In collaboration with the University of Oxford

WORLD ECONOMIC FORUM

Future Series:

Cybersecurity, emerging technology and systemic risk

INSIGHT REPORT

NOVEMBER 2020

In collaboration with the University of Oxford

Future Series: **Cybersecurity, emerging technology and systemic risk**

The Future Series report was a joint venture between the World Economic Forum and the University of Oxford. It was designed to convene a range of experts in the field to discuss and research the issues arising from critical emerging technologies. The programme involved interviews, workshops and research, and this is the final output in the series.

This report has been produced in collaboration with the University of Oxford Global Cyber Security Capacity Centre (GCSCC) and its research sponsor AXIS Capital. The World Economic Forum would like to thank the University of Oxford and the Centre for Cybersecurity community, including its founding partners Accenture, Palo Alto Networks, Sber Bank, Fortinet, Saudi Aramco and Salesforce for their contributions to this programme.

Contents

Foreword

In less than a decade since cybersecurity first featured in the Global Risks report, it has emerged as one of the most important systemic issues for the global economy. Collective global spending has now reached $145 billion a year and is predicted to exceed $1 trillion by 2035. The Future Series: Cyber 2025 was launched at the World Economic Forum Annual Meeting on Cybersecurity in 2019 to answer a single question:

Will our individual and collective approach to managing cyber risks be sustainable in the face of the major technology trends taking place in the near future?

This programme brought together more than 100 leading experts from businesses, government, academia and civil society. Through a series of workshops and structured interviews, the participants examined four technologies that will transform the global digital landscape in the next 5–10 years: ubiquitous connectivity; artificial intelligence (AI); quantum computing; and next-generation approaches to identity management. These interactions underpinned the research presented here, which offers insights into the future challenges we face.

The work concluded that, while progress has been made in improving cybersecurity across the ecosystem, the increased complexity, pace, scale and interdependence shown by our forward look at technological trends will overwhelm many current defences. Without interventions now, it will be difficult to maintain the integrity of and trust in the emerging technology on which future global growth depends.

The recommendations made in this report are far-reaching and will require concerted effort from technologists, industry leadership and the international community. The rewards will be significant. These technologies will transform our world – but only if they are secure and we can give our citizens and businesses confidence that they are so.

Sadie Creese
Professor of Cyber Security, Department of Computer Science, University of Oxford

Jamie Saunders
Oxford Martin School Fellow, University of Oxford

Louise Axon
Research Associate in Cybersecurity, University of Oxford

William Dixon
Head of Future Networks and Technology

Executive summary

Our forward look at technology trends shows a picture of increased complexity, pace, scale and interdependence. The emerging technology environment will overwhelm many of the risk mitigations that are currently deployed. Without interventions now, it will be difficult to maintain the integrity of and trust in the emerging technology on which future global growth depends. Our analysis shows that:

CONCLUSION 1

Systemic risks

There are hidden and systemic risks inherent in the emerging technology environment, which will require significant changes to the international and security community response to cybersecurity. Policy interventions are required that incentivize collaboration and accountability on the part of both businesses and governments.

CONCLUSION 2

Capability gaps

There are gaps in the current operational cybersecurity approaches that need to be addressed. Defending ourselves against evolving threats requires new cybersecurity tools, as well as an understanding of how to effectively deploy these new solutions, at pace, throughout global systems. The attack surface associated with new technology use needs to be addressed. Policy that incentivizes higher standards of care in technology and service delivery is needed.

CONCLUSION 3

Leadership action

Business leaders need the ability to plan more strategically for emerging risk so they can ensure that the organizations delivering the most critical infrastructures do not suffer failures that are catastrophic for societies.

Managing cyber risk within organizations is already a major leadership challenge. The costs for enterprises are increasing – building and maintaining cybersecurity capability is expensive, and the return on investment is uncertain. The risks associated with cyberthreats are often opaque, and it is difficult to calibrate the right nature and scale of investment in cybersecurity. Regulatory requirements are increasing and are often different among jurisdictions, and there is a risk that divergent approaches to tackling cybersecurity will act as a strategic barrier to cross-border data flow and e-commerce. Current approaches to supply-chain cybersecurity assurance are broken: Friction is being introduced by the need to provide security attestation, which does not necessarily give the level of assurance required, thus diverting resources away from more effective cybersecurity capacity investments.

These challenges are exacerbated by the continued failure of the community to tackle the problem at source. Many incidents are caused by a small number of cybercrime groups that face limited consequences for their actions. There is still a lack of credible deterrence.

There must now be a paradigm shift in the approach to cybersecurity. Enterprise leaders need to think in terms of assuring the integrity and resilience of the interconnected business and social processes that sit on top of an increasingly complex technology environment – rather than cybersecurity being simply an issue of protecting systems and networks. Organizations need to keep abreast of how new technologies will affect their exposure to cyber risk and ensure that the necessary mitigations are put in place to keep risk within a tolerable and sustainable level. Ensuring that organizations have the visibility and insight to do this is a major challenge.

Action at the individual enterprise level alone will not, however, be enough to tackle the range of complex ecosystem-wide challenges that were identified in the report. The conclusion of the Future Series is that the emerging cybersecurity risks will not be a simple continuation of current challenges, and incremental progress will not be sufficient to address them. The nature of the change in the technology environment is such that growing systemic risks will emerge, for which new collective action will be required:

- First, the **security and technology community** needs to prioritize a number of interventions to improve the collective response that will be essential to cybersecurity operations and controlling cyber risk effectively within business and critical national infrastructures. These are described below.

- Second, **industry and government leadership** need to drive a set of policy actions that incentivize take-up of security solutions, and that underpin greater trust and transparency between different components of the ecosystem: to clarify issues of liability; to reduce friction in current assurance and regulatory models; and to promote international business and trade in data and digital services.

- Finally, interventions are required from the **international community** to ensure that security issues are addressed in such a way that the benefits of emerging technology are inclusive, with particular regard to the needs of developing countries and the need for collective efforts to reduce cross-border cybercrime.

The analysis considered four representative transformative technologies that will contribute to the changing dynamics of cyberspace: ubiquitous connectivity; artificial intelligence (AI); quantum computing; and next-generation approaches to identity and access management. We do not claim that this is the complete set of technology innovations that will define the future, nor that they illustrate all of the risks faced. However, the technologies chosen are sufficiently representative to illuminate the range of risk that the community is likely to face in the next 5–10 years.

Below are the key interventions recommended to address the systemic issues and to enable the management of cyber risks in the near future. If these collective actions cannot be taken forward, the global community risks creating an ecosystem that is not resilient to the emerging threat landscape, where cybersecurity could become a barrier to unlocking the full potential of technology and cyberspace.

Security and technology community

The community needs to collaborate to identify the emergent gaps that are opening up in defensive operational capabilities and design, develop and deliver effective solutions:

1. New models and enriched information-sharing frameworks need to be developed to deliver situational awareness and facilitate real-time and automated defence in the face of increasingly complex technology environments. These need to be effective across national boundaries as well as throughout supply chains, recognizing divergent national security and regulatory regimes, and must be respectful of personal privacy.

2. Security principles and tools need to be developed to protect AI and advanced machine learning assets, and in tandem protect the privacy of individuals where personal data is being processed.

3. The community needs to convene to develop the security model for quantum computing that encompasses the integrity of algorithms and the secure integration of quantum into hybrid computing environments.

