ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 2, pp: (1-21), Month: April - June 2022, Available at: www.researchpublish.com

Quantum Computing Policy and Strategy Recommendations for Facilitating Wider Adoption of Emerging Technologies to Safeguard National Security

Andrew Vance[1], Taylor Vance[2]

[1]Senior Researcher, Cyber Institute, Center for Cyber Risk Research & Policy, New York, NY 10003

[2]Senior Researcher, Cyber Institute, Center for Cyber Risk Research & Policy, New York, NY 10003

[1]Doctoral Candidate, Capitol Technology University, Quantum Computing Department, Washington D.C., 20708

[2]Doctoral Candidate, Capitol Technology University, Artificial Intelligence Department, Washington D.C., 20708

Published Date: 16-April-2022

Abstract: **Quantum computing technologies are poised to enable a wider adoption of emerging technologies. A significant factor for the potential increase in cyber conflict is technological evolution of emerging technologies. Being a leader in these technologies is of strategic economic and social importance to nation states while at the same time, it is creating significant national security concerns. This research identifies the current geopolitical framework affecting quantum computing and affected emerging technologies and correlates policy evolution. It surveys current proposals on cyber legislation and U.S. government policy since 1985 to address the challenges of establishing a unified legal framework over the modern arms race of quantum computers and other emerging technologies to explore potential solutions for the international governance over cyber warfare. Our findings exposed critical gaps in legal frameworks for policymakers who must plan how to effectively promote the development, application, and implementation of general-purpose quantum technologies to promote the larger economic and social benefits for their nation state, while simultaneously mitigating foreseeable risks to privacy, safety, security, and inclusion to prevent cyber conflict. We identify specific normative constraints for international accords to define acts of cyberwar: cyber-attacks on critical infrastructure, direct interference in or manipulation of electoral and political processes, and activities designed to damage the availability or integrity of the public core of the internet to bring policy into alignment with agreed upon norms. We examined the problem from a pre-emptive, non-proliferation perspective regarding quantum computing allied with international policy development. Instituting a unified legal framework involving quantum computers and exploring potential solutions for governance over cyber warfare is critical to reign in the modern arms race. Our research produced several primary findings on the character of and prospects for quantum computing legislation. It proposes recommendations for the international governance to mitigate the modern arms race of quantum supremacy implicating cyberwarfare.**

Keywords: **Budapest Convention, Cyberwarfare, Emerging Technologies, National Security, Policy, Quantum Computing.**

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 2, pp: (1-21), Month: April - June 2022, Available at: www.researchpublish.com

I. INTRODUCTION

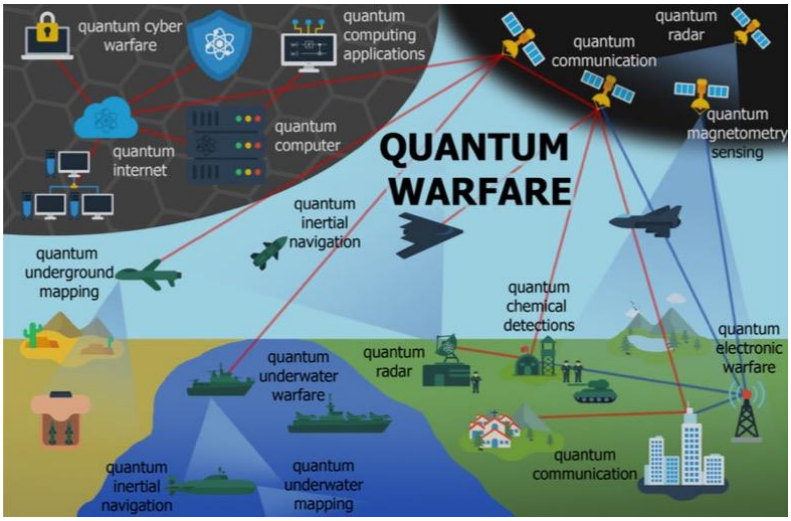

Figure 1: Concept of Quantum Enhanced Cyberwarfare.

According to the World Economic Forum's (WEFs) 2019 Global Risks Report, the fifth most significant strategic and economic risk that nation-states purport that they face is cyberwar [1]. Exhibiting importunity nearly a half-decade later, cyber threats continue to be among the top five global risks, according to WEFs 2022 Global Risks Report [2]. The fragmentation of enforcement mechanisms across geopolitical jurisdictions hampers nation-state efforts to control and collaborate as governments demonstrate that they are unwilling or unable to effectively regulate cyberattacks that transgress borders [3]. Emerging technologies are poised to further exacerbate these efforts. Quantum computing is considered an emerging technology that will change the future conduct of warfare and the outcomes of a state's ambitions [4]. Nation-states are developing state-of-the-art military capabilities with emerging technologies [5]. It is predicted that sixth-generation modern warfare will be hybrid; a combination of kinetic and emerging technology enhanced cyber [6][7].

Although current quantum technologies are still considered nascent, they have tremendous disruptive and destructive potential. Quantum technologies for military applications offer the development of improvements and new capabilities. They will also require the development of new strategies, tactics, and policies addressing threats to global peace and security and ethics issues involving quantum-enabled cyberwarfare [5]. The weaponization of quantum technology signifies an evolution and escalation of warfare [8]; a facet known as quantum warfare (Fig. 1). There is little debate among nation-state experts that quantum warfare will increase a state's global cyber-attack dominance and affect geopolitical supremacy [9][10]. Nation-states weaponizing emerging technologies such as quantum computing are involved in a nuclearesque arms race to achieve quantum supremacy [11][12][13]. Weaponized quantum technologies are expected to play a significant role in command and control (C2) systems. C2 systems analyze and present situational awareness and assist with planning and monitoring, including simulation of various possible scenarios to provide the best conditions for the best decision. They are dependent on technologies to perform extensive data processing and analysis. Quantum computing is envisaged to improve and speed up scenario simulations involving ISR (Intelligence, Surveillance, and Reconnaissance) data for enhanced situational awareness for warfare decision-making. [14]. Quantum computing will enhance classical machine learning (ML) and artificial intelligence (AI) [15] for defense applications [16]. Recent studies show that quantum ML provides an advantage even if just for some specific problems [17]. Research reveals that quantum computing will potentially enhance classical ML/AI applications for defense, automating cyber operations, algorithmic targeting, situation awareness, understanding and automating mission planning [18]. It is predicted that in less than a decade, quantum ML/AI will be one of the most state-of-the-art military capabilities towards enabling nation-state supremacy [19]. To safeguard national security, it is necessary to develop, interpret, and apply relevant policy. Retrospective analysis of current agreements indicate that policymakers struggle to consider how to effectively promote the development, application, and implementation of quantum technologies to not only realize economic and social benefits, but to mitigate anticipated risks to privacy, safety, and security [20]. They fail to articulate bilateral, informal commitments with other powers to refrain from certain categories of cyber aggression. It prevents consensus on existing

initiatives attempting to establish and evolve cyber norms, including building a common position on prohibited behaviors with other nation-states. Cooperation and coordination challenges are transboundary by transformative norms, geopolitical policy must be brought into alignment with norms that would restrain the use of weaponized emerging technologies in cyber-attacks [21]. The goal of this research is to retrospectively review quantum related policy on the character of and prospects for future quantum computing legislation to produce principal findings strategy recommendations for facilitating wider adoption of emerging technologies to safeguard national security.

II. SCOPE AND METHODOLOGY

This study qualitatively and quantitatively examined data generated from a retrospective review of published research, policy, and standards from authoritative resources. The scope was limited to current research to analyze multi-disciplinary legislation analysis from authoritative sources: Global Cyberlaw Tracker from United Nations Conference on Trade and Development Cybercrime Legislation Worldwide; Asian School of Cyber Law Global Cyber Law Database; NYU Cybersecurity Center International Law Repository, U.S. Federal Archives, IEEE Xplore, Science Direct, Google Scholar, Scopus, Academia, ResearchGate, and resources.data.gov. These were analyzed to develop the main principles for a global policy framework in cyberspace. Governance and regulations not reviewed are those not directly addressing national security of the 16 Homeland Security identified critical infrastructures. Examples of policy not reviewed are Federal Privacy Act of 1974 (FPA), Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), EU-US Privacy Shield. This research is not an exhaustive list of all quantum research nor an introduction to the field. This research does not review the conceptions or misconceptions of quantum computing's computational power; particularly compared to classical computing. Adequately abridged studies already exist [22]. We made a concerted effort to focus on identifying decisive research and advising on solutions to address legislative and policy gaps.

III. PROBLEM STATEMENT

A significant factor in the potential increased global cyberwarfare is technological evolution. Growing global interconnectivity involving critical infrastructures, exacerbates the issue, as it provides a larger attack surface and increases the number of cyber actors [23][24]. A covert and precursor to feasibly signaling escalations to cyberwar is cyber espionage [25]. An increasing concern for the U.S. is foreign efforts to harm election security or legitimacy through cyber means [26]. With emerging technology tools at threat actors' disposal, there is potential for unprecedented espionage and surveillance capabilities. As with new technology, the regulatory environment that constructs a framework for safe and effective use often lags, leaving otherwise innocuous devices susceptible to exploitation. Among the key issues, is the lack of clear red lines that set expectations and implications for the use of cyber weapons by state and non-state actors. The current environment is one in which cyber-attacks that cross an unclear threshold or cause unintended consequences could escalate into armed conflict. An absence of established norms to guide nation-state and non-state actors' behavior exacerbates confusion over the status of acceptable or tolerable nation-state cyber operations. While the rules of engagement are still evolving and imprecise, the Pentagon has affirmed that any state-sponsored cyber-attack can be constituted as an act of war that may lead the U.S. to respond either by cyber or traditional military force [27]. The lack of rules and consequences has resulted in policy challenges, namely a tacit tolerance of cyber-attacks that fall below the current threshold of war. This implicit acceptance creates a condition for apathy for achieving a consensus of rules, driven by disingenuous approaches to deterring disruptive and destructive cyber-attacks. By comparison, industry appears to be more ambivalent about the capabilities and impact of quantum computing on existing technology, such as cryptography; governments have expressed concerns about the detrimental effects of emerging technologies on cybersecurity and privacy [28]. There is a lack of international consensus on cyberwar norms influencing nation-state behavior, including clear redlines for when cyber effects become an act of war [29]. The concept of quantum-enabled cyber warfare has been intensifying and disturbing the current development of cybersecurity innovations and degenerating the current understanding of cyberattack capabilities and attempts to achieve geopolitical consensus and regulations [30]. Data currently encrypted is vulnerable to future quantum hackers. In a process called harvest and decrypt, nation states are collecting vast amounts of encrypted information today and stockpiling it in government data centers for when quantum computers can break current encryption schemes [31]. The U.S. has been engaged for almost a decade in international negotiations over agreed normative constraints on such activities. The international community has yet to implement a legal framework to regulate cyberattacks and warfare. There has been little progress at the international level in establishing uniform expectations of state conduct, considering that this long-speculated-about possibility has largely

become a reality [32]. Growing distrust in nation state motives regarding quantum computing had led to underestimating risks in other areas, particularly in cybersecurity. Non coordinated efforts in standardization, benchmarks, and roadmaps neglect to integrate diverse communities of stakeholders in defining the development of quantum computing technologies. A non-collaborative global governance evolution could lead to a "balkanization" [33] of digital infrastructures due to incompatible standards unintentionally causing the covert development of quantum computing capabilities. This neglect could lead to wider emerging technology risks such as the destabilization of governance protocols in emerging technologies such as blockchain networks relying on proof of work (e.g., Grover's algorithm providing a potential advantage for mining) or other consensus mechanisms, by attacking the authentication layer, could occur. Deprived of unified policies aligned to emerging technology risks, nation-states will continue to confront the fact that current and future regulations are impossible to enforce.

