http://dx.doi.org/10.21544/2359-3075.30330

Quantum Technologies: a matter of national sovereignty

Fernando M. Araújo-Moreira[1]
Vítor G. Andrezo Carneiro[2]
Juraci Ferreira Galdino[3]

ABSTRACT

The foundations of quantum physics (or mechanics) were presented by German scientist Max Planck in 1900. With revolutionary scientific content, these foundations established new paradigms that supported the so-called First Quantum Revolution, from which products such as lasers, GPS and semiconductor chips, which are essential today, were derived. In 1950, Chien Shiung Wu and Irving Shaknov conducted what is now known as the WS experiment, which became the key to the emerging manifestation of the second quantum revolution, which includes new technologies grouped into four broad areas: quantum devices (sensors, biosensors, detectors, and actuators); quantum communication and teleportation, and two-dimensional materials; quantum computing, cryptography, and the quantum internet; and technologies derived from quantum materials of application, for example, in the area of energy. This article aims to search for evidence that the field of Quantum Technologies is essential not only for National Security and Defense, but also for shaping the geopolitical landscape. They suggest that, together, Quantum Technologies, Artificial Intelligence (AI) and Cybernetics will promote a great technological revolution of humanity, and particularly in military affairs. Thus, the article presents arguments for these areas of knowledge and technological development to be considered strategic and priority for the country, in view of the centrality of these technologies in economic growth, social development, security, defense and sovereignty of a nation in the context of the 4th Industrial Revolution and the Knowledge Age.
Keywords: quantum technologies; cyber defense; national sovereignty.

[1] Brazilian Army. Military Institute of Engineering/Nuclear Engineering Section. Rio de Janeiro, RJ, Brazil. https://orcid.org/0000-0002-5423-0405 http://lattes.cnpq.br/1809254923092721

[2] Brazilian Army. Military Institute of Engineering/Electrical Engineering Section. Rio de Janeiro, RJ, Brazil. https://orcid.org/0000-0002-5738-168X http://lattes.cnpq.br/6739848742248437

[3] Brazilian Army. Military Institute of Engineering/Command. Rio de Janeiro, RJ, Brazil. https://orcid.org/0000-0001-7805-0452 http://lattes.cnpq.br/3588063339399737

> "Therefore, I say that it is a narrow policy to suppose that this or that country is to be marked out as the eternal ally or the perpetual enemy of England. We have no eternal allies, and we have no perpetual enemies. Our interests are eternal and perpetual, and it is our duty to follow them."
> — Henry John Temple, 3rd Viscount Palmerston

INTRODUCTION

Quantum technologies explore probabilistic physical phenomena that occur at atomic and subatomic scales. The probabilistic nature of these phenomena was the subject of the world-famous debate between Albert Einstein and Niels Bohr during the Fifth Solvay Conference on Quantum Physics, held in October 1927 in Brussels, whose main objective was to discuss the newly formulated quantum theory. This event brought together 29 of the most prominent scientists of the time, 17 of whom later became Nobel Prize winners.

In 1900, in what became known as the "debate of the century," Niels Bohr, one of the fathers of quantum theory (which is inherently probabilistic) as presented by Max Planck, defended the new theory formulated by Werner Heisenberg, while Albert Einstein attempted to uphold a cause-and-effect model (i.e., an essentially deterministic one). Einstein famously stated, "God does not play dice" (referring to the probabilistic nature of quantum mechanics), to which Niels Bohr responded, "Einstein, stop telling God what to do." Today, the scientific community agrees that Bohr won the debate. This means that, at the quantum scale, the world does not follow a fixed cause-and-effect scenario (deterministic) but is instead fundamentally random. In other words, one can know everything about the atomic and subatomic world without knowing exactly what will happen next. This conception gave rise to the so-called First Quantum Revolution, which led to practical developments such as lasers, GPS, and semiconductor chips—technologies that remain highly useful today.

The probabilistic paradigm allowed for a better understanding of some key properties of atomic and subatomic particles, such as tunneling, superposition, and entanglement, as well as advances in

other applied areas such as information technology, nanotechnology, and precision mechanics. In 1950, Chien-Shiung Wu and Irving Shaknov conducted what is now known as the WS experiment, often regarded as the first experiment capable of demonstrating the phenomenon known as quantum entanglement. Along with tunneling and superposition, this quantum phenomenon became the key to developing the Second Quantum Revolution, which includes new technologies grouped into four major areas: quantum devices (sensors, biosensors, detectors, and actuators); quantum communication, quantum teleportation, and two-dimensional materials; quantum computing, cryptography, and the quantum internet; and technologies derived from quantum materials applied in fields such as energy.

Highly advanced communication systems with superior data security and transmission speed, a wide range of ultra-sensitive sensors, and data processing devices capable of achieving speeds of up to terabits per second (Tb/s) are some of the innovations envisioned by experts in the short and medium term. Emerging Quantum Technologies could significantly influence Security and National Defense, heavily impacting future military capabilities across all dimensions of modern operational theaters. Some authors suggest that these advances may give rise to Quantum Warfare—a new paradigm for crises and armed conflicts. Consequently, countries that lag behind in these technological advancements will face severe vulnerabilities to their sovereignty, in addition to economic, scientific, and technological stagnation, and social development barriers.

Given all this, it is evident that advances in quantum technologies are disruptive and will influence various aspects of national power. They may become essential for economic growth, social development, and the security, defense, and sovereignty of a nation. Despite the vast scope and impact of these innovations, this article focuses on their implications for the field of Defense. Keeping up with such advancements from a technical perspective—especially in an area as complex as Quantum Mechanics—can be particularly challenging, especially in Defense, where information is often classified or selectively disclosed.

Thus, this article aims to provide a qualitative and exploratory foresight of the main advancements in the field of Quantum Technologies, summarizing them based on the technical experience of the authors in implementing some of these technologies. The methodology includes

an extensive bibliographic review of Quantum Technologies, aiming to present and organize references related to their applications in Security and Defense. Given that many of these technologies are still under development for a highly sensitive area such as National Sovereignty, relevant references are often only found in brief news articles, requiring specialists to have a keen eye to grasp the technical aspects of ongoing developments.

Therefore, this article seeks to offer a comprehensive approach to a world undergoing constant changes, particularly regarding the scientific, technical, and geopolitical aspects of second-generation quantum technologies and their influence on security and national defense in Brazil and globally. Additionally, some of the new paradigms inherently linked to security and defense are presented, along with discussions on key trends in these technologies, which could further drive the Fourth Industrial Revolution and develop critical elements of future warfare capabilities.

Promoting the accumulation of technological capabilities, generating knowledge, and fostering innovations in sensitive and critical areas such as quantum technologies is both a great challenge and an extraordinary opportunity for economic growth, social development, and national sovereignty. Quantum technologies are expected to significantly impact all aspects of National Power, but their most profound implications are anticipated in the Military Domain due to their potential consequences across all combat dimensions—land, naval, aerial, space, and cyber—as illustrated in Figure 1.

Figure 1: Applications of Quantum Technologies in National Defense (adapted from KRELINA, M., 2021).

These technologies not only enhance existing ones but can also create powerful and innovative military capabilities, driving a Revolution in Military Affairs or even a Military Revolution. The expectations for change are so significant that some authors even foresee the emergence of a new generation of warfare: Quantum Warfare. Others consider quantum technology not just a new generation of warfare but also a new dimension of combat.

According to Krelina, Quantum Warfare is warfare that utilizes quantum technologies for military applications that impact intelligence, security, and defense capabilities across all domains of warfare. This introduces new military strategies, doctrines, scenarios, and peace-related issues, as well as ethical concerns.

Among other possibilities, Quantum Technologies will enable the measurement or detection of objects that are currently undetectable with existing technological paradigms, solve complex problems that are currently unsolvable, and elevate cyber operations beyond their current level. This includes both security advancements, such as quantum cryptography, and data processing improvements through quantum computing and quantum algorithms.

In the field of Security and Defense, some applications stand out due to their importance and potential short- and medium-term impact. The following section discusses three key Quantum Technologies with possible applications in Security and Defense: quantum devices, quantum communication, and quantum computing.

This article focuses on these three Quantum Technologies because they are in a more advanced stage of development and have significant impacts, particularly in the field of Cybersecurity, considering the world's current heavy reliance on computers. However, Quantum Science possesses so many disruptive characteristics that the authors could not refrain from commenting on other possible impacts on Security and Defense.

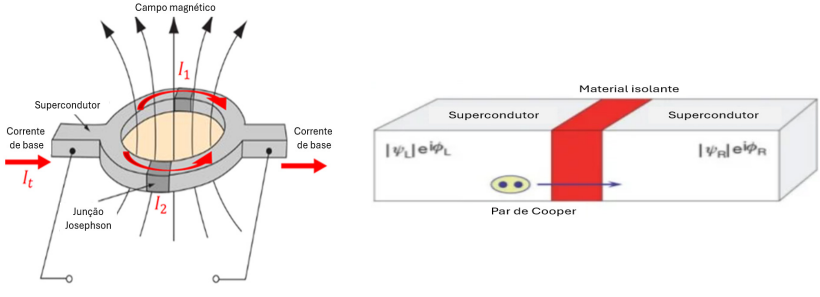
(a) Quantum Devices

In this context, we will discuss quantum sensing devices, particularly sensors, biosensors, detectors, and actuators that utilize the quantum principles of tunneling, superposition, and entanglement. These allow for the measurement of physical quantities with sensitivities

far beyond classical limits. There are already commercial sensing technologies that use quantum phenomena to achieve high precision in measurements, including applications in atomic clocks, nuclear magnetic and paramagnetic resonance, and electron microscopes.

