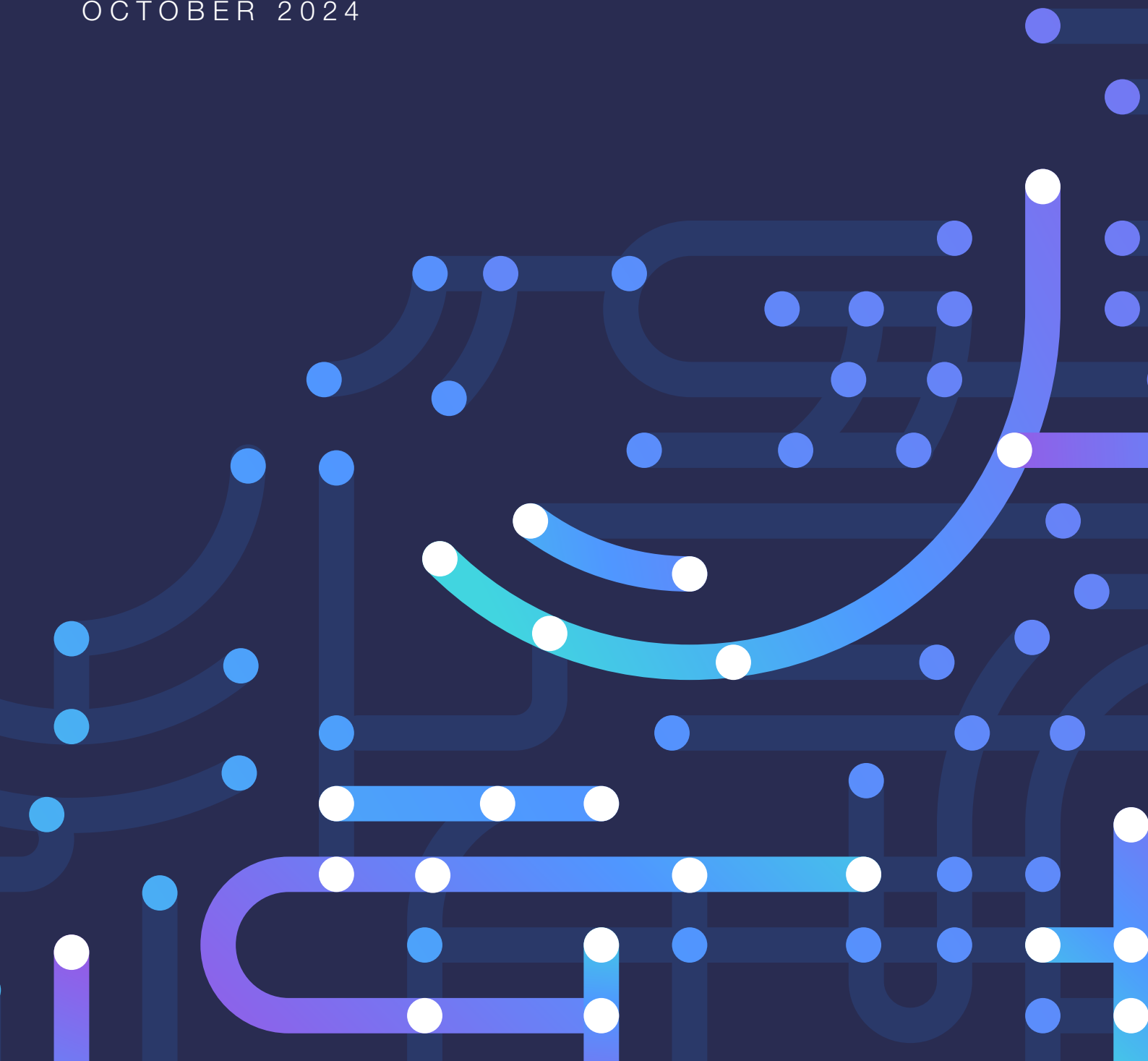
WORLD ECONOMIC FORUM

Navigating Cyber Resilience in the Age of Emerging Technologies: Collaborative Solutions for Complex Challenges

WHITE PAPER

OCTOBER 2024



Images: Getty Images

Contents

Executive summary

As society moves further into the digital age, emerging technologies bring unprecedented opportunities for economic growth, operational efficiency and societal advances.

Emerging technologies such as artificial intelligence (AI), quantum computing, the internet of things (IoT), blockchain and biotechnology are rapidly transforming industries and redefining societal norms. AI, for example, is revolutionizing industries by enhancing decision-making and automating complex processes, while IoT is reshaping supply-chain management with real-time data analytics.[1] Meanwhile, quantum computing, on the brink of significant breakthroughs, has the potential to solve problems previously considered unsolvable, opening new avenues in cryptography, drug discovery and materials science.[2]

However, these advances are accompanied by a significant increase in cybersecurity risks, necessitating a fundamental shift in approach to technology development and deployment. The traditional mindset of "security by design", which focuses on embedding security features into new technologies from the outset, is no longer sufficient in the face of the complex and evolving threat landscape. Instead, there is a pressing need to adopt a "resilience by design" approach, which goes beyond mere protection to ensure that systems can withstand and recover from the inevitable attacks that will occur as these technologies continue to evolve and proliferate.

Key findings

1. **Expanding technological landscape:** More than 200 critical and emerging technologies are shaping today's digital ecosystem, far beyond the commonly discussed AI and IoT. This diversity requires a broad, inclusive approach to technology assessment and security strategy development.

2. **Increased attack surface:** The proliferation of connected devices, expected to reach more than 32 billion by 2030, significantly expands the potential entry points for cyberattacks. Each device represents a potential vulnerability, necessitating robust security measures and comprehensive monitoring.

3. **AI-specific threats**: AI systems introduce new vulnerabilities such as data poisoning, model manipulation and adversarial attacks. The dual nature of AI as both a cybersecurity tool and potential weapon requires advanced defence strategies and continuous innovation.

4. **Quantum computing risks:** Quantum computing poses significant threats to current encryption methods, with some actors already harvesting encrypted data for future decryption. This emphasizes the urgency of developing quantum-resistant cryptographic solutions.

5. **Supply-chain vulnerabilities:** The complex, global nature of ICT supply chains makes them prime targets for cyberthreats, necessitating comprehensive security measures throughout the entire chain.

6. **Regulatory challenges:** The speed of technological advances often outpaces existing regulatory frameworks, creating governance gaps. There is a need for flexible, adaptive regulations that balance innovation and security.

7. **Skills gap:** A significant shortage of cybersecurity professionals with expertise in emerging technologies presents challenges for organizations attempting to secure new systems and respond to evolving threats.

Recommendations

1. **Investment in R&D:** Continuously invest in research and development to create innovative solutions for emerging threats, including new cryptographic techniques and AI-driven cybersecurity tools.

2. **Collaboration and capacity-building:** Strengthen partnerships among government, industry and academia to address cybersecurity challenges collectively. Invest in initiatives to enhance cyber skills and expertise in emerging technology areas.