IV. RESEARCH FINDINGS

Many nations, including China, are pursuing quantum computing capabilities. Several nations, including the U.S., United Kingdom, Australia, and the European Union, have announced large research initiatives and programs to become leaders in the technology and to advance their geopolitical influence [21]. In 2017, China established its own Quantum national laboratory. With an initial $1 billion investment and an anticipated $9 billion allocated, China challenged their National Laboratory for Quantum Information Sciences (QIS), and associated institutions like the Shanghai Quantum Lab, to achieve significant quantum breakthroughs by 2030. Correspondingly, in 2018, the U.S. National Strategic Overview for QIS, recommended the Federal government research the security implications of advances in QIS science and technology. It established the Subcommittee on QIS (SCQI) to educate government agencies of the defense implications and to help balance the benefits of economic growth with potential risks created by the technology. It also recommended review of export control mechanisms to ensure continued research and economic opportunities, while also protecting national security [34]. In 2019, Moscow allocated $790 million over five years for quantum research at its national laboratories. That same year, the U.S. Global Leadership in Advanced Manufacturing Act of 2019 established research in several emerging technologies, including QIS and Artificial Intelligence (AI) [30]. Quantum computing has the potential to transcend current computational boundaries and will have a transformational impact on the economy and society. Being a leader in this technology is of strategic economic and social importance to the nation states. With quantum computing introducing a new computing paradigm, existing knowledge about the opportunities and risks of a new technology as well as the necessary understanding to adjudicate between them will, in many cases, be insufficient or at least call for a reassessment of how such opportunities and risks are managed. There is a lack of consensus defining when cyberattacks against a sovereign nation rise to the level of an armed attack, such that they warrant a reaction of justifiable self-defense or a declaration of war. Policy gaps resulted from failed articulation of bilateral, informal commitments with other powers to refrain from shared concepts of cyber aggression. Given the fact that any country in possession of a large-scale, practical quantum computer could break today's asymmetric cryptosystems, the impact of ceding leadership in quantum computing brings significant national security implications; U.S. quantum supremacy is in dispute.

A. Associatory Emerging Technologies

Quantum computing is likely to power future AI systems and holds enormous promise, but it could also be very dangerous in the wrong hands [35]. AI is considered a national security issue by the U.S. In June 2018, the U.S. Department of Defense (DoD) established the Joint Artificial Intelligence Center to scale AI and its impact across the DoD, accelerate translating AI research into military capabilities, and strengthen our Nation's defense. The Defense Advanced Research Projects Agency (DARPA) announced in September 2018 a multi-year investment of more than $2 billion in new and existing programs called the AI Next campaign include automating critical DoD business processes, such as security clearance vetting or accrediting software systems for operational deployment; improving the robustness and reliability of AI systems; enhancing the security and resiliency of machine learning and AI technologies [36]. AI is becoming smarter, faster, and more humanlike due to the anticipated advancement of quantum computing. It has become a critical emerging technology strategy for the U.S. since 2019 [37]. AI is of paramount importance to maintaining the economic and national security of the U.S. and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities [38]. Blockchain and its associated cryptocurrency technology falls under the Financial Sector of Critical Infrastructure. In 2020, the U.S. took proactive measures to prevent competing nation states from exploiting quantum affected blockchain encryption [39]. The key points include promoting U.S. leadership in technology and economic competitiveness, support technological advances and ensure responsible development and use

of digital assets calling to produce more reports and research on the topic. It outlined a government strategy to safeguard national security [40].

B. Advancing Military Capabilities

Quantum enhanced cyberattacks are predicted to have more devastating effects that intensifies the prospect of cyberwar. Quantum enabled cyberwarfare, creates a seismic shift of policy and it has the potential to transform warfare into a hybrid war, non-kinetic and kinetic warfare. Distinctive characteristics of cyberwar share similarities with its traditional counterpart. Espionage and sabotage have technologically merged cyberwar as states threaten each other with prepositioned malware in each other's previously probed critical infrastructures. This shift of warfare has been tacitly adopted by the U.S., Russia, and China [41]. What is not been adopted are the geopolitical norms and policies on which emerging technology-based cyberwarfare is based [42]. The literature reviewed reveals that, while dearth, there is current technical research attempting to address these threats. However, relying on technical solutions alone to protect a country's critical infrastructure is alarmingly incomplete. Senior U.S. Defense Officials declare that it is not possible for nation states to respond against such rapidly changing cyber-attacks [43]. A challenge in classifying a definition of cyberattack arises from the fact that nation states are often unable to determine whether an attack was civilian or military in origin, or more importantly, whether the attack was ordered by a hostile state or committed by a rogue private actor. Cyber-attacks conducted by non-state actors on the behalf of a nation state employing emerging technologies offer various ways to conduct cyberwarfare operations without attribution [44] which enable covert cyber espionage, network reconnaissance scans and social engineering attempts. Due to the common practice of intentional misdirection by cyber threat actors, many scholars and legal practitioners have criticized the very notion of expanding the U.N.'s scheme of self-defense under Article 51 to include responses to alleged cyberattacks [45]. If sovereign nations lack the capacity to accurately and timely determine the source of an attack, acting in self-defense is problematic given the substantial risk of misdirected retaliation. Emerging technology-based capabilities, such as the development of quantum-resistant algorithms and technologies, could indeed provide a means of defense for developed nations. Such a solution is not viable for those states without the technological capability to shield against attacks from quantum computers.

C. Supremacy Seeking, Capacity Building, and Funding

U.S. National Defense Authorization Act established the Air Force Quantum Information Science Innovation Center as part of a broader defense effort to accelerate research, while also coordinating with the National Quantum Coordination Office for workforce development, enhancing awareness and reducing risk of cybersecurity threats, and the development of ethical guidelines for the use of quantum technology [46]. National Quantum Initiative Act coordinated, ten-year national strategy to support quantum technologies with approximately $1.275 billion in total funding over five years [47]. The Act, facilitated by Executive Order 13885 established the National Quantum Initiative Advisory Committee under the Office of Science and Technology Policy to provide a framework and investment mechanism through which the National Science Foundation, National Institute for Standards and Technology (NIST), and Department of Energy (DoE) can support research, development, and application of quantum technology. The law also directs DoE to establish multiple National Quantum Information Science Research Centers and requires NIST to support human resources development in all aspects of quantum information science as well as identify future cybersecurity standards that support robust quantum developments [47]. National Strategic Overview for Quantum Information Science developed by the National Science and Technology Council's (NSTC) Subcommittee on Quantum Information Science (SCQIS) to create a quantum-smart workforce, deepening engagement with industry, providing critical infrastructure to support research and application, and advancing international cooperation [48].

In a significant supremacy seeking approach, the U.S. National Security Presidential Memorandum 13 frees the military to engage, without a lengthy approval process, in actions that fall below the use of force or a level that would cause death, destruction, or significant economic impacts [49]. Correspondingly, the NATO Tallinn Manual stipulates nation-states will breach a state's sovereignty if the attacking states cause damage to NATO cyberinfrastructure or if it causes interruption to NATO governmental functions [50]. Executive Order 13702 was a precursor to the National Quantum Initiative Act that aimed to advance U.S. leadership in the quantum field by establishing a National Strategic Computing Initiative in which the SCQIS published the National Strategic Overview for Quantum Information Science which stated one of the key efforts is to maintain national security [47].

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 2, pp: (1-21), Month: April - June 2022, Available at: www.researchpublish.com

The successful development of technologies based on quantum computing will enable increasingly more advanced quantum research as well as supporting and benefiting emerging technologies such as artificial intelligence, blockchain, and Internet of Things (IoT) which have all be linked to research towards improving critical infrastructure; another key initiative NSTC. Creating new markets and industries enhance a state's ability to address national security needs, but the scientific and economic advances lead to new risks. There is an expansion of the relevant Federal and industrial infrastructure and support activities the U.S. states is needed to accelerate progress and prepare for the adoption the ensuing quantum technologies. The U.S. defense and intelligence communities have been strong investors in quantum research and development for the last twenty years. National security requirements drive the advancement of new science and technology and enable economic development through enhanced Government investments, dedicated initiatives, and cross agency collaborations. The quantum technologies are anticipated to provide solutions to national security concerns. Current funding is primarily focused on quantum sensing (Fig. 2). Correspondingly, it should be inferred that the lack of funding in direct quantum security focused research areas lack the contingent governance and regulation policies to authorize and mandate such Federal expenditures.