According to the NSF (National Science Foundation), the U.S. equivalent of CNPq, several opportunities will arise over the next ten years regarding next-generation quantum devices for applications in biotechnology, defense, positioning and navigation, and timekeeping systems useful for both the military and the civilian sector. At the same time, these technologies will create new opportunities to address complex problems in material science, chemistry, and physics. These applications have broad implications in critical areas such as energy and security, impacting everyday life for the general population.

One of the most important quantum sensing devices is the so-called SQUID (Superconducting Quantum Interference Device), used to measure magnetic fields (Figure 2a). It is formed by the combination of one or more Josephson junctions (Figure 2b). One of the most interesting aspects of this junction is that it serves as the foundation for the quantum bit (abbreviated as qubit), which is used in one of the technological approaches for developing quantum computers. The qubit is formed by a particle or physical property that assumes a superposition state, meaning it can represent both logical states, 1 and 0, simultaneously. The state (1 or 0) is only defined at the moment of measurement, and the probability of each outcome depends on the type of process that generated the qubit14.



(a) (b)

Figure 2: (a) SQUID sensor schematic; (b) Josephson junction schematic.

For example, in the energy sector, quantum sensing applications are quite extensive, including renewable energy, nuclear energy, nuclear waste management, fossil energy, geothermal energy, electricity, and vehicle electrification. The potential applications of quantum sensing in fossil energy areas are shown in Table 1. The different types of quantum sensors are presented in Table 2.

Table 1: Potential applications of quantum sensing in fossil energy areas.

Área de energia fóssil	Aplicação de sensoriamento
Utilização de CO2 e beneficiamento de carvão	Detecção rápida e sensível de emissão e vazamentos de CO2, detecção de metais de alto valor de carvão e subprodutos de utilização de carvão.
Upstream de Petróleo e gás	Gravímetros quânticos para a detecção de depósitos de petróleo / gás.
Midstream de Petróleo e gás	Monitoramento da integridade da tubulação durante o transporte e armazenamento.
Downstream de Petróleo e gás	Monitoramento da emissão de CO2 durante o consumo.
Captura e armazenamento de carbono	Detecção rápida e sensível de emissão de CO2 e vazamentos.
Extração e recuperação de carvão	Detecção de elementos metálicos críticos de carvão e subprodutos de utilização de carvão, gravímetros para exploração de carvão, segurança de minas de carvão.
Geração de eletricidade	Sensores que monitoram campos eletromagnéticos.
Transporte e distribuição de eletricidade	Monitoramento de temperatura em transformadores.
Física e energia nuclear	Monitoramento da segurança nuclear nacional, dispositivos de interferência quântica supercondutora (SQUIDs).

Table 2: Different types of quantum sensors and their associated technologies.

Tecnologia	Características quânticas	Condições experimentais	Vantagens vs. sistemas clássicos	Desafios
Sensores quânticos não fotônicos	Spin *qubits*, átomos neutros, íons presos	Medições de múltiplos parâmetros	Alta sensibilidade, baixo ruído	Decoerência, ruído de projeção quântica
Detecção remota de alvos	Iluminação quântica, emaranhamento quântico	Interferometria quântica	Relação sinal-ruído aprimorada	Muito frágil em relação à perda óptica
Radar quântico	Iluminação quântica de micro-ondas	Interferometria quântica	Expor alvos furtivos	Falta de conversores de fóton-micro-ondas
Espectroscopia quântica	Emaranhamento quântico, fótons únicos	Medições de correlação de intensidade	Além do limite de ruído de disparo, aproximando-se do limite quântico final	Decoerência quântica
Microscopia quântica	Emaranhamento quântico,	Microscopia e detecção quântica	Super resolução além do limite de Rayleigh	Localização desconhecida do centroide de origem
Interferômetros quânticos	Estados emaranhados, luz espremida	Interferômetros de menor escala	Escala de Heisenberg	Muito frágil em relação à perda óptica
Detector de ondas gravitacionais	Luz espremida	Interferômetros de tamanho quilômetro	Escala de Heisenberg	Muito frágil em relação à perda óptica
Leitura quântica da memória óptica clássica	Discriminação de canal quântico	Interferômetro e fonte de fóton único	Leitores ópticos mais rápidos e sem erros e memórias mais densas	Uso de fontes de fótons e detectores com altíssima eficiência

Figure 3 presents a summary of ten-year forecasts for the quantum sensor market by sensor type and their applications.

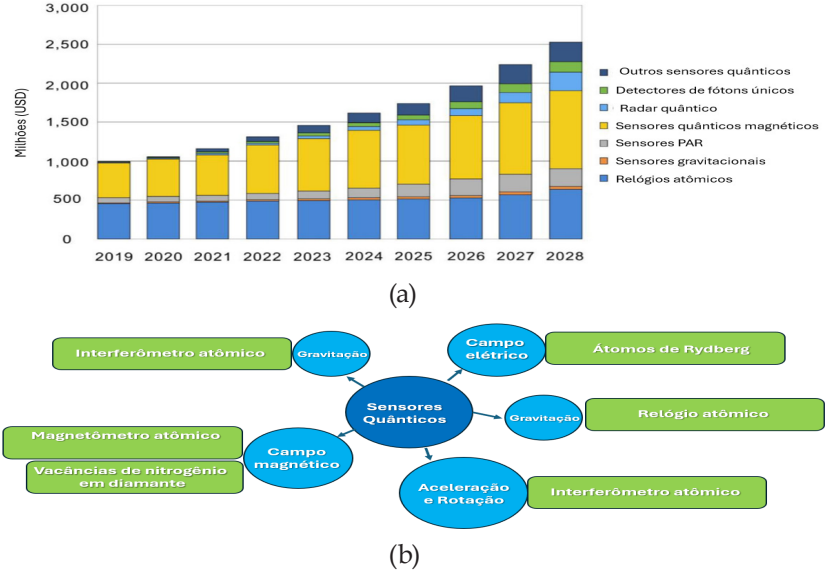


Figure 3: (a) Summary of ten-year forecasts for the quantum sensor market by sensor type; (b) applications of quantum sensors.

Specifically, in the area of National Security and Defense, quantum sensing is expected to have numerous applications across different theaters of operations and combat domains. For example, it can be used in the development of sensors and detectors for explosives and chemical, biological, radiological, and nuclear warfare agents. Quantum Position, Navigation, and Timing (PNT) devices can serve as reliable inertial navigation systems, enabling navigation without an external reference, such as GPS. Once fully developed, this capability could be revolutionary for both underwater navigation and terrestrial platforms.

Another highly significant application of quantum sensing, with major implications for the Theater of Operations and currently at an intermediate stage of technological maturity, is the detection, identification, and estimation of the PNT of submarines and stealth aircraft. A brief example of advancements in this sector is presented below.

At the end of 2023, the Canadian government announced the purchase of 88 units of the F-35 Lightning, considered the second most advanced fighter jet in the world. Manufactured by the American company Lockheed Martin, the total cost of the deal was approximately 14 billion U.S. dollars, meaning each unit cost around USD 160 million (or BRL 0.96 billion per unit). This high cost is justified by the F-35 Lightning's cutting-edge features, including the world's most powerful engine, produced by Pratt & Whitney; advanced sensors that create comprehensive battlefield images, enhancing situational awareness required for C4ISR operations (an acronym in English for Command, Control, Communications, Computing, Intelligence, Surveillance, and Reconnaissance); a sophisticated robotic system called VLO Stealth, which offers unparalleled enemy detection and penetration into contested airspace; and an "Electronic Warfare System" that detects enemy threats and jams radars. Due to its multifunctional sophistication, the F-35 allows pilots to operate in any environment against any threat. However, what truly sets it apart from other fighter jets is its stealth capability (also known as stealth mode or simply stealth), which enables it to remain invisible to enemy radars.

Nevertheless, the stealth capability of the F-35 and other stealth aircraft may become obsolete with the development of a next-generation quantum sensor designed to function as a radar, as announced by China. The R&D for this radar began in the past decade. It is currently believed to have reached a Technology Readiness Level (TRL) above 6, suggesting

that it could render current stealth technologies ineffective. This is one of the many paradigm shifts in the Defense sector brought about by the production of quantum sensors.

China's advancements in this sector have been contested by the United States. Jeffrey Shapiro, a physicist and professor at the Massachusetts Institute of Technology (MIT), as well as a pioneer in the concept of quantum radar, has expressed skepticism, stating that there are still numerous technological challenges to overcome before the radar becomes truly effective. On the other hand, the China Electronics Technology Group Corporation (CETC) has unveiled a prototype, claiming it could identify stealth aircraft in flight. Additionally, Chinese scientists have explained that high-energy quantum particles could acquire targets that are invisible to conventional radars. Despite the ongoing narrative battle, it is important to consider that Chinese researchers claim to have successfully demonstrated stealth detection effects, with targets at significant distances, as well as the technological demonstrators that China has been presenting.

Figure 4: YIC-8E, the world's first anti-stealth quantum radar, created by China.

Demonstrando sua capacidade tecnológica no setor, a China apresentou, recentemente, um radar revolucionário no Zhuhai Airshow: o YLC-8E. Esse radar quântico, que vem sendo desenvolvido pela China (Figura 4), utiliza fótons de micro-ondas emaranhados como método de detecção e, pelo menos em princípio, poderá anular a tecnologia stealth dos chamados aviões invisíveis. Esse desenvolvimento é visto como um grande desafio para os jatos de combate F-35 e F-22 altamente avançados dos EUA.

Figure 5: Images of the new Russian stealth drone S-70.

