Crowell

DSIT's latest findings on AI, other emerging technologies and cyber security

What You Need to Know

Key takeaway #1

AI is likely to have an outsized impact on technology convergence in emerging technologies, and this AI impact is widely seen as “paradigm shifting”.

Key takeaway #2

Emerging technology pairings provide innovative tools for enhancing cyber security but simultaneously introduces new risks to security. The cyber risk landscape is becoming increasingly complex due to the dynamic interactions.

Key takeaway #3

Security needs to be flexible and adaptable to respond to the constantly evolving threats. Zero trust is the preferred model.

Key takeaway #4

Cross sector collaboration is essential, given how different sectors may end up interacting and the vast use cases. We anticipate this may also justify the anticipated mandatory reporting requirements for ransomware attacks (see our previous article on the recent ransomware consultation **here**).

Key takeaway #5

Much like existing data protection principles with a requirement for ‘privacy by design’, security must be built into design and integrated from earliest stages of innovation and development.

Key takeaway #6

Organisations should build resilience and preparedness to emerging threats and be proactive in risk assessment threat modelling.

Key takeaway #7

A lot of emerging technology is under-researched, so there are still impacts on unknown security risks. Being an early adopter may bring more risks, as there are potential unknowns with a lack of research in certain areas.

Key takeaway #8

Data manipulation (also known as data poisoning), where data is polluted by cyber attackers to produce unreliable outputs or outcomes, is becoming an area of increasing concern.

Client Alert | 14 min read | 08.14.25

On 8 August, the UK Department for Science, Innovation & Technology ("**DSIT**") published a **report** titled "Emerging technologies and their effect on cyber security" (the "**Report**"). It examines how the convergence of AI, IoT, Quantum, Edge Computing, Blockchain and other emerging technologies is transforming the cyber threat landscape. We've summarised below some of their key findings and takeaways. In the pursuit of growth and efficiencies many companies are considering how to adopt emerging technology into their operational processes, and the Report provides a useful guide as to emerging cyber risks and where the UK Government's attention is focused as it launches the Cyber Resilience Bill later this year.

The key concepts and methodology

DSIT defines a number of terms in the Report including the following:

- Technology Convergence—The tendency for technologies that were originally unrelated to become more closely integrated and even unified as they develop and advance.
- Emerging Technology—a technology whose development, practical applications, or both are largely unrealised. These technologies are generally new, but also may include old technologies finding new applications.
- Converged Technology Pairing—Two technologies that are likely to converge as they develop, as each technology supports and augments the capability of the other.
- Converged Technology Grouping—A group of more than two technologies that are likely to converge as they develop, as each technology augments the capability of the group.

The overall questions DSIT looked at are:

1. Which groups or pairings of emerging technologies are likely to create novel/compounding cyber security risks?
2. Which industries will be affected by such novel/compounding cyber security risks?
3. Which applications of emerging technologies are most likely to be affected by technology convergence?

Technology pairings and new security risks

The Report provides an analysis of specific use cases and examples of Converged Technology Pairings, whilst presenting the cyber concerns that arise due to such convergence. Some examples from the Report are set out below.

