that dual-use technology is no longer a viable dichotomy for applying to emerging critical technologies such as QT. The variation of enabling technologies which QT will apply to, the significance in differences between comparative jurisdictions, the lack of precision on identifying what dual-use risk should be the subject of inquiry, and the impossibility of a precise forecast of QT capabilities and development timeframes all militate against continuing to consider QT through the dual-use technology lens. That in turn raises questions for the utility of dual-use technology to apply to, and guide discussions about, emerging technologies more broadly and across national and transnational lines. Undue focus on 'shoehorning' such technologies into one category of dual-use or another is likely to conceal or obstruct a proper, timely examination of the actual (as opposed to the potential or merely fanciful) national security implications of technological research and development.

QT will obviously shape national security considerations in the conduct of research and development, and the protection of same through the deployment of research security; however, QT will (like other emerging technologies) shape discussions regarding the proper place of controls for economic competitiveness and foreign policy as well. A cooperative and collaborative research enterprise that fulsomely brings together the domestic infrastructure for sovereign technology development (i.e., government policy, intelligence agencies, universities and individual academic researchers) is crucial to having those discussions in a way that best serves the body politic.

Author contributions
As the sole author of the manuscript, BWM conceived, designed and performed the analysis and review, and wrote the paper. The author read and approved the final manuscript, and consents to its publication.

Authors' information
B. Walker-Munro is a Senior Lecturer in Law at Southern Cross University, and an Expert Associate (Adjunct) of the National Security College at Australian National University, Canberra.

Funding information
No funding was provided for the research in this article.

Data availability
Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The author has completed paid consultancies for the Australian Strategic Policy Institute (ASPI) and Independent National Security Legislation Monitor. The author is appointed as an Adjunct Expert Associate for the National Security College, and as a Senior Research Fellow for the Social Cyber Institute.

Received: 6 August 2025 Accepted: 14 November 2025 Published online: 26 November 2025

References

1. Kelley H. Dual-Use Technology and U.S. Export Controls. Center for New American Security. 2023. https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls. Accessed 4 August 2025.
2. Vella V. Is there a common understanding of dual-use?: the case of cryptography. Strateg Trade Rev. 2017;3(4):103–22.
3. Marsili M. Emerging and disruptive strategic implications and ethical challenges of dual-use innovations. Strateg Leadersh J. 2025;1:57–71.
4. Ilovača K. Implementation of dual-use technologies in defense and public security. Am J Polit Sci Law Criminol. 2025;7(6):40–8. https://doi.org/10.37547/tajpslc/Volume07Issue06-08.