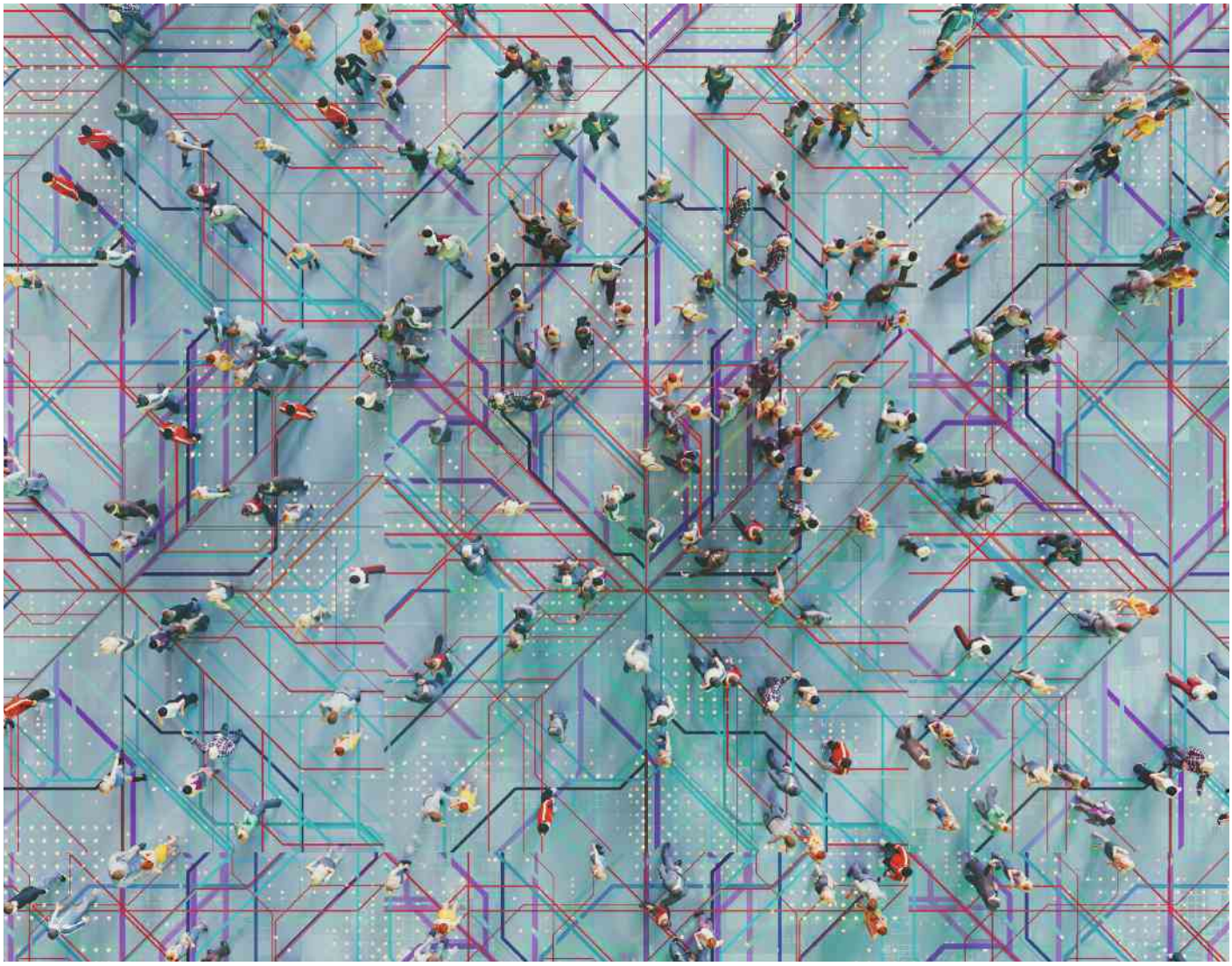
3. **Regulatory reform and standardization:** Develop regulatory frameworks that promote security by design and facilitate international cooperation. Standardize cybersecurity practices to streamline compliance efforts and improve interoperability across sectors.

4. **Cyber-resilience planning:** Develop and regularly test comprehensive incident response plans that account for emerging threats to ensure rapid recovery from cyber incidents.

5. **Governance frameworks:** Establish robust governance structures to guide the responsible development and deployment of emerging technologies, integrating risk assessment and management processes throughout their life cycle.

6. **Continuous monitoring and adaptation:** Implement mechanisms for ongoing monitoring of emerging technology environments and adapt cybersecurity strategies in response to evolving threats.

Establishing a proactive, collaborative approach to cyber resilience is essential in the face of rapidly evolving technologies. By integrating security and resilience by design, stakeholders can ensure the development of secure digital ecosystems while driving innovation. Balancing the risks and opportunities presented by emerging technologies is key to maintaining a secure and resilient digital future.



Introduction

New digital technologies are accompanied by a daunting threats landscape that requires investment in a comprehensive novel cyber-resilience ecosystem.

Emerging technologies are expanding the digital attack surface at an unprecedented rate, creating new vulnerabilities and complexities that traditional security measures may not adequately address.[3] The anticipated surge of internet of things (IoT) devices, projected to surpass 32 billion globally by 2030,[4] introduces countless potential entry points for cyberattacks. Similarly, integrating AI into critical infrastructure, while offering enhanced capabilities, also exposes systems to risks such as data poisoning, adversarial attacks and deepfakes, which can manipulate AI algorithms to behave unpredictably or maliciously.

The increasing interconnectivity of these technologies results in a more complex and dynamic threat landscape. A breach in one system can trigger cascading effects across multiple interconnected networks, potentially disrupting critical infrastructure and services on a massive scale. This interconnectedness, while beneficial for operational efficiency, necessitates a comprehensive and adaptive approach to cybersecurity – one that not only protects against potential breaches but also ensures robust recovery mechanisms to maintain continuity and trust in digital systems.

Moreover, the speed of technological innovation often outpaces the development of regulatory frameworks and cybersecurity measures. The absence of standardized security protocols and regulations creates governance gaps, making it difficult for organizations to implement consistent cybersecurity strategies. Compounding these challenges is a significant shortage of cybersecurity professionals skilled in emerging technologies, underscoring the urgent need for targeted education and training initiatives. This skills gap highlights the importance of building a resilient workforce capable of addressing the complexities of next-generation cyberthreats.

While these challenges are significant, they also present a unique opportunity to rethink the approach to cybersecurity. Moving from a “security by design” to a “resilience by design” mindset involves embedding resilience principles into every stage of technology development and deployment. This shift recognizes that, in today’s landscape, preventing all cyberattacks is unrealistic; instead, the goal should be to design systems that can absorb attacks, maintain critical functions and recover quickly with minimal impact. For example, in quantum cryptography, while it is essential to develop algorithms resistant to quantum attacks, it is equally important to ensure that cryptographic systems can continue to operate securely even under attack. Similarly, AI and machine learning can be used not only to detect threats but also to predict and pre-emptively respond to potential vulnerabilities, enhancing overall system resilience.

Adopting a “resilience by design” approach requires a paradigm shift in how organizations and policy-makers think about cybersecurity. It involves building systems that are not only secure but also flexible and adaptive, capable of evolving in response to new threats. This approach emphasizes continuous monitoring, rapid response and the ability to learn from incidents to strengthen defences over time. For instance, organizations could implement AI-driven predictive analytics to identify potential threats and automatically deploy countermeasures, thereby reducing response times and limiting the damage caused by cyber incidents.

The distinction between critical and emerging technologies further complicates the cybersecurity landscape. Critical technologies, such as AI and quantum computing, are already essential to national security and economic competitiveness, demanding immediate and sustained investments to protect them from cyberthreats. In contrast, emerging technologies, including post-quantum cryptography and synthetic biology, are still at the developmental stage but have the potential to become critical as their applications expand and their strategic importance becomes more apparent.[5] This fluidity necessitates a flexible approach to cybersecurity that can adapt to both current and future risks, ensuring preparedness for a range of possible scenarios.

By focusing on resilience rather than mere security, organizations can better navigate the complex and evolving technological landscape. This involves integrating resilience into the design and development of technologies, ensuring that systems are robust, adaptive and capable of withstanding the new scale of cyberthreats. It also requires fostering a culture of continuous improvement, where learning from past incidents informs future strategies, and where collaboration among stakeholders is prioritized to build a more resilient digital ecosystem.

To effectively navigate this complex environment, stakeholders in government, industry, academia and civil society must collaborate closely. Developing comprehensive cyber-resilience frameworks that are adaptable to the rapidly changing technological landscape and capable of addressing the unique challenges posed by each technology is crucial. International cooperation is also vital, as cyberthreats are inherently global and call for a coordinated, well-managed response.

The path forward lies in embracing a balanced approach that weighs both the risks and opportunities presented by emerging technologies. By promoting an environment in which innovation can thrive without compromising security or societal values, the full potential of these technologies can be harnessed while safeguarding against their potential threats. This requires investing not only in technological advances but also in human and organizational capabilities to manage and secure these innovations effectively. A culture of continuous improvement, adaptation and collaboration will be essential to ensure that cybersecurity evolves alongside the technologies it aims to protect.

This paper explores the multifaceted risks and opportunities associated with emerging technologies, offering data-driven insights and recommendations for enhancing cyber resilience. By understanding the evolving technological landscape and the security challenges it presents, organizations can better navigate the complexities of the digital age, ensuring that innovation and security are advanced together in a balanced and sustainable manner. This approach not only protects the present but also ensures a secure, resilient and prosperous future in the face of emerging technological challenges.

1 Expanding the focus: Clarity beyond the current landscape of emerging technologies

It is important to consider the full range of technological innovations.

While much of the current discourse around emerging technologies focuses on a small cluster of prominent developments such as AI, it is crucial to broaden this view to encompass the full spectrum of more than 200 critical and emerging technologies shaping today's technological landscape. Emerging technologies span a wide range, including advanced materials, biotechnology, quantum-resistant cryptography, augmented reality and others, each with unique cybersecurity implications.

The Australian Policy Institute's development of a parameter for evaluating global readiness for critical technology investments provides further insight into how countries are positioning themselves to integrate and capitalize on these technologies. This parameter assesses various factors, such as technological maturity, economic impact and geopolitical significance, offering a comprehensive framework for understanding global technological readiness. The rapid growth in investments in emerging technologies – from approximately $4 billion in 2018 to more than $3.2 trillion today – demonstrates a significant surge in global interest and development, underscoring the need for a broad, inclusive approach to technology assessment and strategy development.[6]

2 Defining the landscape: Critical vs. emerging technologies

Distinguishing between critical and emerging technologies brings clarity to the cyber-resilience debate.

