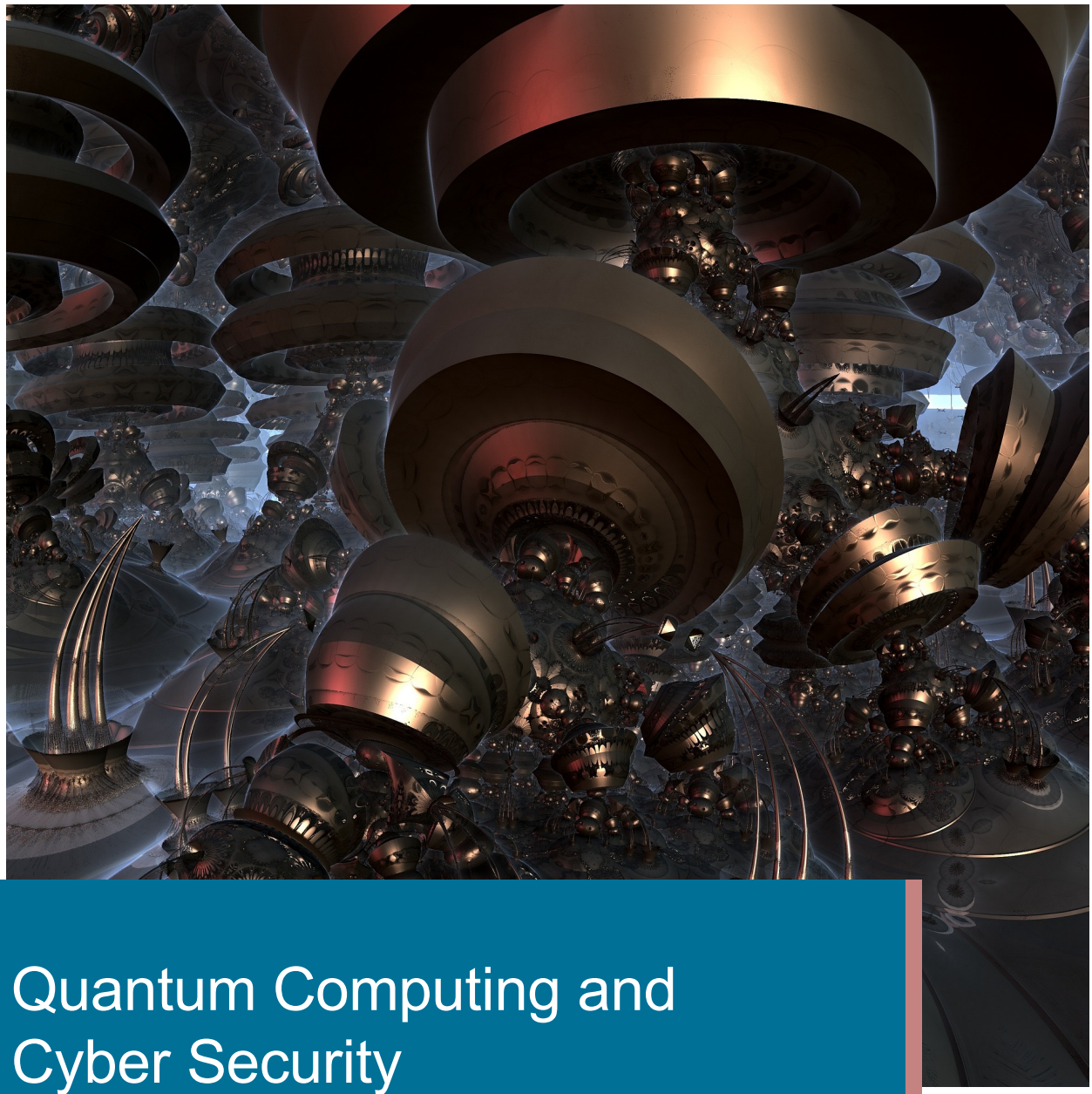
CYSTEL



Quantum Computing and Cyber Security

www.cystel.org

Quantum Computing and Cyber Security: A New Challenge for the Digital World

Quantum computing is a revolutionary technology that promises to solve complex problems faster than classical computers. However, it also poses a serious threat to cyber security, as it could potentially break the encryption schemes that protect our data and communications. In this blog post, we will explore what quantum computing is, how it works, and what impact it could have on cyber security in the near future.