5. Harris ED. Governance of dual-use technologies: theory and practice. American Academy of Arts & Sciences; 2016. https://www.amacad.org/sites/default/files/publication/downloads/GNF_Dual-Use-Technology.pdf. Accessed 2 August 2025.
6. Krelina M. Quantum technology for military applications. EPJ Quantum Technol. 2021;8:24. https://doi.org/10.1140/epjqt/s40507-021-00113-y.
7. Dowling JP, Milburn GJ. Quantum technology: the second quantum revolution. Philos Trans R Soc Lond A, Math Phys Eng Sci. 2003;361(1809):1655–74.
8. Qureca. Quantum Initiatives Worldwide 2025. July 9, 2025. https://www.qureca.com/quantum-initiatives-worldwide/. Accessed 5 August 2025.
9. QED-C. State of the Global Quantum Industry 2025. Quantum Consortium. 2025. https://quantumconsortium.org/publications/stateofthequantumindustry2025/. Accessed 4 September 2025.
10. Kania EB, Costello JK. Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership. Center for New American Security. 2018. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf. Accessed 5 August 2025.
11. Morton R. Quantum Shadows: When University Labs Become Battlegrounds for Espionage. Medium. May 30, 2025. https://spyauthor.medium.com/quantum-shadows-when-university-labs-become-battlegrounds-for-espionage-e3a85b2dfc13. Accessed 27 July 2025.
12. Krelina M. Military and Security Dimensions of Quantum Technologies: A Primer. Stockholm International Peace Research Institute (SIPRI). July 2025. https://www.sipri.org/sites/default/files/2025-07/0725_military_and_security_dimensions_of_quantum_technologies_0.pdf. Accessed 2 August 2025.
13. Krelina M. An Introduction to Military Quantum Technology for Policymakers. Stockholm International Peace Research Institute (SIPRI). March 2025. https://www.sipri.org/sites/default/files/2025-03/2025_03_quantum_1.pdf. Accessed 5 August 2025.
14. National Academies of Sciences, Medicine, Global Affairs, Committee on Science, Law, Committee on Dual Use Research of Concern, Options for Future Management. Dual use research of concern in the life sciences: current issues and controversies. 2017. https://pubmed.ncbi.nlm.nih.gov/29001489/. Accessed 5 August 2025.
15. Singh J, Bhangu KS. Contemporary quantum computing use cases: taxonomy, review and challenges. Arch Comput Methods Eng. 2023;30:615–38. https://doi.org/10.1007/s11831-022-09809-5.
16. OECD. Integrity and Security in the Global Research Ecosystem. Science, Technology and Industry Policy Papers No. 130. June 2022. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/06/integrity-and-security-in-the-global-research-ecosystem_2bd8511d/1c416f43-en.pdf. Accessed 4 August 2025.
17. Sá C, Pashayeva A, Weidenslaufer C. Canada's leap forward in research security. Minerva; 2025. https://doi.org/10.1007/s11024-025-09591-1.
18. Walker-Munro B. Shifting the needle: making Australia's research security ecosystem work smarter. 30 June 2025. https://www.aspi.org.au/report/shifting-the-needle-making-australias-research-security-ecosystem-work-smarter/. Accessed 3 August 2025.
19. Keselman G, Murray F. Dual-Use Is a Strategy, Not a Category (Nor a Trap), War on the Rocks. January 2, 2025. https://warontherocks.com/2025/01/dual-use-is-a-strategy-not-a-category-nor-a-trap/. Accessed 5 August 2025.
20. Casadevall A, Dermody TS, Imperiale MJ, Sandri-Goldin RM, Shenk T. Dual-use research of concern (DURC) review at American Society for microbiology journals. mBio. 2015;6(4):10–128.
21. Patrone D, Resnik D, Chin L. Biosecurity and the review and publication of dual-use research of concern. Biosecur Bioterror. 2012;10(3):290–8.
22. Drew TW, Mueller-Doblies UU. Dual use issues in research–a subject of increasing concern? Vaccine. 2017;35(44):5990–4.
23. Berger KM. Technological advances that test the dual-use research of concern model. In: Applied biosecurity: global health, biodefense, and developing technologies. Cham: Springer; 2021. p. 133–60.
24. European Commission. Council Recommendation of 23 May 2024 on enhancing research security. 23 May 2024. C/2024/3510. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510. Accessed 5 August 2025.
25. National Science Foundation. Research Security at the National Science Foundation. 2025. https://www.nsf.gov/research-security. Accessed 3 August 2025.
26. FBI. Protecting Quantum Science and Technology. April 12, 2024. https://www.fbi.gov/news/stories/protecting-quantum-science-and-technology. Accessed 5 August 2025.
27. Department of Home Affairs. Technology Foreign Interference Taskforce. February 18, 2025. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/technology-foreign-interference-taskforce. Accessed 5 August 2025.
28. Cokelaere H. Dutch government plans to screen scientists for national security risks. Politico. April 7, 2025. https://www.politico.eu/article/dutch-government-scientists-tech-national-security-espionage/. Accessed 3 September 2025.
29. Pannier A. Balancing security and openness for critical technologies challenges for French and European research. Etudes de L'Ifri. 2023. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_pannier_balancing_security_openness_critical_technologies_2023.pdf. Accessed 4 September 2025.
30. Weinberg S. Lectures on quantum mechanics. Cambridge: Cambridge University Press; 2015. https://doi.org/10.1017/CBO9781316276105.
31. Wei G. Definition and the state-of-art applications of quantum state. Theor Nat Sci. 2023;10(1):47–52. https://doi.org/10.54254/2753-8818/10/20230308.
32. Del Medico B. Quantum entanglement explained to all. New York: Science; 2024.
33. Vestergaard C, McAllister C, Mueller-Kaler J, Cupitt R, Manning RA, Turner G, Scoggin K. A Critical Juncture: Global Security and the Age of Converging Technologies. Stimson. July 30 2025. https://www.stimson.org/2025/a-critical-juncture-global-security-and-the-age-of-converging-technologies/#elementor-toc__heading-anchor-0. Accessed 3 July 2025.
34. Daniels M, Krige J. Knowledge regulation and national security in postwar America. Chicago: University of Chicago Press; 2022.

