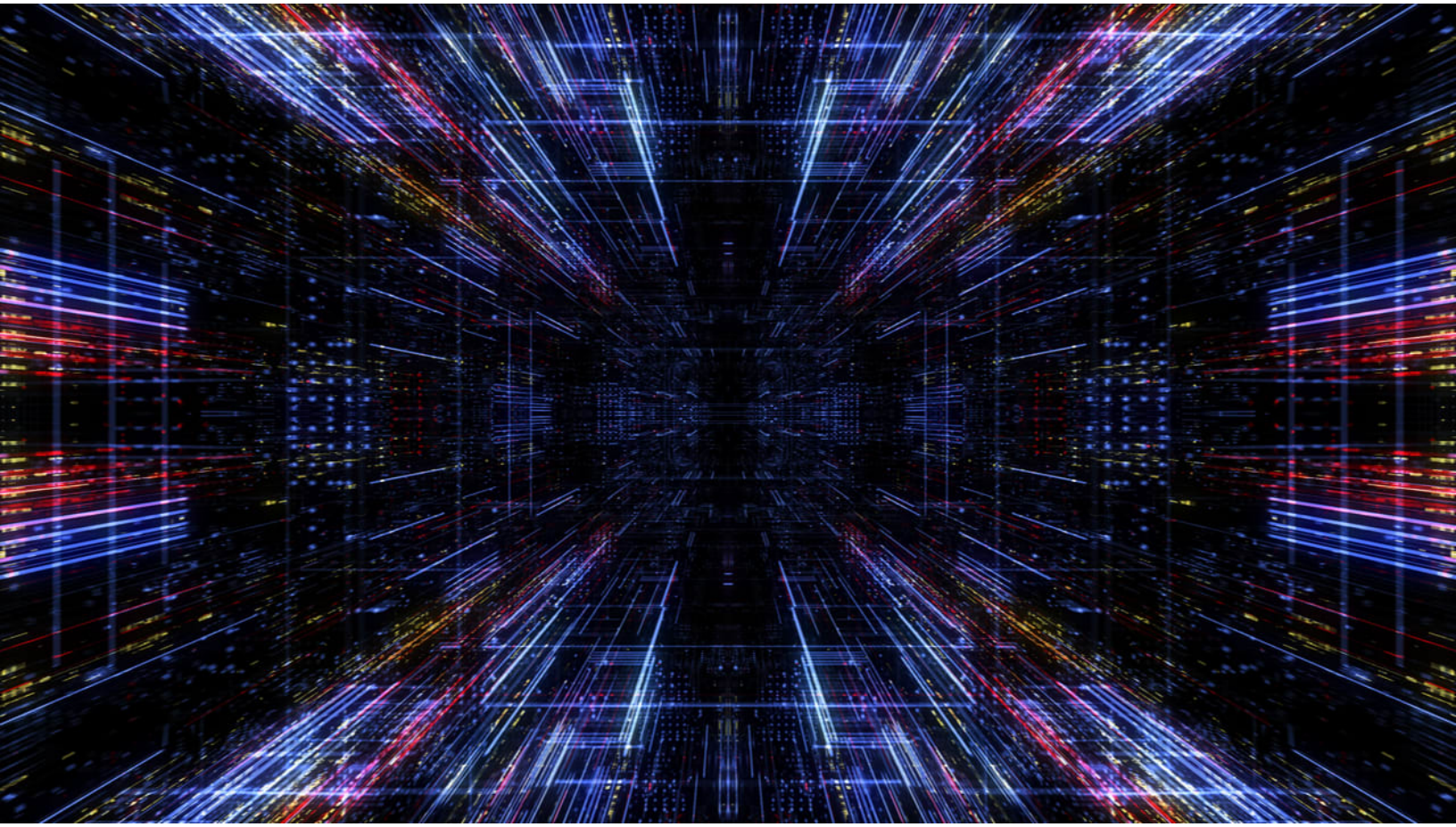

Royalty-free stock illustration ID: 1065741941

Jan 26, 2021 17:38 GMT

The cyber landscape in 2021 and beyond: an opportunity to learn from the present

2020 was one of the most turbulent but transformational years that we, as a society, have experienced for many decades. Despite its challenges, it saw us take advantage of more technologies and digital ways of working than ever. Many of these changes have accelerated digital transformation by several years and will last well into the future.

Now that we have entered 2021, it is important for us to take a step back to assess evolving threats, dissect current and future opportunities and ask

ourselves if the mitigations, regulations and legislation that we currently have in place are fit for this accelerated digital age.

Below, our global CTO, Ollie Whitehouse, shares his thoughts on the tools and mechanisms that will be crucial to strengthening society's resilience against cyber threats, and what is needed to create regulatory and legislative regimes fit for 2021 and beyond**.** All of which have been recently explored in conversations with lawmakers and parliamentarians across the UK and other territories, offering further indication as to where their thinking is on the challenge of finding the political, policy and regulatory answers to some of the most challenging and complex questions facing us in terms of governing cyberspace.