Actions are required to identify which parts of the ecosystem have an individual and collective dependence on cryptography, in addition to other security functions that rely on the complexity of computation, which is potentially threatened by quantum computing. This will require urgent action, both to identify the systemic nature of the risk and also to govern the management of it.

4. There needs to be a convening of security and business experts to establish how the quantum cryptography issue will affect end-to-end distributed business processes and who should take responsibility for mitigating the risk.

Capacity in the workforce will need to be developed to ensure that new approaches to operational defence can be delivered across the ecosystem.

5. Existing cybersecurity skills and education programmes need to be reviewed and enhanced to ensure that they reflect the impact of emerging technologies. These need to be made available globally.

The technical and security community needs to promote security standards that can help ensure interoperability throughout the enterprise functions, including not only technology standards but also regulatory standards. This is true for all systems, but is most pressing in the digital identity environment due to its heterogeneous and distributed nature, and the need to ensure trust and privacy throughout the systems.

6. Global interoperability trust standards for next-generation digital identity systems are required that enable projection of trusted identity and personal privacy across heterogeneous systems and jurisdictions in order to support trade.

Industry and government leadership

New education, guidance and governance tools are required for enterprise leadership to address the security impact and risk associated with the use of emergent technology within their organizations and in the wider operational environment. This is essential in order to enable leaders to promote an agenda of increased and meaningful security, and to ensure solutions are developed that protect organizations and better prepare leaders for when significant incidents occur.

7. Enterprise leaders need tools for making decisions on how best to prepare for emerging risks. Greater transparency over incidents and their impacts will improve leaders' collective response.

The increasing entanglement of businesses and supply-chain interdependencies – as well as the growing regulatory and related security attestation processes – is creating an urgent need to deliver a mechanism for ensuring trustworthy and reliable

organizational cybersecurity behaviours to underpin confidence across different components of the ecosystem. This is most pressing in areas where there is increasing shared reliance on infrastructure, such as major cloud and shared service providers. This will require the identification of gaps in incentive models and interventions to address them.

8. New and internationally applicable methods for security attestation are required to make governance cost-effective and meaningful. Standard-of-care models will need to be developed to support this and to underpin general confidence in supply chains.

9. Business will need to work with regulators and policy-makers to consider and promote clear responsibility and liability models. These need to be able to operate across international boundaries in order to support trade and reduce unnecessary friction.

10. Regulations and attestations need to reflect the dynamic real-time nature of the underlying technology and risk environment.

International community

The international community needs to develop policy interventions to ensure a level of cybersecurity capacity that will enable global inclusivity. Capacity needs to span all dimensions of cybersecurity, such that cybersecurity does not act as a strategic barrier to the wider adoption of technology and its potentially transformative value to the global economy. The capacity requirements include the need to maintain a skilled workforce and establish assured access to the more complex cyber-defensive capabilities.

11. Countries need to collaborate to provide equitable access to cybersecurity capacity. Frameworks should be developed for identifying national cybersecurity capacity in response to emerging risks, and policy interventions adopted to ensure strategic investments in such capacity can be made. An emerging technology risk register would assist in this process.

Collective action against the known cybercrime groups needs to be significantly enhanced and interventions designed to close the gaps in collective investigation in order to promote more robust deterrence models for malicious behaviour in cyberspace.

12. Greater emphasis should be placed on the attribution and disruption of threat actors behind cybercrime. This requires increased collaboration between countries, international bodies and the technology businesses that deliver the underpinning infrastructure.

13. International capacity and commitment to combating cybercrime (and other related threats to the integrity of the global digital economy) should be strengthened by the establishment of standards and the effective promotion of legal, regulatory and operational measures.

There are increasing cross-border and cross-sectorial interdependencies between different components of national and international critical infrastructure.

14. An internationally consistent approach to the identification of critical national infrastructure components is required in order to ensure that cross-border risk aggregation is not hidden, and that systemic risk in cyberspace can be properly identified and prepared for.

15. International specialist trade bodies should develop the capacity for identifying emerging technology risks to their sectors and membership communities.

Cyberspace dynamics

01

The dynamics of cyberspace are changing

The nature of the digital systems we are creating today represents a significant evolution away from the technology of the past – where we could design systems with a clear scope and function. Our future will see a cyberspace underpinned by technologies that together form a platform for innovation whose structure, components, relationships and processes are constantly changing to support emerging ideas, services and business needs.

As a result, the underlying dynamics of cyberspace are changing:

Scale: Cyberspace is growing rapidly, as new connected devices, networks, services and data emerge. This brings changes in the scale not only of networks, but also of data volumes, storage capacity, processing systems and the knowledge space that we collectively create. The scale of cyberspace is already difficult for most to conceptualize.

Speed: Communications and data-processing can be carried out at an ever-accelerating pace, and this enables a speeding up of business transactions and processes, relationship creation, publishing and sharing of content and ideas, and generation of value. The change in pace is so substantial that it may mean current forms of management for our relationships, content, image and processes are too slow and no longer fit for purpose.

Interconnectivity: There is an increasing level of interconnectivity of systems and interdependence of actors across cyberspace, throughout organizations and supply chains.

Dynamism: Together these changes result in a fundamental shift in the dynamism with which we experience cyberspace. Many feel that that is so complex, with increasingly sophisticated characteristics, that our role will change so that we become observers of a system increasingly outside our control.

New technology brings significant opportunity

Business and government have understood the potential of technology for many years, and are engaged in ongoing programmes of digital transformation. This will now feel like a continuous journey – no longer a project with a clear end point, but rather a move towards embracing a constant level of technology change within the core of our organizations. This brings opportunity, and the World Economic Forum will continue to help business deliver that opportunity.

It has been clear for some time that technology will critically underpin solutions to key global challenges.[1] [2] [3] [4] Furthermore, we can expect significant progress to be made in the areas of health, carbon footprint reduction, delivering new economic opportunities to the poorest nations, farming in order to feed the world's population, and making our public and critical infrastructures safer and more efficient.

This report focuses on four representative transformative technologies that will contribute to the changing dynamics of cyberspace. We do not claim that this is the complete set of technology innovations that will define our futures, nor that they illustrate all the risks we face. However, they are sufficiently representative to illuminate the range of risk we are likely to face in the next 5–10 years.

Four transformative technologies

1. **Ubiquitous connectivity:** Devices, networks and services are increasingly hyperconnected and interdependent, operating on sophisticated shared infrastructures. Factors such as the speed, reliability, low latency, agility and *intelligence* of communications architectures are leading to significant changes in the way in which they are used and relied upon pervasively throughout our environments.

2. **Artificial intelligence/advanced machine learning:** As it becomes possible to automate increasingly sophisticated calculations, activities can be carried out in cyberspace faster and on a larger scale – and most importantly, using huge datasets for training. The ability to aggregate and process such data will lead to huge increases in the predictive powers of algorithms.

3. **Quantum:** Quantum computers will demonstrate an advantage over classical computers in solving a range of computational and modelling problems (although predictions of the timelines on which this will happen vary). Some problems may become tractable for the first time, enabling new functionalities and presenting new risks to conventional security measures.

4. Emerging next-generation approaches to **identity and access management** will enable new services, applications and operating models, with efficiency and low friction that can support the fast speed and large scale of the emerging cyberspace.