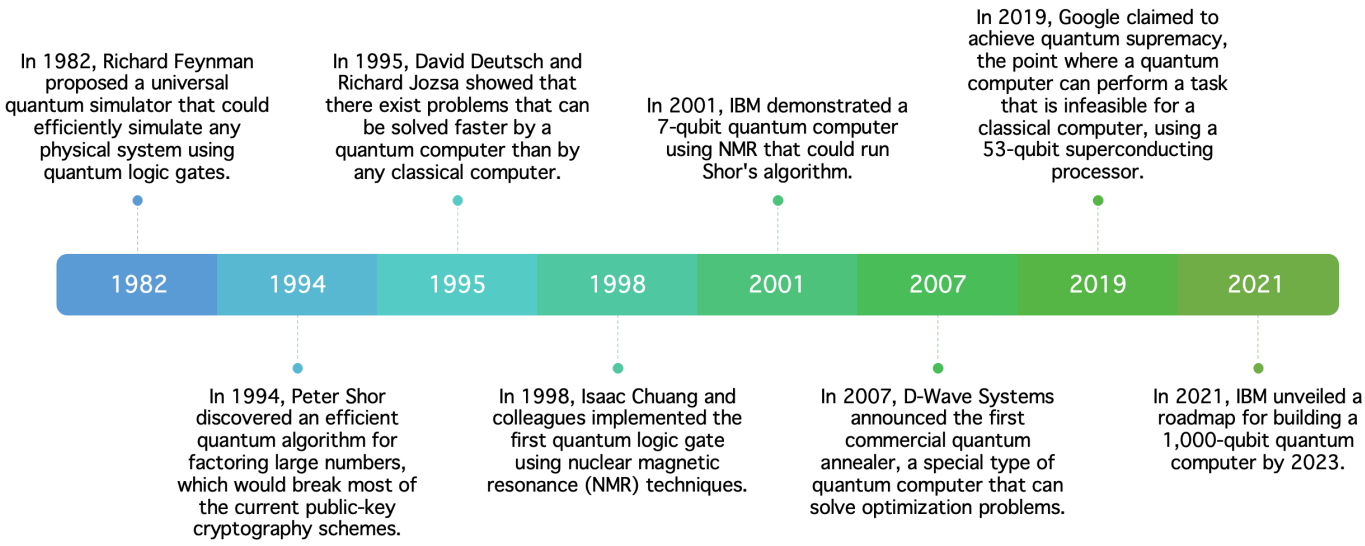
Developments in Quantum Computing

Quantum computing is based on the principles of quantum mechanics, which describe the behavior of subatomic particles such as electrons and photons. Unlike classical bits, which can only store either 0 or 1, quantum bits (qubits) can exist in a superposition of both states at the same time. This means that a qubit can store more information than a bit, and that multiple qubits can be entangled, meaning that their states are correlated even when they are separated by large distances.

By manipulating qubits with quantum gates, quantum computers can perform parallel operations on multiple inputs simultaneously, resulting in an exponential speedup over classical computers.

For example, a quantum computer with 50 qubits could theoretically perform 2^50 operations in one step, while a classical computer would need 2^50 steps to do the same.

To predict the development of quantum computers let's first look at the timeline of its development:



IBM – WORLD LEADER IN QUANTUM

IBM is a world leader in quantum computing research and development. In November 2022, it unveiled its latest QC, Osprey. Boasting 433 qubits, Osprey is currently the highest qubit count QC in the world, more than triple IBM's previous record of the 127-qubit Eagle QC. IBM is on track to develop 4,000-qubit QCs by 2025 with a roadmap of 1,121 qubits in 2023 (Condor QC) and 1,386 qubits in 2024 (Flamingo QC). GlobalData predicts that full-scale commercial quantum computing will likely begin in 2027.