35. Maher R. The covert campaign against Iran's nuclear program: implications for the theory and practice of counterproliferation. J Strateg Stud. 2021;44(7):1014–40.
36. Winter C. Research Security and Open Scholarship in Canada. Open Scholarship Policy Observatory. November 17, 2023. https://ospolicyobservatory.uvic.ca/research-security-and-os-in-canada/. Accessed 5 August 2025.
37. Long G. Fundamental Research Security. MITRE. December 2019. https://apps.dtic.mil/sti/trecms/pdf/AD1108106.pdf. Accessed 3 August 2025.
38. van Daalen O. From encryption to quantum computing: the governance of information security and human rights. Springer; 2024.
39. Gannon JC, Meserve RA, Zuber MT. Reconsidering research security. Issues Sci Technol. 2025;41(2).
40. Pappalardo D. Hypersonics: between rhetoric and reality. Air Space Oper Rev. 2022; 1(4).
41. Marchant G, Bazzi R, Bowman D, Connor J, Davis III RA, Kang E, Konkoly-Thege K, Liu D, Lloyd-Jones S, Manwaring K, Moses LB. Learning from emerging technology governance for guiding quantum technology. Rich JL & Tech. 2024;31:266.
42. Lukoseviciene A. Regulating quantum computers: insights into early patterns and trends in academic regulatory conversations on the 'quantum revolution'. Law Innov Technol. 2025;17(1):241–70.
43. Ponkin I. Quantum technologies for military purposes: concepts, species diversity, realities, regulation. Int J Open Inf Technol. 2025;13(4):158–69.
44. Balarabe K. Quantum computing and the law: navigating the legal implications of a quantum leap. Eur J Risk Regul. 2025; 1–20.
45. Johnson WG. Governance tools for the second quantum revolution. Jurimetrics. 2019;59:487–521.
46. Nguyen A. Short-circuiting technological sovereignty? Assessing the governance of semiconductor supply chain (chokepoints) through the lens of emerging multilateral export control regimes. In: Bäumler J, Binder C, Bungenberg M, Krajewski M, Rühl G, Tams CJ, Terhechte JP, Ziegler AR, editors. European yearbook of international economic law 2024. Cham: Springer; 2025. p. 343–72. https://doi.org/10.1007/8165_2024_136.
47. EU Directorate-General for Research and Innovation. Unlocking the potential of dual-use research and innovation. 2025. https://orbi.uliege.be/bitstream/2268/333542/1/unlocking%2520the%2520potential%2520of%2520dual-use%2520research%2520and%2520innovation-KI0125058ENN.pdf. Accessed 4 September 2025.
48. Marr B. Why You Should All Be Worried About Q-Day and the Collapse of Digital Security. Forbes. July 31 2025. https://www.forbes.com/sites/bernardmarr/2025/07/31/why-you-should-all-be-worried-about-q-day-and-the-collapse-of-digital-security/. Accessed 31 July 2025.
49. Lague D. US China race to shield secrets from quantum computers. Reuters. December 14, 2023. https://www.reuters.com/investigates/special-report/us-china-tech-quantum/. Accessed 5 August 2025.
50. Herman A, Friedson I. Quantum Computing: How to Address the National Security Risk. Hudson Institute. August 2018. http://media.hudson.org.s3.amazonaws.com/files/publications/Quantum18FINAL3.pdf. Accessed 4 July 2025.
51. Katwala A. The Quantum Apocalypse Is Coming. Be Very Afraid. Wired. March 24, 2025. https://www.wired.com/story/q-day-apocalypse-quantum-computers-encryption/. Accessed 4 August 2025.