Another demonstrative example of the advances in the application of quantum devices in the defense area is the Russian super-heavy attack drone (S-70 from Sukhoi-MIG), called Okhotnik (or Hunter), seen in Figure 5. It was experimentally deployed in 2019, weighs 20 tons, has an autonomy of 6,000 km, and can reach a maximum speed of 1,000 km/h. Its operational characteristics of invisibility (stealth degree) and high sensing capacity indicate the possible use of quantum sensors, given their high sensitivity and precision.

Figure 6: Chinese supersonic Stealth bomber, H20.

The H-20, the new Chinese supersonic bomber (Figure 6),

presented during the two sessions of the National People's Congress, is another significant innovation that suggests China's high technological capacity in quantum technologies, particularly in quantum devices. In an interview with the Hong Kong Commercial Daily in March 2024, Wang Wei, the deputy commander of the People's Liberation Army Air Force, revealed that the H-20 will be officially announced to the public soon, and denied that there are technical bottlenecks, stating that the H-20 "is something to be proud of and excited about." The significance is great. One of the characteristics of the H-20 is the number of quantum sensing and detection devices both onboard and in the attack equipment..

(b) Quantum Communication

Currently, the goal is to ensure the security of data in both civilian and military communications through techniques like encryption and frequency hopping, the latter having a greater impact on military communications. This occurs both in confined communications, such as fiber-optic cables, and in non-confined communications, like wireless communications commonly used in Operational Theaters with military tactical communication radios. In a network environment, cryptographic key exchange is also used to make communications more secure.

However, these conventional communication systems rely on electromagnetic phenomena that are vulnerable to interference, interception, and hacker actions, which can copy bits in transit without leaving traces. The new paradigm of quantum communications allows for the preservation of confidentiality during transmission.

Quantum communication, on the other hand, takes advantage of the laws of quantum physics to protect information. These laws allow particles – typically photons of light – to assume a state of superposition, forming the communication qubit. From a cybersecurity perspective, when a hacker attempts to infiltrate the system while these data are in transit, the state of the qubit is altered, leaving a trace of their invasion. Thus, a hacker cannot tamper with the qubits without leaving a revealing signal of their activity.

As a result, much research has been conducted to create highly sensitive data transmission networks based on a process known as Quantum Key Distribution (QKD), which, in theory, are ultra-secure. In this process, the quantum properties of certain particles are used to generate

a secret key, known only to the two parties interested in communicating. The photon became the natural candidate for implementing qubits in quantum communications. As it is typically transmitted through fiber-optic cables or Free-Space Optics (FSO) links, the importance of research groups worldwide working with photonics or quantum optics has grown.

The secret of QKD lies in cryptographic keys, which are created and transmitted in the form of qubits, offering great security. However, the keys created are used to encrypt data in a classical manner. In one of the QKD approaches, the BB84 Protocol, named after its creators (Charles H. Bennett and Gilles Brassard) and the year of proposal (1984), one end creates the key and sends it through an optical channel. Then, both ends compare part of their keys, known as key refinement, to check if they have the same key. Additionally, another process, known as key distillation, can detect if the key has been intercepted by a hacker. If this happens, the key is discarded, and new ones are generated until a secure key is successfully shared.

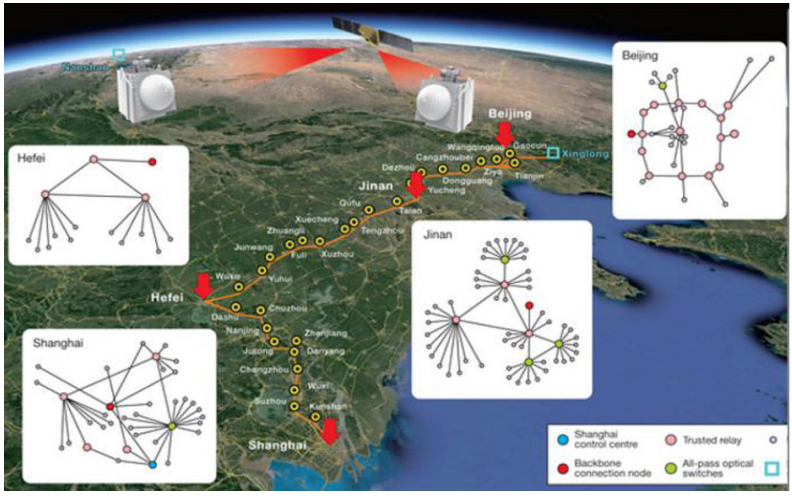


Figure 7: QKD communication network between Beijing and Shanghai.

China has been demonstrating successive advances in the development of quantum communications. In 2016, China launched the first quantum communication satellites, which used FSO links to establish a QKD communication between two ground stations separated by 2,600

km. In 2017, there was already a quantum communication network, over 2,000 km long, between Beijing and Shanghai, via optical fiber links, with several repeaters and two satellites to assist in the generation and transmission of quantum keys (Figure 7). By 2021, researchers had already increased the maximum reach of a purely terrestrial QKD link to over 500 km, using a technology known as Double Field QKD (TF-QKD)30.

Despite these advances, there is still much room for research in quantum communication networks. For example, the quantum communication channel may be noisy or have imperfections that generate errors. Such errors can be confused as being caused by the presence of a spy and lead to the discarding of the generated keys. Another problem to be studied is the quantum repeaters, needed for long-distance networks. The Beijing-Shanghai network uses about 30 repeaters, known as trusted nodes, where the quantum keys are decrypted into bits and then retransmitted quantumly. A hacker who invades these nodes can copy the bits without being detected.

To mitigate these risks, some researchers work with another approach, known as quantum teleportation. This technology is based on the creation of entangled photon pairs, which are transmitted to the two ends of the channel. Whenever a subsequent interaction changes the state of the entangled photon at one end, the state of the photon at the other end is also changed due to quantum entanglement. No quantum channel is necessary for this. Only a classical channel that transmits the result of the measurement made by the transmitter. However, creating a teleportation network with many nodes is still a significant challenge. Researchers around the world are seeking reliable ways to produce entangled photons, on demand, at scale, and maintain their entanglement over large distances.

In 2015, a published study demonstrated the teleportation of two quantum states of the photon, its spin and its angular momentum. Both were used as qubits. In 2017, the Chinese Micius satellite was used to teleport two photons between Austria and China, in a quantum communication experiment spanning 7,600 km.

Notably, China is the most advanced country in this technology (Figure 8). In 2022, the country established a Quantum Secure Direct Communication (QSDC) channel of 102.2 km, setting a new record for this type of communication. The previous record for this type of channel was 18 km. A QSDC channel performs different tasks from a QKD system, in the sense that a quantum channel is created for secure and

reliable transmission, both regarding noise and eavesdropping. Typically, the creation of this secure channel involves the generation of entangled photons.

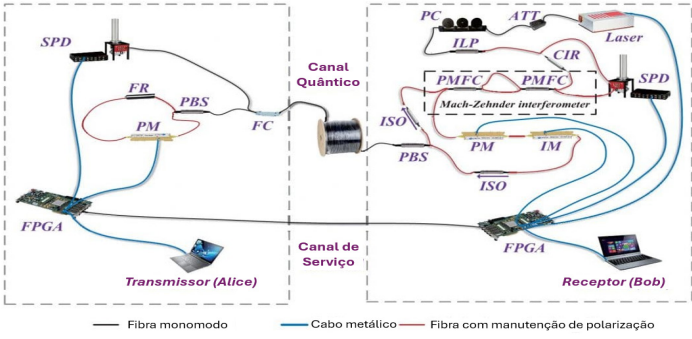


Figure 8: Network created by China breaking the QSDC distance record (adapted from ZHANG, H. et al., 2022).

In the field of Defense in Brazil, the project led by the Instituto Militar de Engenharia (IME) stands out, with the collaboration of other research centers in Brazil, aiming to propose a model for quantum communication, based on the generation and distribution of entangled photons. Called the Rede Hermes Quântica (RHQ), the project intends, initially, to establish a network with three nodes between the IME, the ECEME (Escola de Comando e Estado Maior do Exército), and the CBPF (Centro Brasileiro de Pesquisas Físicas) (Figure 9a). In this network, a QKD protocol will be established, based on entanglement and FSO links.

(a) (b)

Figure 9: (a) Quantum Hermes Network (RHQ): the red lines represent the links from IME to the Army Command and General Staff College (ECEME) and to Pão de Açúcar; the blue line shows the link from IME to the Brazilian Center for Physics Researchs (CBPF); (b) Rio Quantum Network (RRQ) with its extension.

This strategic project for the Armed Forces is supported by the CBPF, UFF (Federal Fluminense University), PUC-Rio (Pontifical Catholic University of Rio de Janeiro), and UFRJ (Federal University of Rio de Janeiro). Another important partner is UFPE (Federal University of Pernambuco), whose Department of Physics has been working on the development of quantum devices necessary for end-to-end quantum computing and communication, without the need for signal repeaters that use the conventional paradigm. The results from UFPE's research are crucial for the next phases of RHQ, which are expected to involve long-distance optical fiber links. In March 2024, IME signed a Technical Cooperation Agreement with UFPE, and this institution is one of the partners in RHQ.

The RHQ is synergistic and complementary to another important project being carried out by the same institutions: the Rio Quantum Network (RRQ), a project led by UFF. The main goal of this project is to establish a metropolitan quantum communication network, connecting these institutions and IME. Some of the links extend for tens of kilometers via optical fiber. There is also a plan for an airborne link of about 7 km crossing the Guanabara Bay (Figure 9b).