To develop effective cyber-resilience strategies, it is essential to understand the distinction between critical and emerging technologies, as well as their respective impacts and strategic importance. The line between critical and emerging technologies can often be fuzzy. Some technologies may fit both categories simultaneously, depending on their stage of development and adoption in different sectors or regions, and classifications can change quickly with development.

– **Critical technologies** are those that are essential for national security, economic competitiveness and societal well-being. They often have dual-use potential, serving both civilian and military applications, and are considered strategically important. Examples of critical technologies include AI, quantum computing, semiconductors and biotechnology. These technologies are generally more established, having attracted significant investment from government and industry due to their immediate and long-term strategic value. The maturity of critical technologies means they are already integrated into national and economic infrastructure, making them indispensable for maintaining strategic advantage and operational continuity.

– **Emerging technologies** are innovative technologies that are still in development or in the early stages of adoption. They have the potential to significantly affect various sectors but are not yet fully established or widely implemented. They often go beyond the Fourth Industrial Revolution, encompassing areas such as post-quantum cryptography, gene editing, precision medicine and the convergent effects of multiple technologies. Unlike critical technologies, emerging technologies are more speculative, attracting investments focused on research and development rather than immediate deployment. However, their rapid evolution and the increasing recognition of their transformative potential indicate that they may become critical technologies over time.

2.1 Key differences between critical and emerging technologies

1. **Maturity:** Critical technologies are typically more established and integrated into essential national and economic infrastructure. In contrast, emerging technologies are still evolving and may not yet have reached widespread adoption or maturity.

2. **Strategic importance:** Critical technologies are deemed essential for national interests, including security, economic competitiveness and societal well-being. Emerging technologies, while potentially transformative, may or may not achieve the same level of strategic importance.

3. **Current impact:** Critical technologies have already had a significant impact on society, the economy and security. Emerging technologies are in the process of demonstrating their full potential, with impacts that are anticipated but not yet fully realized.

4. **Investment focus:** Due to their established importance, critical technologies attract substantial investments and strategic focus from governments and industries. Emerging technologies, being more speculative, typically attract funding aimed at research, development and exploratory applications.

The distinction between critical and emerging technologies is fluid: emerging technologies may become critical over time as their potential and impact become more apparent. This dynamic landscape necessitates continuous monitoring and adaptation of cybersecurity strategies to remain effective against evolving threats.

3 Framing cybersecurity concerns for emerging technologies

Cybersecurity threats to new technologies include dangers specific to AI and quantum computing as well as vulnerabilities in the supply chain and data privacy concerns.

Framing cybersecurity concerns for emerging technologies involves addressing a range of complex and interrelated risk factors. The rapid development of technologies presents both opportunities to enhance cyber resilience as well as challenges that could increase vulnerabilities. Understanding these dynamics is crucial for developing robust strategies to protect against emerging threats while maximizing the potential benefits of new technologies.

1. Technological arms race

Emerging technologies are accelerating a technological arms race in cybersecurity. This is characterized by a continuous cycle of innovation and counter-innovation between defenders and attackers. As defenders develop new tools and techniques, such as quantum-resistant encryption and decentralized systems, attackers are simultaneously advancing their methods to exploit these innovations. The cybersecurity market, driven by these needs, is projected to grow from $188 billion in 2023 to $288 billion by 2027, reflecting the increasing demand for advanced solutions to counter sophisticated cyberthreats.[7]

2. Ethical and legal challenges

The deployment of emerging technologies also raises significant ethical and legal challenges. For example, blockchain technology offers enhanced security and transparency through decentralized ledgers, but it also raises issues regarding privacy, data ownership and the potential for misuse in illegal activities such as money laundering or the financing of terrorism.[8] Legal frameworks around the world struggle to keep pace with these rapid advances, often resulting in a patchwork of regulations that are difficult to enforce globally. There is a critical need for comprehensive, globally harmonized legal frameworks and ethical guidelines that govern the use of these technologies.

3. Digital divide

A significant challenge in the context of emerging technologies is the digital divide, which creates disparities in access to and the understanding of advanced technologies. Developed nations with substantial technological infrastructure and resources are better positioned to make use of emerging technologies for cybersecurity. In contrast, developing nations often lack the financial resources, technical expertise and regulatory frameworks needed to implement these technologies effectively. This divide makes these nations more vulnerable to cyberthreats and limits their ability to contribute to and benefit from global cybersecurity advances. To address this, there needs to be a concerted effort to build capacity and promote collaboration among different regions.

4. Privacy concerns

Emerging technologies can also heighten privacy concerns, particularly as they become more integrated into daily life and critical infrastructure. IoT devices, for example, collect vast amounts of data that can provide detailed insights into personal behaviour and habits. While this data can enhance operational efficiency and user experience, it also poses significant privacy risks if not properly managed. Blockchain technology, although offering increased security, can also be misused to track transactions and identify individuals. The challenge lies in balancing the benefits of data collection and use with the need to protect individual privacy rights. This tension is likely to intensify as technologies such as edge computing and 5G networks expand, further increasing the volume and granularity of data collected. Effective data governance policies and privacy regulations are critical to managing these concerns while promoting trust in emerging technologies.

5. Economic impact

The dual-use nature of emerging technologies means they can be put to work for both beneficial and malicious purposes, leading to significant economic implications. For example, blockchain technology can secure transactions and reduce fraud in financial systems, potentially saving billions of dollars. However, it can also be exploited for criminal activities, such as ransomware payments and illegal trades. The World Economic Forum estimates that cyberattacks could cost businesses worldwide more than $10 trillion annually by 2025.[9] Organizations must factor in these economic impacts when planning their cybersecurity strategies, balancing the potential benefits of adopting new technologies with the risks associated with their misuse.

6. Geopolitical shifts

The race to develop and control emerging technologies is reshaping global power dynamics, with significant geopolitical implications. Nations that lead in the development of advanced technologies such as quantum computing and AI are likely to gain strategic advantages in both economic and military domains.[10] Controlling these technologies could lead to new forms of economic influence, significantly affecting international relations. Ensuring that the development and deployment of emerging technologies are guided by international norms and agreements is critical to maintaining global stability.

7. Skills gap and educational needs

The rapid evolution of emerging technologies has created a significant skills gap in the cybersecurity workforce. Advanced technologies such as quantum computing, synthetic biology and blockchain require specialized knowledge that is not widely possessed by the current workforce. This gap poses a serious challenge for organizations attempting to secure new systems and respond effectively to evolving threats. The demand for cybersecurity professionals is expected to exceed supply by a significant margin, with a projected 3.5 million unfilled positions by 2025.[11] To address this gap, there must be a robust investment in education and training programmes that focus on the specific needs of emerging technologies.

8. Trust and confidence in digital systems

As emerging technologies become more integrated into critical infrastructure and daily life, maintaining trust and confidence in digital systems becomes increasingly challenging. Technologies such as quantum computing and blockchain are often perceived as complex and opaque, making it difficult for members of the general public to understand their benefits and risks. Incidents such as data breaches, misuse of technology and failures in IoT devices can erode public trust in these systems. Maintaining trust requires a commitment to transparency, robust security measures and clear communication about the risks and benefits associated with emerging technologies.

9. Regulatory challenges

The pace at which emerging technologies are being developed often outstrips the ability of regulatory frameworks to adapt. This creates significant challenges for policy-makers and regulators, who must balance the need for innovation with the need to protect against new and evolving threats. Over-regulation can stifle innovation and slow technological progress, while under-regulation can leave critical vulnerabilities unaddressed. A flexible, adaptive approach to regulation is needed, one that can evolve in tandem with technological advances and ensure robust cybersecurity protections without hindering innovation.

10. Interdisciplinary collaboration

Addressing the challenges posed by emerging technologies requires unprecedented levels of interdisciplinary collaboration. Technologists, policy-makers, ethicists and other stakeholders must work together to develop comprehensive cybersecurity strategies that consider not only the technical aspects of emerging technologies but also their social, economic and ethical implications. For example, collaboration between the tech industry and public health experts could help ensure that advances in biotechnology are used safely and ethically.

11. Increased attack surface

Emerging technologies such as IoT, AI and cloud computing significantly expand the attack surface. The proliferation of IoT devices, expected to reach more than 32 billion connected devices by 2030, represents a massive increase in potential entry points for cyberattacks.[12] Each connected device can serve as a potential point of vulnerability, necessitating robust security measures and comprehensive monitoring to mitigate risks.

3.1 Opportunities and risks of emerging technologies for cyber resilience

Emerging technologies offer both opportunities to enhance cyber resilience and risks that could increase the likelihood of exploitation in cyberspace. Understanding these dual aspects is crucial for developing effective strategies to maximize the benefits while mitigating the associated threats.

Opportunities for enhancing cyber resilience

1. **Quantum-resistant encryption:** The advent of quantum computing provides a unique opportunity to revolutionize cybersecurity through the development of quantum-resistant encryption methods. These advanced cryptographic techniques can safeguard sensitive data against potential future quantum-based attacks, ensuring the long-term security of critical information and communication systems.