52. Chang L, Jiang H, Yang Y, Wu H, Wu Z, Cai J. Coverage simulation of satellites Mozi and Jinan 1 during the quantum key distribution. J Phys Conf Ser. 2025;2977(1):012095. https://doi.org/10.1088/1742-6596/2977/1/012095.
53. Wong HY. Shor's algorithm. In: Introduction to quantum computing: from a layperson to a programmer in 30 steps. Cham: Springer; 2023. p. 289–98.
54. Nedelcu C. The Limitations of Quantum Computers. Medium. October 24, 2024. https://medium.com/@cristian.nedelcu/the-limitation-of-quantum-science-5d707c3ea157. Accessed 3 August 2025.
55. Olsson E, Öhman C. The quantum panopticon: a theory of surveillance for the quantum era. Minds Mach. 2025;35(2):17.
56. Ten Holter C, Inglesant P, Jirotka M. Reading the road: challenges and opportunities on the path to responsible innovation in quantum computing. Technol Anal Strateg Manag. 2023;35(7):844–56.
57. Pavan G, Galati G, Daum F. Lessons learnt from the rise and fall of quantum radar research. Acad Quantum. 2025;2(1).
58. Brooksby A, Smith A, Hickam A, Manda M, Rogers A, LaDuke M. A conceptual framework for describing the future impacts of quantum sensors to national security. Acad Quantum. 2025;2(1).
59. Li X. Quantum international law theories: towards an inclusive international investment-security construct. J World Invest Trade. 2024;25(2):237–75.
60. Uriri S, Ismail Y, Mafu M. Quantum metamaterials: applications in quantum information science. APL Quantum. 2025;2(2).
61. Taha BA, Addie AJ, Haider AJ, Chaudhary V, Apsari R, Kaushik A, Arsad N. Exploring trends and opportunities in quantum-enhanced advanced photonic illumination technologies. Adv Quantum Technol. 2024;7(3):2300414.
62. Der Derian J, Rollo S. "Quantum 3.0": what will it mean for war, peace, and world order? Glob Perspect. 2024;5(1):93888.
63. Goyal RK, Maharaj S, Kumar P, Chandrasekhar M. Exploring quantum materials and applications: a review. J Mat Sci Mat Eng. 2025;20(1):4.
64. McFadden C, Nadi A, McGee C. Education or espionage? A Chinese student takes his homework home to China. NBC News. July 24, 2018. https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881. Accessed 3 July 2025.
65. Da Silva W. Quantum Warriors: New Weapons from Spooky Physics. Medium. October 10, 2019. https://medium.com/discourse/quantum-warriors-new-weapons-from-spooky-physics-81e467b3e4b8. Accessed 6 August 2025.
66. Dixon T. The grey zone of cyber-biological security. Int Aff. 2021;97(3):685–702.
67. Kyrie V, Broudy B. Cyborgs R Us: the bio-nano panopticon of injected bodies? Int J Vaccin Theory Practice Res. 2022;2(2):355–83.
68. Chapman J. Reliance on Dual-Use Technology Is a Trap. War on the Rocks. September 8, 2022. https://warontherocks.com/2022/09/reliance-on-dual-use-technology-is-a-trap/. Accessed 5 August 2025.
69. Walker-Munro B. Google "Toaster Laser". Issues Sci Technol. 2025;41(4).
70. National Academies of Sciences, Engineering, and Medicine. National science, technology, and security roundtable capstone: proceedings of a workshop. Washington: National Academies Press; 2025. https://doi.org/10.17226/27976.