We reflect on the question of whether current approaches to cybersecurity and cybercrime will cope with these new innovations – *will our individual and collective approach to managing cyber risks be sustainable in the face of the major technology trends taking place in the near future?*

Opportunities emerging tech brings to the world

Environment

Digital technologies could help reduce the global carbon footprint. Energy delivery will be optimized through smart grids, while instrumentized urban environments (smart cities), industrial processes, and transport and logistics systems will operate more efficiently and produce less waste.[5 6]

Safety

Advances in robotics are creating opportunities to remove humans from hazardous environments (e.g. in manufacturing) and to remove human error from safety-critical decisions. Advances in sensing and analytics could help predict natural disasters.[7 8 9]

Health

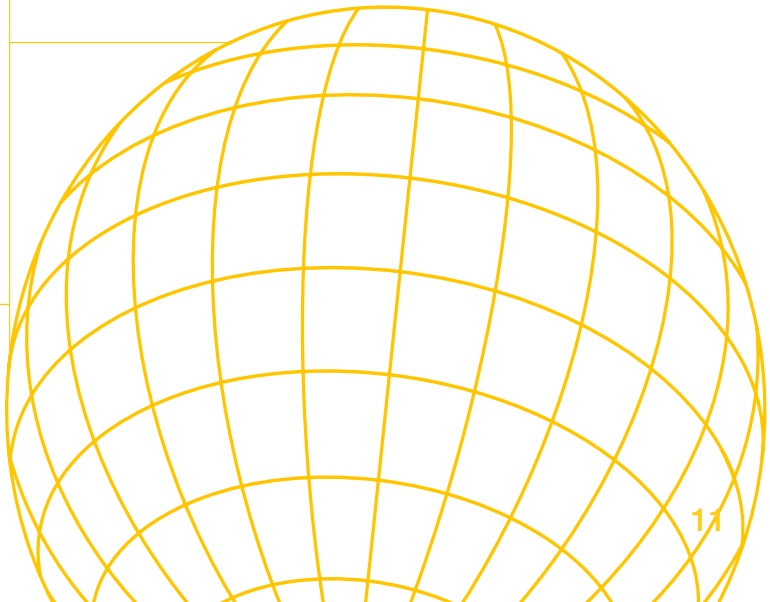
The delivery of healthcare will be revolutionized, with the potential for more effective, accessible and personalized treatment, and accelerated drug discovery.[10]

Feeding humanity

Precision agriculture and instrumenting for farming in extreme environments could help to sustainably feed the rapidly growing global population.[11 12]

Global economy

Efficient manufacturing in the Fourth Industrial Revolution will increase productivity, and new economic opportunities and means of data exploitation will arise. Emerging technologies have the potential to improve financial inclusion and economic development worldwide.[13 14]



Key systemic risks and challenges

02

Hidden cyber-resilience deficit

Whenever new technology is introduced, it has the potential to change the risks organizations face. The nature of risk and resulting harms is such that they can propagate through systems and supply chains.

Changing the risk equation

Increased and evolving threat

Amplified speed and scale
(attack automation, speed of computation and communications)

Broader range of threat actors
(high value creates threat interest, automation means less expertise needed)

New opportunities
(deepfakes, quantum computers, disruptive applications of tech)

Stealth
(self-evolving malware)

Widening attack surface

Systems
(adoption of new technologies by industry, scale-up of IoT devices and systems)

Increasingly shared
(high-value shared infrastructure and resources)

Data
(generated by device scale-up, "big" datasets for AI training, long lifespans of sensitivity)

New attack vectors
(insecure technologies, unauthorized access, outsourcing risks)

Structural weaknesses

Opacity
(reduced human oversight, reduced visibility of entangled supply chains, undetected manipulation of algorithms)

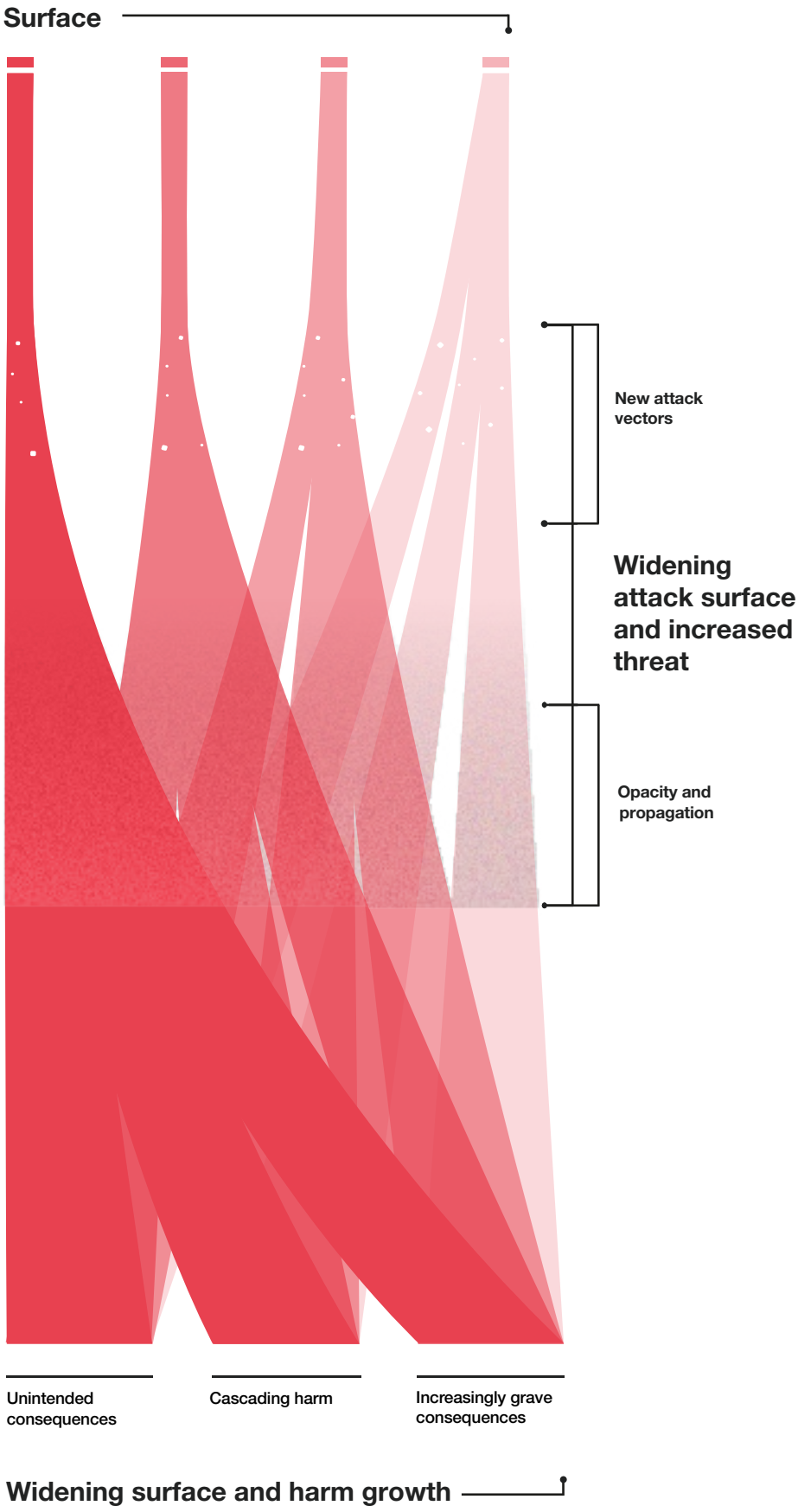
Propagation of threat through attack surface
(e.g. Propagation of malicious code due to connectivity)