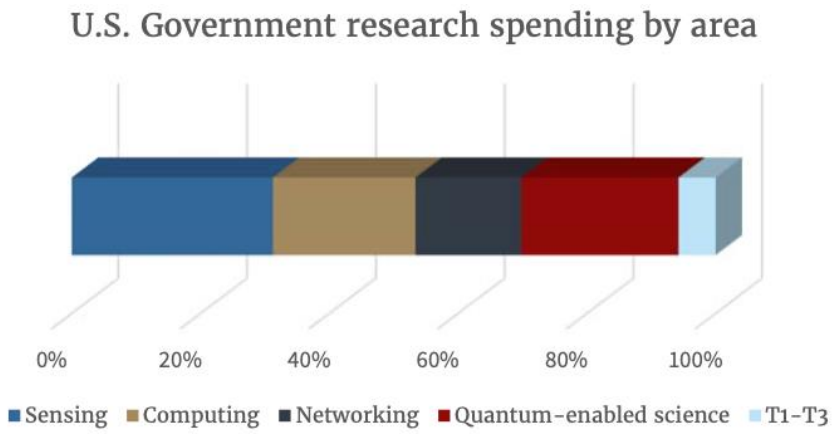

Figure 2: 2021 Federal Funding Areas in Quantum Computing.

D. Challenge to Policy and Regulation

Global investments, development of quantum technologies, and related research and policy development dialogue, are all still in the early stages. Industry has faced challenges as in not fully participating in dialogue [51]. The Digital Geneva Convention was expanded after Microsoft met criticism for focusing solely on state responsibilities. Microsoft acknowledged that norms are not just for governments, and in addition to offensive and defensive norms, there are industry norms that should focus on defense and incident-response teams that collaborate to maintain security Despite progress in industry, the United Nations Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, purport the most fundamental issue under dispute is not industry but the claim from autocratic regimes like China and Russia the right to control their information borders claiming cyber sovereignty [52]. Nonetheless, the reality of cyberattacks and cyberwarfare necessitate consensus on defining cyber-attack and establishing multi-lateral nation-state norms as to their rights to defend against an attack, distinguish attribution of attack, and determine appropriate response [53]. The status of international discussion does not provide the basis for believing that any large-scale agreements on emerging technology norms are feasible in the near term. While nations compete with one another in quantum innovation, the laws governing cyberwarfare remains indeterminate and unsettled [54].

As previously asserted, the challenge in classifying a definition of cyberattack arises from the fact that nation states are often unable to determine whether an attack was civilian or military in origin, or more importantly, whether the attack was ordered by a hostile state or committed by a rogue threat actor. The difficulty of attributing cyberattacks lies in the fact that there are generally no flags being flown, no soldiers to question, and no physical weapons to determine the country of origin. There is generally a considerable amount of time that elapses before it is clear from which actor or nation the attack originated. Due to the common practice of intentional misdirection by cyber actors, many scholars and legal practitioners have criticized the very notion of expanding the U.N.'s construction of self-defense under Article 51 to

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 2, pp: (1-21), Month: April - June 2022, Available at: www.researchpublish.com

include responses to alleged cyberattacks [45]. If sovereign nations lack the capacity to accurately and timely determine the source of an attack, acting in self-defense is unwise, critics argue, given the substantial risk of misdirected retaliation.

E. Current U.S. Governance and Regulation

The U.S. government has been funding quantum research for over 20 years and collaboration with industry and government increased, in December 2016, at the Information Technology & Innovation Foundation's (ITIF), The Future of Quantum Computing: Policy Implications for National Security and Industrial Competitiveness conference [55]. Tim Polk, assistant director of cybersecurity at the White House Office of Science and Technology Policy, emphasized the role that government and industry must play in the quantum research and development. The U.S. established a systematic, national approach to quantum information research and development, organized under a single brand and coordinated by the National Science and Technology Council's (NSTC) Subcommittee on Quantum Information Science (SCQIS). However, much of existing policy attention surrounds research and development strategy rather than governance. The National Quantum Initiative (NQI) Act, a multi-agency program spanning the National Science Foundation, the Department of Energy, and the National Institute of Standards and Technology to support research and workforce development for Quantum Information Science (QIS). It authorized $1.2B for research spending and workforce development over five years and established mechanisms to coordinate research across the Federal agencies [56]. Following the passage of the NQI Act, the NSTC released the National Strategic Overview for quantum, addressing the actions needed to translate scientific progress in quantum with industry. The NQI fostered public-private partnerships, by creating a Quantum Economic Development Consortium (QED-C) which unites industry, academic, and other stakeholders with support from multiple government agencies (Fig. 3). By identifying gaps in technology, standards, and workforce development and addressing those gaps collectively, QED-C aims to support the development of a commercial quantum industry and supply chain.

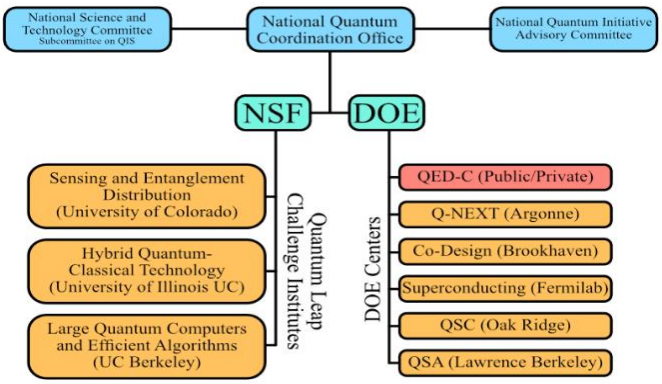

Figure 3: U.S. agencies governing the National Quantum Initiative Act and research funded.

F. Current International Governance and Regulation

The Budapest Convention, also known as the Treaty 185: Convention on Cybercrime, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Ratified in 2001, the treaty's main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime (50). The North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn, Estonia invited an independent group of experts to produce a manual on the international law governing cyber warfare, which became the Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare. The use of cyber weapons continued, notably by Russia during its war with Georgia in 2008 and by Israel and the U.S. against Iran in 2010, prompting the CCDCOE to invite a new International Group of Experts to expand the Tallinn Manual's scope to include governance of cyber operations during peacetime. This developed into the Tallinn Manual. Although NATO's product has spurred international cooperation in cyberwarfare, it has not been internationally adopted as a legal protocol for war and peace-time cyber conflict.

The U.S. position is that international law applies in cyberspace, it recognizes that not all states agree with that interpretation [29]. NATO member states agree that in cyberspace, state sovereignty extends beyond physical borders, reaching "any cyber infrastructure located on their territory and activities associated with that cyber infrastructure" [57]. More broadly, the United Nations is taking note of the U.S.'s emerging technology priorities and strategy [58]. If the U.S., or its allies and partners, employs offensive cyber means more widely, it risks creating a pattern of state behavior suggesting that any norms in this area will not be reliably observed. An important step for this effort to build trust, credibility, and leadership should involve a senior-level speech that clearly lays out the criteria that govern U.S. cyber operations. Emphasis to establish trust between nation states to ensure quantum computing technology does not fall into the wrong hands is viable but recognizing the inability of arms control to adequately prepare for quantum computing necessitates continued research to develop solutions to harden devices, systems, and networks against EDT threats. Governments, scholars, nongovernmental organizations (NGOs), and private-sector companies have made dozens of proposals for rules and norms to govern cyber activities, including some grounded in international law. The U.S. government has for several years been engaged in multiple international forums to advance the goal of building cyber norms. In May and June 2021, with the release of the latest United Nations Group of Governmental Experts (GGE) report on cyber norms and the proposals for norms raised in the June summit between the U.S. and Russia [59]. Since 2010, each GGE had been able to make significant landmark advances in international consensus on ICT issues, but this pattern of cooperation came to an end at the closure of the 2017 GGE. The representatives were unable to come to a consensus regarding the identification of threats to information security. Between 2019 and 2021, the GGE conducted its latest series of meetings, culminating in the issuance of a report in May 2021. This session ended on a more positive note, with a report that, in the words of Michael Schmitt, "managed to resurrect"40 the GGE process after the failure of the previous round. The 2021 GGE report reemphasizes the risks posed by information threats and reaffirms the call on all UN member states to seek security and stability in this realm. Another international proposal in cyber norms emerged in 2018, with the French government's announcement of the Paris Call for Trust and Security in Cyberspace [60]. It is a combined public-private set of commitments and is therefore not an intergovernmental process per se, but dozens of states have signed the accord. By December 2020, 79 states, 32 public authorities at other levels, 368 nongovernmental groups, and 680 private-sector companies had endorsed its principles. The Paris compact includes nine principles to maintain cyber peace and stability. These overlap with many proposed norms of the GGE process and other suggested normative frameworks for cyber peace and stability. CGE and to date has not analyzed whether an operation using a quantum computer constitutes the use of force comparatively to the Nuclear Non-Proliferation Treaty (NPT) and Chemical Weapons Convention (CWC) which offer examples of treaties in other dual use areas that are analogous to cyber space. These treaties seek to terminate the use or possession of chemical and nuclear weapons, while promoting the use of chemicals and nuclear power for nonmilitary purposes. For both the CWC and NPT, the Security Council of the United Nations could become involved if members violate these treaties. Member-states would still be permitted to use quantum computing for non-military purposes. Enforcement challenges are involved, but the success of these treaties can provide the international community a plausible way forward.

V. DISCUSSION AND RECOMMENDATIONS

The U.S. views emerging technologies such as quantum computing and artificial intelligence as transformative and mutually enabling technologies that impact national security. National security needs often drive advancements in new science and technology and enable economic development. In the Artificial Intelligence and Quantum Information Science Report, the White House has aligned research and development funding to accelerate aligned innovations [61]. The global quantum technology market will reach $42.4 billion by 2027. Quantum computing will lead the market at $16.1 billion by 2027 and 39.4% compound annual growth rate [62]. The capabilities of these emerging technologies create significant national security concerns, both in the U.S. and for other countries investing heavily in quantum technologies, such as China. Quantum computing is among the technologies that require significant resource investment, giving rise to issues of equity, access and distribution of benefits and risks, especially for under-resourced nations. It is an emergent and potentially disruptive technology that introduces the potential for new capabilities, such as improving the effectiveness of existing capabilities and even introduction new ones, towards nation state supremacy [5]. The quantum component is an escalation option towards a full spectrum cyberwar used conjunction with kinetic military engagements involving all five domains of warfare: cyber being the newest [43][54]. Quantum Warfare is the latest technological advancement of warfare (Fig. 1). It represents an evolution of nation-state capabilities (63). Unlike the other domains, the conflicts in cyberwar to date, have not involved acknowledged nation-state military-on-military

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 2, pp: (1-21), Month: April - June 2022, Available at: www.researchpublish.com

engagements. Development and implementation of quantum technologies are expected to have a significant impact on our ability to address some of the most complex national security problems [64].