Converged Technology Pairing	Key novel/emerging security risks	Industries affected by cyber security risks from convergence	Applications of emerging technologies likely to be affected by convergence
AI and Digital Twins: AI enhances digital twins (being a virtual representation of a real-world system) by improving situational awareness and risk assessments as AI-powered digital twins can analyse historical and real-time data to predict cyber threats.	• **Increased exposure of sensitive data and attack surface**: Amplified complexity of securing systems due to the reliance of data collection from extensive networks of Internet of Things ("**IoT**") devices which expand the attack surface. • **Integrity/model poisoning**: Attacks can include unauthorised modification or injection of misleading data that can corrupt virtual models and impact decision-making or lead to operational failures.	• Industries: • Manufacturing • Transport • Energy and Utilities • Aerospace and Space Exploration • Construction and Infrastructure • Healthcare • Defence and Military • Telecommunications	• Cyber-Twins: Virtual environments mirroring real-world cyber systems can provide safe simulation of diverse attack scenarios without impacting live operations. • Digital Twin Metaverse Network: A metaverse-like digital twin environment integrates AI, IoT, and simulation in a shared virtual space.
AI and IoT: AI adds an intelligence layer onto IoT networks by analysing and acting on the generated data.	• **Attacks on AI models:** AI models integrated into IoT devices may be attacked, leading to misclassification of data, bypassing detection systems or triggering false positives – leading to incorrect decisions. This may be critical in healthcare/smart cities (e.g. incorrect dosages of medications from smart infusion pumps). • **Interception**: IoT devices transmit vast amounts of data, combined with AI algorithms risking interception and further risks around a lack of standardised security protocols in IoT devices.	• Healthcare & Medical IoT • Smart Cities & Infrastructure • Manufacturing & Industrial IoT (IoT) • Autonomous Vehicles & Transportation Systems • Energy & Smart Grids • Retail & Smart Supply Chains	• Smart healthcare and wearable devices: AI powered IoT devices have many use cases in health care. Whilst AI may enhance threat detection, it simultaneously amplifies other risks. • Autonomous vehicles and traffic management: AI processes real-time IoT sensor data to optimise traffic flow. • Smart Manufacturing: AI IoT manufacturing improves efficiency and monitoring of machinery.
Low Earth Orbit ("LEO") Satellites and Quantum Communications: Quantum communications theoretically provide security immune to tampering or interception, and when combined with satellite could enable secure global networks for data transmission.	• **Communication resilience**: Whilst quantum communications may provide security, the use of LEO satellites lead to some potential interception when information is transmitted across free space, leading to potential denial-of-service. • **Physical security**: Quantum communication relies on security of trusted nodes, in this case being LEO satellites. • **Side channels**: These attacks are unintended information leaks from a system, which can be found by analysing hardware imperfections, optical signals or measure fluctuations to infer secret quantum key exchanges.	• Defence • Telecommunications	• SAGIN Networks: The Report provides a detailed use case study, where Space-Air-Ground Integrated Networks are likely to use quantum communications to provide secure global connectivity. • Large scale IoT: As IoT deployments increase in coverage, such communications could provide global secure networks.

The above is a brief selection of what DSIT examined for the purposes of this article. The Report also details other pairings.

Commentary

Organisations across all industries are now expected to keep up with technological advancements to maintain a competitive edge, and this will likely lead to adoption of more emerging technologies that converge. Of course there are benefits to being an early adopter, but there are several risks associated including the cyber ones shown above. To facilitate growth, efficient innovation and information governance can be both a competitive differentiator and an essential to mitigating compliance risks. Businesses should have in place governance that allows you to make the right competitive decisions, whilst having full knowledge to mitigate against cyber risks and adopt the right security protocols.

Organisations should be aware that emerging technology convergence could attract future regulatory scrutiny. DSIT's findings show an overlap with existing frameworks, and sector specific rules (such as security by design). Considerations should be made in multi-vendor ecosystems and contracts should address and reflect the risks that come from combined technologies and be forward looking on advancements. Vetting of vendors should consider looking at interdependencies, especially as technology converges it may be difficult to differentiate between which party is at fault particularly in relation to cybersecurity incidents.

Businesses should also review incident response processes to ensure there are mechanisms to adapt processes to innovation – especially as additional emerging technologies are adopted. It will be important to ensure collaboration between suppliers. Regulatory reporting triggers may also overlap across regimes as these convergences become more complex – mapping out such requirements may reduce delays when you come across an incident.

As organisations navigate the complexities of emerging technologies, a proactive approach to governance, regulatory compliance, and collaborative incident response will be essential in safeguarding against cyber risks.

Contacts

Emma Wright
Partner
London D | +44.20.7413.1315
ewright@crowell.com

Rafi Azim-Khan
Partner
London D | +44.20.7413.1307
San Francisco D | +1.415.365.7282
rafi@crowell.com

Clare Sellars
Counsel
London D | +44.20.7413.1309
csellars@crowell.com

Grace Tang
Associate
London D | +44.20.7413.1353
gtang@crowell.com