Growth in harm

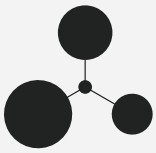
Increasingly grave consequences
(critical applications of technologies, cyber-physical safety)

Cascading harm
("monoculture" of providers, interdependencies between sectors)

Unintended consequences
(undetected algorithmic biases, resource contention in shared infrastructure)

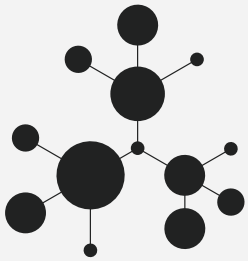


While organizations have had a level of digital interdependence for years, the emerging dynamics of cyberspace are increasing their interdependence and mutual reliance on the digital environment, thus creating multiple possible sources of systemic risk, which in the future may mean that supply chains and sectors will experience risk propagation at levels and speeds not previously witnessed:



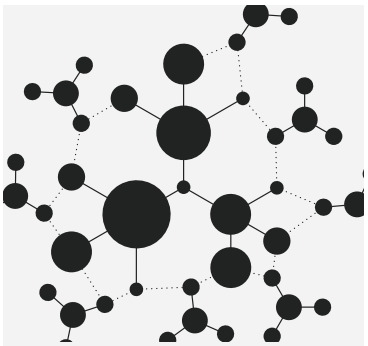
Level 1

The pervasiveness of a particular technology or vendor throughout economies could mean that cyberattacks can successfully penetrate high numbers of organizations almost simultaneously. This could result in incidents and related losses occurring within a short period of time and spanning multiple supply chains.



Level 2

Interdependencies between organizations are growing, as organizations increase their reliance on shared technology-service providers and supply chains. This means that the impacts of a cybersecurity failure in one organization have the potential to cascade across its dependent organizations with systemic consequences.



Level 3

Cybersecurity failure could be systemically catastrophic to economies and societies, as cyber harms have the potential to cascade through a widening scope of critical functions across industrial and critical infrastructures. Multiple heterogeneous sectors could fail, leaving no alternative providers while systems are recovered.

It is a fact that even today many organizations can find themselves unknowingly dependent on components of the ecosystem due to a lack of transparency downstream and upstream in supply chains. Without intervention, this may simply grow in complexity: Dependencies will become increasingly unmanageable and opaque as the ecosystem becomes more entangled. This means that it will not be possible to account for the aggregation of cyber risk, and where there is a lack of resilience within organizations, we may be developing a growing and hidden cyber-resilience deficit.

The COVID-19 pandemic already accelerated the adoption of collaboration and cloud technologies as the world rapidly scaled up home working, and is likely to accelerate the development of other emerging technologies, e.g. remote healthcare. This could lead to greater critical dependency on internet-based technologies, and possibly heighten the cyber-resilience deficit where cybersecurity capacity is insufficient.

Five emerging challenges to securing the digital ecosystem

As systemic risk grows, organizations can no longer simply consider their own individual capabilities in order to ensure cybersecurity and resilience. As organizations become increasingly mutually dependent on each other, the resilience and security of the wider ecosystem begins to matter critically to them. Failure to ensure resilience and security in one part will affect others with increasingly harmful consequences, and the sources of this risk could be increasingly hidden.

It is therefore in the interests of participants to come together to address the systemic risk to the ecosystem as a whole. This means ensuring that the baseline level of cybersecurity and resilience is sufficient, and that risk aggregation can be identified and monitored within end-to-end services and supply chains, as well as shared infrastructures. The community faces a number of key challenges, which will need to be addressed through collective action.

1. **Widening cybersecurity skills gap:** There is already a global capacity shortage in cybersecurity (both specialists and across the wider workforce), and as new technologies emerge, the existing skills gap in delivering cybersecurity is likely to grow. Unless education and training are accelerated significantly, the workforce will not have the necessary cybersecurity capacity and mindset. A lack of cyber literacy among leaders and innovators will prevent appreciation of the risks to organizations and the ecosystem, and prevent the necessary investments being made for cyber resilience.

2. **Fragmentation of technical and policy approaches:** Emerging technologies are driving an increasing interdependence and entanglement at a time when global governance of cyberspace is weak. Many of the relevant technical standards and governance principles are divided into jurisdictional and sectoral siloes. There is a risk of further divergence at the public policy level; geopolitical divergence and protectionist stances make this difficult to reconcile. A lack of interoperability at a governance level could lead to: a failure to realize the potential value of a secure global digital ecosystem: incompatible security-compliance requirements; and suboptimal (and thus costly) security in parts of the ecosystem.

...it will not be possible to account for the aggregation of cyber-risk, and where there is a lack of resilience within organisations, we may be developing a growing and hidden cyber-resilience deficit.

3. **Existing operational-security capabilities and technologies not fit for purpose:** Mitigating threats and responding to incidents individually and collaboratively will require new approaches. Existing operational capabilities are not sufficient technically to address new technologies and data formats and will not deliver the pace and scale of collaborative operations (including information sharing, collective response, and detection, disruption and deterrence of cybercrime) that will be needed to address the emerging risks. There is a need to increase the level of automation within cyber-defence capabilities, ensure that the cybersecurity tools developed can interoperate effectively, and support enriched intelligence sharing at the pace necessary to address emerging threats.

4. **Underinvestment in support (knowledge, guidance, research investment) and incentives (market forces, regulation) for developing emerging technologies securely:** Security is not being considered an integral component of technology innovations. This means it is likely that technologies will be developed with little or no consideration for malicious threats, as has happened in the past. Without the right incentives to prevent this, there is a risk of insufficient security functionality and later costly retrofit. Further, the complexity of supply chains and systems may mean that innovators will make false assumptions about the security inherent in the systems upon which their solutions are layered, causing hidden risk. This hidden risk may also manifest where organizations exploit machine learning without an ability to determine the integrity of and absence of bias in the algorithms.

5. **Ambiguous accountability:** While shared dependence widens the pool of actors affected by the resilience of a part of the ecosystem, it can also create ambiguity in the accountability for ensuring this resilience. Complexity and entanglement are exacerbating a lack of clarity about accountability and where the liability lies for assuring end-to-end services and shared critical infrastructures. Risk transfer (e.g. via contracts or via tech E&O [errors and omissions] insurance) cannot cover the full scope of sideways exposure.

It is therefore in the best interests of leaders to instigate, now, initiatives that will ensure the resilience and security of the wider ecosystem. This is where the calls to action made in this report are focused. If the emerging challenges are not addressed globally, in a way that creates sufficient assurance, transparency and trust, and that is globally interoperable (in terms of both technical solutions and governance principles), there is a danger that:

- The world will end up reliant on a digital ecosystem that is not resilient to the emerging systemic threat and risk landscape
- The full potential benefits of the global digital ecosystem may not be realized

Information-sharing challenges

Information sharing is an important part of collaborative operational security, increasingly important for addressing growing systemic risks. By sharing information on the threats targeting them, indicators of compromise and responses, organizations can collectively improve their defence capabilities and raise the cost of cybercrime for attackers. Information-sharing challenges already exist – technical challenges, and issues about privacy and IP retention. This area is about to become even more challenging:

New types of information

Need codified methods of communicating and sharing information about AI attack and defence algorithms (especially given that they evolve based on data input) and their outputs

Biometrics and behaviour-based information – signals that are newer and less well understood

Speed and scale

Addressing high-speed, large-scale threats will need timely sharing of information on a large scale.