(c) Quantum Computing

The first steps towards the development of quantum computing began in the 1950s. In 1981, during a conference at MIT, one of the fathers of modern quantum mechanics, physicist Richard Feynman, proposed the use of quantum systems in computers, which would then have processing power superior to that of classical computers. In 1985, David Deutsch from the University of Oxford described the first quantum computer as a Quantum Turing Machine.

After Deutsch, it wasn't until 1994 that news of quantum computing emerged. In New Jersey, at AT&T's Bell Labs, applied mathematics professor Peter Shor developed an algorithm (Shor's Algorithm) capable of factoring large numbers at a much faster speed than conventional (classical) computers. In 1996, Lov Grover, also from Bell Labs, developed Speedup, the first algorithm for quantum database search. In 1999, the first prototypes of quantum computers based on thermal principles were built at MIT.

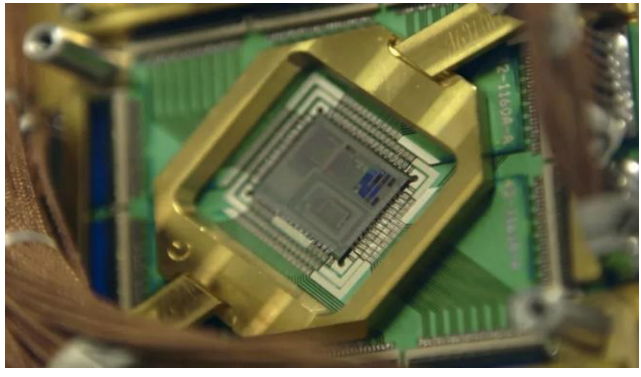


Figure 10: The main element of a quantum computer: the chip that stores the qubit structure.

In 2007, Orion, a 16-qubit quantum processor capable of performing practical tasks, was introduced. It was developed by the Canadian company D-Wave Systems, based on superconductivity principles. In 2011, the company launched the first commercial quantum computer, called D-Wave One, with a 128-qubit processor. However, the D-Wave One was not yet fully independent and needed to be used in conjunction

with conventional computers. In 2017, the same company launched the D-Wave 2000Q, a quantum computer with 2,000 qubits, priced at $15 million. Currently, D-Wave has quantum computers with over 5,000 qubits. Although the number of qubits is no longer a determining factor in the evolution of a computer, as the most advanced chips are focusing on the quality and better control of qubits, 5,000 qubits represent a significant development milestone.

Figure 11 shows the main global players in the field of quantum computer manufacturing and the type of qubit used for their development.

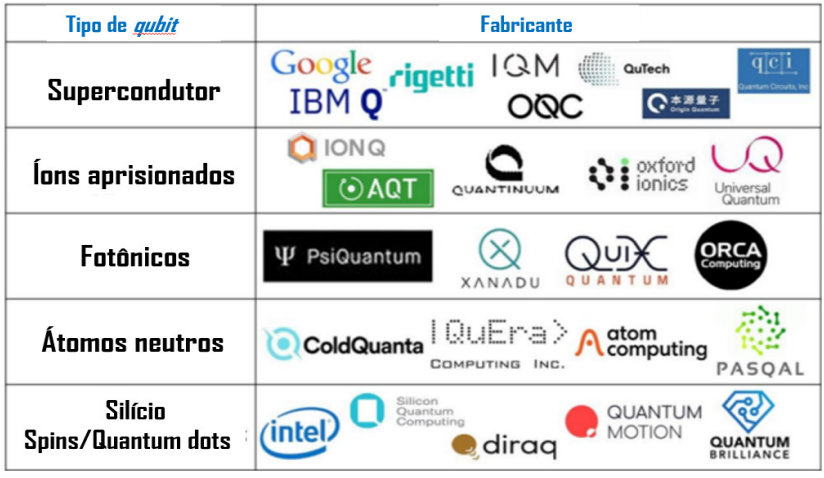


Figure 11: Main global players in the field of quantum computer manufacturing and the type of qubit used for their development.

Among the numerous possibilities envisioned for the application of quantum computing, one stands out: integer factorization. This is a class of mathematical problems that classical computers take an extraordinarily long time to solve (on the order of thousands of billions of centuries), while quantum computers can solve it efficiently in just a few hours.

In number theory, integer factorization is the decomposition of a composite number into a product of smaller integers. If these factors are restricted to prime numbers, for example, the process is called prime factorization. Despite being very old, the problem of factoring large integers has not yet been solved efficiently. The interest in finding a solution to this problem is growing because the security of current public-key cryptography methods, such as RSA (acronym composed of the initials of

Ron Rivest, Adi Shamir, and Leonard Adleman), depends on the current efficiency of factorization methods. When the numbers are sufficiently large, no efficient non-quantum integer factorization algorithm is known. Many areas of mathematics and computer science are involved with this problem, initially algebraic number theory and more recently quantum computing.

Additionally, there are already quantum algorithms to solve these problems and decrypt digital communications, such as Shor's Algorithm, mentioned earlier, which can only be executed on a quantum computer. This algorithm can analyze and factor integers of any size. For example, Gidney and Ekera suggest that it is possible to factor a 2048-bit integer in just 8 hours using a computer with 20 million qubits. With current technology, it would take thousands of years.

Thus, quantum computing will have many applications in the analysis of large amounts of data. However, this new technology not only accelerates conventional computing but also provides greater processing power for certain types of problems, in addition to factoring very large numbers, such as: DNA sequencing, artificial intelligence, and weather forecasting, among other areas.

The secure transmission of data through quantum communication and quantum computing applied to cybernetics are of fundamental importance. In terms of security and national defense, quantum computing will be crucial, especially when applied to cybernetics since most of the global digital infrastructure and almost all activities carried out online, such as video conferencing, sending emails, and remote access to bank accounts, are based on encryption methods that rely on the inability of existing computational resources to solve large integer factorization.

Although quantum computers do not yet have the processing power to decrypt most cryptographic methods, ways to protect against this threat need to be found, as advances in the capability of these computers have been significant and, with increasing investment in scientific research and technological development, the trend is that the pace of this growth will not slow down. As mentioned earlier, it is estimated that a quantum computer would need about 20 million qubits to break the current RSA encryption – used for sending confidential data over the Internet. Considering that the largest quantum computer today has 5000 qubits (D-Wave), it can be said that it will still take a long time to break this encryption.

In summary, although there are still no commercial quantum computers for the general population (only educational devices with a low number of qubits), developments in this area are already at an intermediate stage of technological maturity. With the prospect of the development of commercial quantum computers, it is conceivable that encrypted information from current communication systems is being stored to be used in decryption when the new technology becomes available.

Indeed, quantum computing is an urgent threat to cybersecurity in society in general and to the systems used in the area of National Security and Defense in particular. To combat it, the entire digital infrastructure must be completely updated. In this sense, some approaches discussed below deserve attention.

One possibility to protect current information against future computers is to implement what is known as post-quantum cryptography (PQC). Despite the name, it involves new classical cryptographic algorithms (i.e., not quantum), whose solution by quantum computers would be as time-consuming as that of current classical algorithms.

The U.S. equivalent to Brazil's INMETRO, the NIST (National Institute of Standards and Technology), conducted an international competition/consultation, where three PQC algorithms were selected for global standardization and adoption. The process began in 2016, and in August 2023, public comments were requested regarding the three finalists. The comment period ended in November 2023, and the final decision by NIST was made in August of this year. One of NIST's goals is for the selected algorithms to be interoperable with existing communication protocols and networks. With the standardized algorithms, it is expected that the IETF (Internet Engineering Task Force), responsible for developing and promoting Internet standards, will incorporate them into new versions of protocols such as IPSec (Internet Protocol Security) and TLS (Transport Layer Security) by 2025.

Another option would be to wait for quantum communication, via quantum cryptography, quantum teleportation, or another more modern implementation, to mature enough to use this type of communication to protect against decryption attacks carried out by quantum computers. The most well-known implementation of quantum cryptography is QKD protocols.

Investing in quantum communication (QKD or quantum teleportation), promoting its maturity with the expectation that it will offer

resilience to the quantum threat, is an approach being adopted by various Brazilian research groups, such as the initiatives promoted by the IME and the universities of the RRQ project. Public policymakers and leaders at all levels should be attentive and prepared for the need for updates in the cybersecurity area.

.

(d) Global Race for Quantum Technology Domination

Quantum Technologies are transversal and have a broad spectrum of application in National Security and Defense, being fundamental to the development of new military capabilities essential for the War of the Future.

The advances in areas associated with Quantum Technologies are surprising, particularly due to the great governmental and private interests that mobilize extraordinary financial resources to promote basic research, applied research, and research and development, as well as to train highly qualified human resources to explore all the yet undiscovered facets of quantum technologies.

Figure 12 shows the investments made worldwide in 2022, totaling approximately $30 billion (around R$ 160 billion). In 2023, this amount surpassed USD 38 billion (approximately R$ 228 billion), and the forecast is that by 2040 it will exceed USD 106 billion, more than half a trillion reais. China appears as the largest investor in the field (USD 15 billion). Brazil appears with modest USD 12 million investments in 2023.

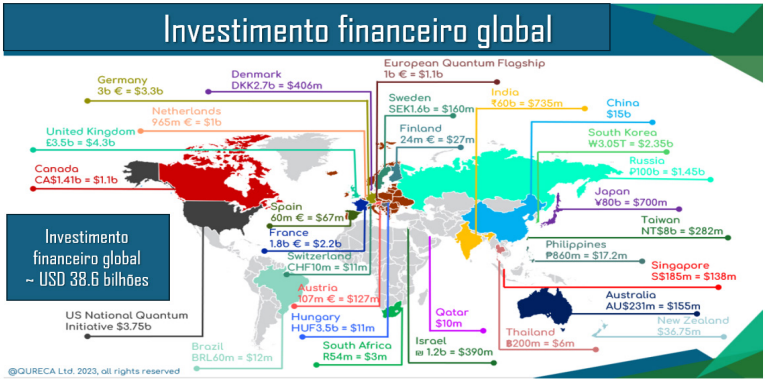


Figure 12: Investments made worldwide in 2023.

