Bernold Nieuwesteeg

# Should we insure ourselves for the risk of quantum computers breaching our cyber defenses?

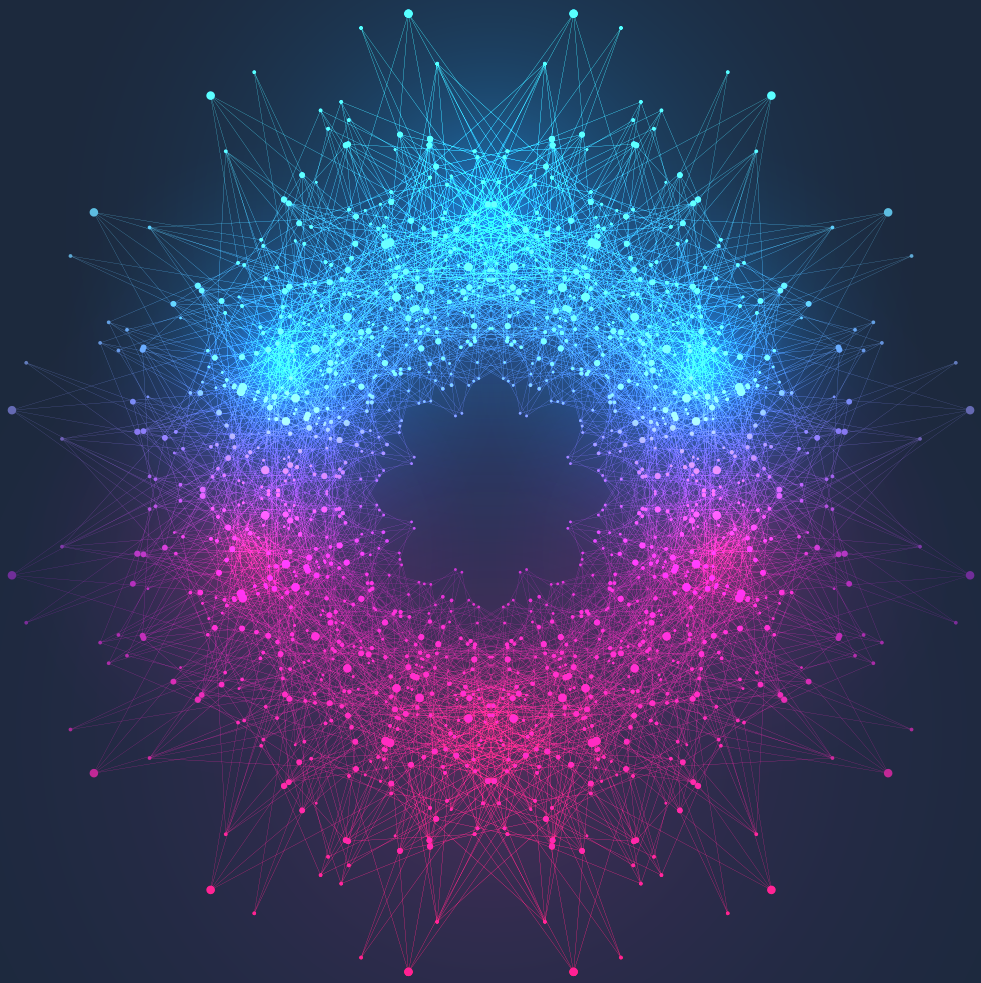
**Imagine it is 2052. The Chinese head of the quantum computer development program connects the first fully operable quantum computer to the internet. His team is under direct supervision of Xi Mingze, the daughter of XI Jinping. She has become the new General Secretary of the Chinese Communist Party. During a smooth transition period, she took over the office from her father in 2035. The Chinese operator waits a second, but then the magic machine switches on and starts to gather data from the world wide web. The first target of the Chinese operator was already determined several months before this moment. The first Chinese quantum computer shall try to access intellectual property of European and US competitors of Chinese firms. The Chinese government wants to look into essential secrets of the western world's most profitable companies. A new era has begun. China has the 'atomic bomb' of the digital age. This quantum computer enables "God Mode" and breaches cyber defenses within seconds. It takes ordinary computers several decades to perform the same operation. And now western secrets are no longer safe.**

Naturally, the above scenario is just a thought experiment of what could happen if the quantum computer is ready for practical use. As you might know, a quantum computer utilizes the phenomena of quantum mechanics, such as superposition, interference, and entanglement. Some mathematical problems, such as attacks on certain cryptographic systems, can be solved much faster with quantum computers. But do not panic: a quantum computer that can breach our cyber defenses is not there yet. However, there is something to worry about: in June last year, a Chinese prototype already succeeded in solving an extremely complicated calculation, which now takes a computer eight years, in one hour.

> "Look at investing in a quantum computer as a form of insurance."

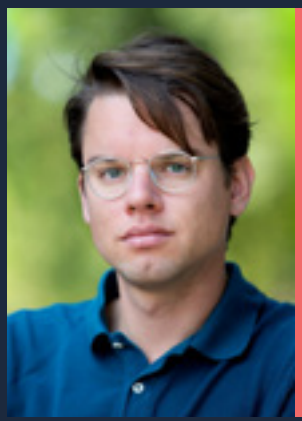
And where does the European Union stand? Europe is lagging behind in the development of quantum computers. The development is scattered over the different countries of the European Union. The scattered budget makes it hard to coordinate and prioritize. The European policy maker does see the potential hazard of quantum computers with regards to cybersecurity. But it currently only scrambles a budget for the development of quantum computers that is only a small percentage of what the Chinese government was capable of putting together. The result is that in thirty years, the likelihood that we Europeans do not have a quantum computer and the Chinese do, is high. This has potential huge ramifications for cybersecurity.

It is not certain whether the quantum computer will ever be developed towards a practical feasible tool or weapon as you like. Some argue that if the quantum computer will be developed into a product with practical application, it will be deployed for specific tasks, such as studying chemical reactions. Some people say it will be at most a minor addition to current 'classical' computers with bits and bites.



So how should we look at the quantum computer in relation to cybersecurity? Well, maybe we should look at investing in a quantum computer as a form of insurance. Maybe the quantum computer will never be fully operational but you rather have an answer to this high impact low likelihood scenario. Compare it with nuclear arsenal: if you as a country are able to press the nuclear button, it has a deterrent effect. Maybe this will be the dynamic that comes into play when quantum computers are developed. Maybe countries with quantum computers can indeed turn on God Mode and spy on everybody, but benefit more from an equilibrium where there is still some secrecy. Another development possibly even makes an insurance package obsolete: currently, scientists are working hard to develop cryptographic algorithms that are 'quantum proof'. They already developed algorithms that are considered to be relatively secure against attacks by quantum computers.

Imagine that quantum proof algorithms prove to be successful and widely applicable. Will it be necessary, from a cybersecurity perspective, to put hundreds of billions of dollars in the development of a product that maybe never sees the light of day? We also have other societal problems that require huge investments and knowledge such as the energy transition. Hence, the question we need the answer is whether we need insurance for quantum computers and which trade-offs we like to make as a society.



**About the author**
Bernold Nieuwesteeg is director of the Centre for the Law and Economics of Cyber Security at Erasmus University and entrepreneur. He recently founded www.cybersecuritybooster.nl, a webinar series that boosts cybersecurity knowledge.