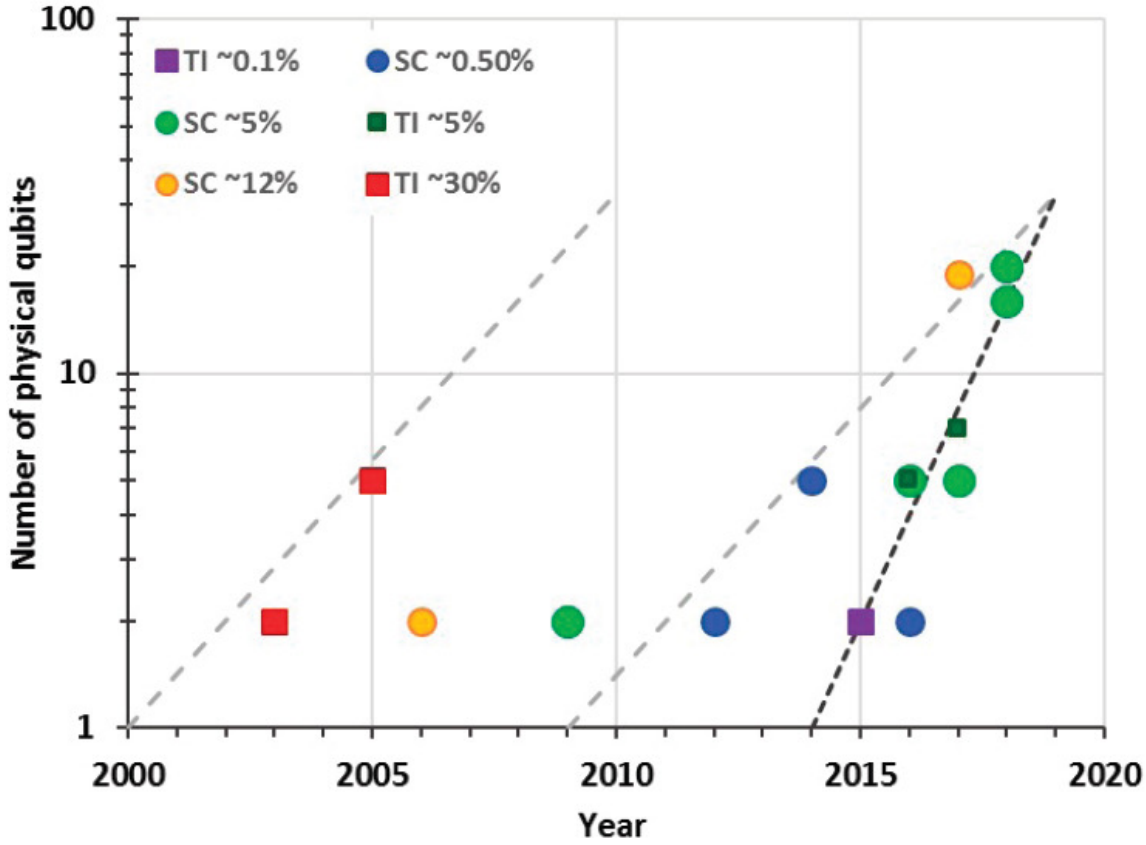


Figure 1: The number of qubits in superconductor (SC) and trapped ion (TI) quantum computers versus year; Data for trapped ions are shown as squares and for superconducting machines are shown as circles. Approximate average reported two-qubit gate error rates are indicated by color; points with the same color have similar error rates. The dashed gray lines show how the number of qubits would grow if they double every two years starting with one qubit in 2000 and 2009, respectively; the dashed black line indicates a doubling every year beginning with one qubit in 2014. Recent superconductor growth has been close to doubling every year. If this rate continued, 50 qubit machines with less than 5 percent error rates would be reported in 2019

National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

How does quantum computing affect cyber security?