2. **Distributed ledger technologies (DLT):** Technologies such as blockchain enhance cybersecurity by decentralizing data storage and processing. This decentralization reduces the risk associated with centralized databases, which are common targets for cybercriminals.

3. **Autonomous systems:** The deployment of autonomous systems, including self-healing networks and AI-driven incident response tools, represents a significant advance in cybersecurity capabilities. These systems can automatically detect threats in real time, respond to incidents more quickly than traditional methods and even predict future vulnerabilities.

4. **Edge computing:** Edge computing processes data closer to its source, reducing the need for data transmission to centralized servers. This distributed approach minimizes latency and bandwidth costs while reducing the risk of data interception during transit, which can protect critical infrastructure from attacks targeting centralized systems, thereby enhancing resilience.

Risks of accelerating exploitation

1. **Quantum computing risks:** Despite its potential benefits, quantum computing poses a significant threat to current encryption standards. Cyber adversaries are already employing tactics such as "steal now, decrypt later", in which encrypted data is harvested with the intention of decrypting it once quantum capabilities are sufficient.

2. **IoT vulnerabilities:** The rapid growth of the IoT has dramatically expanded the cyberattack surface. Many IoT devices are deployed without adequate security measures, making them attractive targets for cybercriminals. The unregulated and diverse nature of IoT ecosystems requires robust security frameworks to protect against breaches and prevent attackers from exploiting these devices.

3. **Blockchain exploitation:** While blockchain technology provides enhanced security through decentralization and immutability, it is not immune to exploitation. Vulnerabilities in smart contracts, for example, can be exploited for financial gain, leading to significant economic losses. The decentralized and pseudonymous nature of blockchain can also facilitate illegal activities, such as money laundering, posing additional challenges for regulatory bodies and law enforcement.

4. **AI-specific threats**: The integration of AI into cybersecurity introduces new vulnerabilities, such as data poisoning, model manipulation and adversarial attacks. AI can also be exploited to generate sophisticated phishing attacks, deepfakes and automated exploits, increasing the scale and complexity of cyberthreats.

5. **Supply-chain vulnerabilities**: The increasing complexity and interconnectedness of global supply chains, particularly in the ICT sector, have made them prime targets for cyberthreats. Emerging technologies often rely on intricate supply chains that are difficult to secure. Protecting these supply chains involves securing intellectual property, ensuring the integrity of components during transport, and implementing zero-trust architecture in which each component continuously verifies the others.

The interplay between the opportunities and risks associated with emerging technologies requires a careful, strategic approach to cybersecurity. While technologies such as quantum computing, DLTs, autonomous systems and edge computing offer significant potential to strengthen cyber defences, they also introduce new vulnerabilities that can be exploited by malicious actors. To deploy these technologies for cyber resilience effectively, a comprehensive strategy that includes continuous investment in research and development, robust regulatory frameworks and international collaboration is essential. By balancing the opportunities and risks, organizations can better prepare for the evolving threat landscape and build a more secure and resilient digital future.

3.2 Examples of emerging technologies and their security implications

The complex nature of emerging technologies introduces unique security challenges that require targeted strategies and solutions. While emerging technologies hold great promise for innovation and advancement across sectors, it is essential to consider the potential security challenges they bring. The following section outlines some risks associated with these technologies under **extreme, worst-case scenarios**, which, though theoretically possible, are highly unlikely. It is important to note that the majority of these technologies are being developed with strong security measures in place, and many of the challenges mentioned are being actively mitigated through ongoing research, regulation and industry best practices.

1. **Semiconductors:** There is a growing focus on securing the entire semiconductor supply chain. This includes protecting chip design intellectual property, securing fabrication processes and ensuring the integrity of chips during transport and installation. Developing "zero-trust" architecture, which involves components continuously verifying each other within the chips themselves, is becoming a key focus area.[13]

2. **Digital assets:** Digital assets such as cryptocurrencies, non-fungible tokens (NFTs) and tokenized real-world assets present unique security challenges. Cryptocurrencies face issues such as 51% attacks, smart contract vulnerabilities and wallet security.[14] The rise of decentralized finance (DeFi) introduces new attack vectors such as flash loan attacks and oracle manipulation. Flash loan attacks involve attackers borrowing large amounts of cryptocurrency without collateral for a single transaction, manipulating market prices for profit. Oracle manipulation is the act of providing false data to smart contract oracles, which are trusted sources of external information, to exploit DeFi protocols.[15] NFTs also face challenges related to proof of authenticity, copyright infringement and the security of the

platforms hosting them. Tokenized real-world assets (e.g. real estate or art) require secure links between the digital token and the physical asset, raising questions about legal frameworks and enforcement.

3. **Quantum technologies**: Beyond the threat quantum computing poses to current encryption, quantum sensing could potentially detect stealth technologies or underground facilities, affecting national security. Quantum communication networks, while potentially offering unbreakable encryption, could be vulnerable to denial-of-service attacks at their classical interfaces. Post-quantum cryptography is being developed to resist quantum attacks, but transitioning global infrastructure to these new systems presents enormous logistical and security challenges.[16]

4. **Advanced AI systems:** AI security is a growing concern because adversarial attacks on AI models could manipulate their outputs in subtle, hard-to-detect ways. AI systems might also be vulnerable to data poisoning during training, leading to biased or malicious behaviour. The use of AI in critical decision-making processes (for example, financial systems) raises concerns about accountability and control. There is also a rising threat of AI systems being used to generate deepfakes or conduct large-scale social engineering attacks.[17]

5. **Biotechnology and synthetic biology:** Biotechnology advances such as DNA data storage technologies raise questions about long-term data security and potential biological data breaches. Synthetic biology could potentially be used to create designer pathogens or manipulate existing organisms in unforeseen ways. The convergence of AI and biotechnology raises concerns about the potential for creating self-evolving biological systems.[18]

6. **Advanced energy systems:** New energy technologies such as nuclear fusion reactors present unique cybersecurity challenges due to their complexity and potential novel vulnerabilities. Advanced battery technologies, crucial for the renewable energy transition, face risks of cyberattacks that could lead to overcharging, thermal runaway (where a temperature increase triggers a cascade of events that produce even more heat, creating a dangerous feedback loop) or grid instability (where fluctuations or imbalances in an electrical power system that can compromise its reliability and performance). Wireless power transmission systems could be vulnerable to interception or disruption, potentially affecting critical infrastructure.[19]

7. **Space technologies:** The expansion of space technologies, including mega constellations of satellites (a large network of satellites deployed in low Earth orbit), introduces new challenges in space traffic management and the potential for large-scale disruptions. Issues of space debris, light pollution and the environmental impact are becoming increasingly important.[20]

8. **Molecular electronics:** Molecular electronics is an emerging field that presents vast opportunities, especially in miniaturized technologies for applications such as bioelectronic devices and hybrid systems. One exciting aspect is the integration of molecular-scale circuits into bioelectronics, which holds promise for advancements in medical devices, environmental sensors and energy-efficient systems. However, with these opportunities come security concerns, particularly regarding potential surveillance uses and bioelectronic hybrid threats. Rigorous research is currently being conducted to address these security risks, ensuring that the application of molecular electronics is safe and reliable. Studies in bioelectronics, for example, are exploring how to establish the ethical and secure use of bioelectronic systems, such as hydrogels for safe signal transduction and brain-computer interfaces (BCIs), which highlight the importance of security in these new technologies.[21]

9. **Neuromorphic computing:** Neuromorphic computing is an approach to computer engineering that designs hardware and software systems to mimic the structure and function of the human brain.[22] This development may help improve efficiency and allow machines to perform more complex tasks. However, brain-like computing architecture may be vulnerable to new types of attack that exploit their learning capabilities. There is potential for bias, as well as potential data extraction from neuromorphic systems that have “learned” sensitive information, and the unpredictability of these systems raises concerns about their use in critical applications.

10. **Volumetric displays and holography**: Advanced 3D displays could be used for sophisticated phishing or social engineering attacks. Securing the data used to generate holograms becomes crucial in preventing unauthorized replication, and there is potential for the creation of false environments that could manipulate decision-making in critical situations.

These additional examples further illustrate the complex and interconnected nature of security challenges in emerging technologies. They underscore the need for forward-thinking security strategies that can anticipate and address potential vulnerabilities before they can be exploited. The rapid pace of technological advances means that security considerations must be integral to the development process, requiring collaboration across disciplines and sectors to effectively address these challenges.

4 Quantifying impact, measurement and data analysis

Quantifying the impact of emerging technologies is a complex but essential task in today's rapidly evolving landscape.

Effective measurement involves several key considerations.

1. **Developing comprehensive metrics:** A balanced set of metrics is required to accurately measure the impact of emerging technologies. This should include both quantitative measures, such as economic outcomes and number of cybersecurity incidents, and qualitative measures such as an assessment of societal, ethical and regulatory implications. For instance, evaluating the societal impact of AI might include assessing its effect on employment, privacy and decision-making autonomy.