71. Starks B, Tucker C. Export control compliance and American academia. Strateg Trade Rev. 2017;3(4):69–80.
72. Martins BO, Ahmad N. The security politics of innovation: dual-use technology in the EU's security research programme. In: Emerging security technologies and EU governance. London: Routledge; 2020. p. 58–73.
73. Evans SW. When all research is dual use. Issues Sci Technol. 2022;38(3):84–7.
74. Sánchez Cobaleda A. Definitions of concepts: dual-use goods. In: A decade of evolution of dual-use trade control concepts: strengthening or weakening non-proliferation of WMD. University of Liège, European Studies Unit. 2020. https://orbi.uliege.be/bitstream/2268/246711/1/full.pdf. Accessed 2 August 2025
75. Rajput T. Restricting international trade through export control laws: national security in perspective. In: Regulation of risk. Brill Nijhoff; 2022. p. 603–45.
76. Walker-Munro B. A missed opportunity: amending the Defence Trade Controls Act 2012 (Cth) and research security. J Strateg Trade Control. 2024;2:1–34.
77. Kharon Staff. Weeks After BIS Listed these Chinese Tech Companies, They Spun up Unrestricted Subsidiaries. Kharon. July 28, 2025. https://www.kharon.com/brief/bis-50-percent-rule-commerce-department-china-tech. Accessed 1 August 2025.
78. Peters MA. Semiconductors, geopolitics and technological rivalry: the US CHIPS & Science Act, 2022. Educ Philos Theory. 2023;55(14):1642–6.
79. Luo Y, Van Assche A. The rise of techno-geopolitical uncertainty: implications of the United States CHIPS and Science Act. J Int Bus Stud. 2023;1.
80. Whang C. Trade and emerging technologies: a comparative analysis of the United States and the European Union dual-use export control regulations. Secur Hum Rights. 2021;31(1–4):11–34.
81. Kanetake M. Balancing innovation, development, and security: dual-use concepts in export control laws. Cambridge: Cambridge University Press; 2018.
82. Stalenhoef C, Kanetake M, van der Wende M. The implications of the EU's dual-use export control regulation 2021/821 for universities and academics. Utrecht Univ Sch Law Res Pap. 2022.
83. Williams-Jones B, Olivier C, Smith E. Governing 'dual-use' research in Canada: a policy review. Sci Public Policy. 2014;41(1):76–93.
84. Dizon MA, McHugh PJ. Encryption laws and regulations in one of the five eyes: the case of New Zealand. Inf Commun Technol Law. 2022;31(2):220–39.
85. Gill B, Ebata K, Stephenson M. Japan's export control initiatives: meeting new non-proliferation challenges. Nonprolif Rev. 1996;4(1):30–42.
86. Hayakawa K, Ito K, Fukao K, Deseatnicov I. The impact of the strengthening of export controls on Japanese exports of dual-use goods. Int Econ. 2023;174:160–79.
87. Sherzer HG, Yesner DL. Export controls over direct commercial sales of military and strategic goods and technologies: who's in charge. Boston College Int Comp Law Rev. 1984;7:303.
88. Barker JP. Managing compliance with US Treasury Department OFAC obligations: even if your business is exclusively outside the US. Glob Trade Cust J. 2010;5(5).
89. Voetelink J. Limits on the extraterritoriality of United States export control and sanctions legislation. In: NL ARMS Netherlands annual review of military studies 2021. 2021. p. 187.
90. Mahfoud T, Aicardi C, Datta S, Rose N. The limits of dual use. Issues Sci Technol. 2018;34(4):73–8.
91. Walsh JP. Education or enforcement? Enrolling universities in the surveillance and policing of migration. Crime Law Soc Change. 2019;71(4):325–44.
92. Corradi A, Popham J. Safety in numbers: security on campus and the importance of the corporatization of universities. Secur J. 2022;35(2):628–48.
93. Walker-Munro B. National security, foreign investment & research security: the current state of art. Griffith Law Rev. 2024;33(2):167–88.
94. Lai K. National security and FDI policy ambiguity: a commentary. J Int Bus Policy. 2021;4(4):496–505.
95. Chilton AS, Milner HV, Tingley D. Reciprocity and public opposition to foreign direct investment. Br J Polit Sci. 2020;50(1):129–53.
96. Bickenbach F, Liu WH. Chinese direct investment in Europe–challenges for EU FDI policy. CESifo Forum. 2018;19(4):15–22.
97. Directorate-General for Research and Innovation. Unlocking the potential of dual-use research and innovation. Independent Experts' Report. June 2025. https://orbi.uliege.be/bitstream/2268/333542/1/unlocking%2520the%2520potential%2520of%2520dual-use%2520research%2520and%2520innovation-KI0125058ENN.pdf. Accessed 30 July 2025.
98. Bromley M, Brockmann K. Controlling technology transfers and foreign direct investment: the limits of export controls. Stockholm International Peace Research Institute (SIPRI) Yearbook; 2019. p. 538.
99. Li J, Shapiro D, Ufimtseva A. Regulating inbound foreign direct investment in a world of hegemonic rivalry: the evolution and diffusion of US policy. J Int Bus Policy. 2024;7(2):147–65.
100. Nouwens M, Legarda H. Emerging technology dominance: what China's pursuit of advanced dual-use technologies means for the future of Europe's economy and defence innovation. International Institute for Strategic Studies/Mercator Institute for China Studies China Security Project. 2018; 12:9780429198533.
101. Pagano JA. Contrary to national security: the rise of the entity list in U.S. policy towards China and its role in the national security administrative state. Columbia J Transnatl Law. 2023;61(2):453–507.
102. Kim C. Ex-Harvard professor Charles Lieber gets house arrest over China ties. BBC News. April 27, 2023. https://www.bbc.com/news/world-us-canada-65402979. Accessed 5 August 2025.
103. Shih T. The role of research funders in providing directions for managing responsible internationalization and research security. Technol Forecast Soc Change. 2024;201:123253.
104. Hagmann J, Cavelty MD. National risk registers: security scientism and the propagation of permanent insecurity. Secur Dialog. 2012;43(1):79–96.
105. Yip T. Covert interference and the UK foreign influence registration scheme. RUSI J. 2024;169(7):44–54.
106. Rath J, Ischi M, Perkins D. Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. Sci Eng Ethics. 2014;20(3):769–90.