There is a need for global guidelines to assess and manage the opportunities and risks of quantum computing, providing a shared set of principles for all stakeholders, to shape the technology and benefit humanity [2]. Attacks by quantum computers, particularly in a world in which only a handful of states have access to them, present unique challenges for defining a cyberattack. Indeed, even if the international community were to settle on a definition for cyberattacks in general, it may not be adequate to address the profound power disparity presented by the control of quantum computing by a few states or sub-national actors. Lack of collaboration contributes to the lack of uniformity of existing cyberwarfare policy, but a more significant problem with policy development is the historical length of accord discourse. Approximately 20 years since the Budapest Convention. Given the expert estimates that quantum supremacy will likely be achieved within the next 10 years, Quantum policy need to occur more quickly. In the same way that states had to re-conceptualize the use of force after the advent of nuclear weapons, quantum computing requires us to reconsider how we approach cyberattacks. Even if the effects-based approach is the most plausible standard for cyberattacks in general, it matters if an attack is made with a quantum computer. Until the international community's cyber systems have evolved in such a manner to reduce the threat of quantum computing attacks to that of conventional cyberattacks, this proposed approach would provide nations with a viable and efficient means of responding with appropriate force to a quantum computing attacks as they arise. Atomic bomb 1945, first nuclear weapons treaty 1963; 18 years. The U.S. has acknowledged there is an issue with cybersecurity policy and has outlined strategies going forward. However, there continues a lack of effective policy development, response to incidences, and metrics to determine progress. Nation state military power is increasingly becoming synonymous with development of emerging and disruptive technologies (EDTs). Studies vary in focus, most of them concentrate on the medium term, which includes EDTs that are likely to mature in the 2040s, with early adoptions beginning in the mid-2030s and late adoptions by 2050 [11]. This is the perspective taken by the NATO Science & Technology Organization, the U.S. National Intelligence Council's Global Trends Project, and other notable efforts [65]. A 2022 report by the European Leadership Network on Nuclear decision making, complexity and EDTs cite studies involving artificial intelligence and nuclear deterrence, quantum technology and nuclear deterrence, and space weapons and nuclear deterrence. Many EDTs have the potential to reshape international politics by changing the nature of military and economic power. These include technologies that could shift the cost of attacking compared to defending, technologies that render some forms of military power completely obsolete or irrelevant, technologies that change the nature of economic production, and technologies that facilitate innovation and further technological development. The option of asymmetric response would depend on whether EDT effects could be tailored to destroy, disrupt, or disable certain set of targets, including targets in all five domains of the battlefield. Using EDTs as an alternative to a nuclear strike would require nation states to have an "ace in the hole", a pre-planned option for strategic non-nuclear attack sufficient to bring an adversary to defeat or to the negotiations without risking all out nuclear war for conflict situations. The current nuclear decision-making model could provide a basis for an asymmetric EDT response (Fig. 4).

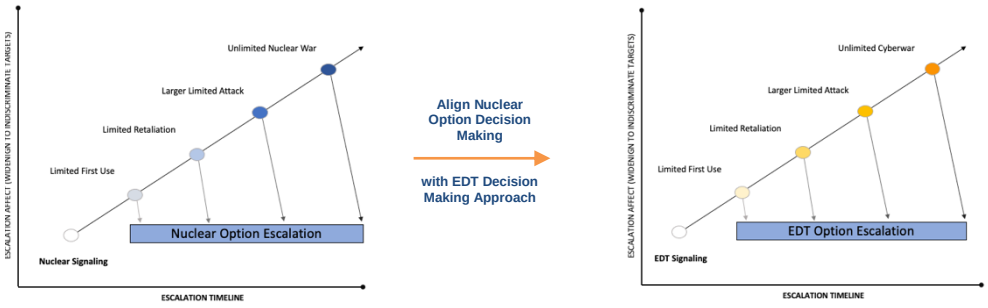

Figure 4: Nuclear Escalation Decision Model as a Basis for Weaponized Emerging Technology Employment Model.

The first step, nuclear signaling would be a nation state announcement such as Russia President Putin to the West against their involvement in the Russian and Ukrainian War [66]. The first step in EDT signaling is yet to be observed but could be a nation state announcement such as U.S. President Obama warning China of cyber retaliation [67]. Each of the

escalating steps would have similar demarcations and focus, limited first use could be targeting a specific nation state capability like a nuclear arms program. Limited attacks to unlimited 'war' could be expanding targets to include critical infrastructures with the intent of affect damaging military capabilities but also causing collateral civilian damages to unlimited indiscriminate use of WMD (of which EDTs would now be considered) against civilian targets. Developing an escalation model for EDTs could paradoxically serve as a de-escalation approach for nation states to prevent indiscriminate quantum-enabled cyberwar. The proliferation of EDTs among global powers is predicted to accelerate during the next thirty years. As the dawn of quantum computing technology approaches, and as developed nations continue to express a clear reluctance to forfeiting highly effective technologies, the world could enter a 'Quantum Cold War'. Just as the threat of mutually assured destruction by nuclear warfare caused the U.S. and Soviet Union to exhibit restraint in the use of their own unclear stockpiles. Disarmament of quantum computers, perhaps through a 'Weaponized Quantum Computer Convention' modeled after the CWC, and NPT would provide a framework for countermeasures, sanctions, and law enforcement for signatory states. There is a reciprocal link between nuclear capabilities, proliferation, and deterrence and quantum capabilities, proliferation, and deterrence as the first quantum-based technology resulted in nuclear weapons and energy; and now, with the quantum-based computer such as atoms, ions, electrons, photons, molecules, or various quasiparticles. While it can be argued that Western deterrence and policies in a traditional sense have led to a state of relative peace since 1945, this same policy-driven leadership has not been present when it comes to the use and regulation of cyber capabilities. Western governments have not been consistent in their response to hold actors accountable for cyber incidents [68]. This is part due the diverse set of actors in cyberspace, the creation of policy reactively, and the difficulty of attribution when it comes to cyberattacks.

A. Cyberwarfare and Policy Trend Analysis

Geopolitical cyber decision-making and policy development has been predominately reactive and driven by specific cyber-attack events. International cyber-attacks accelerated with Stuxnet, Duqu, Wiper and Flame; collectively known as SDWF. Stuxnet deactivated 1,000 centrifuges of 5,000 in Iran and delayed its nuclear program for 1.5 to 2 years. This attack was the successor of the cyber-attack program started by the Bush government under the codename "Olympic Games" and continued through the Obama government [69]. So too has policy development parallelly during the same timeframe. Other examples include the 2007, possibly Russian, cyber-attacks against Estonia. This is a series of cyber-attacks targeted websites of the prime minister, communication infrastructure, and finance sector. As a temporary solution, Estonia has isolated itself so that no one could get into the country, digitally. This had a consequence that people with bank accounts but outside the country at that time could not access their accounts. After the attack, NATO's Cooperative Cyber Defense Centre of Excellence was established in Tallinn, Estonia [70]. When Russia declared war on Georgia in 2008 for its independence from South Ossetia, cyber-attacks blocked channels of communication. Russian cyber-attacks on Georgian government websites indicated the first use of integrated cyber and kinetic attacks; hybrid warfare. [71]. Both Estonia and Georgia attacks involved a nation state employing cyberwarfare aligned with military action. In 2021, the White House blacklisted eight Chinese quantum computing companies over concerns that the technology they possess poses a threat to national security. The companies were cited by the White House to prevent U.S. emerging technologies from being used for the China's quantum computing efforts that support military applications, such as counter-stealth and counter-submarine applications and the ability to break encryption or develop unbreakable encryption [72]. These actions were preliminarily taken under the authority of the Export Control Reform Act of 2018 and its implementing regulations, the Export Administration Regulations (EAR). However, there have been challenges because while the EAR currently includes AI, it does not include quantum computing. The Department of State manages the export of dedicated military technologies with the U.S. Munitions List (USML), while additional regimes and international law frameworks support nonproliferation of nuclear, chemical, biological, and missile technologies (i.e., Arms Export Control Act, 1976), these regulatory tools were built for explosives, jet fighters, and nuclear weapons. New regulatory rules could help to overcome these challenges and effectively control potential threats from new technologies without stifling innovation.

We plotted policy event trajectories to determine future probabilistic trends provides visualization of statistical inference on real data considering optimized temporal rules to describe the course of measured variables over age or time (Fig. 5). The cyberwarfare attack occurrence reveals that while they are the impetus for nation state cyber policies, analysis of normalized data point trajectories indicate that policies are not being equitably established or evolved in correlation of their shared events. Scatter plot chart aggregation depicts the different points with value on the chart scattered randomly,

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 10, Issue 2, pp: (1-21), Month: April - June 2022, Available at: www.researchpublish.com

while also showing the relationship between the two variables in linear regression line equation is expressed as a correlation coefficient, R^2 (R-squared). Plotting convergence (Fig. 5) of cyberwarfare attack occurrence to nation state cyber policies, the variance for both methods is proportional to $1n1n$, the order of convergence is $(1n\surd)\ O\ (1n)$. The scatter plot chart depicts two random variables from a probabilistic analysis, against each other on the same plot. The visualization of this convergence indicates that correlated attack and policy events have equitably occurred in relation to their shared events given their standard deviation with respect to the sample size.

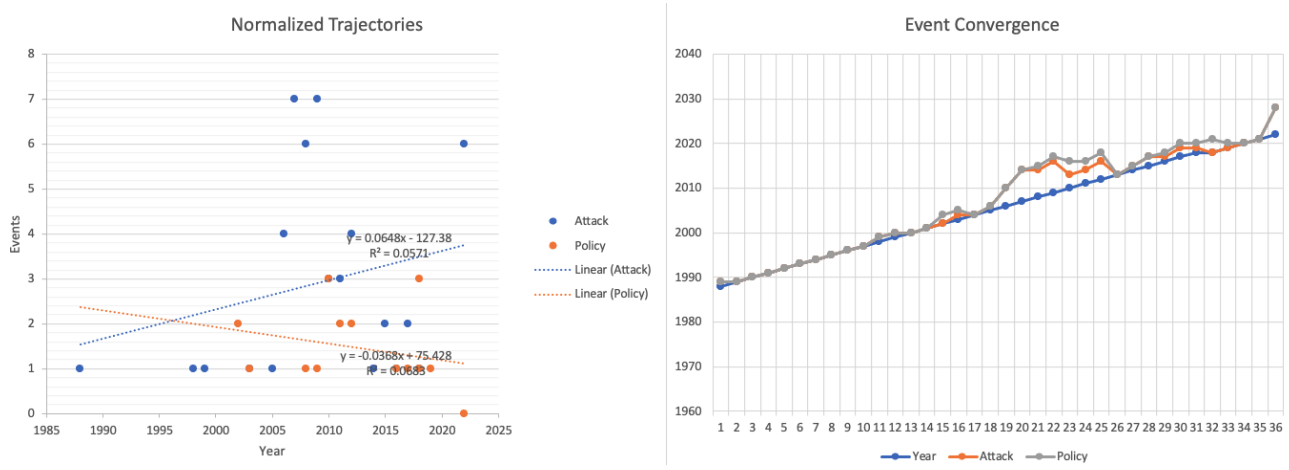

Figure 5: Correlating Cyberattacks with Policy Development.

