In light of this menace, security experts are furiously casting a renaissance for RSA encryption (Rivest, Shamir, Adleman) needed to crack it, for example. A wait-and-see approach could prove itself costly for manufacturers who ignore this risk could end up performing costly recalls or retrofits of long-lived products such as automobiles or refrigerators.

This scenario wasn't plucked out of thin air, either. The NSA revealed that the National Security Agency (NSA) was crafting a quantum supercomputer – one powerful enough to store them until the advent of a quantum computer strong enough to decrypt them – in potentially ten years or less. This option is allowed to stockpile encrypted data for as long as is needed to crack it, for example.

This doesn't mean that the matter is a sideshow – but one with a considerable threat potential. A quantum computer can crack many an established encryption method in seconds – a feat that would take billions of years with a conventional computer. At that point, the "s" in "https" will stand for "so long, privacy!"

In a heartbeat. Companies are at risk in a heartbeat. In a heartbeat.

They have been in many cutting-edge fields of technology: horror stories of evil-minded hackers would revert to what are known as "quanta" problems.