Existing models (e.g. ISACs) may not scale to meet the demands of increasingly interdependent and complex environments

Distribution of actors

Need to share with potentially distributed sets of actors (between which there could be trust deficits)

Existing models (e.g. ISACs) may not scale to meet the demands of increasingly interdependent and complex environments

Scale of data

Need to extract relevant information from increasing volumes of data

Possible solution

Emerging tech may form an important part of the solution, e.g. automated approaches to information sharing are seeing increasing use.

Insurance challenges

Emerging technologies and systemic risks are creating growing challenges for insurers in assessing the risk exposure of organizations, underwriting aggregated losses across industries and understanding the total risk exposure of an insurance portfolio.

Ubiquitous connectivity

03

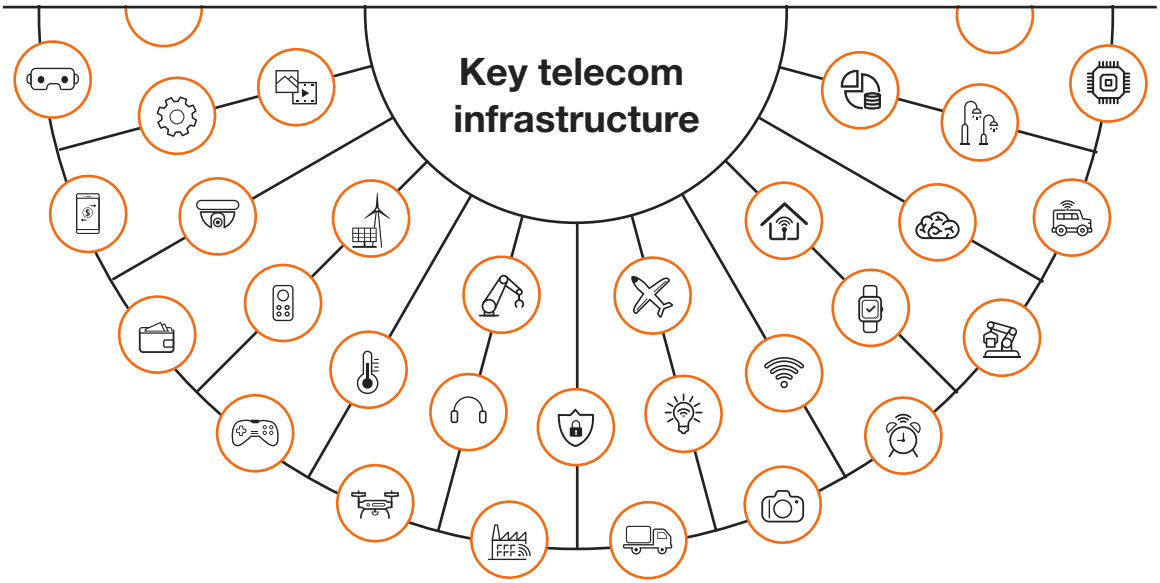
The rapid increase in the number of connected devices and networks on a global scale means that relationships across the digital ecosystem have become increasingly intertwined. From a security perspective, this brings about a number of challenges; in particular, how can organizations receive clarity and assurance on the security of the digital foundations of many of their operations from end to end? This is also relevant for governments, which increasingly rely on digital systems for many of their critical infrastructures and services.

A more holistic approach is urgently required that considers the resilience of the ecosystem as a whole. Greater coherence and consistency are needed in terms of security requirements and standards, with increased collaboration across the vast number of actors in the global ecosystem.

Interdependence arising from ubiquitous connectivity

In recent years, the number of internet-connected systems and devices has grown significantly. The smartphones, wearables and smart-home devices of individuals are improving the user experience. Industry has begun to exploit the opportunities that data-sensing, mobile communications and increasing automation in control systems bring to derive efficiency and new service opportunities. The scale of digitization is bringing about ubiquitous connectivity, with a rapid acceleration in the scale, pace and complexity of the resulting systems – often referred to as the internet of things (IoT).

A core component of this emerging communications and computational environment is the 5G technology that will enable significantly faster and more reliable mobile communications for a substantially greater number of devices. Associated shifts in communications and analytics architectures (network virtualization, slicing and seamless roaming, and edge computing)[15] [16] [17] promise agile and tailored networks with unparalleled computational power and analytics supported by the cloud. Such technologies are being piloted and rolled out across the world.

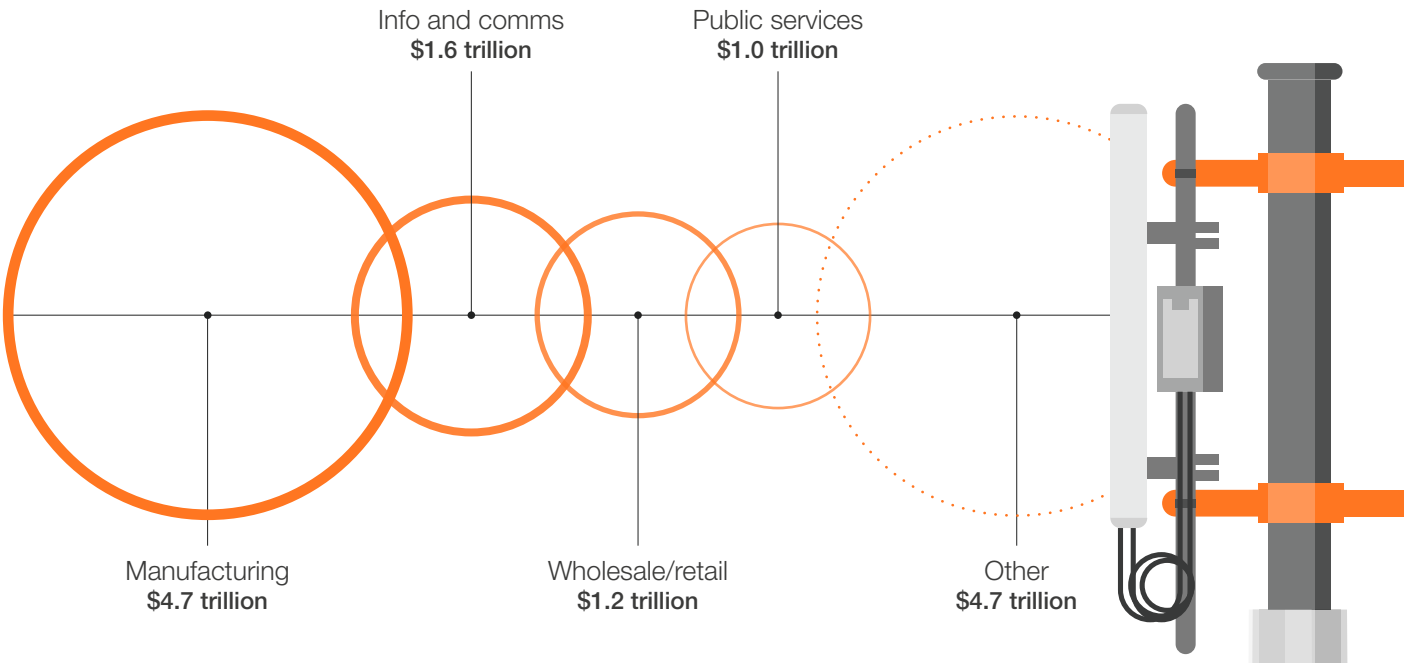


Number of connected devices and reliance on key telecoms infrastructure

Ability to support up to 1 million devices per km²

Over 25 billion connected devices predicted by 2025

The value of 5G to the global economy is set to reach $13.2 trillion by 2035



Source: Based on IHS Markit, The 5G Economy: How 5G will contribute to the global economy, 2019.