2. **Holistic risk assessment:** Evaluating emerging technologies such as AI, quantum computing and IoT requires a holistic risk assessment framework. This should consider the increased attack surface, the complexity of threat analysis and potential skills gaps within organizations. Developing a structured approach to identifying, assessing and mitigating risks is crucial for maintaining a resilient cybersecurity posture.

3. **Standardized measurement approaches:** To enable meaningful comparisons and benchmarking throughout different sectors and regions, standardized methods for measuring the impact of emerging technologies are necessary. This could involve developing industry-wide or global standards for assessing technological readiness, security and performance, allowing for a consistent and comparable analysis of the impact of different technologies.

4. **Data collection and analysis:** Robust data-collection mechanisms are essential for accurate impact assessment. They should gather comprehensive data on technology adoption rates, economic outcomes, cybersecurity incidents and societal effects. Advanced analytics and AI can process this data to derive actionable insights, supporting more informed decision-making and policy development.

5. **Contextual analysis:** The impact of emerging technologies can vary significantly based on the context in which they are deployed. Measurements should therefore take into account factors such as an organization's position in the supply chain, its relationship to critical business processes and the broader national or regional context in which the technology is used. This contextual understanding is crucial to accurately assess the risks and benefits of technology adoption.

6. **Interdisciplinary approach:** Quantifying the impact of emerging technologies requires input from multiple disciplines, including technology experts, economists, social scientists and ethicists. An interdisciplinary approach such as this ensures a comprehensive assessment that considers technological performance and the broader societal, economic and ethical implications.

7. **Continuous monitoring and adaptation:** Given the rapid pace of technological change, impact measurement should be an ongoing process. Regular reassessment and adaptation of metrics and analysis methods are necessary to stay up to date with evolving technologies and their effects, ensuring that measurement approaches remain relevant and effective.

8. **Transparency and accessibility:** Ensuring that data and analysis results are widely accessible promotes transparency and enables further research. Making these findings available promotes collaboration and leads to a more comprehensive understanding of the technological impacts, contributing to the development of more effective and inclusive policies.

By focusing on these aspects, organizations can develop a more robust and nuanced approach to quantifying the impact of emerging technologies, leading to better-informed decision-making and policy development.

4.1 Solutions and mitigation strategies

To effectively address the cybersecurity risks posed by emerging technologies, organizations must adopt comprehensive solutions and mitigation strategies.

1. **Building a resilient digital environment:** Creating a secure digital environment requires establishing security by design and default as standard practice, developing layered security approaches and creating incentive frameworks to redistribute security burdens among stakeholders. This holistic approach ensures that security is integrated into every layer of technology development and deployment.

2. **Promoting cyber equity:** Bridging the cybersecurity skills gap is essential for building a resilient digital landscape. Increasing access to cybersecurity resources, tools and training programmes can empower individuals and organizations to better protect themselves against emerging threats. Developing specialized training programmes in AI security, for example, can help prepare the workforce for the unique challenges posed by AI-driven threats.

3. **Enhancing data exchange and collaboration:** Breaking down information barriers and promoting better data exchange within and between countries is critical to enhancing collective cybersecurity efforts. Advocating for harmonized standards and reporting frameworks can facilitate collaboration and information-sharing, enabling a more coordinated response to global cyberthreats.

4.2 Priorities for cyber resilience and future directions

To maintain robust cyber resilience in the face of emerging threats, several priorities must be addressed.

1. **Investment in research and development:** Continuous investment in research and development (R&D) is critical to developing innovative solutions to emerging threats. This approach should include exploring new cryptographic techniques to counter quantum computing threats, advancing AI-driven cybersecurity tools and enhancing IoT security frameworks.

2. **Collaboration and capacity-building:** Strengthening partnerships among government, industry and academia is essential for addressing cybersecurity challenges collectively. Investing in capacity-building initiatives can enhance cyber skills and expertise, particularly in emerging areas such as synthetic biology and quantum computing.

3. **Regulatory reform and standardization:** Developing regulatory frameworks that promote security by design and facilitate international cooperation is crucial for building a resilient digital landscape. Standardizing cybersecurity practices can streamline compliance efforts and improve interoperability among sectors.

4. **Cyber-resilience planning:** Developing and testing comprehensive incident response plans that account for emerging threats is essential to ensure rapid recovery from cyber incidents. These plans should be regularly updated and tested to reflect the evolving threat landscape.

5 Use cases and multistakeholder collaborations

The complexities of managing cybersecurity in the age of emerging technologies are best understood through practical examples.

Real-world case studies from leading organizations and nations provide valuable insights into how emerging technologies can be effectively integrated into broader cybersecurity frameworks while managing the associated risks.

5.1 Motivation for case studies

The motivation for presenting these case studies is threefold.

1. **Demonstrating practical applications:** Examining how organizations and nations have integrated emerging technologies into their cybersecurity strategies delivers a deeper understanding of the practical applications and the tangible benefits such technologies offer. These case studies showcase the innovative use of technologies to enhance cyber resilience, improve operational efficiency and maintain competitive advantage.

2. **Highlighting risk management strategies:** Emerging technologies are double-edged swords; while they offer significant benefits, they also introduce new risks. The case studies provide examples of how these risks are managed through comprehensive strategies that include robust governance frameworks, rigorous risk assessments and continuous monitoring and adaptation.

3. **Encouraging collaborative approaches:** The case studies underscore the importance of collaboration among various stakeholders – governments, private-sector organizations, research institutions and international partners. Such collaboration is crucial for developing and implementing effective cybersecurity measures that use the potential of emerging technologies while safeguarding against their misuse.

CASE STUDY 1

One type of approach to cybersecurity with emerging technologies

The Schneider Electric case study illustrates how an organization can effectively use emerging technologies to enhance cybersecurity while managing the associated risks.

Technology and innovation enabler for broader cybersecurity strategy

Schneider Electric, a global industrial technology leader, drives sustainable impact through its expertise in electrification, automation and digitization. The combination of its electrical and automation technologies with its leadership in software and services accelerates sustainable impact. To harness the benefit of the digital solutions and technology, the company has a team dedicated to Cybersecurity Technology and Innovation, with an associated technology validation process.

This dedicated team continuously scans the company's security data protection capabilities, both for the digital core infrastructure and offerings and for emerging technologies. Insights that shape the roadmap come from audit and penetration testing observations, vulnerability and incident learnings, scoring agency reports and customer queries – demonstrating that this central team influences the digital organization, business and operational units.

The focus includes both conventional and emerging technologies, encompassing AI, cloud technologies, deception technology, secure industrial communications and quantum encryption. Additionally, it explores established technologies such as zero trust in operational technology segments. The goal is to ensure cybersecurity integration through ongoing education and collaboration.[23]

The technology validation process at Schneider Electric ensures compliance with current regulations (e.g. EU AI Act, Export Control Rule), follows "secure by design" requirements, and validates secure implementation, known as "security by operations". This process, also referred to as digital certification, is a company-wide mechanism for validating emerging digital technologies for business and operational use. All new digital assets undergo technology validation before deployment, involving various stakeholders to provide a holistic risk assessment – for instance, data protection impact assessments when the technology processes sensitive personal data.

Emerging technology use case: PLC code generation with generative AI

One example of the above measures is the Schneider Electric use case for AI-generated code. The company uses generative AI (GenAI) for programmable logic controller (PLC) code generation within industrial control systems. More simply put, in many factories and industrial settings, machines are controlled by specialized computers called programmable logic controllers (PLCs). These PLCs need to be programmed with specific instructions to operate the machinery correctly. Traditionally, human programmers would write the instructions, but in this case, AI is being used to help the human programmers create the instructions automatically. This application of AI can help to enhance operational efficiency and strengthen cybersecurity measures by automating code generation and improving code quality. When combined with the above measures for cybersecurity, an environment can be created whereby the organizational risk management strategy can help to ensure secure AI integration, addressing potential threats such as unauthorized access and system vulnerabilities.

Conclusion and future outlook

The above strategic approach to integrating emerging technologies into an organization – using a series of checks and balances, control mechanisms that allow constant evaluation of the cybersecurity risks and benefits – highlights the importance of balancing innovation with robust cybersecurity measures. This is just one example of how to safely and securely implement emerging technology, and many organizations will need to weigh up the impact of these technologies against their capacity to implement robust controls.

CASE STUDY 2

UAE's emerging tech model

The United Arab Emirates (UAE) is an example at the national level of using emerging technologies to drive technological innovation while still considering the importance of cyber resilience.

