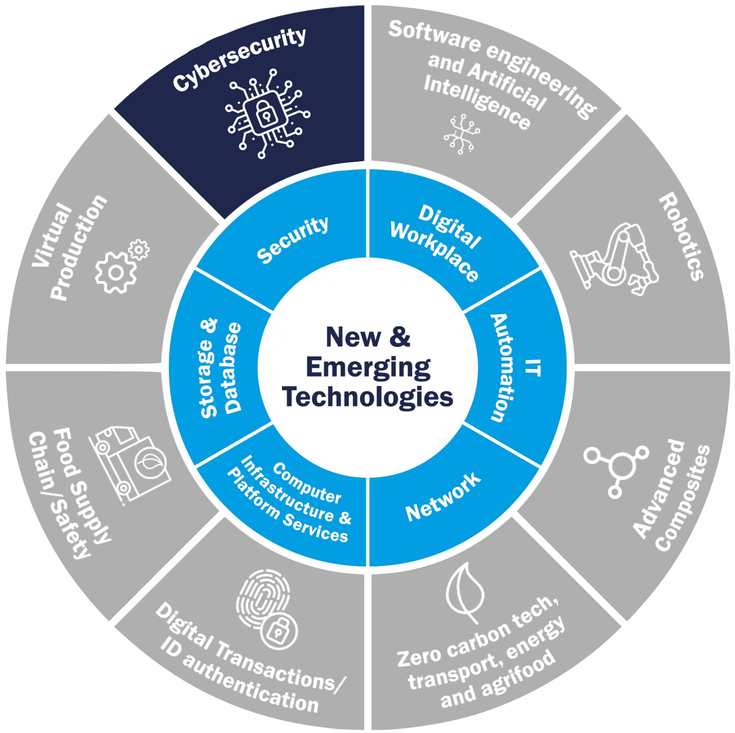


Sources	New Electronics	Date	May 2021

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

Around the world the critical infrastructure that supports and sustains modern societies is coming under attack, whether from nation-states or non-state-affiliated actors such as criminals or terrorists. These attacks are able to undermine critical infrastructure - the power grid, the transport network and information and communication systems, for example - by not only damaging equipment but by interrupting operations which, in turn, can cost organisations millions of pounds to resolve.

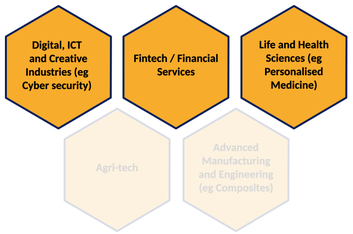
The scale of attacks is astonishing. According to recent reports from Carbon Black, 88% of UK companies have suffered breaches in security in the past twelve months; one small business in the UK is hacked every 19 seconds.

The threat to state actors is equally challenging and certainly growing. Earlier this year a computer hacker gained access to the water system of a city in Florida, looking to pump in a 'dangerous' amount of a chemical into the city's water treatment system. This wasn't an isolated case. It's happened in the US before and in 2020 there were multiple, if unsuccessful, attacks on the Israeli water supply.

Around the world water, electricity, nuclear plants and transport are being probed for any sign of weakness with hackers looking to exploit out-of-date and vulnerable IT systems. The pace of digitalisation is also causing problems and organisations need to be aware that cyber-attacks are not only growing but constantly evolving and changing; the activities of hackers are now being automated as they target critical infrastructure.

In the UK the new chief executive of the NCSC, Lindy Cameron recently suggested that basic cyber hygiene is as important a life skill as knowing how to wire a plug - and that digital literacy is as non-negotiable in boardrooms as financial literacy. Cameron said, "Cyber security is still not taken as seriously as it should be, and simply is not embedded in UK boardrooms."

At the end of the day critical infrastructure needs to be made as hard a target as possible for those that might seek to disrupt it and the data generated and processed needs to be properly protected, she warned.



SECURING INFRASTRUCTURE

Hackers are turning their attention to targeting national infrastructure directly

Home Page
www.10xhorizonscan.online