In addition to the financial aspect, it is also important to consider

the national infrastructure for data storage and processing. What is commonly known as the "cloud" is nothing more than distributed servers in massive data centers, responsible for storing and processing systems on the internet. This is a matter of data sovereignty: countries that do not have sovereignty over their infrastructure and local physical databases run the risk of having their data used by other countries for the development of quantum technologies. Furthermore, quantum technologies, particularly quantum computing and communication, will also require data centers prepared to accommodate quantum hardware.

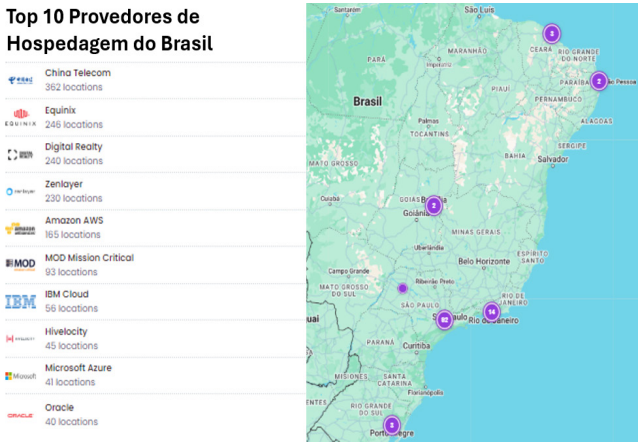


Figure 13: Distribution of the main hosting providers in Brazil.

OBrazil has a still small, poorly distributed data center network controlled by large foreign corporations, as shown in Figure 1346. There are 117 data centers across the country, distributed in only 6 states and controlled by 26 suppliers, most of them foreign. These data centers store the main information of Brazilian systems. Therefore, it is a matter of sovereignty that quantum software and hardware should not be hosted in locations controlled by foreigners.

REFLECTIONS OF QUANTUM TECHNOLOGIES AND THE 4TH INDUSTRIAL REVOLUTION ON NATIONAL DEFENSE

The Fourth Industrial Revolution is characterized by the fusion of physical, digital, and biological spheres, with technologies being developed

in these three areas for a faster development of the productive sector. In this revolution, there is a synergy of breakthroughs and disruptive innovations across various sectors of science and technology, which, when combined, impact the most diverse areas of society, economic growth and development, national security and sovereignty, international relations, and particularly the nature of conflicts and wars. In this revolution, some trends have been identified, which will be analyzed in more detail in this text, such as hyperconnectivity, digitalization, and digital convergence, as well as the sharing of information, for example, stored in the "cloud." These trends have a significant impact on Cybersecurity, an area that will be strongly affected by Quantum Technologies.

As a consequence of this rapid advancement, it is possible to identify today a ubiquitous and efficient mobile internet; reduced size and cost and increased capacity of sensors that emerge to monitor the most varied phenomena and objects; as well as robots; the Internet of Things (IoT), Internet of Battlefield Things (IoBT), smart cities, autonomous vehicles, additive manufacturing, wearable technologies, drone swarms, smart weapons, among many others. Given the vast number of technologies in this revolution, this text focuses on the discussions and interdependencies between AI, Cybernetics, and Quantum Technologies, and some possible trends arising from the joint use of these technologies in the field of Defense.

Despite its theoretical foundations and the first proofs of concept emerging in the 1950s, AI has provided an increasing number of important innovations in recent years, thanks to easy access to large amounts of data, which is necessary for "intelligent" algorithms to converge and learn from the environment; the exponential increase in processing power (Moore's Law) and storage capacity, essential to enable the execution of AI algorithms in real-time; advances in the development of search algorithms and deep learning techniques; the availability of sensors that collect large amounts of data in real-time; and advances in actuators, which are often essential for carrying out actions originating from AI-powered devices. As new quantum technologies become embeddable, AI may be further enhanced, potentially resulting in an extraordinary leap in the performance of devices and systems such as autonomous vehicles, drone swarms, and robotics.

From the perspective of the defense industry, notable uses of AI include Cybernetics, Wireless Sensor Networks, Simulation, Object

Detection, Unmanned Aerial Vehicles (UAVs), Command and Control Systems, and Mechatronic Systems. Thus, target selection, detection, and engagement, as well as the automated use of drone swarms, are some of the possibilities for employing AI in Future Warfare. AI is a technology that already existed earlier in a different format, initially created to achieve greater efficiency in specific tasks, not generative ones. More recently, artificial intelligence, with ChatGPT (or GPT-3, Generative Pre-Trained Transformer) from OpenAI as its most well-known representative in the general population, has indicated the scientific, technological, and social revolution taking place in the AI field.

The GPT-4 is expected to use 100 trillion parameters, much larger than the 175 billion parameters of GPT-3. Some scientists believe the new version, GPT-5, could become Artificial General Intelligence (AGI). To make this possible, we still have to wait for the next results. Versions ChatGPT-3.5 and 4 are known to degrade when extensively used by multiple users, a phenomenon known as behavioral drift or "model drift." Overcoming these obstacles, AI, combined with the processing and storage capabilities of Quantum Technologies, is expected to exhibit much greater capabilities than those currently known.

Embedded electronics and software-based components are beginning to play an important role in aerial, maritime, and terrestrial artifacts and vectors. The advent of cognitive networks, cloud computing, and advancements in digital communications through wireless channels are increasing connectivity. The key technologies supporting these issues enable Armed Forces to develop cyber warfare principles, employ complex command and control systems, and perceive battlefield situations in an intuitive manner and with unprecedented detail. Security—supported by protocols based on quantum technologies—will be at the forefront of designing and operating intelligent warfare systems and their support networks. Progress is significant for those who master these critical technologies but will represent a significant setback and great threats for countries with low technological capacity in key areas.

In the context of the 4th Industrial Revolution, Cyber Warfare emerges, where security vulnerability increases with dependence on technology, especially with the advent of quantum technologies. The first formal definition of Cyber Warfare is often attributed to researchers John Arquilla and David Ronfeldt in a 1993 report published by the RAND Corporation think tank. They defined Cyber Warfare as: "Conducting

and preparing to conduct military operations according to information-related principles. This means attacks aimed at disabling, interrupting, or destroying adversary information and communication systems, while protecting one's own systems." With the 4th Industrial Revolution, critical infrastructures become interconnected with networks and cyberspace, making the impacts of such warfare even greater. Quantum Technologies will amplify this impact.

Between June and October 1999, Jonathan—a 15-year-old American teenager—hacked NASA and the Pentagon, among other smaller targets. He became the first person in the world to enter the Defense Threat Reduction Agency (DTRA) system, a Department of Defense (DoD) division tasked with analyzing threats to the United States. The same feat was achieved in relation to the Pentagon by other hackers, such as Gary McKinnon, who is accused of hacking NASA, the Pentagon, the Army (USARMY), the Air Force (USAF), and the Navy (USNAVY) from February 2001 to March 2002. U.S. prosecutors accused McKinnon of completely shutting down a network of more than 2,000 computers for 24 hours. Russian hacker attacks have made headlines since the last U.S. presidential elections and more recently during the Russia-Ukraine War.

In 2016, a simple photo (Figure 14), shared by Mark Zuckerberg to celebrate Instagram's 500 million users, brought the issue of hackers back to the forefront. The image showed the Facebook creator covering the webcam and microphone of his notebook with tape. Clearly, no one in the world is safe from hackers.

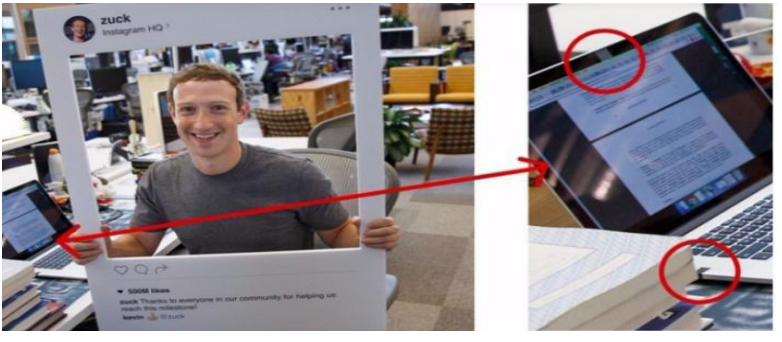


Figure 14: A photo shared by Mark Zuckerberg to celebrate Instagram's 500 million users brought the topic of hackers back to the forefront.

In 2018, China was accused of hacking into the U.S. Navy

systems. According to information obtained by The Washington Post from unidentified U.S. military officials, Chinese hackers allegedly infiltrated the systems of a third-party company providing services to the U.S. Armed Forces and accessed about 614 GB of confidential data.

In mid-June 2023, the U.S. Navy was once again breached by Chinese hackers. Microsoft issued a warning, as did intelligence agencies, including the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and cybersecurity agencies from four other nations. The alerts warned corporate and public entities that a sophisticated hacker group, supported by the Chinese government, had successfully exploited a vulnerability in a popular cybersecurity package. With Volt Typhoon, this alleged Chinese group affected critical cyber infrastructure across various sectors. According to the report, the Chinese hackers targeted communications and maritime sectors in Guam, in the Pacific Ocean, which hosts a major U.S. military base.