Background

The UAE has positioned itself as a leader in the adoption of emerging technologies. Key regulatory bodies such as the Dubai Electronic Security Center (DESC), the Telecommunications and Digital Government Regulatory Authority (TDRA), the Virtual Asset Regulatory Authority (VARA), the UAE Cyber Security Council (CSC) and the Ministry of Artificial Intelligence provide clear examples of the development of national infrastructure with the mandate to specifically develop and secure the nation's digital infrastructure. These bodies, as well as other government bodies, have clearly expressed their intention to develop technologies such as AI, blockchain, quantum computing, 5G, IoT, digital assets, connected vehicles and smart cities with the goal of transforming sectors across the UAE, establishing it as a leader in technological innovation.

Collaboration and ecosystem development

The UAE's technological ecosystem provides a unique case study as it involves government entities, private-sector companies, research institutions and international partners in an integrated way. Public–private partnerships, such as the Dubai Blockchain Platform, aim to allow the UAE to pilot and scale new technologies, while international collaborations position the country to take advantage of global knowledge, which ultimately contributes to the expertise used to develop these technologies. While this model is not applicable to all countries, it is an important consideration as all nations must reckon with emerging calls to regulate the technologies that will become ubiquitous in the years to come. Understanding what types of bodies and what types of public–private collaboration lead to the most productive outcomes will ultimately serve more than just a single nation.

Analysis

- **AI:** AI is transforming sectors such as transportation, energy and healthcare in the UAE. Initiatives such as Dubai Road and Transport Authority (RTA)'s autonomous vehicles and the Dubai Electricity and Water Authority (DEWA)'s AI-powered operations are examples of the integration of AI into critical infrastructure while considering safety, efficiency and decision-making. DESC's AI-enabled cybersecurity tools, such as the RZAM platform, demonstrate AI's role in improving cybersecurity posture.[24]

- **Blockchain:** The Dubai Blockchain Strategy aims to transition all government transactions to blockchain by 2025. The plain has three main pillars: government efficiency, industry creation and international leadership. The architects of this initiative expect it to help with the above, but also plan to make the platform available to others. The Dubai Blockchain Platform and the UAE's blockchain-as-a-service initiatives reflect the country's commitment to using this technology.[25]

- **Quantum computing:** Investments in quantum research and collaborations with international partners aim to help the city to prepare for advances in cryptography and optimization, critical for national security and industrial applications.

- **5G and IoT:** The UAE is additionally aiming for 100% 5G coverage by 2025, which would theoretically support smart-city infrastructure and connected vehicles, transforming the digital landscape.

- **Digital assets:** VARA regulates the UAE's digital assets, promoting the growth of blockchain-based financial products. This regulatory body was highly anticipated as it represents one of the first official government bodies dedicated to the regulation of virtual assets.

- **Connected vehicles and smart cities**: The RTA's connected vehicle technology integrates AI, IoT and 5G, aiming to enhance urban mobility. Smart-city initiatives make use of technologies to optimize resource use and support sustainable growth, reflecting the UAE's vision for integrated urban management.

Risk and security considerations

The adoption of emerging technologies comes with cybersecurity risks, necessitating rigorous risk assessments and robust security frameworks. DESC aims to mitigate those where possible by issuing standards and guidelines for technologies such as AI, IoT and blockchain, ensuring secure integration while encouraging innovation. Balancing innovation with security is essential for maintaining resilience and safeguarding digital infrastructure.

Open assessments, testing and validation toolboxes

The UAE has established open assessment and validation tools to ensure the security and reliability of emerging technologies. Initiatives such as DESC's cybersecurity testing and validation platform enable public- and private-sector entities to evaluate the robustness of their systems, promoting a secure and resilient tech ecosystem.

Impact assessment and ethical considerations

Emerging technologies are expected to have a significant impact on the UAE's economy and society, affecting economic growth and quality of life. However, ethical considerations, such as privacy, bias and job displacement, must be addressed through the appropriate regulatory bodies and frameworks to ensure responsible technology use.

Strategic way forward

The UAE's focus on strengthening regulatory frameworks, promoting collaboration and investing in R&D to navigate the challenges and opportunities presented by emerging technologies provides an interesting case study of a nation working to anticipate and adapt to technological changes before they reach their crescendo. By balancing technological advances with ethical considerations and robust security measures, the UAE aims to maintain its leadership in technological innovation and ensure a secure and competitive tech ecosystem.

CASE STUDY 3

Singapore's multistakeholder strategy

Singapore is working to adopt a comprehensive multistakeholder strategy designed to enhance cybersecurity resilience through research, innovation and supply-chain risk management.

Contextual background

Singapore has emerged as a leader in cybersecurity by developing a robust ecosystem for collaboration. The government works with stakeholders in the cybersecurity ecosystem, from industry leaders to academia and foreign governments, with the aim of building a safer cyberspace. Important initiatives include the cybersecurity talent, innovation and growth (TIG) plan and the critical information infrastructure (CII) supply chain programme.

Collaboration and ecosystem development

Singapore's cybersecurity strategy is heavily driven by multistakeholder collaboration. The government works closely with industry partners to raise baseline cybersecurity levels and promote innovation. The TIG plan supports companies in developing cybersecurity solutions and scaling them internationally. This plan also emphasizes building a skilled workforce through training programmes and innovation-driven growth strategies.

Analysis

- **Research and innovation:** Through the TIG plan, Singapore invests in cutting-edge research and innovation to stay ahead of emerging cybersecurity threats. The plan supports initiatives that encourage the development of new cybersecurity solutions and their application in different sectors. This approach promotes a culture of innovation and continuous improvement, ensuring that Singapore remains at the forefront of global cybersecurity.
- **Supply-chain risk management:** The CII supply-chain programme is a critical component of Singapore's cybersecurity strategy. It provides guidelines for managing risks within the supply chain of critical information infrastructure (CII). This programme is a living blueprint that evolves to tackle changing risks and outlines guidelines to support stakeholders in risk management and cyber contracts. It prioritizes international cooperation to support cyber-risk management in supply chains with international and regional partners, working towards harmonizing cybersecurity standards across jurisdictions.

Risk and security considerations

Singapore's multistakeholder approach addresses the complexities of managing cybersecurity risks in a rapidly changing technological landscape. By focusing on innovation and risk management, it ensures that its cybersecurity measures are robust and adaptive, capable of meeting the challenges posed by emerging technologies.

Impact assessment and strategic considerations

The impact of Singapore's cybersecurity strategy is evident in its strong global cybersecurity posture. The TIG plan and CII supply-chain programme work to contribute to raising baseline cybersecurity levels across industries, fostering innovation and promoting resilience. Singapore also focuses specifically on international collaboration and harmonization of cybersecurity standards as a mechanism to enhance its ability to address cross-border cyberthreats effectively.

Strategic way forward

Singapore continues to refine its multistakeholder approach to cybersecurity, focusing on promoting innovation, developing cybersecurity talent and enhancing supply-chain risk management. By strengthening its cybersecurity environment, it aims to maintain its position as a global leader in cybersecurity resilience.

5.2 Tech governance and derisking factors

Effective governance and risk management are essential for navigating the complexities of emerging technologies.

1. **Governance and regulatory frameworks:** Establishing robust governance frameworks to guide the responsible development and deployment of emerging technologies is critical to mitigating cybersecurity risks.