One of the main applications of quantum computing is to solve hard mathematical problems that are beyond the reach of classical computers. Some of these problems are the basis of modern cryptography, which is used to encrypt and decrypt data and messages. For instance, the widely used RSA algorithm relies on the fact that it is very hard to factor large numbers into their prime factors. However, a quantum computer could use an algorithm called Shor's algorithm to factor large numbers in polynomial time, rendering RSA useless.

Another example is the elliptic curve cryptography (ECC), which is based on the difficulty of finding the discrete logarithm of a point on an elliptic curve. A quantum computer could use another algorithm called Grover's algorithm to find the discrete logarithm in square root time, making ECC much weaker.

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM[c]	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} years 1.97×10^{22} years 2.29×10^{32} years	
RSA[d]	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,050 4,098 8,194	8.05×10^6 8.56×10^6 1.12×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete-log problem[e-g]	Asymmetric encryption	256 384 521	128 192 256	Shor's algorithm	2,330 3,484 4,719	8.56×10^6 9.05×10^6 1.13×10^6	10.5 hours 37.67 hours 55 hours	Move to NIST-selected PQC algorithm when available
SHA256[h]	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations[i]	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

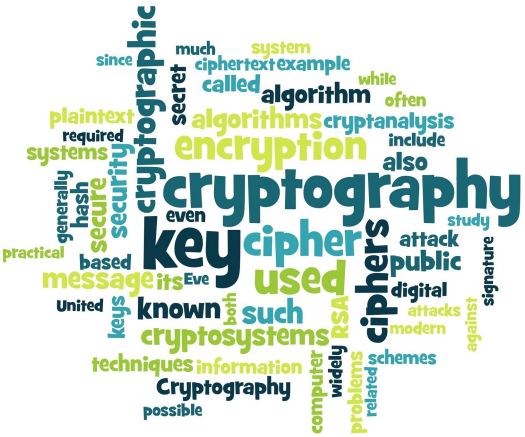
Figure 2: Impact of Quantum algorithms on current cryptographic algorithms; Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

According to a report by the National Academies of Sciences, Engineering, and Medicine (NASEM), a large-scale quantum computer capable of breaking current encryption schemes could be built by 2030. This would have serious implications for cyber security, as it would compromise the confidentiality, integrity, and authenticity of data and communications. For example, a quantum attacker could intercept and decrypt sensitive information such as passwords, credit card numbers, personal data, trade secrets, military secrets, etc. A quantum attacker could also forge digital signatures and certificates, impersonate legitimate users or entities, and tamper with data or messages.

How can we prepare for the quantum threat?

To counter the quantum threat, researchers and practitioners are developing new cryptographic schemes that are resistant to quantum attacks. These schemes are collectively known as post-quantum cryptography (PQC), and they rely on different mathematical problems that are believed to be hard for both classical and quantum computers. Some examples of PQC algorithms are lattice-based cryptography, code-based cryptography, multivariate cryptography, hash-based cryptography, etc.

However, implementing PQC is not a trivial task. It requires careful analysis of the security and performance of the algorithms, as well as standardization and interoperability among different platforms and protocols. Moreover, it requires a timely transition from the current encryption schemes to the new ones, before a quantum computer becomes available. This transition involves updating hardware, software, and infrastructure to support PQC, as well as educating users and stakeholders about the risks and benefits of PQC.



Government Efforts Towards Quantum Computing

Different government organizations have recognized the quantum threat and taken steps to address it.

For example, the National Institute of Standards and Technology (NIST) in the US has launched a competition to develop new standards for post-quantum cryptography, which are encryption methods that can resist quantum attacks. The European Commission has established the Quantum Flagship, a 10-year initiative to support research and innovation in quantum technologies, including quantum communication and cryptography. The UK government has invested in the Quantum Communications Hub, a network of universities and industry partners that aims to develop and deploy quantum-secure communication systems.