Given the disorganized policy regime, a unified regime will be required through an international accord addressing cyber security and its status in international law. The new treaty should define when a cyber-attack rises to the level of an armed attack; clarify which provisions of international law apply during cyber warfare; and provide for enforcement mechanisms in the event of breach [73]. Global problems without cooperative solutions lead to conflicts. Peace is not just the suspension of war. Peace is made up of all the solutions that help reduce international tensions. The Paris Peace Forum is a multilateral and multinational platform of multi-stakeholders seeking to develop coordination, rules, and capacities that answer global problems. The Paris Peace Forum holds the Paris Call for Trust and Security in Cyberspace annually in November since 2018 [60]. The Forum is a candidate to undertake governance of Quantum Computing Cybersecurity issues as it currently is responsible for Governing Artificial Intelligence Cybersecurity issues of AI challenges and opportunities for policymakers: How to reconcile algorithms and inclusive policies [74].

B. Workforce Development Trends

In 2020, the NSF invested $9.75 million in 13 U.S. universities with leading research and instruction in computer science and engineering to encourage them to hire tenured and tenure-track faculty in quantum computing. Congressional legislation introduced in 2020 addresses quantum workforce development with impetus on national security. The Bill's authors purport that quantum plays a critical role in our national security and economy and will be at the forefront of U.S. innovative defense technologies that will help to maintain our military edge over other nation states, specifically China [75]. Senate legislation introduced in 2021 continues to address quantum workforce development with a national security focus. The Bill's authors state it provides public-private talent exchange programs in the U.S. DoD to quantum information sciences and technology research, to increase coordination across agencies and emphasize opportunities in the DoD for quantum information sciences and technology research [76].

VI. RECOMMENDATIONS

Although there is insufficient consensus among nation states towards unified policy, there is consensus among industry in technology, including Google, Amazon, and Microsoft, that quantum computers will be a commercial reality by 2026. A successful legal framework must include a consensus for; defining emerging technology norms, prohibitions on cyberattacks targeting civilian dependent critical infrastructure, restrictions on interference in or manipulation of electoral and political processes, and activities designed to damage the availability or integrity of the public core of the internet. With data privacy and national security at stake, agile and adaptive regulatory strategies are needed to manage the risks of impending quantum computers without thwarting their potential benefits. Quantum computing has benefited from

research and implementation of other emerging technologies, such as AI. It is crucial to keep the discourse on the governance of quantum computing distinct from discussions relating to classical computing technologies. However, there is an opportunity to introduce common standards and benchmarks to ease adoption and acceptance of quantum computing technologies as well as ensure a wider acceptance of related emerging technologies. Developing policy to accelerate the development of emerging technologies that benefit from quantum advantages. A global policy approach at the level of the UN, the World Trade Organization (WTO) or the G7 is vital, and it is time to begin the dialogue. A quantum computing enforcement regime should set clear and enforceable prohibitions for improper use. The U.S. should renounce cyber-attacks and voluntarily promote and participate in nonproliferation agreements in which acts such as the 2012 Stuxnet attack on Iranian nuclear SCADA systems in olive branch effort to facilitate a cyberwar détente. The growing risk posed by cyber threats to national security was powerfully reinforced in the December 2020 revelations about the alleged Russian SolarWinds cyber espionage campaign, in which access to a third-party vendor's software was used to gain access to dozens of governments and private-sector information systems [77]. Although this was a case of cyber espionage, at least so far, and not a direct attack using cyber means, it nonetheless generated multiple calls in the U.S. to retaliate in some way. The event demonstrated once again the general risk, as well as escalatory potential, of cyber aggression.

Shared global aspirational statements has achieved formal recognition and promises of enforcement by all the major cyber powers. However, states continue to act with a cyber impunity, and it is not clear whether any of these powers are willing to agree to enough mutual, voluntary restrictions on their freedom of action in cyberspace to make a broader cyber norms regime possible. The gap on these issues between the U.S., China and Russia remain very wide, and there is limited room for mutually agreed restraints on behavior. China, Russia, and the U.S. are all actively exploring how cyber capabilities could help to shape future battlefields, including by limiting the communications and awareness of adversaries, and disrupting the functioning of sophisticated weapons systems that rely on information technology. Due to its massive capabilities, it is worth considering whether quantum computing technology should have export limitations or be limited to solving humanitarian issues only [60]. Several bills have been introduced that would impose limits on the export of quantum technologies to China, including those related to QIS computing and simulation: China Technology Transfer Control Act of 2019, S. 1459, H.R. 3532; Fair Trade with China Enforcement Act, S. 2, H.R. 704; Uighur Intervention and Global Humanitarian Unified Response (UIGHUR) Act of 2019, H.R. 1025; and U.S. Export Finance Agency Act of 2019, H.R. 3407 [CRS, 2020]. As the EAR has successfully been used to protect U.S. National Security with regards to another emerging technology, AI. In this regard, governments, corporations, and academics should accelerate the development of quantum-proof encryption, and they should push its implementation within their own jurisdictions. U.S. policymakers, for instance, could use the federal acquisition regulation (FAR) to push quantum-safe encryption in federal agencies and across the defense industrial base. The EAR should be immediately updated to include Quantum Computing. All major powers are likely to retain an interest in developing and improving such capabilities, as well as building resilience against their effects when used by others, particularly given the extreme difficulties in verifying any promises of cyber nonproliferation and disarmament in this area. The process of debating and developing such norms has now been underway for roughly 20 years. It began at least with the GGE process in the early 2000s, but even that built on earlier proposals for the role of international law stretching back to the 1990s. In 2004, the U.N. formed GGE to discuss the formal development of international cyber norms and practices. The meeting concluded without consensus, and another meeting of the GGE was scheduled for 2010. This 2010 meeting would prove to be the first in a series of GGE meetings from 2010 to 2021. The U.S. program for promoting and catalyzing norms has been active since at least 2011, with the release of the U.S. cybersecurity strategy. In the years leading up to the 2010 GGE, international cyber-attacks had risen significantly. These incidents included the widespread attack on Estonian organizations in 2007 and the 2008 breach of the U.S. military network, the latter of which led to the creation of the U.S. Cyber Command. The increase in the destructive nature of cyber-attacks highlighted the importance of ICT security in the international sphere. Yet the 2010 GGE did not result in any landmark resolutions, instead concluding with the consensus that there was a lack of shared understanding regarding international norms pertaining to state use of ICTs, and that further dialogue was necessary to avoid misunderstandings and misperception between nations. Following the 2010 GGE, Russia, China, Tajikistan, and Uzbekistan submitted a draft International Code of Conduct for Information Security to the U.N. in September 2011. The document declared that states would lead all elements of society, including its information and communication private sectors, to understand their roles and responsibilities concerning information security. At the 2013 GGE, nations agreed for the first time that international law, and in particular the Charter of the U.N., is applicable in cyberspace. This

agreement was considered a landmark in international cyber discussions, as it was the first time Russia and China had publicly declared this stance. Several bilateral meetings were held to further the international discussion of cyber norms. The U.S. and Russia established a new bilateral working group focused on ICT threats. The group would utilize the Nuclear Risk Reduction Center to increase transparency and avoid miscommunication during cyber incidents.

The consistent nonuse of nuclear weapons since 1945 has been a central feature of the modern strategic environment. The nuclear policy regime may offer a model for policing dangerous yet vital capabilities. Nation states, including most notably the U.S, Soviet Union, and Russia, have amassed tremendous stockpiles of nuclear weapons. While they have not been used in any of the myriad conflicts since 1945, these weapons have played a central role in affecting the decision making of key states the past 75 years. This non-use has been attributed to several factors, including strategic calculations regarding likely adversary reactions to nuclear use, but also to international norms. Nuclear weapons have been categorized as different in nature from conventional weapons, lumped together with biological and chemical weapons as weapons of mass destruction (WMO). With the prospect of quantum capabilities, this new aspect of cyberwar should be seen as also a WMO as the U.S. has adopted a more aggressive offensive cyber policy, with the stated goal of deterring potential attacks on U.S. systems, in its defend forward approach. The new approach should include a linked set of partial agreements, processes, and emergent norms that add up to a strong collective effect. These could include NGO advocacy campaigns; inter- governmental agreements among like-minded states; private-sector conventions; and nongovernmental efforts at detection, notification, and transparency. The nature of the issue, with so many complex subcomponents and stakeholders, and the pervasiveness of the internet, mean that information-security agreements have major ramifications for other issue areas, which would further support such a consultative, collaborative approach. This approach could make modified use of the current U.S. emphasis on international law. Agreements about international legal principles can support the development of norms, but they are not a substitute for it. The U.S. must pursue a broad-based, comprehensive, and multistakeholder approach while still building multilateral support for the idea that international law proscribes certain behaviors. A multistakeholder strategy must continue to reach beyond state actors, however, and embrace non-state NGO groups and industry in the cybersecurity realm. These include, most obviously, cybersecurity firms, whose operations provide critical awareness of ongoing threats and practices; software companies with an obvious stake in global cybersecurity (such as Microsoft, which has been a leader in promulgating private-sector cyber norm proposals); social media platforms; and NGOs leading the discussion on cybersecurity and cyber norms. The U.S. should continue to expand its consultations with such stakeholders in ways that will accelerate the emergence of effective norms and help to build public and international consensus.