Recently, The New York Times reported that the United States is working to identify and eliminate a malicious software code that, according to the article, was installed by China at the heart of networks controlling the critical infrastructure of the U.S. Army. This code could potentially be activated remotely in the event of armed conflict (e.g., in a war between China and Taiwan) and disrupt electricity, potable water, and communication networks supplying U.S. military bases, hindering the deployment of troops. This highlights the potential disastrous consequences that inefficient cybersecurity could cause to the security of any country.

With trends from the Fourth Industrial Revolution and their consequences, such as digitalization and hyperconnectivity, including military systems and materials, the surface of cyberattack threats will increase further. Cyberattacks and digital espionage will intensify, and their consequences will become more severe.

The study of the Fourth Industrial Revolution and cyber warfare has become central to the development of military art and thought. In this new era, dependence on technology will be extremely critical for a country due to the increase in cyber vulnerabilities. Evidence suggests that quantum technologies will be pivotal in balancing greater protection or greater cyber vulnerability, as technological advancements drive innovations for defense and violations of data communication system security. It can be inferred that a protection system based on quantum

communication, quantum computing, encryption, as well as the use of devices (sensors, detectors, and actuators) based on these technologies, will be effective. Thus, achieving quantum supremacy is an essential goal for a country seeking to play a significant role in the international community and promote its own national sovereignty.

By analyzing different theaters of operations from recent conflicts or crises, such as the one between China and Taiwan, we can observe strong signs of technological advancement. One example is the development of the Russian drone called Joker, which can remain dormant (or in hibernation mode) for weeks. Designed to hide from electronic countermeasures, the drone could be prepared for an attack hours, days, or weeks before its operator awakens it to launch the mission. Advancements continue, suggesting the intensive use of quantum technologies by major powers in the medium term, and in the not-too-distant future, warfare may be dominated by quantum technologies, leading to the so-called Quantum Warfare (Figure 01).

The discussions presented in Section 3 bring to mind the famous phrase spoken in 1915 by British Admiral John Fisher. During World War I (1914-1918), he declared that the war will be won by inventions. The characteristics of current conflicts and the trends in scientific-technological evolution, especially in quantum technologies, suggest that this statement is prescient.

However, despite technological advancements, the so-called War of the Future has not yet arrived, as these new concepts are still being incorporated into the different forces. Next-generation AI-powered machines are soon to be a reality. Numerous U.S. states have already begun using Boston Dynamics robots for law enforcement patrols in cities, including Los Angeles, New York, and San Francisco.

Figure 15: Shoulder-fired anti-armor weapon, called Javelin, launches a

guided missile at its target.

Despite the use of ambush tactics and the fact that Russia is not deploying its most modern tanks, the ongoing war between Ukraine and Russia has shown that the technology of Javelin missile launchers (Figure 15) can pose a risk, in terms of firepower, to the Russian fleet of armored vehicles. This shoulder-fired anti-tank weapon was developed and manufactured for the Marine Corps/US Army by Lockheed Martin (Florida) and Raytheon (Arizona), but it still does not incorporate any concepts related to quantum technology, as it is not yet deployable. Once that happens, extraordinary advances could occur in areas such as artificial intelligence, robotics, cybersecurity, communications, and command-and-control systems, with numerous consequences for defense capabilities and combat power.

Amid this surge of technological innovations, a fundamental shift in the defense policy of many countries considered military powers was consolidated in 2021. This shift is characterized by an increase in budgets for digital technology, artificial intelligence, cybersecurity, and quantum technologies, alongside a decrease in funds for conventional equipment and the maintenance of large troops.

FINAL CONSIDERATIONS

This article broadly addressed the influence of technologies derived from the Second Quantum Revolution, particularly in the areas of national security and defense. The evidence presented here suggests that the adoption of a strategic program in this area by the Brazilian Army is a matter of sovereignty. Developed countries or those seeking prominence in the world stage invest heavily in R&D to obtain various military applications of Quantum Technologies. Quantum computing, communication, sensing, and cryptography are the only ways to have secure communication impervious to hackers, situational awareness, and the efficient development of key military capabilities for the War of the Future.

Given the enormous impact of quantum technologies in the field of cybersecurity, and the world's current strong dependence on computers, this study addressed many aspects of Cyber Warfare. In a military, financial, or other types of conflicts, it is common for critical

infrastructures to be attacked early on to destabilize a nation. Currently, all critical infrastructures depend on a sophisticated computing network that is increasingly targeted by aggressors. In all cases, it is foreseen that the best Cyber Security and Defense structure will use Quantum Technologies.

The possibility of gaining unauthorized information within a communication network in extremely short periods, with algorithms like Shor's, is concerning. Thus, the set of quantum technologies applicable to cybersecurity, together with quantum devices (sensors, biosensors, and detectors), is essential for the Armed Forces to carry out their constitutional missions. In the future, the association of these technologies with others, such as AI, will be decisive in robotics, autonomous systems, UAVs, missile technology, and will underpin what is called Quantum Warfare.

Given this great strategic importance and the markedly different objectives of the three main actors—the academic field, companies, and the government, notably the Armed Forces—it is safe to assert that the development and implementation of Quantum Technologies should be managed and led by the Armed Forces, particularly the Brazilian Army, focused on the cybersecurity area. This is because the other forces are responsible for the two other major strategic areas: Nuclear and Aerospace, as outlined in the National Defense Strategy.

Quantum Technologies currently face several technological challenges, such as the frequent need to operate at extremely low temperatures, decoherence, quantum noise, scalability, suitable materials, and still high costs. Although this may be seen as a problem, these challenges also represent an opportunity because it means the technology is not yet ready, leaving room for national development. It is important to highlight that investing in such technology implies competing with other Brazilian public policies.

However, given the global effort in terms of investment in Quantum Technologies, Brazil, and particularly its Armed Forces, cannot remain indifferent. Global investments indicate one thing: those who do not master Quantum Technologies will pay a high strategic price in National Security and Defense, as well as in economic and technological growth and development. Integrated into the National Cyber Defense Program (PDCDN), the Brazilian Army is developing its Strategic Cyber Defense Program, which aims to coordinate and integrate cybersecurity projects and processes, as well as develop the Armed Forces' cyber capabilities

through integration, coordination, and joint actions. Since 2023, the PDCDN has been seeking to provide resources for the development of national Quantum Technologies.

Thus, Brazil cannot ignore the strategic importance of the national development of these technologies and simply opt for importing them, whether products (quantum communication systems, internet and quantum cryptography, and quantum sensors) or services (quantum computers). It is inconceivable that strategic and confidential data about our Armed Forces' operations should be analyzed by foreign quantum computers such as Sycamore (from Google) or Osprey (from IBM) due to the absence of national equipment.

There is little doubt about the urgent and essential need for local development of Quantum Technologies for national security and defense. However, given the enormous scientific and technological challenges and the dual nature of the technologies to be developed, with a significant impact on all Expressions of National Power, to achieve the desired results in these disruptive technologies, a national effort must be promoted to allocate the necessary financial resources to achieve autonomy in this strategic area for the country.

Politicians, strategists, and policymakers who defend the values of freedom, democracy, and sovereignty recognize that their preservation depends on constant vigilance, i.e., a National Defense system capable of repelling current and future threats. Maintaining a system of constant vigilance is the price to pay for something so precious. As Rui Barbosa summarized: "An army can go 100 years without use, but not a minute without preparation." This way of thinking lays the foundations for the sense of self-preservation and national cohesion that will guide investments in the Defense area.

Although various areas of National Power can be mobilized to act for a nation's sovereignty, the State must coordinate, collect, and integrate Military Employment Systems and Materials (SMEM) to strengthen its military system's capabilities. This robustness necessarily requires technological autonomy. In terms of defense technology, nothing is more modern and fundamental than Quantum Technologies. They have the potential to affect almost all aspects of the military environment, from those with little scientific-technological content to the most complex ones.

By relying on homegrown innovations of high added value, essential to the survival of the State and the realization of the so-called

Permanent National Objectives, in general, the Defense sector is the driving force behind scientific and technological development and boosts the multi-million-dollar market of companies that compose the Defense Industrial Base (BID). Indispensable for incentivizing innovative projects, especially those directly related to National Defense, the mechanisms adopted by the State to support the BID have few studies characterizing the factors related to their origin or development. However, it is known that the main players in this domain, such as the United States, the European Union, Great Britain, and Russia, won the great wars of the 20th century thanks to a prosperous Defense industry and a continuous and important financial support in the areas of education, science, and technology, thus demonstrating the importance of this trio for their people in conflict resolution.

It is essential to define short, medium, and long-term objectives; coordinate and assess progress in the academic community and ICTs, as well as contribute with research in the sector, through their ICTs in partnership with the academic community, companies, and other government sectors. This includes not only partnerships with large tech companies but especially with startups, universities, and research institutes, as they are essential for innovation in this type of technology. However, as the content is sensitive and of vital importance for the country's Security and Defense, this process must involve the significant participation of the Armed Forces, especially the Brazilian Army, particularly their teaching, research, development, and innovation organizations. A recent initiative approved by CAPES (PRO-DEFESA-V), coordinated by IME, involves about 100 researchers from 43 civil and military institutions and 23 graduate programs.

For the Armed Forces to truly benefit from these new Quantum Technologies, it is essential that they participate actively in this area and provide both the foundations for development and the adoption of applications for potential uses in the military sector. A strong involvement in the quantum ecosystem will improve the Armed Forces' understanding of the potential risks associated with these new technologies, especially in the cybersecurity area. Such a risk becomes evident when considering the importance of developing quantum internet, based on quantum communication.

