WHAT DOES THE REST OF 2023 HAVE IN STORE FOR EUROPE'S TECH SECTOR?

Strengthening the competitiveness of the European economy through the green and digital transformations has been the EU's strategic goal over the last years. Despite its inbuilt resilience, EU industry is being challenged by high inflation, labour shortages, supply chain disruptions, rising interest rates and spikes in energy costs and input prices. This is paired with strong, and not always fair competition on the fragmented global market. The EU has already put forward several initiatives to support its industry. The EU now needs a more structural answer to the investment needs of its industries. This will support the uptake and scaling up of development and manufacturing of strategic technologies in the EU, in the fields of digital and deep tech, clean tech and biotech. It will help companies seize the opportunities, build resilience and meet the objectives of the green and digital transitions, thereby strengthening European sovereignty.

In recent months, the Commission proposed the Strategic Technologies for Europe Platform ('STEP'). The STEP will reinforce and leverage existing EU instruments to quickly deploy financial support to the benefit of business investments. The STEP will also allow directing existing funding towards technology fields that are crucial for Europe's leadership, thus contributing to a level playing field for investments throughout the Single Market.

Commission President, Ursula von der Leyen, said: "The future of the strategic industries should be made in Europe. With STEP, we set the stage to mobilise the necessary funding available across various EU programmes to stimulate investments in critical technologies and make sure companies grow and flourish in the EU. With the existing funding and an extra €10 billion that we intend to inject, we aim to reach up to €160 billion in investments in the coming years. This will be the precursor to a fully-fledged Sovereignty Fund that would be created in the future."

The STEP will build on existing programmes such as InvestEU, Innovation Fund, Horizon Europe, EU4Health, Digital Europe Programme, European Defence Fund, Recovery and Resilience Facility and cohesion policy funds.

To boost the investment capacity dedicated specifically to promoting STEP objectives, the Commission further proposes to allocate an additional €10 billion to targeted programmes:

- €3 billion for InvestEU, resulting in €75 billion of investments given the 40% provisioning rate and an average multiplier of 10.
- €0.5 billion to Horizon Europe, complemented with €2.13 billion of redeployment and use of decommitted amounts, resulting in €13 billion of investments with an average multiplier of 5.
- €5 billion to the Innovation Fund, resulting in €20 billion of investments given the experience to date under the Innovation Fund.
- €1.5 billion to the European Defence Fund, which could result in up to €2 billion of investments.

We spoke to industry leaders who offer their thoughts on how Europe's digital economy will take shape. . . .

RICHARD CONNOLLY, REGIONAL DIRECTOR FOR THE UKI AND THE DACH REGIONS AT INFINIDAT

Cybersecurity and cyber storage resilience have traditionally been treated separately in the enterprise but this makes it difficult to create a comprehensive enterprise cybersecurity strategy. It also leaves gaps for cyberattackers to exploit. Due to the exponential growth and intensity of cyberthreats – expected to cost over US$8 trillion in 2023 – cyber storage resilience needs to be part of every enterprise's cybersecurity strategy and we will see this become commonplace.

> Another trend to expect for the rest of 2023 is the use of Machine Learning-based automation to hone enterprise security infrastructures.

It will be especially important for datastores that are moving between on-premises enterprise data centres and the public cloud. In hybrid environments, security experts agree that it's vital for enterprises to be investing in creating secure datastores for both primary datasets and for backup datasets that use immutable snapshots and air-gapping. This is leading to enterprises and service providers more proactively deploying enterprise storage products that have baked-in cyber storage resilience capabilities, such as rapid cyber recovery, immutable snaps, air-gapping and fenced forensic environments. To facilitate rapid cyber recovery, copies of data – especially critical data – must be unalterable. Data integrity cannot be compromised while combatting a cyberattack.

> Cyber storage resilience needs to be part of every enterprise's cybersecurity strategy and we will see this become commonplace.

Another trend to expect for the rest of 2023 is the use of Machine Learning-based automation to hone enterprise security infrastructures. CIOs and CISOs will increasingly be looking to enterprise storage solutions that are not only AI/ML-friendly, but also have autonomous automation that makes the infrastructure smarter to nullify and/or recover from cyberattacks.

Autonomous automation allows an enterprise to deal with its massive amounts of data that are simply too much for storage and IT administrators to handle alone. This has ramifications for security. The adoption of these more sophisticated tools will only increase over time. While ML-based automation is definitely an area that enterprises need to fully utilise, cybercriminals are simultaneously also using AI/ML to automate their cyberattacks. They are using various model stealing and data-poisoning techniques. Metaphorically and literally, there is a battle underway of corporate automation vs. criminal automation on the security front.

Organisations that are not properly cyber secure will see more cyberattacks in the months and years ahead, not fewer attacks. And companies won't just get hit once and then have years to recover. Hackers have become highly skilful at hiding malicious code. The attacks have become an onslaught that requires a different way of thinking about how both cybersecurity and enterprise storage are better aligned. ◻