Our research provides several primary findings on the character of and prospects for quantum computing legislation; Regulatory Policy and Norms, Workforce Skills and Training, and Quantum Technology Access. The first is there is no clear or common, emerging on consensus for unified policy norms. While some principles are common to international aspirational statements, no one internationally accepted accord has been achieved by all the major cyber nation states, all of whom continue to act with significant degree of cyber impunity. The second is education; there is a growing need to educate the quantum workforce towards developing fundamental skills required for not only research and development but also for technology sustainment and policy creation. The third is removing barriers to access; without hands-on (albeit virtually through the cloud) accessibility for students through industry from all socio-economic communities, the first two recommendations (policy and education) would suffer from lack of cognitive diversity which is essential for innovation [78].

A. Regulatory Policy and Norms

Creating an agile and adaptive regulatory strategy that creates global standards to reduce the risks arising from quantum computing. With the fifth domain purporting new approaches to wartime and the intensifying of nation-states' offensive strategies [79], it is vital to implement a less ambiguous international legal framework. There is a myriad of competing published policies from various nation-states and international political bodies that complicate coordinated responses. Further work is necessary at all levels to adequately address the challenges posed by cyberterrorism and other forms of large-scale attacks on and through computer systems, which threaten the national security, public safety, or the economic well-being of states. Quantum policy strategies will help nation states prepare quantum computers without undermining innovation, drawing on technical standards and codes of conduct as regulatory tools. Government alignment to private standards will be critical for enabling industry adoption and government regulation of emerging technologies. The Institute of Electrical and Electronics Engineers Standards Association (IEEE) is currently working on setting

standards for terminology and performance metrics in quantum computing. Given the global authority and reputation of IEEE, these standards, when adopted, provide government insight on development trajectories. These voluntary, technical standards can give government and industry a common language to speak by creating agreed-upon definitions. Technical standards can facilitate policy conversations about how powerful quantum computers really are and what types of risks are realistic and deserve policymakers' attention. Effective political policies and strategies tend to have characteristics that are less complex and less abstract [29]. However, these characteristics pose challenges to developing norms to govern behavior in cyberspace. Many types of cyber behavior that policymakers may wish to govern can be highly technical in nature and more difficult to simplify. Based on previous attempts to achieve formal mutually agreed upon policy on other national security issues, as those issues involving cyberwarfare, it is not clear whether any of these powers are willing to agree to enough mutual, voluntary restrictions on their freedom of action in cyberspace to make a broader regime of quantum computing norms. Emerging technologies has specific characteristics that may impede the development of norms to restrict state behavior preventing the weaponization of such capabilities. Policy and strategy recommendations for facilitating wider adoption of emerging technologies to safeguard national security will likely rely on promoting behavior norms through aligned efforts with entities that have effective, collaborative, international members such as nongovernmental organizations (NGOs), experts from more broad civil society, and globally venerated academia institutes may overcome the stigma and suspicion of government-imposed principles. Policy must be able to attribute international law's application to state and state-sponsored operations in cyberspace. Proliferation of quantum supremacy or quantum enabled capabilities should be monitored and mitigated. Leveraging international collaboration to further advance international peace and stability.

B. Workforce Skills and Training

Growth within industry, academia, and Government requires maintaining and expanding a broad and viable workforce, a quantum-smart workforce, able to enact critical elements of the research and development enterprise. Within an organization's quantum workforce, some positions will require very advanced quantum knowledge and skills, often at the PhD level, while other positions will include "non quantum" engineers, software developers, and technicians who contribute immensely to the designing, making, selling, and supporting of products. These other non-quantum roles are essential yet require much less formal training in quantum. Such a workforce will attract and retain key jobs throughout the Nation and enable new industrial and academic efforts that rely upon quantum computing as a base technology. There will be an ever-increasing need for effective and scientifically accurate communication by those who describe new quantum technologies to the public. When considering the response of higher education to train this workforce, the full range of job types must be considered. ISACA, a leader in technology-based industry certifications, provides a series of emerging technology certifications: Blockchain Fundamentals, IoT Fundamentals, Artificial Intelligence Fundamentals that make up their Certified in Emerging Technology certification [80]. NSF launched the National Q-12 Education Partnership, an initiative to expand access to K-12 quantum information science education. In addition, industry-led consortiums, such as QED-C, which was established by the National Quantum Initiative Act, are working to identify gaps in the "workforce that need to be filled to realize diverse applications." The target participants in such a training program would include a broad swath, from training technicians without necessarily advanced degrees, to outreach programs that introduce high school students to the concepts of quantum computing, to bringing PhD scientists into the quantum workforce from an adjacent field, to contributing scientists from supporting fields (e.g., computer science, materials science, electrical engineering, cryogenic engineering, etc.) that require or desire specific training and experience in quantum (computing) topics specifically. To support this, funding and/or dedicated facilities should be provided for workforce training that makes quantum systems accessible to under-represented institutions and populations [81]. Quantum computers are reliant on a developing workforce; to educate and train them, knowledge needs to be shared more widely, and hence there is an opportunity to convince corporations developing quantum computing to grant wider access beyond purely commercial considerations. The commercial sector has demonstrated a prototype model for a quantum research cloud. IBM, D-Wave and Google all have publicly accessible quantum clouds for academic institutions, national labs, and startups accessible over the Internet [82].

C. Quantum Technology Access

Current prototype access models are limited to a prohibitively small community. Future access models must meet the needs of quantum researchers to facilitate the emerging technology research, stimulate quantum computing industry innovations, educate quantum computing workforce, and accelerate advancement of quantum computer capabilities. In

increase research community access, a cloud-based model could represent a lower barrier of entry due to infrastructure and funding constraints. Google and NASA have been working cloud-based quantum prototypes with the D-Wave 2000 and IBM [83][84]. Federal government could help make use of systems and access to facilities easier by providing tools and agreements for special access and facilitating training programs for these resources, including internship programs to develop the pipeline of quantum researchers and funding for meritorious science proposals. Research groups are using publicly available quantum computers built and maintained by IBM to run and test algorithms; users have performed 275,000 experiments and produced about 15 research papers [84]. Through the IBM-Q program, IBM offered in 2006 the first professional quantum developer certification program [85]. D-Wave, a company based in Burnaby, Canada, has also developed a quantum computing service on the cloud. First offered in 2010, D-Wave's quantum cloud platform, The Leap^{TM}, is not entirely free. It's first minute is free but then costs $2,000 an hour afterwards. It is also not universal as it has can only run a limited number of quantum algorithms. However, in response to COVID-19, D-Wave has provided quantum cloud access for anyone working on responses to the pandemic crisis [86]. In 2021, Google offered Google Quantum AI to preapproved researchers with projects to scientists. To ensure the broadest range of qualified researchers, including those at Minority-Serving Institutions (MSIs), can access these resources, the DOE should prioritize creating a national quantum computing research cloud that provides academic researchers with affordable access to high-end quantum computing infrastructure. Broader and permanently affordable access to these systems will enable researchers to fully utilize state-of-the-art quantum hardware for many who would not otherwise be able to do so because of funding limitations or the lack of having close ties with a research group that is willing to collaborate. The U.S. currently is leading the effort to increase international access as an alternative to industry efforts. The U.S. DOE solicited input from stakeholders to assist the Federal government in developing a roadmap for access to quantum systems, including the nature of quantum systems that should be considered. It attracted about 40,000 users from more than 100 countries confirming the need for such initiatives [87].

VII. CONCLUSION

Quantum computing is an enabler and accelerator of future capabilities for nation states and is critical to the future of society and security [9]. The proliferation and regulation of emerging technology-based capabilities will reshape the cyber balance of geopolitical power. Deficiency of understanding on the part of decisionmakers regarding the nature of emerging technologies in policy, and a sustained escalation of nation-state on nation-state cyberattacks, without proper rules of engagement regarding accepted proportionality, the geopolitical community could witness events escalate to conventional or nuclear war [68]. This becomes nearer to reality with NSPM-13 loosening the restrictions on offensive cyber operations, moving the U.S. to defend forward more aggressively in cyberspace [88]. The potential implications of the defend forward are increased state sponsored cyber-attacks escalating the potential for a hybrid war. The UN ITU asserts that each nation-state has the responsibility to collaborate to achieve a consensus of norms toward reducing cyberwar tensions, it must include apposite consensus on policy cooperation to unify national strategies [89]. Correspondingly, we examined the problem from a pre-emptive, non-proliferation perspective regarding quantum computing allied with international policy development. Instituting a unified legal framework involving quantum computers and exploring potential solutions for governance over cyber warfare is critical to reign in the modern arms race. We argue that a uniform international policy and legal framework is needed, as opposed to the singular perspective that a technology-based solution will protect developed nations against attacks by quantum computers. Just as the 20th Century "Mutually Assured Destruction" doctrine policy abated global devastation, new international legal frameworks should adopt a doctrine of 'Mutually Beneficial Existence' in the 21st Century. Mutually Beneficial Existence would shape the new legal framework by incentivizing economic growth and development for member states versus economic sanctions as currently ratified. Political will for progress is an essential precursor to cultivate international norm development. This unified approach, legal framework harmonization, controlled technology development, political consultations, private and public actors' cooperation, and development and popularization of cybersecurity culture are the main elements to promote international peace in the fifth domain towards Mutually Assured Existence. The U.S. for its part needs to support intergovernmental, public-private, and nongovernmental organizations and processes designed to ratify the commitment of various coalitions of stakeholders to emergent cyber norms and expand public profile and attention to reaffirm and expand confidence-building mechanisms with Russia and China.