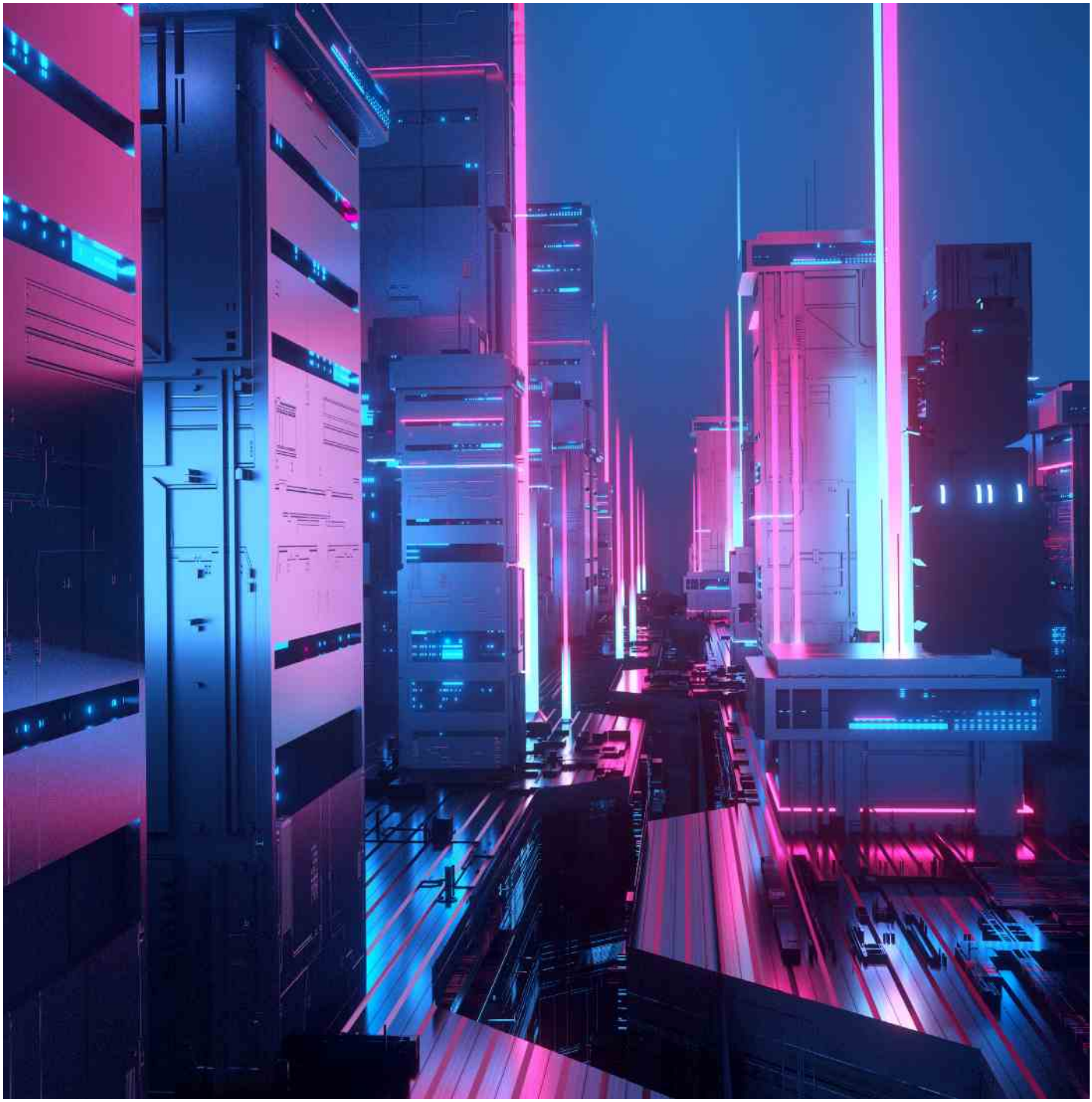
2. **Risk assessment and management:** Integrating risk assessment and management processes into the development life cycle of emerging technologies can help identify and mitigate potential cybersecurity threats early in the process.

3. **Continuous monitoring and adaptation:** Implementing mechanisms for continuous monitoring of emerging technology environments and adapting cybersecurity strategies in response to evolving threats is essential to maintain a strong security posture.

4. **Transparency and accountability:** Promoting transparency and accountability in the development and use of emerging technologies ensures that stakeholders are aware of potential risks and their responsibilities in managing them.

Conclusion: Practical recommendations for building a resilient and sustainable cyberspace

A proactive, collaborative approach is essential for promoting cyber resilience in the age of emerging technologies.



As society advances further into the digital age, emerging technologies such as quantum computing, blockchain, IoT, biotechnology, advanced materials and others are rapidly transforming industries and redefining societal norms. These technologies offer immense opportunities for economic growth, operational efficiency and societal advances.

However, the rapid development and integration of these technologies also comes with heightened cybersecurity risks, necessitating a shift from traditional "security by design" approaches to a more comprehensive "resilience by design" strategy. This shift recognizes that preventing all cyberthreats is increasingly unrealistic in a highly interconnected world. Instead, the focus must be on building systems and infrastructure that can withstand attacks, maintain critical functions and recover quickly from any disruptions.

To create a secure and resilient digital environment that takes full advantage of emerging technologies while mitigating risks, leaders in government, industry and academia should consider the following practical recommendations.

1. **Invest in research and development for resilience:** Continuously investing in research and development across various emerging technology domains is crucial for promoting innovation and enhancing cyber resilience. Establishing dedicated research centres focused on fields such as quantum computing, blockchain, IoT and biotechnology will build the expertise needed to develop resilient systems. This will ensure that new technologies are designed with inherent capabilities to detect, respond to and recover from cyberthreats.

2. **Encourage international collaboration for cyber resilience**: Building a resilient cyberspace requires collaboration beyond borders. International partnerships should be used to share knowledge, develop joint research projects and harmonize cybersecurity standards. Collaborative efforts will help create a global framework for technology and cyber governance, ensuring that emerging technologies are securely and ethically integrated worldwide.

3. **Integrate emerging technologies with resilient infrastructure:** Emerging technologies should be strategically integrated into critical infrastructure sectors such as energy, healthcare, finance and transportation. Technologies such as quantum-resistant cryptography, IoT-enabled predictive maintenance and blockchain-based security protocols can enhance the resilience of these sectors. Leaders should prioritize developing applications that bolster the integrity and reliability of critical infrastructure against cyberthreats.

4. **Develop data-driven frameworks for technology and cyber governance:** Establishing data-driven frameworks for technology governance is essential to manage the complexities of emerging technologies. Such frameworks should include clear metrics for evaluating technology readiness, impact assessments and risk management. Quantifiable measures of risk assessments, such as threat modelling and risk scoring, should be standardized across industries to ensure a consistent approach to assessing and mitigating cybersecurity risks.

5. **Enhance workforce development and capacity-building in cybersecurity:** Addressing the evolving cybersecurity landscape requires a skilled workforce equipped to handle the complexities of emerging technologies. Continuous education and training programmes focused on emerging technology security, such as quantum computing, IoT and biotechnology, should be developed. Building a robust talent pipeline is essential for maintaining a resilient cybersecurity posture and supporting sustainable innovation.

6. **Promote cross-sector collaboration to build comprehensive cyber resilience:** Collaboration among various sectors – government, industry, academia and civil society – is critical for developing holistic cybersecurity strategies. Cross-sector partnerships can develop comprehensive solutions that integrate diverse perspectives and expertise, enhancing resilience across all domains affected by emerging technologies.

7. **Implement ethical guidelines and responsible technology use:** As emerging technologies evolve, ethical considerations must be integrated into their development and deployment. Clear ethical guidelines should be established to govern the use of technologies such as AI, biotechnology and IoT, ensuring they are developed in a manner that upholds human rights, privacy and ethical standards. Ethical governance will foster trust and confidence in digital systems, which is crucial for sustainable cyber resilience.

8. **Leverage predictive analytics for proactive cyber defence**: Using predictive analytics and advanced monitoring tools can help organizations anticipate potential threats before they materialize, enabling pre-emptive responses and mitigation measures. Integrating these capabilities into cybersecurity strategies enhances resilience by ensuring that systems can adapt to evolving threats and maintain continuity in the face of cyber incidents.

9. **Promote resilient digital ecosystems through secure design principles:** Creating secure digital ecosystems involves adopting "resilience by design" principles, where security is built into every stage of technology development and deployment. This approach ensures that technologies are not only secure but also adaptive and capable of withstanding and recovering from cyberthreats. Organizations should prioritize the design of systems that can absorb attacks and continue to function, even in adverse conditions.

10. **Support the development of indigenous technologies and innovations:** To build a sustainable cyberspace, it is vital to develop indigenous research and development capabilities. Moving beyond merely adopting existing technologies, countries should focus on creating novel solutions tailored to local needs. This approach reduces dependency on external technologies and promotes local innovation ecosystems, contributing to national and economic resilience.

11. **Strengthen regulatory frameworks to manage emerging technology risks:** Developing flexible and adaptive regulatory frameworks is crucial for managing the risks associated with emerging technologies. These frameworks should promote security by design and resilience by design, balancing innovation with robust security measures. Policy-makers should work closely with technology developers to ensure regulations are both effective and conducive to promoting innovation.

12. **Promote start-up ecosystems to drive innovation in cyber resilience**: Start-ups play a crucial role in exploring new applications and driving technological disruption. Policies and initiatives should be developed to support emerging technology start-ups, providing access to funding, mentorship and innovation hubs. Encouraging a vibrant start-up environment can accelerate the development of resilient technologies and contribute to building a sustainable cyberspace.

13. **Use energy-efficient approaches in technology development:** The development and deployment of emerging technologies should consider energy efficiency to minimize the environmental impact. Integrating technologies with renewable energy initiatives and adopting green computing practices (for example, programmes that focus on e-waste reduction, responsible disposal and extending the lifespan of hardware) can enhance sustainability while maintaining high performance, aligning with global efforts to reduce carbon footprints and promote sustainable development.

14. **Implement continuous monitoring and incident response planning:** Organizations should establish robust monitoring systems and incident response plans to detect and respond to cyberthreats promptly. Continuous monitoring and regular updates to incident response plans are essential to address the dynamic threat landscape, ensuring that organizations can recover quickly from cyber incidents and maintain operational continuity.

15. **Promote transparency and accountability in cybersecurity practices:** Building trust in emerging technologies requires transparency and accountability in cybersecurity practices. Organizations should communicate openly about their cybersecurity measures, risks and responses to incidents. Transparent governance practices build confidence in digital systems and encourage the responsible adoption of emerging technologies.