It is difficult to imagine a more current and relevant statement than the one made in 1915 by British Admiral John Fisher when he

declared, "The war will be won by inventions." Analyzing this in light of the previous text, the words of the 3rd Viscount Palmerston—"We have no eternal allies, and no perpetual enemies. Our interests are eternal and perpetual"—clearly show the pressing need for us to develop our own Quantum Technologies related to Security and Defense. Quantum technologies are essential for economic growth, development, and sovereignty. By missing the opportunity to adequately explore some technological revolutions, such as microelectronics and nanotechnology, Brazil suffered incalculable and irreversible losses. Countries that do not master Quantum Technologies may face a true catastrophe in terms of sovereignty and socioeconomic development.

In 2025, the world celebrates the International Year of Quantum Science and Technology, an initiative of the UN. Brazil has all the conditions to accelerate its pace and take advantage of the political and financial resources that should come from this celebration. In Brazil, the Ministry of Science, Technology, and Innovation (MCTI) has also created a working group to formulate proposals in the Quantum area. It is expected that this initiative will lead to the creation of the Brazilian Quantum Strategy, in the same vein as the Brazilian Artificial Intelligence Strategy (EBIA). In other words, the national political sphere is already becoming convinced of the importance of this issue.

Either we develop the necessary Quantum Technologies internally, or our national Security and Defense sectors will become obsolete in a short time, with disastrous and irreversible consequences. No one will do our homework for us.

REFERENCES

ADVANTAGE: The most connected and powerful quantum computer built for business. **D-Wave Systems**. Disponível em: https://www.dwavesys.com/solutions-and-products/systems/. Acesso em: jun. 2024.

ALVAREZ, Raúl. Jonathan James, el joven que con sólo 15 años hackeó y puso de cabeza a la NASA y al Pentágono. **Xataka**, 18 fev. 2020. Disponível em: https://www.xataka.com/historia-tecnologica/joven-que-solo-15-anos-hackeo-puso-c abeza-a-nasa-al-pentagono. Acesso em: jun. 2024.

ARAÚJO-MOREIRA, Fernando M. et al. Tecnologias quânticas: a inovação disruptiva como diferencial estratégico para a Defesa Nacional. **Seven Editora**, [S. l.], 2023. Disponível em: https://sevenpublicacoes.com.br/editora/article/view/1561. Acesso em: jun. 2024. DOI: 10.56238/tecavanaborda-042.

ARAUJO-MOREIRA, F. M.; Supremacia quântica e Defesa nacional: a nova realidade. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 245–247, 2023. ISBN 978-65-87080-44-4.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming!. **RAND Corporation**, 1993. Disponível em: https://www.rand.org/pubs/reprints/RP223.html. Acesso em: nov. 2024.

BARONE, A.; PATERNÒ, G. **Physics and applications of the josephson effect.** New York: John Wiley & Sons, 1982. DOI:10.1002/352760278X.

BARZANJEH, S. et al. Microwave quantum illumination using a digital receiver. **Science Advances**, v. 6, n. 19, p. 1-9, 8 mai. 2020. DOI:10.1126/sciadv.abb0451.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: public key distribution and coin tossing. **International Conference on Computers, Systems & Signal Processing**, Bangalore, vol. 1, p. 175–179, 1984. Disponível em: https://www.karlin.mff.cuni.cz/~holub/soubory/BB84original.pdf. Acesso em: jun. 2024.

BERENDSEN, René G. **The Weaponization of Quantum Mechanics: Quantum Technology in Future Warfare**. 2019. 60f. School of Advanced Military Studies, US Army Command and General Staff College. Dissertação de Mestrado, mai. 2019. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1083173.pdf. Acesso em: jun. 2024.

BOTHNER, Daniel; RODRIGUES, Ines C.; FRANSE, Jasper; STEELE, Gary. TN2953-P The Josephson junction: Quantum tunnelling and interference in an electrical circuit. **NS Web**. Disponível em: https://nsweb.tn.tudelft.nl/~gsteele/SQUID_practicum/TN2513-P%20SQUID%20Prac ticum%20 Manual.html. Acesso em: jun. 2024.

BOUTIN, Chad. NIST releases first 3 finalized post-quantum encryption standards. **NIST**, 13 ago. 2024. Disponível em: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-q uantum-encryption-standards. Acesso em: outubro de 2024.

BRANDOM, Russell. Google's quantum computer just flunked its first big test. **The Verge**, 19 jun. 2014. Disponível em: https://www.theverge.com/2014/6/19/5824336/google-s-quantum-computer-just-flunk ed-its-first-big-test. Acesso em: jun. de 2024.

BRASIL. Ministério da Defesa. **IME se destaca em Programa de Ensino e Pesquisa em Defesa**. Exército Brasileiro, 26 ago. 2024. Disponível em: https://www.eb.mil.br/web/noticias/w/ime-se-destaca-no-pro-defesa-v-principal-edital -da-capes-destinado-a-area-da-defesa. Acesso em: junho de 2024.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. **Portaria nº 8.194, de 19 de maio de 2024**. Institui grupo de trabalho com o objetivo de debater e propor as bases e diretrizes para o estabelecimento de uma Iniciativa Brasileira para Tecnologias Quânticas. Diário Oficial da União: seção 1, Brasília, DF, n. 97, p. 87, 21 mai. 2024. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mcti-n-8.194-de-19-de-maio-de-2024-56075 5075. Acesso em: out. 2024.

BRAZIL data centers locations. **Datacenters.com**, 2024. Disponível em

https://www.datacenters.com/locations/brazil. Acesso em: nov. 2024.

CHEN, Stephen. The end of stealth? New chinese radar capable of detecting 'invisible' targets 100km away. **South China Morning Post**, Beijing, 21 set. 2016. Disponível em: https://www.scmp.com/news/china/article/2021235/end-stealth-new-chinese-radar-capable-detecting-invisible-targets-100km. Acesso em: jun. 2024.

CLARKE, John. SQUIDs. **Scientific American**, v. 271, n. 2, p. 46–53, ago. 1994. DOI: 10.1038/scientificamerican0894-46.

CORREIA, Flávia. China quebra recorde de distância de comunicação direta com segurança quântica. **Olhar Digital**, 20 abr. 2022. Disponível em: https://olhardigital.com.br/2022/04/20/ciencia-e-espaco/china-quebra-recorde-de-dist ancia-de-comunicacao-direta-com-seguranca-quantica/. Acesso em: jun. 2024.

COWING, Keith. The world's first integrated quantum communication network. **SpaceRef**, 7 jan. 2021. Disponível em: https://spaceref.com/newspace-and-tech/the-worlds-first-integrated-quantum-commu nication-network/. Acesso em: jun. 2024.

CRAWFORD, Scott E. et al. Quantum sensing for energy applications: review and perspective. **Advanced Quantum Technologies**, v. 4, n. 8, ago. 2021. DOI: 10.1002/qute.202100049.

DÓLAR cotado a R$ 6,00 em novembro de 2024. **Banco Central do Brasil**, 2024. Disponível em: https://www.bcb.gov.br. Acesso em: nov. 2024

EMMERT-STREIB, Frank. Is ChatGPT the way toward artificial general intelligence. **Discover Artificial Intelligence**, v. 4, n. 32, 2024. DOI: 10.1007/s44163-024-00126-3.

FACEBOOK: esta simple foto ha revelado que Mark Zuckerberg es muy paranoico. **RPP Noticias**, 21 jun. 2016. Disponível em: https://rpp.pe/virales/facebook/facebook-esta-simple-foto-ha-revelado-que-mark-zuc kerberg-es-muy-paranoico-noticia-973116. Acesso em: jun. 2024.

FRANÇA JUNIOR, J. A.; GALDINO, J. F. Gestão de sistemas de material de emprego militar: o papel dos níveis de prontidão tecnológica. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 13, n. 47, p. 155-176, 23 jul. 2019.

FANCHINI, Felipe. Brasil precisa acelerar o passo para se beneficiar da segunda onda de inovação quântica. **The Conversation**, 23 jul. 2024. Disponível em: https://theconversation.com/brasil-precisa-acelerar-o-passo-para-se-beneficiar-da-se gunda-onda-de-inovacao-quantica-226799. Acesso em: out. 2024.

GALANTE, Alexandre. Radar quântico – fim do stealth?. **Poder Aéreo**, 7 mai. 2018. Disponível em: https://www.aereo.jor.br/2018/05/07/radar-quantico-fim-do-stealth/. Acesso em: jun. 2024.

GALDINO, J. F.; SCHONS, D. L. Maquiavel e a Importância do Poder Militar Nacional. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 16, n. 56, p. 353-368, 2022.

GALDINO, J. F. Base industrial de Defesa: ambivalência e sustentabilidade. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 397–400, 2023. ISBN 978-65-87080-44-4.

GALDINO, J. F. Lições sobre os desafios enfrentados pela indústria de Defesa do Brasil no período de 1950 a 1990. In: SANCHES, J. C.; ARAUJO-MOREIRA, F. M. (org.). **Collection of opinion articles on strategic studies in defense and security**. [S.l.]: [s.n.], p. 393–396, 2023. ISBN 978-65-87080-44-4.

GARDNER, Frank. As armas de guerra do futuro que já são realidade. **BBC News Brasil**, 7 jan. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-59904239. Acesso em: jun. 2024.

GIDNEY, Craig; EKERA, Martin. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. **Quantum**, v. 5, p. 433, 2021. Disponível em: https://quantum-journal.org/papers/q-2021-04-15-433/. Acesso em: out. 2024. DOI: 10.22331/q-2021-04-15-433.