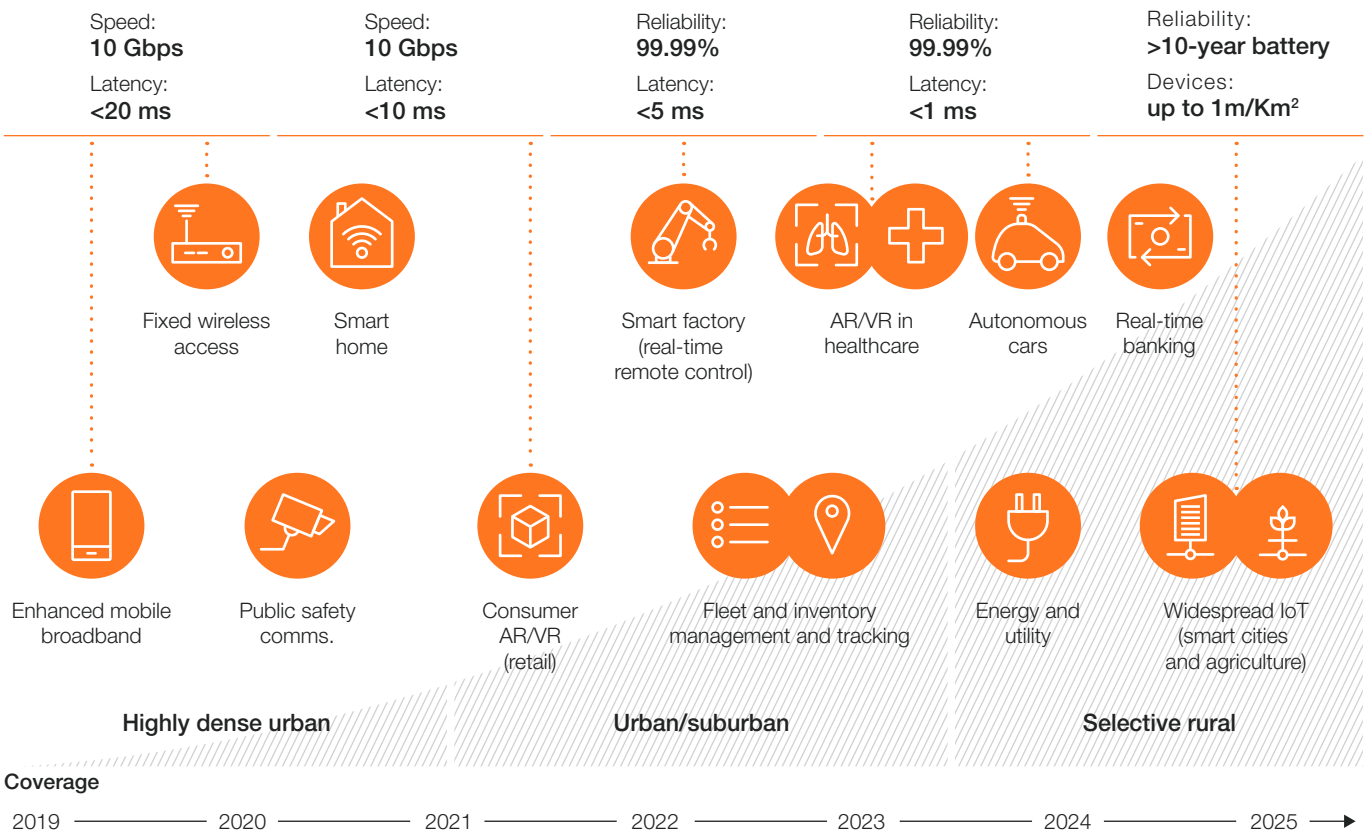
These developments create the opportunity to use communications and data analysis to more efficiently and reliably monitor and control previously unconnected critical systems in the physical world.[18] Organizations are changing their operational model, and becoming increasingly dependent on connectivity as telemetry and insights are used to drive decision-making and physical control, creating efficiency and effectiveness gains. New products (e.g. connected autonomous vehicles)[19] and services are emerging based on predictive and real-time decision support. This will make possible the delivery of global strategic initiatives to address some of the world's most pressing economic challenges.[20]

As a result, the role of wireless connectivity in economies and across societies is growing. It is becoming possible to support a range of transformative personal, societal and industrial use cases. Industry leaders are adapting to derive value from the emerging networking technologies. The relationship between different elements of the supply chain is changing.

Taken to their logical conclusion, the developments taking place now will end in ubiquitous connectivity, where devices, networks and services are hyperconnected and interdependent, operating on sophisticated shared infrastructures and relied on to support critical functions across society and industry.

Participation in the connected ecosystem is becoming imperative as maintaining standalone approaches becomes uneconomical for organizations. This is resulting in some fundamental changes to industry, which will be accelerated as the technologies mature and adoption becomes increasingly widespread in the near future. Taken to their logical conclusion, the developments taking place now will end in ubiquitous connectivity, where devices, networks and services are hyperconnected and interdependent, operating on sophisticated shared infrastructures and relied on to support critical functions across society and industry.

Key applications of ubiquitous connectivity



AR = augmented reality; VR = virtual reality; IoT = interent of things

Source: PwC Strategy and World Economic Forum, "5G for the Fourth Industrial Revolution", 2019

Systemic risk

The evolution towards ubiquitous connectivity is creating new business models and introducing systemic cybersecurity risk. Key features of hyperconnected environments are already beginning to have significant impacts on the risks faced, which will be accelerated as the technologies mature and adoption becomes more widespread in the near future.

Scale and criticality

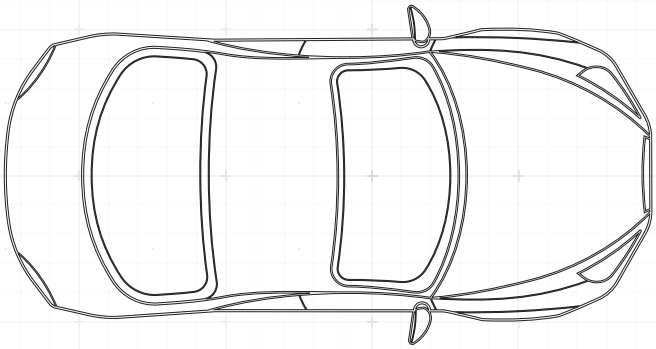
The sheer scale of the connected ecosystem means that the potential attack surface is expanding rapidly. As previously unconnected systems become connected to each other and to the internet, there is an increased risk to the confidentiality, integrity and availability of digital assets – whether it's data, information, algorithms or digital services. The potential implications in terms of compromise for industry and society are becoming more severe.