REFERENCES

[1] C. Payne, L. Finlay. "International Law Cannot Keep Up with Cyber-Criminals". World Economic Forum. Feb. 25, 2019. Available at https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks

[2] World Economic Forum. "Global Risks Report 2022". Global Risk Report, World Economic Forum. Jan. 11, 2022. Available online: https://www.weforum.org/reports/global-risks-report-2022

[3] World Economic Forum. "Quantum Computing Governance Principles". Insight Report. Jan. 2022. Available online: https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf

[4] H. Andas. "Emerging Technology Trends for Defence and Security". FFI-RAPPORT, Norwegian Defence Research Establishment. Apr. 7, 2020. Corpus ID: 231660708. Available online: https://publications.ffi.no/nb/item/asset/dspace:6728/20-01050.pdf

[5] M. Krelina. "Quantum Technology for Military Applications". EP Journal Quantum Technology, Springer Open Journal. Aug. 24, 2021. https://doi.org/10.1140/epjqt/s40507-021-00113-y

[6] W. Lind. "Understanding the Fourth Generation of War". Disruptive and Game Changing Technologies in Modern Warfare. Sep. 28, 2019. Marine Corps Mil. Rev. 2004. Available online: https://link.springer.com/chapter/10.1007/978-3-030-28342-1_1

[7] M. FitzGerald. "The Russian Military's Strategy for "Sixth Generation" Warfare". Orbis, Science Direct, Vol. 38, Issue 3, Summer 1994, pp. 457-476. https://doi.org/10.1016/0030-4387(94)90008-6

[8] R. Berendsen. "The Weaponization of Quantum Mechanics: Quantum Technology in Future Warfare". A Monograph, Royal Netherlands Army. Technical Report, Published by Defense Technical Information Center. May 23, 2019. Available online: https://apps.dtic.mil/sti/pdfs/AD1083173.pdf

[9] Information Technology & Innovation Foundation (ITIF). "The Future of Quantum Computing: Policy Implications for National Security and Industrial Competitiveness". Dec. 6, 2016. Available online: https://itif.org/events/2016/12/06/future-quantum-computing-policy-implications-national-security-and-industrial

[10] U.S. Congress. "QUANTUM for National Security Act". Senate Bill S.1197, 117th Congress, Apr. 2021. Available online: https://www.congress.gov/bill/117th-congress/senate-bill/1197?s=1&r=3

[11] European Leadership Network. "Nuclear Decision Making, Complexity and Emerging and Disruptive Technologies: A Comprehensive Assessment". ELN Report. Feb. 14, 2022. Available online: https://www.europeanleadershipnetwork.org/report/nuclear-decision-making-complexity-and-emerging-and-disruptive-technologies-a-comprehensive-assessment/

[12] A. Vance, R. Campbell, T. Vance. "A Qualitative Meta-Analysis of Contemporary Research Correlating Post-Quantum Vulnerabilities and Opportunities to Cybersecurity". Journal of European Academic Science and Research, Vol. 1 No. 25, Feb. 28, 2022. ISSN 2789-1968

[13] D. Gariso. "China is Pulling Ahead in Global Quantum Arms Race, New Studies Suggest". Quantum Computing, Scientific American. Jul. 15, 2021. Available online: https://www.scientificamerican.com/article/china-is-pulling-ahead-in-global-quantum-race-new-studies-suggest/

[14] A. Middleton. T. Steele. "Quantum Information Processing Landscape 2020: Prospects for UK Defence and Security". Research and Analysis Report DSTL/TR121783, Defence Science and Technology Laboratory. UK Ministry of Defense. Jul. 7, 2020. Available online: https://www.gov.uk/government/publications/quantum-information-processing-landscape-2020

[15] V. Dunjko, J. Taylor, H. Briege. "Quantum-Enhanced Machine Learning". Physical Review Letters. 2016;117(13). https://doi.org/ 10.1103/ physrevlett.117.130501

[16] J. Wilson. "The Future of Artificial Intelligence and Quantum Computing". Military & Aerospace Electronics. Aug. 2020. Available online: https://www.militaryaerospace.com/computers/article/14182330/

[17] Lockheed Martin. "Quantum Computing: Spot-Checking Millions of Lines of Code". Lockheed Martin News Feature. 2017. https://www. lockheedmartin.com/en-us/news/features/2017/quantum-computing-spot-checking-millions-lines-code.html

[18] J. Dijk. "Artificial Intelligence and Machine Learning in Defense Applications". Proceedings of SPIE, Vol. 11543. Oct. 13, 2020. Available online: https://spie.org/Publications/Proceedings/Volume/11543?SSO=1

[19] A. Chancé. "Quantum Machine Learning is Going to be the Biggest Application of Quantum Computing in the next Ten Years". Quantum World Association, Sep. 2018. Available online: http://quantumwa.org/wp-content/uploads/2018/09/Peter-Wittek-Quantum-machine-learning-is -going-to-be-the-biggest-application-of-quantum-computing-in-the-next-ten-years.pdf.pdf.

[20] A. Iyer, E. Rosenfeld, and M. Lukin, et al. "Tech Factsheets for Policymakers". Belfer Center for Science and International Affairs, Harvard Kennedy School. Spring 2020. Available online: https://www.belfercenter.org/publication/technology-factsheet-quantum-computing

[21] A. Vance. "Post-Quantum Computing Technologies Intensifying Nation State Conflict: An Analysis of Quantum Based Cybersecurity Innovations and Adoptions". International Journal of Computer Science and Information Technology Research, Vol. 10, Issue 2, Apr. 2022 – Jun. 2022. ISSN 2348-1196 (print), ISSN 2348-120X (online)

[22] P. Wallden, E. Kashefi. "Cyber Security in the Quantum Era". Communications of the ACM. Vol. 62, No. 4. Apr. 2018 doi:10.114/3241037

[23] M. Carr, F. Lesniewska. "Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance". International Relations, Sage Journals, Vol. 34, Issue 3, pp. 391-412. Sep. 2020. https://doi.org/10.1177/0047117820948247

[24] C. Kavanagh. "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?". Carnegie Endowment for International Peace. Aug. 28, 2019. Available online: https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736

[25] Information Warfare Monitor. "Tracking GhostNet: Investigating a Cyber Espionage Network". Citizen Lab Report JRO2-2009. Mar. 29, 2009. Available online: https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf

[26] S. Park, M. Specter, N. Narula, et al. "Going from Bad to Worse: From Internet Voting to Blockchain Voting". Journal of Cybersecurity, Vol. 7, Issue 1, Feb. 16, 2021. https://doi.org/10.1093/cybsec/tyaa025

[27] K. Anderson. "Pentagon Concludes Cyber Attack Can Be Act of War". International Commission of Jurists. May 30, 2011. Available online: http://opiniojuris.org/2011/05/30/pentagon-concludes-cyber-attack-can-be-act-of-war/

[28] C. Whyte, B. Mazanec (2018). "Understanding Cyber Warfare Politics, Policy and Strategy". Routledge Taylor & Francis Publishing. Dec. 19, 2018. ISBN 9781138640627

[29] M. Mazarr, B. Frederick, E. Ellinger, et al. "Competition and Restraint in Cyberspace; The Role of International Norms in Promoting U.S. Cybersecurity". RAND RR-A1180-1. Paperback ISBN/EAN: 1-9774-0731-5. https://doi.org/10.7249/RRA1180-1

[30] Congressional Research Service. "Quantum Information Science: Congressional Activity and Federal Policy Recommendations". Apr. 28, 2020. Available online: https://www.everycrsreport.com/files/2020-0428IF11524500 6928af7f0284ebbb8ffc9bd2a 342e30a3fb44.pdf

[31] M. Lee. "Quantum Computing and Cybersecurity". Cyber Project, Harvard Belfer Center. Jul. 2021. Available online: https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

[32] U.S. Department of State. "Remarks to the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security", May 28, 2021. Available online: https://usun.usmission.gov/remarks-to-the-un-group-of-governmental-experts-on-advancing-responsible-state-behavior-in-cyberspace-in-the-context-of-international-security/

[33] M. Burrows, J. Mueller-Kaler, K. Oksanen, et al. "Counting the Costs of Technonationalism and the Balkanization of Cyberspace". Technology and Innovation Foresight Report, Atlantic Council. Dec. 8, 2021. Available online: https://www.atlanticcouncil.org/ blogs/geotech-cues/counting-the-costs-of-technonationalism-and-the-balkanization-of-cyberspace/

[34] White House. "National Strategic Overview for Quantum Information Science". The White House National Science and Technology Council, Sep. 2018. Available online: https://www.quantum.gov/wp-content/uploads/2020/10/2018_NSTC_National_Strategic_Overview _QIS.pdf

[35] F. Werner. "Quantum Computing: New Threats Require New Security Approaches". Artificial Intelligence, Cybersecurity/Trust, Emerging Trends Report, United Nations International Telecommunication Union (ITU). Mar. 28, 2017. Available online: https://news.itu.int/quantum-computing-new-threats-require-new-security-approaches/

[36] DARPA. "Artificial Intelligence Next Campaign". Defense Advanced Research Projects Agency, Sep. 2018. Available online: https://www.darpa.mil/work-with-us/ai-next-campaign

[37] White House. "American Artificial Intelligence Initiative". The White House Office of Science and Technology Policy, Feb. 2020. Available online: https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf

[38] White House. "Artificial Intelligence and Quantum Information Science R&D Summary". White House Office of Science and Technology Policy, Aug. 2020. Available online: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/Artificial-Intelligence-Quantum-Information-Science-R-D-Summary-August-2020.pdf

[39] Bureau of Industry and Security. "Commerce Lists Entities Involved in the Support of PRC Military Quantum Computing Applications, Pakistani Nuclear and Missile Proliferation, and Russia's Military". U.S. Department of Commerce, Nov. 2021. Available online: https://www.commerce.gov/news/press-releases/2021/11/commerce-lists-entities-involved-support-prc-military-quantum-computing

[40] White House. "Executive Order on Ensuring Responsible Development of Digital Assets". Mar. 09, 2022. Available online:https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

[41] Information Warfare Monitor. "Tracking GhostNet: Investigating a Cyber Espionage Network". Citizen Lab Report JRO2-2009. Mar. 29, 2009. Available online: https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf

[42] E. Van Wie Davis. "Shadow Warfare; Cyberwar Policy in the U.S., Russia and China". Rowman and Littlefield Publishing. Feb. 2021. ISBN: 978-1-5381-4966-9

[43] Department of Defense, Defense Science Board. "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat". The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013. Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber- 081.pdf

[44] F. Delerue. "Cyber Operations and International Law". Cambridge University Press. Dec. 31, 2020. ISBN: 9781108490276. DOI: 10.1017/9781108780605

[45] United Nations. "Article 51". Chapter VII, Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Repertory of Practice of United Nations Organs, Aug. 23, 2016. Available online: https://legal.un.org/repertory/art51.shtml

[46] H.R. 5515. "Policy of the U.S. on Cyberspace, Cybersecurity, Cyber Warfare, and Cyber Deterrence". National Defense Authorization Act. Jul. 2018. Available online: https://docs.house.gov/billsthisweek/20180723/CRPT-115hrpt863.pdf