Cyber as a science and quantifying cyber resilience

There is a growing appreciation of the value of data-driven decisions and science more generally in society, which has been largely driven by the pandemic. This is also true for cyber security, particularly to determine priorities for investment, understand what works and what does not and enabling comparison.

More and more, we're seeing that governments, regulators and end organisations value the ability to benchmark resilience using various data points. For governments and regulators, this benchmarking provides thematic insights to allow them to not only understand where systemic risks sit, but also where investment or regulation is or is not working.

Vendors are also increasingly seeing the value in quantifying the efficacy of their cyber security solutions, and investors are undertaking technical due diligence to assure themselves that their investments have the greatest chance of returns.

NCC Group has been working across all of these areas for a number of years

now to drive cyber as a science forward.

Ruthless adversaries will continue unabated

Despite our societal adversaries' increasing technological sophistication, their unique selling point is the brazenness with which they pursue their objectives. In a lot of cases, they don't care if their cyber operations get detected for the most part. From organised cybercrime through to nation states, we expect continued ruthless escapades in pursuit of tactical and strategic goals.

And the truth of the matter is that every organisation is potentially a target. Attacks against assumed organisations of all types occur each day, so the concept of cyber defence and resilience becomes even more crucial. The sooner we can put to bed the outdated dichotomy of an organisation is secure or not secure, the better.

Therefore, it is crucial that government, industry and academia continue to educate individuals and businesses alike on the cyber threats facing them, while also developing the solutions that can reduce the impact and harm from adversaries.

Unlocking new models of service delivery through cyber security infrastructure

We should fix digital identity as an underlying fundamental of the future, based on cryptographic primitives and other means of authentication beyond the password.

In doing so, this allows us to unlock new models of service delivery. Simply, this means creating a strong root of trust, but one that is replaceable if compromised, unlike biometrics today.

We need to be able to do this without falling into the trap of doing innovation in the way things have always been done. While most countries have a spark of ingenuity, we often fall down when it comes to speculatively investing in something that could be risky.

Future data markets and the democratisation of data

We need to unlock opportunity by turning global financial hubs into trusted and well-regulated centres for global data trading, and drive forward the democratisation of data. This would involve finding ways to ensure that as much data is available to as many people to derive value, whilst allowing the individual citizen to monetise their personal information.

Third-party data brokers and markets for data already exist, but it's clear that they are fragmented, and nobody has yet grasped the opportunity at scale.

Several countries have a distinct advantage here. For example, the UK's financial centres and widespread prevalence of common law presents an opportunity and fundamental basis to build a future data market. The UK also has the credibility to establish international data norms and set out what global data trading would look like and then build the legislative and regulatory regime(s) to turn that into reality.

Ultimately, a number of the financial hubs across the globe should set out the workable answer to the question of how a private citizen can make the most of their data, if they so wish, by providing a framework for data commerce. If organisations would like to buy a dataset to train their machine learning models, these future data trading markets will facilitate this in an ethical, fair, secure and transparent way.

Future-proofing legislation and regulationby being adaptable to future needs

A regulatory and legislative system that is able to adapt to the unforeseeable in the future of rapid technological innovation is crucial at sectoral, national

and international levels.

This includes finding a solution which ensures that ransomware does not pay for criminals, reforming ageing legislation which hinders cyber security such as the Computer Fraud and Abuse Act (USA) and the Computer Misuse Act (UK), and defining what good corporate citizenship and governance looks like in a technology-first world.

The risks of hyper connected environments and complex interconnected supply chains

Red and purple team assessments – evidence-based real-world validation of organisations' cyber resilience – have moved the compliance game on immeasurably in the last five years.

However, the next big challenge to tackle will be technology themes, such as risk assessing and assuring connected places and environments (smart cities, transport, health), along with securing connected agriculture and distribution where there is no single point of accountability.

Supply chains of all types will increasingly need assured resilience and thus will also come under further scrutiny in the years to come, as more organisations recognise the threats that working with and across multiple businesses in multiple countries pose, and the highly disruptive and costly impact an attack or breach could have. Insurers will be a forcing function here as they are the ones who will be exposed by their underwritten policies and thus it will be in their interests to address.

The 2021 landscape

The last twelve months have been a challenge, but have also shown the resilience and tenacity of the human race.

It is clear however that cyber resilience is a multi-dimensional challenge for a rapidly evolving situation for which there is little or no precedent.

We have ever aggressive set of threat actors looking to leverage cyber for tactical and strategic aims.

We have a large and at times not insignificant legacy technology base built on free-market and capitalist models which favour short-term behaviours.

We have increasingly complex, hyper connected and interdependent technology and service supply chains.

We have an evolving regulatory, legislative and international norms environment across the spectrum of cyber.

We have cyber security, as a discipline, maturing slowly from dark art to an emerging science.

All of which draws us to the conclusion that 2021 will be a small step on our evolutionary path. It won't provide all the answers – the environment in which we operate will continue to change, but we will know more and have better insights at the end of it.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970