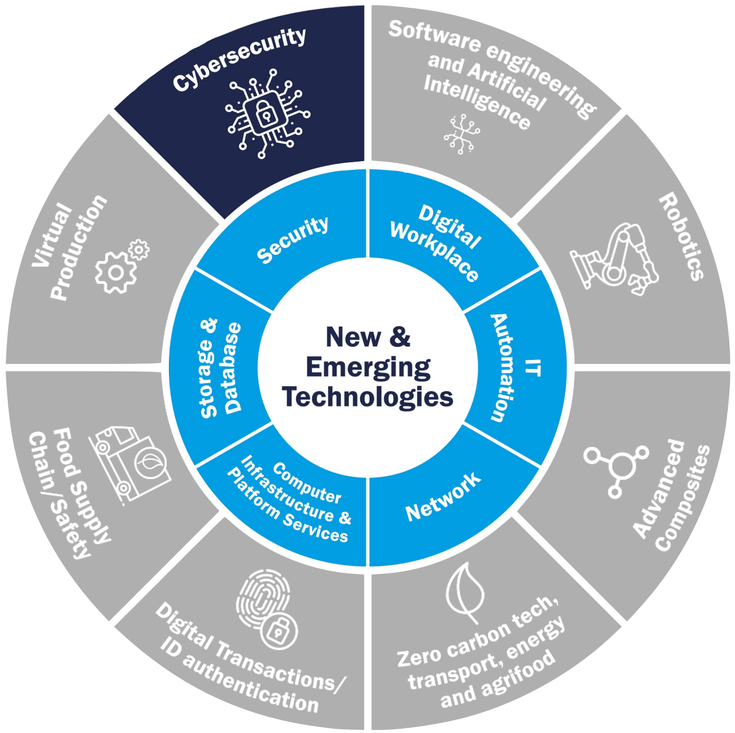


Sources	Wired	Date	January 2021

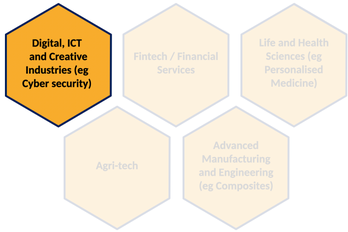
Potential scale of impact	Certainty of outcome	Impact horizon
★★★★	★★★★	H1 H2 H3

[The technologies and standards](#) that underpin communication around the world are, for the most part, global and interoperable. Common standards mean that designs can be checked once by all interested parties; interoperability means that errors and vulnerabilities are likely to be caught early. From a cybersecurity perspective, this is positive, enabling nations to secure systems at a scale that was previously impossible. This stability and interoperability is, however, under threat as nations states edge closer to balkanisation of technology and standards.

States have been weaponising information for some time now, breaking into other countries' networks to steal data, seed misinformation or disrupt infrastructure. And now - because they don't like the increase in strategic dependence on other states - they are developing their own standards and technologies that diverge from global commons and which embody their values. This signals a fundamental shift in how technology is developed, owned, accessed and leveraged by nation states and companies. New alliances will form around the creation of indigenous and sovereign versions of the technology we use to communicate and manage modern life. We will see standards bodies fragment and supply chains and infrastructure redesigned to align with these new realities. States will start to take more drastic action to ensure that their supply chains are protected, and that their sovereign "silicon-to-service" technology stacks are insulated from the actions of others and enforce their national values.

The global debate around 5G security has led to a position where we will likely see two independent camps moving forward, ostensibly led by the US and China. Other nations will have to decide which camp better serves their national interest, since the companies that produce this technology are bound to those countries. This will establish a pattern which will be repeated across other critical technologies. In this world, the multi-stakeholder approach to standards that ensures no one party has too much power will be critical to ensure we can continue to do cybersecurity at scale.

If we fail, the world will become less connected, less resilient and less secure.



UNCOMMON STANDARDS

Competing approaches to cybersecurity threaten global stability

Home Page
www.10xhorizonscan.online