[47] H.R. 6227. "National Quantum Initiative Act". Dec. 2018. Available online: https://www.congress.gov/bill/115th-congress/house-bill/6227/text

[48] H.R. 8279. "Quantum Network Infrastructure and Workforce Development Act". Sep. 2020. Available online: https://www.congress.gov/bill/116th-congress/house-bill/8279/text

[49] G. Corn. "National Security Decision-Making in the Age of Technology: Delivering Outcomes on Time and on Target". Journal of National Security Law & Policy, Vol. 12, No. 61, 2021. https://digitalcommons.wcl.american.edu/facsch_lawrev/1997?utm_source=digitalcommons.wcl.american.edu%2Ffacsch_lawrev%2F1997&utm_medium=PDF&utm_campaign=PDFCoverPages

[50] Council of Europe. Budapest Convention Treaty No. 185: Convention on Cybercrime, Council of Europe. Nov. 23, 2001. https://www.coe.int/en/web/cybercrime/the-budapest-convention and https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[51] Department of Energy (DOE) (2021). "Request for Information: Access to Quantum Systems. Office of Science, Department of Energy". National Archives, Federal Register. August 16, 2021. Available online: https://www.federalregister.gov/documents/2021/08/16/2021-17520/request-for-information-access-to-quantum-systems

[52] United Nations. "Advancing responsible State behavior in cyberspace in the context of international security", 2019. Available online: https://digitallibrary.un.org/record/3839870?ln=en

[53] Harvard Kennedy School. "Technology Factsheet: Quantum Computing". Belfer Center for Science and International Affairs Technology and Public Purpose Project. Harvard Kennedy School, 2020. Available online: https://www.belfercenter.org/publication/technology-factsheet-quantum-computing

[54] T. Vance, O. Bulda, A. Vance. "International Law in Cyberspace: The Need for Collaboration and Coordination to Promote International Peace in the Fifth Domain". Journal of Cybersecurity Awareness and Education, Vol. 2 No. 1, 2020 and in the proceedings of Ninth Annual Cambridge International Law Conference on International Law and Global Risks: Current Challenges in Theory and Practice, University of Cambridge. United Kingdom. Available online: https://www.researchgate.net/publication/358833124_International_Law_in_Cyberspace_The_Need_for_Collaboration_and_Coordination_to_Promote_International_Peace_in_the_Fifth_Domain

[55] ITIF. "The Future of Quantum Computing: Policy Implications for National Security and Industrial Competitiveness". Information Technology and Innovation Foundation. Dec. 6, 2016. Available online: https://itif.org/events/2016/12/06/future-quantum-computing-policy-implications-national-security-and-industrial

[56] [56]. K. Seetharam and M. DeMarco. "Catalyzing the Quantum Leap". MIT Science Policy Review. Aug. 30, 2021. DOI: 10.38105/spr.lcbqcligt5

[57] NATO. "The Tallin Manual". NATO Cooperative Cyber Defence Centre of Excellence, 2017. Available online (rev.): https://ccdcoe.org/research/tallinn-manual/

[58] UNESCO. "UNESCO Science Report, The Race Against Time for Smarter Development". United Nations Educational, Scientific and Cultural Organization, October 2021. ISBN: 978-92-3-100450-6

[59] United Nations. "Group of Government Experts". United Nations Office for Disarmament Affairs. 2021. Available online: https://www.un.org/disarmament/group-of-governmental-experts/

[60] Ministry of Europe and Foreign Affairs (2018). "Paris Call for Trust and Security in Cyberspace". Paris Peace Forum, French Foreign Ministry. November 12, 2018. Available online: https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace

[61] White House. "Artificial Intelligence & Quantum Information Science R&D Summary". Aug. 2020. Available online:https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/Artificial-Intelligence-Quantum-Information-Science-R-D-Summary-August-2020.pdf

[62] Research and Markets. "Quantum Technology Market by Computing, Communications, Imaging, Security, Sensing, Modeling and Simulation 2022 – 2027". Technology Market Research Report, Mind Commerce Publishing. Feb. 2022. MCMS-ID 5317365

[63] S. Johnstun, and J. Van Huele. "Understanding and compensating for noise on IBM quantum computers". American Journal of Physics. Aug. 21, 2021. Available online: https://doi.org/10.1119/10.0006204

[64] Lawrence Livermore National Laboratory. "Request for Information: Access to Quantum Systems". U.S. Department of Energy, Sep. 28, 2021. DoE LLNL-TR-827217.

[65] Office of the Chief Scientist. Science & Technology Trends 2020-2040: Exploring the S&T Edge, NATO Science & Technology Organization, Mar. 2020. Available online: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/ 190422_Tech_Trends_Report_2020-2040.pdf

[66] M. Tsvetkova. "Putin puts nuclear deterrent on alert; West squeezes Russian economy". World, Reuters. Feb. 27, 2022.Available online: https://www.reuters.com/world/india/war-with-ukraine-putin-puts-nuclear-deterrence-forces-alert-2022-02-27/

[67] J. Fabian. "Obama says he's prepared to retaliate against China". Cybersecurity, The Hill. Sep. 16, 2015. Available online:https://thehill.com/policy/cybersecurity/253826-obama-says-hes-prepared-to-retaliate-against-china-for-cyberattacks/

[68] J. Lancelot. "Cyber-diplomacy: Cyberwarfare and the Rules of Engagement". Journal of Cyber Security Technology, Vol. 4, Issue 4, pp. 240-254. Dec. 31, 2018

[69] M. Kaminski. "Operation Olympic Games: Cyber-sabotage as a tool of American Intelligence Aimed at Counteracting the Development of Iran's Nuclear Programme". Security and Defense Quarterly, War Studies University, Vol. 29, pp. 62-71, Feb. 2020. Available online: https://doi.org/10.35467/sdq/121974

[70] T. Gill, D. Fleck. "The Handbook of the International Law of Military Operations". Oxford University Press, 2nd Ed., Feb. 10, 2016. ISBN: 9780198744627

[71] J. Richet. "Cybersecurity Policies and Strategies for Cyberwarfare Prevention". Information Science Reference, An Imprint of IGI Global, Georgetown Law and University of France. Jul. 2015. ISBN13: 9781466684560. DOI: 10.4018/978-1-4666-8456-0.

[72] The Daily Hodi. "White House Blacklists 8 Chinese Quantum Computing Companies Citing National Security Risk". Communications of the ACM, Nov. 30, 2021. Available online: https://cacm.acm.org/news/257108-white-house-blacklists-8-chinese-quantum-computing-companies-citing-national-security-risks/fulltext

[73] P. Reich, S. Weinstein, C. Wild, et al. "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity", European Journal of Law and Technology, Vol. 1, Issue 2, 2010. Available online: https://ejlt.org/index.php/ejlt/article/view/40/58

[74] Paris Peace Forum. "Governing AI and Ensuring Cybersecurity". Paris Peace Forum Priority Theme, 2022. Available online: https://parispeaceforum.org/en/our-priorities/

[75] H.R. 1837. "Quantum User Expansion for Science and Technology (QUEST) Act". Mar. 2021. Available online: https://projects.propublica.org/represent/bills/117/hr1837

[76] S. 1197. "Quantum National Security Act". Apr. 2021. Available online: https://www.congress.gov/bill/117th-congress/senate-bill/1197/all-info

[77] J. Cianci. "The SolarWinds Software Hack: A Threat to Global Cybersecurity". Jolt Digest, Harvard Law School, Feb. 8, 2021. Available online: https://jolt.law.harvard.edu/digest/the-solarwinds-software-hack-a-threat-to-global-cybersecurity

[78] C. Ostergaard, B. Timmermans, K. Kristinsson. "Does a Different View Create Something New? The Effect of Employee Diversity on Innovation". Research Policy, Science Direct, Vol. 40, Issue 3, pp. 500-509, Apr. 2011. https://doi.org/10.1016/j.respol.2010.11.004

[79] GAO. "Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations". GAO 19-570, Reports and Testimonies, Aug. 15, 2019. Available online: https://www.gao.gov/products/gao-19-570

[80] ISACA. "Drive Your Understanding and Abilities to the Forefront of Emerging Tech, Certified in Emerging Technology". Available online: https://www.isaca.org/credentialing/cet

[81] C. Aiello, D. Awschwalom, et al. "Achieving a quantum smart workforce". Quantum Science and Technology, IoP Publishing. Apr. 12, 2021. Available online: https://iopscience.iop.org/article/10.1088/2058-9565/abfa64/pdf

[82] C. Dilmegani. "Cloud Quantum Computing & Top Cloud QC Vendors in 2022". AI Multiple, Quantum Computing, 2022. Available online: https://research.aimultiple.com/quantum-computing-cloud/

[83] D-Wave. "D-Wave Provides Free Quantum Cloud Access for Global Response to COVID-19". Mar. 31, 2020. Available online: https://www.dwavesys.com/company/newsroom/press-release/d-wave-provides-free-quantum-cloud-access-for-global-response-to-covid-19/

[84] D. Castelvecchi. "IBM's quantum cloud computer goes commercial". Nature Journal, Springer Publishing. Mar. 9, 2017. ISSN 0028-0836. Available online: https://www.nature.com/articles/nature.2017.21585.pdf

[85] IBM Training. "IBM Certified Associate Developer - Quantum Computation using Qiskit v0.2X". Certification overview, objectives, exam preparation and registration, 2022. Available online: https://www.ibm.com/training/certification/C0010300

[86] J. Sud, V. Li. "A Quantum Annealing Approach to Reduce Covid-19 Spread on College Campuses". Quantum Artificial Intelligence Lab, Universities Space Research Association. Nov. 22, 2021. Available online: https://arxiv.org/pdf/2112.01220.pdf

[87] Federal Register. "Request for Information: Access to Quantum Systems". 86 FR 45715, Federal Register, Vol. 86, Issue 155, Aug. 16, 2021. Available online: https://www.govinfo.gov/app/details/FR-2021-08-16/2021-17520

[88] Federation of American Scientists. "National Security Presidential Memoranda (NSPM), NSPM-13, United States Cyber Operations Policy, White House, Mar. 13, 2020. Available online: https://irp.fas.org/offdocs/nspm/index.html

[89] ITU Journal. "Future and Evolving Technologies". Vol. 2, Issue 1, 2021. Available online: http://handle.itu.int/11.1002/pub/81817c94-en