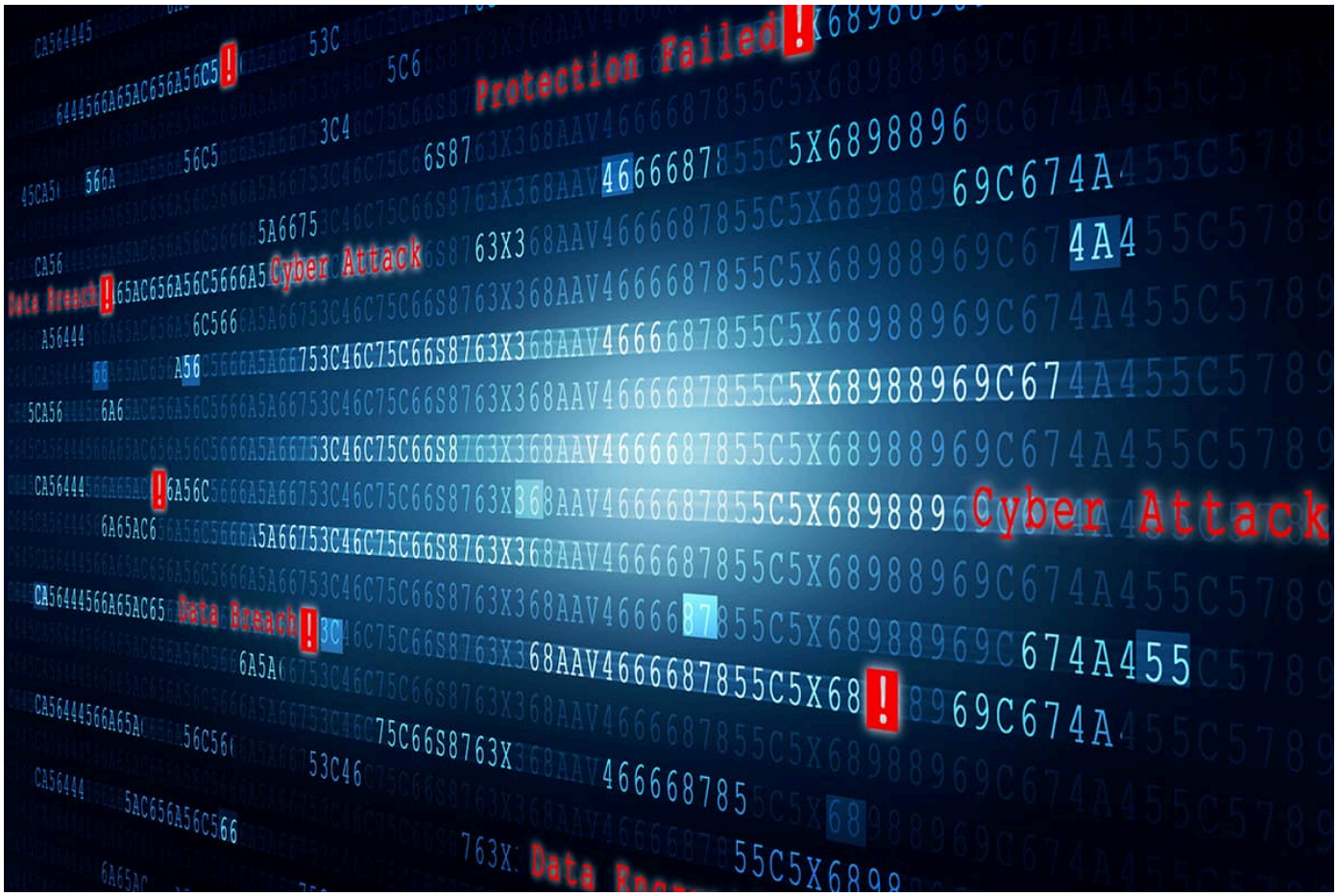
physicsworld

QUANTUM NEWS

MEPs call for 'urgent action' to implement post-quantum encryption standards

12 Apr 2024



Code breakers: Experts estimate that the commonly used RSA-2048 encryption keys could be cracked by a quantum computer within 24 hours (courtesy: shutterstock/jijomathaidesigners)

Twenty members of the European Parliament have called for urgent action to develop a new standard for data encryption that would protect against quantum computers being used for malicious purposes. In their letter, the members urge the European Commission to develop security measures and regulations to ward off the threat of quantum computers for cybercrime and data breaches.

Quantum computers, once fully developed, have the potential to calculate complex processes that cannot be easily carried out by classical devices. There is, however, a real threat that they may also be used to hack encrypted information, even present-day information that is currently considered unhackable.

Experts estimate that the commonly used RSA-2048 keys can be cracked by a quantum computer within 24 hours. This puts secret information, for example held by governments or companies, at risk of being stolen.

Even though practical quantum computers still need years, if not decades, to become practical, the complexity of any new encryption standard could take a similar amount of time to implement. Transitioning to a new cryptographic standard to incorporate a wide range of technological domains, such as internet servers, banking and internet-of-things devices, has already started.

The National Institute of Standards and Technology (NIST) in the US has determined the algorithms that will be included as post-quantum encryption standards and these are currently being developed by collaborations around the world. The new standards will be applied to public-key encryption and for digital signatures.

In their letter, the MEPs urge the European Commission to create an inventory of current encryption algorithms that are used by organisations. They want a review of which new (classical) cryptographic libraries can be easily included in current infrastructure and are keen to ensure that hybrid – classical as well as post-quantum cryptographic – encryption is deployed where possible. The MEPs also want a phased implementation to begin as soon as NIST has adopted relevant standards.

"The [relevant] commissions should play an important role in spurring this transition now, by explaining in joint guidance what taking 'appropriate' security measures under the different regulatory regimes means, in the view of the development of quantum computers," the letter states.

Martijn Boerkamp is a science writer based in the Netherlands