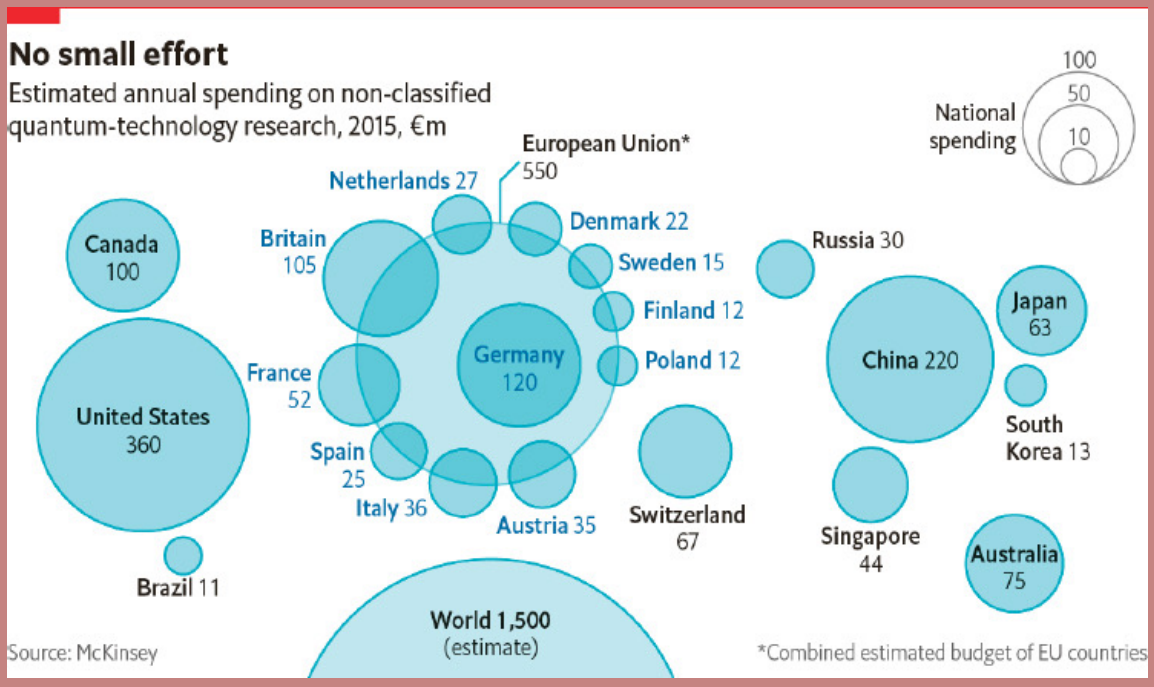


Figure 3: Estimated annual spending as of 2015 on nonclassified quantum technology research by nation, in millions of euros. Estimated investment levels due to more recently announced national R&D initiatives (as of mid-2018) are provided in Table 7.2. SOURCE: Data from McKinsey, as reported by The Economist. Reprinted with permission of The Economist, from "Here, There, and Everywhere: Quantum Computing Is Beginning to Come into Its Own," March 9, 2017; permission conveyed through Copyright Clearance Center, Inc.
National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

Conclusion

Quantum computing is a double-edged sword:

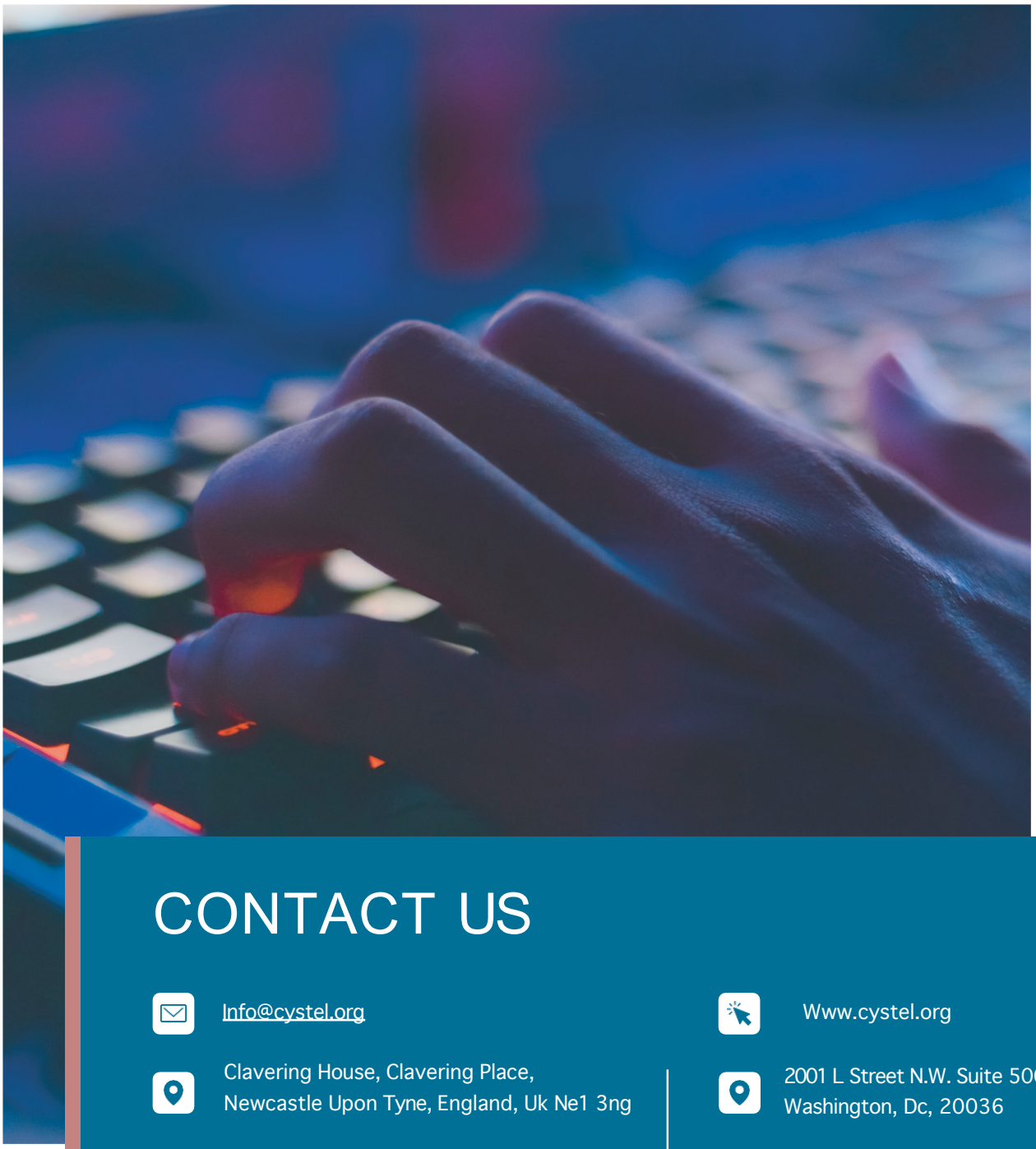
It can offer great benefits for science and technology, but it can also pose great challenges for cyber security. To protect our data and communications from quantum attacks, we need to adopt post-quantum cryptography as soon as possible. However, this requires a coordinated effort from researchers, developers, policymakers, and users to ensure a smooth and secure transition to the post-quantum era.

Author:

Lucy Sharma

Applied Cryptographic Analyst at Cystel

CYSTEL



CONTACT US

Info@cystel.org

Clavering House, Clavering Place,
Newcastle Upon Tyne, England, Uk Ne1 3ng

+44 333 1223 372

Www.cystel.org

2001 L Street N.W. Suite 500
Washington, Dc, 20036

+1 833 838 6754