107. Kirby DA. Creating entrepreneurial universities in the UK: applying entrepreneurship theory to practice. J Technol Transf. 2006;31(5):599–603.
108. National Research Council, Global Affairs, Security, Cooperation, Committee on Scientific Communication, National Security, Committee on Science, Security, Prosperity. Beyond "fortress America": national security controls on science and technology in a globalized world. National Academies Press; 2009.
109. Yang Y. The evolution and trend of US export control laws and China's response. US-China L Rev. 2024;21:336.
110. Forge J. A note on the definition of "dual use". Sci Eng Ethics. 2010;16(1):111–8.
111. Vaynman J, Volpe TA. Dual use deception: how technology shapes cooperation in international relations. Int Organ. 2023;77(3):599–632.
112. Massachusetts Institute of Technology. Introducing the MIT Dual-Use Readiness Levels™. 2025. https://dualuse.mit.edu/. Accessed 6 August 2025.
113. Bunde T. Lessons (to be) learned? Germany's Zeitenwende and European security after the Russian invasion of Ukraine. Contemp Secur Policy. 2022;43(3):516–30.
114. Jakob U, Kraemer F, Kraus F, Lengauer T. Applying ethics in the handling of dual use research: the case of Germany. Res Ethics. 2025;21(2):228–44.
115. Heinrichs JH, Aslan SE, Alex K, Brenneis A, Conradie NH, Hähnel M, Kropf M, Kuck J, Lev O, Philippi M, Risse V. Guideline on dual use and misuse of research for committees for ethics in security relevant research (KEFs). https://philpapers.org/archive/HElGOD.pdf. Accessed 5 August 2025.
116. Brenneis A. Assessing dual use risks in AI research: necessity, challenges and mitigation strategies. Res Ethics. 2025;21(2):302–30. https://doi.org/10.1177/17470161241267782.
117. Bernstein M, Levi M, Magnus D, Rajala B, Satz D, Waeiss C. ESR: Ethics and Society Review of Artificial Intelligence Research. 2021. http://arxiv.org/pdf/2106.11521v2.
118. Grinbaum A, Adomaitis L. Dual use concerns of generative AI and large language models. J Res Innov. 2024;11(1):1–18. https://doi.org/10.1080/23299460.2024.2304381.
119. Kaffee LA, Arora A, Talat Z, Augenstein I. Thorny roses: investigating the dual use dilemma in natural language processing. Findings of the association for computational linguistics: EMNLP. 2023. p. 13977–13998.
120. Miller S. Dual use science and technology, ethics and weapons of mass destruction. Cham: Springer; 2018.
121. Selgelid MJ. Ethics and censorship of dual-use life science research. In: Gross ML, Carrick D, editors. Military medical ethics for the 21st century. London: Routledge; 2013. p. 139–54.
122. Streitwieser B, Allen K, Duffy-Jaeger K. Higher education in an era of violent extremism: exploring tensions between national security and academic freedom. J Deradicalization. 2019;18:74–107.
123. Mulbry E. Arms control 2.0: updating the cyberweapon arms control framework. Mich Telecommun Technol Law Rev. 2021;28(1):175–95.
124. Johnson J. Securing secrets: the need for a treaty addressing state-sponsored economic espionage. West Va Law Rev. 2021;124:327–47.
125. Gervais D. The regulation of inchoate technologies. Houst Law Rev. 2010;47(3):665–706.
126. Lewis MK. Criminalizing China. J Crim Law Criminol. 2021;111(1):145–225.
127. Morgan A, Voce A. The cost of espionage: special reports. Canberra: ASIO. 2025. https://www.aic.gov.au/publications/special/special-21. Accessed 4 August 2025.
128. Brenneis A. Assessing dual use risks in AI research: necessity, challenges and mitigation strategies. Res Ethics. 2025;21(2):302–30.

Publisher's note