For example, safety-critical functionalities including intelligent transport systems and surgical procedures in healthcare are set to become increasingly reliant on the integrity and availability of communications, with compromise threatening human safety and potentially even leading to loss of life.

Interdependency

A range of new entangled relationships between actors in the digital ecosystem is evolving. The emergence of new products and growth of new service-based models is creating complex interdependencies between organizations, supply chains, sectors and individuals. This interdependency creates a risk of unforeseen cascade effects: Incidents occurring in one part of the ecosystem could harm those actors and systems dependent on it. Imbalance in perceptions of risk could lead to situations where high-value business

Interdependency, complexity case study



Integrity of training data sources

Integrity of sensors and sensed data

Integrity of communicated information from other vehicles

Data from other sources – cars, roadside infrastructure

Real-time connections to other cars and roadside infrastructure for road safety and traffic flow

Sensing of environmental data (cameras, light detectors, radar, ultrasonic)

Communication of data to continuously training neural networks

AI-based driving decision-making based on multiple data sources

Sensing of driving performance data

In-car voice assistants, connection to service provider

Security of source code from multiple providers

Real-time connections to manufacturers of the car's components for diagnostics

Connection to satellite navigation

In-dash apps with connections to multiple service providers

Connection to multiple service providers creates potential for risk propagation

assets are connected to third-party systems whose owners assess them to be low risk and that therefore do not have the appropriate levels of protection. A failure to maintain the visibility and assign the accountability that is needed to assure end-to-end processes across multiple parts of the ecosystem could lead to gaps in security and heightened risk.

Shared resources

Many entities are sharing a growing dependence on a concentrated underpinning infrastructure and set of shared services, including cloud, internet service providers, hardware, software and the equipment supply chain. This creates an attack surface of high-value shared resources with a high probability of attack, and the potential for compromise to have severe and systemic impacts. The homogeneity of the shared technology infrastructure that results from its being delivered by a small pool of providers may result in systemic risk, as the exploitation of a vulnerability found in a widely used resource could affect vast swathes of the ecosystem. Similarly, there is a risk of collateral damage occurring as a result of targeted attacks against a single client via this shared infrastructure. Identifying the critical shared resources, who owns them and their key dependencies is a complex task.

Challenges and required action

Fragmented standards and principles

The full potential benefits of ubiquitous connectivity will be achieved only if there is sufficient interoperability of cybersecurity functionality between companies, sectors and countries. Currently, a variety of technical and governance standards and principles that relate to the security of the hyperconnected ecosystem exist or are emerging. Ongoing initiatives are making progress towards achieving a level of unification. Industry alliances are creating shared security principles, interoperable solutions and baseline device-security certifications,[21] [22] [23] [24] reviews are being made of the requirement to integrate standards for the emerging digital era,[25] [26] and intergovernmental organizations are working towards the development of common principles for digital security, international policy recommendations[27] [28] and international norms.[29]

These standards and principles apply primarily to how systems are built and operated. More attention needs to be given to how they are used in business, and how this use is governed and regulated. There is a need to ensure that technical interoperability and security assurance are not compromised as a result of incompatible policy and regulatory requirements, and that companies operating across jurisdictions do not face compliance conflicts. The community requires a process for identifying any emerging and material inconsistencies in regulatory and policy approaches for the hyperconnected ecosystem in order to develop and promote resolutions to these inconsistencies. Inaction will result in a compliance-based approach that does not necessarily represent meaningful progress in cybersecurity, but simply a minimal-effort approach to market access.

The emergence of new products and growth of new service-based models is creating complex interdependencies between organisations, supply-chains, sectors and individuals.

Lacking transparency and assurance

Ultimately, organizations are accountable for assuring their own services. This is challenging and many struggles to achieve this today, as the security and availability assurance levels of the services on which they depend are not always sufficiently defined or transparent. This challenge will be exacerbated as the ecosystem becomes increasingly complex. The consequence is that it may become difficult for organizations to determine the optimal risk mitigations for their purpose, and to ensure that suppliers are meeting their requirements.

The ecosystem will need to establish a base level of trust within the supply chain, with transparency in regard to security functions, if customers are to be assured of making the right risk-management decisions. While some sector- and country-specific examples of progress in these areas exist (e.g. in the UK, the development of legislative approaches in regards to the responsible party in the case of autonomous and connected vehicles,[30] and the regulation of the security and privacy of IoT-connected devices provided by manufacturers in California),[31] there is a need for clear policy surrounding the regulation of cybersecurity in these environments that is mutually supportive internationally. It must be clear where any transfer of liability occurs, so that those responsible for delivering cybersecurity functionality do so with a full understanding of their own accountability. This is a long-standing challenge and a contested issue.

Achieving sufficient transparency and assurance depends on having the right level of real-time end-to-end visibility across the ecosystem.

It is critical to ensure that the development of a new generation of operational cybersecurity capability is not outpaced by the fast-growing risk landscape.

Licence to participate

For certain actors with pivotal roles to play, it may be necessary to establish the concept of a "licence to participate" in the market: a baseline level of security assurance and accountability that an actor, dependent on the specific role they play, should have to continuously demonstrate in order to participate in the ecosystem.

This concept is well established for organizations defined as critical national infrastructure (CNI): In most jurisdictions, CNI providers require licences to operate and are subject to a range of regulatory requirements, reflecting the economic and public-safety implications should things go wrong. However, some infrastructure that does not necessarily fall within the remit of CNI obligation is becoming an increasingly critical component of the supply chain, as reliance on communications infrastructure grows and organizations (including those in CNI sectors such as healthcare, transport and energy) become dependent on shared underpinning digital infrastructure and third-party suppliers while not being granted access to spectrum resources to develop resilient and secure private network alternatives." at the end of the sentence after "suppliers.

Shifting CNI

There is a need to identify changes in what constitutes the CNI, its interdependencies and risk-ownership models. In particular, there is a need to examine the components of the ecosystem that are critical to the operation of multiple different services, and establish how to reflect their critical status. While it is important not to overburden companies with regulation, it should be recognized that the market has failed to deliver technological systems free from vulnerability, and therefore policy solutions will need to be found that can deliver integrity and promote innovation.

The approaches developed will need to be able to adapt to rapid changes in the underpinning technology environment while preserving the high level of security and resource assurance needed to ensure compliance with safety and availability standards. This activity should build on various existing CNI cybersecurity regulations and frameworks.[32] [33] Furthermore, there are international differences in the responsibility models for mission assurance in the CNI (e.g. the balance that regulators place between standards-based compliance measures and threat-based testing), and as services are rolled out on a global basis there is a need to ensure international interoperability of these schemes.

Gaps in operational cybersecurity capabilities

There is an operational cybersecurity capacity deficit in general, and this will become more acute in emerging systems where current risk controls are unlikely to be sufficient. Technical solutions are evolving, yet significant challenges remain, associated with the speed and scale of the hyperconnected environment and the need to be interoperable among multiple organizations. A range of current operational capabilities will be challenged. Information-sharing

models need to evolve to keep pace with the increasing scale and complexity of the technology and threat, for example.