GIRARDI, Romullo; FRANÇA JUNIOR, J. A.; GALDINO, J. F. Criticidade tecnológica na área de defesa em países em desenvolvimento: conceitos e critérios. **Revista de Gestão e Secretariado**, v. 15, n. 4, p. 3618, 2024. ISSN: 2178-9010.

GIRARDI, R.; FRANÇA JUNIOR, J. A.; FERREIRA GALDINO, J. A customização de processos de avaliação de prontidão tecnológica baseados na escala TRL: desenvolvimento de uma metodologia para o Exército Brasileiro. **Coleção Meira Mattos: revista das ciências militares**, Rio de Janeiro, v. 16, n. 57, p. 491-527, 28 set. 2022.

HACKERS patrocinados pelo estado chinês se infiltraram na infraestrutura naval dos EUA, diz secretário da Marinha. **Poder Naval**, 26 mai. 2023. Disponível em: https://www.naval.com.br/blog/2023/05/26/hackers-patrocinados-pelo-estado-chines se-infiltraram-na-infraestrutura-naval-dos-eua-diz-secretario-da-marinha/. Acesso em: jun. 2024.

HACKER que invadiu Pentágono perde novo recurso para evitar extradição. **Globo.com**, 31 jul. 2009. Disponível em: https://g1.globo.com/Noticias/Tecnologia/0,,MUL1249916-6174,00.html. Acesso em: jun. 2024.

IYER, Kaanita. Autoridades dos EUA procuram software chinês invasor que pode afetar operações militares. **CNN Brasil**, 30 jul. 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/autoridades-dos-eua-procuram-software chines-invasor-que-pode-afetar-operacoes-militares/. Acesso em: jun. 2024.

JAVELIN Weapon System. **Lockheed Martin**. Disponível em: https://www.lockheedmartin.com/en-us/products/javelin.html. Acesso em: jun. 2024.

KRATIUK, Anton. Russian stealth drone S-70 uses high-tech components of Western manufacture: ukrainian experts present evidence. **Gagadget**.com, 8 nov. 2024. Disponível em: https://gagadget.com/en/528077-russian-stealth-drone-s-70-uses-high-tech-components-of-western-manufacture-ukrainian-experts-present-evidence/. Acesso em: nov. 2024.

KRELINA, M. Quantum technology for military applications. **EPJ Quantum** Technology. v. 8, n. 24, 2021. DOI: 10.1140/epjqt/s40507-021-00113-y.

LANÇADA a pedra fundamental da Rede Rio Quântica. **Portal Gov.br**, 11 mai. 2023. Disponível em: https://www.gov.br/cbpf/pt-br/assuntos/noticias/lancada-a-pedra-fundamental-da-red e-rio-quantica. Acesso em: jun. 2024.

LEFFER, Lauren. Yes, AI models can get worse over time. **Scientific American**, 2 ago. 2023. Disponível em: https://www.scientificamerican.com/article/yes-ai-models-can-get-worse-over-time/. Acesso em: nov. 2024.

MALIK, Mehul; MAGAÑA-LOAIZA Omar S.; BOYD, Robert W. Quantum-secured imaging. **Applied Physics Letters**, v. 101, n. 24, 10 dez. 2012. DOI: 10.1063/1.4770298.

MCFADDEN, Christopher. Russia has developed a new kind of 'sleeper' drone called the 'Joker'. **Interesting Engineering**, 26 jul. 2023. Disponível em: https://interestingengineering.com/innovation/russia-sleeper-drone-the-joker. Acesso em: jun. 2024.

MONTEIRO, Luís N. C. S. Guerras de 4a geração. **Revista Militar**, Lisboa, v. 2591, p. 1001-1014, dez. 2017. Disponível em: https://www.revistamilitar.pt/artigo/1288. Acesso em: jun. 2024.

MÜLLER, Léo. China é acusada de hackear marinha dos EUA e roubar projeto bélico. **Tecmundo**, 8 jun. 2016. Disponível em: https://www.tecmundo.com.br/seguranca/131129-china-acusada-hackear-marinha-eua-roubar-projeto-belico.htm. Acesso em: jun. 2024.

MURRAY, W.; KNOX, M. A. **Evolução da arte da guerra**: das guerras medievais aos ataques relâmpagos 1300 - 2050. Rio de Janeiro: BIBLIEx, 2022, 292 p.

NEWDICK, Thomas. Russia's S-70 hunter drone was armed when shot down by friendly fighter over Ukraine. **The Warzone**, 7 out. 2024.

Disponível em: https://www.twz.com/air/russias-s-70-hunter-drone-was-armed-when-shot-down-by-fr iendly-fighter-over-ukraine. Acesso em: nov. 2024.

O QUE é comunicação quântica?. **Mit Technology Review**, [s. l.], 1 set. 2020. Disponível em: https://mittechreview.com.br/o-que-e-comunicacao-quantica/. Acesso em: jun. 2024.

PADILHA, Luiz. YlC-8E: o primeiro radar anti-stealth do mundo. **Defesa Aérea & Naval**, 8 out. 2021. Disponível em: https://www.defesaaereanaval.com.br/ciencia-e-tecnologia/ylc-8e-o-primeiro-radar-a nti-stealth-do-mundo. Acesso em: jun. de 2024.

PADILLA CRUZ, A. M. **Quantum Technology and its influence in Global Power Politics**. 2020. 101f. Dissertação (Mestrado Internacional em Segurança, Inteligência e Estudos Estratégicos) - Charles University. 16 set. 2020. Disponível em: https://dspace.cuni.cz/bitstream/handle/20.500.11956/177264/120370453.pdf?seque nce=1&isAllowed=y. Acesso em: nov. 2024.

PANASOVSKIY, Maksim. Chinas Tarnkappenbomber H-20 wird Atomwaffen tragen und konventionelle Einsätze fliegen. **Gagadget.com**, [s. l.], 27 out. 2023. Disponível em: https://gagadget.com/de/342722-chinas-tarnkappenbomber-h-20-wird-atomwaffen-tr agen-und-konventionelle-einsatze-fliegen/. Acesso em: jun. 2024.

PAYÃO, Felipe. China cria radar quântico que revela qualquer caça stealth no mundo. **Tecmundo**, 26 set. 2016. Disponível em: https://www.tecmundo.com.br/tecmundo-auto/109884-china-cria-radar-quantico-revela-qualquer-caca-stealth-mundo.htm. Acesso em: jun. 2024.

PICCHI, Aimee. Los Angeles approves $278,000 robot police dog despite "grave concerns". **CBS News**, 24 mai. 2023. Disponível em: https://www.cbsnews.com/news/los-angeles-robot-police-dog-approved-despite-grave-concerns/. Acesso em: jun. 2024.

PRESKILL, John. Quantum computing 40 years later. **Quantum Physics**, 19 jun. 2021. DOI: 10.48550/arXiv.2106.10522.

POST-QUANTUM Cryptography. **NIST**, 2017. Disponível em: https://www.nist.gov/pqcrypto. Acesso em: jun. 2024.

QUANTUM Manifesto - A new era of technology. **TNO**, 2016. Disponível em: https://www.tno.nl/media/7638/quantum_manifesto.pdf. Acesso em: jun. 2024.

QUANTUM RESOURCES AND CAREERS. Quantum Initiatives Worldwide 2023. **QURECA**. Disponível em: https://www.qureca.com/quantum-initiatives-worldwide/. Acesso em: out. 2024.

RIVEST, Ronald L.; SHAMIR, Adi; ADLEMAN, Leonard M. A method for obtaining digital signatures and public key signatures. **ACM Digital Library**, vol. 21, n. 2, 1 fev. 1978. DOI: https://doi.org/10.1145/359340.359342.

RUSSIAN combat UAV Sukhoi S-70 Okhotnik made first flight. **Army Recognition Group**, 5 ago. 2019. Disponível em: https://www.armyrecognition.com/news/army-news/2019/russian-combat-uav-sukhoi s-70-okhotnik-made-first-flight. Acesso em: nov. de 2024.

SHOR, Peter W. Algorithms for quantum computation: discrete logarithms and factoring. **35th Annual Symposium on Foundations of Computer Science**, Santa Fé, p. 124-134, 1994. DOI: 10.1109/SFCS.1994.365700.

TECHNOLOGY Readiness Level of Quantum Computing Technology (QTRL). **Jülich Forschungszentrum**, 19 jul. 2022. Disponível em: https://www.fz-juelich.de/en/ias/jsc/about-us/structure/research-groups/qip/technolog y-readiness-level-of-quantum-computing-technology-qtrl. Acesso em: jun. 2024.

TREATY of Adrianople - Charges Against Viscount Palmerston. **UK Parliament [Hansard, House of Commons Debate]**, vol. 97, p. 66-123, 01 mar. 1848. Disponível em: https://api.parliament.uk/historic-hansard/commons/1848/mar/01/treaty-of-adrianople -charges-against. Acesso em: nov. de 2024.

VAN AMERONGEN, Michiel. Quantum technologies in defence &

security. **NATO Review**, 3 jun. 2021. Disponível em: https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html. Acesso em: jun. 2024.

WU, Chien Shiung; SHAKNOV, Irving. The angular correlation of scattered annihilation radiation. **Physical Review**, v. 77, n. 1, 1950. DOI: 10.1103/PhysRev.77.136.

XUANZUN, Liu. China's in-development H-20 bomber worth the excitement: PLA Air Force deputy commander. **Global Times**, 11 mar. 2024. Disponível em: https://www.globaltimes.cn/page/202403/1308604.shtml. Acesso em: nov. 2024.

ZHANG, H.; SUN, Z.; QI, R. et al. Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states. **Light Science & Applications**, v. 11, n. 83, 2022. DOI: 10.1038/s41377-022-00769-w.