Creating a resilient and sustainable cyberspace in the evolving landscape of emerging technologies requires a multifaceted approach that integrates security, resilience, sustainability and quantifiable risk measurements into all aspects of technology development and deployment. By adopting these practical recommendations, leaders can enhance cyber resilience, promote responsible innovation and build a secure digital future. This approach emphasizes the importance of international collaboration, ethical governance, data-driven frameworks and continuous improvement in navigating the complex digital landscape. Prioritizing resilience by design, investing in workforce development and supporting local innovation ecosystems are key to ensuring that emerging technologies contribute positively to global cybersecurity efforts while minimizing the associated risks.

Contributors

Lead Authors

Hoda Al Khzaimi
Director, Centre for Cybersecurity, New York University Abu Dhabi, United Arab Emirates

Gretchen Bueermann
Knowledge Lead, Centre for Cybersecurity, World Economic Forum, Switzerland

Additional Contributors

Bushra AlBlooshi
Senior Consultant, Research and Innovation, Dubai Electronic Security Center (DESC), United Arab Emirates

Christophe Blassiau
Senior Vice-President, Cybersecurity & Product Security, Global Chief Information Security Officer and Chief Product Security Officer, Schneider Electric, France

Chua Kuan Seah
Deputy Chief Executive, Cyber Security Agency of Singapore (CSA), Singapore

J. Michael Daniel
President & Chief Executive Officer, Cyber Threat Alliance, USA

Dorit Dor
Chief Technology Officer, Check Point Software Technologies, Israel

Cathy Foley
Chief Scientist, Australian Government, Australia

Öykü Işık
Professor, Digital Strategy and Cybersecurity, IMD Business School, Switzerland

Yurie Ito
Founder and Executive Director, CyberGreen Institute, USA

Andreas Schmitt
Global Manager, Cyber Underwriting, Zurich Insurance Company, Switzerland

Vikram Sharma
Founder and Chief Executive Officer, QuintessenceLabs, Australia

Rob Wainwright
Group Chief Information Security Officer, UBS, United Kingdom

Wendi Whitmore
Senior Vice-President, Unit 42, Palo Alto Networks, USA

Production

Michela Liberale Dorbolò
Designer, World Economic Forum

Alison Moore
Editor, Astra Content

Endnotes

1. Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey Global Institute. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/disruptive-technologies; Accenture. (2023). *Technology vision 2023: When atoms meet bits: The foundations of our new reality*. https://investor.accenture.com/~/media/Files/A/Accenture-IR-V3/investor-toolkit/accenture-technology-vision-2023-full-report.pdf
2. National Institute of Standards and Technology (NIST). (2024). *Post-quantum cryptography standardization*. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization; IBM. (n.d.). *What is quantum computing?*. Retrieved September 18, 2024, from https://www.ibm.com/topics/quantum-computing; Accenture. (2023). *Think beyond ones and zeros*. https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-54/accenture-807510-quantum-computing-rgb-v02.pdf
3. United Nations Web TV. (2023). *Day 3 Morning Session: Emerging technology and cybersecurity risks*. United Nations Open-ended Working Group (OEWG) on ICT Security; Open-Ended Working Group on Information and Communication Technologies. (2024). *Letter from OEWG Chair – 11 July 2024*. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_11_July_2024.pdf
4. Statista. (2024). *Number of internet of things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033.* https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
5. European Commission. (2024). *Strategic Technologies for Europe Platform (STEP)*. https://strategic-technologies.europa.eu/index_en; European Union. (2024). *A strategy for research on future and emerging technologies in Europe*. https://eur-lex.europa.eu/EN/legal-content/summary/a-strategy-for-research-on-future-and-emerging-technologies-in-europe.html; European Commission. (2024). *White paper on enhancing support for research and development involving technologies with dual-use potential*. https://research-and-innovation.ec.europa.eu/document/download/7ae11ca9-9ff5-4d0f-a097-86a719ed6892_en; European Commission. (2022). *Digital path to recovery and resilience in the European Union*. https://joinup.ec.europa.eu/sites/default/files/news/2022-03/Report_Digital%20path%20to%20recovery%20and%20resilience%20in%20the%20European%20Union.pdf
6. United Nations Conference on Trade and Development (UNCTAD).(2021). *Technology and Innovation Report 2021*. https://unctad.org/publication/technology-and-innovation-report-2021#:~:text=The%20report%20also%20calls%20for,impact%20of%20frontier%20technologies%20on; United Nations Conference on Trade and Development (UNCTAD). (2023). *Trade and Development Report 2023*. https://unctad.org/tir2023
7. Gartner. (2023). *Forecast: Information security and risk management, worldwide, 2021–2027, 4Q23 Update*. https://www.gartner.com/en/documents/4488199
8. European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
9. Muggah, R., & Margolis, M. (2023, January 2). *Why we need global rules to crack down on cybercrime*. World Economic Forum. https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/
10. Deloitte. (2019). *Navigating regulatory change for emerging technologies: Future of risk in the digital era*. https://www2.deloitte.com/us/en/pages/advisory/articles/regulatory-change.html
11. ISC2. (2023). Cybersecurity workforce study 2023: *How the economy, skills gap and artificial intelligence are challenging the global cybersecurity workforce*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
12. Statista. (2024). *Number of internet of things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
13. Brown, R. (2024, February 27). *Zero Trust Industry Days 2024 Scenario: Secluded Semiconductors, Inc*. Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/library/zero-trust-industry-day-2024-scenario-secluded-semiconductors-inc/
14. A 51% attack happens when someone gains control of more than half of a cryptocurrency's network. With this much power, they can change the blockchain and cheat the system.
15. Conti, M., Sandeep Kumar, E., Lal, C., & Ruj, S. (2010). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452. https://ieeexplore.ieee.org/document/8369416
16. National Institute of Standards and Technology (NIST). (2024). *Post-quantum cryptography standardization*. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization; IBM. (n.d.). *What is quantum computing?*. Retrieved September 18, 2024, from from https://www.ibm.com/topics/quantum-computing
17. World Economic Forum. (2024). *The global risks report 2024*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
18. National Library of Medicine. (2022). Emerging threats of synthetic biology and biotechnology: Addressing security and resilience issues. https://www.ncbi.nlm.nih.gov/books/NBK584259/; Sanz, J. A., Dunlap, G., Nolan, N., & O'Leary, C. (2022). Biosecurity risks and governance in the age of synthetic biology. *MIT Science Policy Review*, *3*, 136. https://sciencepolicyreview.org/wp-content/uploads/securepdfs/2022/08/MITSPR-v3-191618003014.pdf

19. U.S. Department of Energy. (2024). *AI for energy: Opportunities for a modern grid and clean energy economy*. https://www.energy.gov/sites/default/files/2024-04/AI%20EO%20Report%20Section%205.2g%28i%29_043024.pdf; World Economic Forum. (2024). *Nuclear fusion news: The science behind the energy technology, explained*. https://www.weforum.org/agenda/2024/02/nuclear-fusion-science-explained/; World Energy Council. (2019). *Cyber challenges to the energy transition*. https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC_MMC_2019.pdf

20. Virgili, B.B., Dolado, J.C., Lewis, H.G., & Metz, M. (2016). Risk to space sustainability from large constellations of satellites. *Acta Astronautica*, 126, 154–162. https://www.researchgate.net/publication/301759630_Risk_to_space_sustainability_from_large_constellations_of_satellites; World Economic Forum. (2024). *Space: The $1.8 trillion opportunity for global economic growth*. https://www3.weforum.org/docs/WEF_Space_2024.pdf; Manulis, M., et al. (2021). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security, 20(3)*. https://researchgate.net/publication/341331628_Cyber_security_in_New_Space_Analysis_of_threats_key_enabling_technologies_and_challenges

21. Sunwoo, S. H., et al. (2020, December 2). Advances in soft bioelectronics for brain research and clinical neuroengineering. *Matter*, 3(6), 1923-1947. https://doi.org/10.1016/j.matt.2020.10.020

22. For more information, see: IBM. (2024, June 27). *What is neuromorphic computing?*. https://www.ibm.com/think/topics/neuromorphic-computing?mhsrc=ibmsearch_a&mhq=IBM%26period%3B%20%26quot%3BWhat%20is%20neuromorphic%20computing%26quest%3B%26quot%3B

23. Benestelli, B., & Kambic, D. J. (2022, July 18). *IT, OT, and ZT: Implementing zero trust in industrial control systems*. Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/blog/it-ot-and-zt-implementing-zero-trust-in-industrial-control-systems/

24. Dubai Electronic Security Center. (n.d.). *RZAM Web Extension*. Retrieved September 17, 2024, from https://desc.gov.ae/rzam/index.html

25. Digital Dubai. (n.d.). *Dubai Blockchain Strategy*. Retrieved September 17, 2024, from https://www.digitaldubai.aeinitiatives/blockchain

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org