It is critical to ensure that the development of a new generation of operational cybersecurity capability is not outpaced by the fast-growing risk landscape. It is also critical that a sufficient cadre of experts is maintained, who can operate in a blended operational technology (OT)/information technology (IT) environment. New technologies are widening skills gaps, and operational conflicts are emerging between OT-safety and IT-security approaches. The impact of the digital transformations of businesses on the technology development and operational skills required will need to be identified, and approaches to addressing skills shortages established.

Operational capability challenges arising from ubiquitous connectivity

Artificial intelligence

04

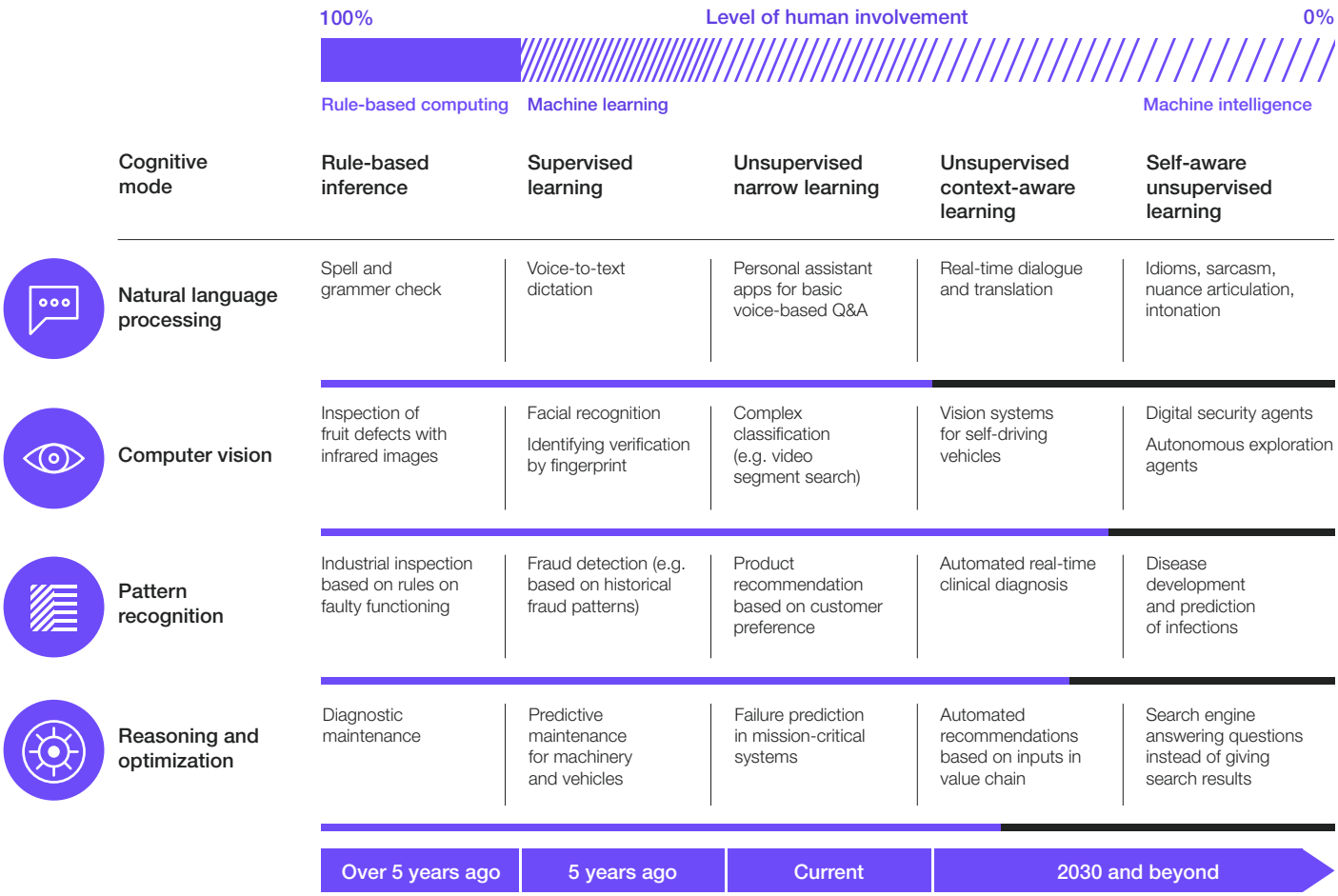
The increased pervasiveness of artificial intelligence (AI) across a range of often critical business processes and functions places a heavy reliance on the algorithms. However, there is a lack of assurance about how these algorithms are designed, developed and used. AI is already being deployed by both network defenders and those attacking them. It is difficult to tell where the balance of advantage lies.

New tools are required to protect AI-based processes and to enable defenders to collaborate against the whole range of AI-enabled threats. Security principles for AI are needed that cover secure design, life-cycle management and incident management. Such principles can provide the basis of a more robust assurance regime to support the governance of AI-associated cyber risks.

The growing *intelligence* of autonomous machines

The global race to develop AI technologies is accelerating, with rapid developments in its applications across swathes of the global economy. The field of AI aims to build reasoning systems: technologies that can perform tasks normally requiring human intelligence (such as decision-making, visual perception and speech recognition) and adapt to changing circumstances. High-level machine intelligence ("strong AI") would be achieved when unaided machines can "think" exactly like humans, creating advantages across reasoning tasks in general. This is unlikely to be achieved in the near future.[34] It is "narrow AI", focused on creating reasoning systems that achieve specific advantages in specific applications, which is more immediately relevant.

What AI is, and its applications



Source: A.T. Kearney; A.T. Kearney/World Economic Forum workshop, November 2016; expert interviews

Substantial investments are being made in AI research and development globally, in particular using machine learning techniques. Global spending on AI was estimated to be $37.5 billion in 2019, and is forecast to reach $97.9 billion in 2023,[35] with China and the US dominating global AI funding.[36] The emerging technologies are capable of faster, more precise analytics and decision-making, and of deriving insights from big data, outperforming traditional digital approaches and some aspects of human capabilities in diverse fields such as transport, manufacturing, finance, commerce and healthcare.

Large corporations in every industry are seeking to create value by taking advantage of new means of data exploitation, business-process improvements (e.g. in sales, production and supply-chain management), cost-efficiency gains and the ability to enhance customer experiences.[37] It is anticipated that within the next 5–10 years, AI systems will play an increasingly critical and unsupervised role within organizations, including the use of robotics in physical manufacturing tasks, for example.[38]

The shifting attacker-defender balance

AI is already being deployed by both network defenders and those attacking them. It is difficult to tell where the balance of advantage will ultimately lie.

In the long term, offensive AI may create completely new ways of attacking (using reinforcement learning, for example) – similar to how AlphaGo found completely new tactics and strategies in the "meta-game" of Go.[52]

Dangerous attackers: speed and scale, precision and stealth

The first generation of AI-enabled offensive tools is emerging. Evidence of AI being used by attackers in the wild is limited but growing.[39] As the technology matures and becomes more widely accessible over the next few years, the malicious use of AI will be accelerated and become increasingly sophisticated.[40] [41] [42] Adversaries will take advantage of enhanced capabilities throughout the stages of a cyberattack.[43] [44]

- **Speed and scale:** By automating attacks or attack components, attackers will be able to speed up and scale up their operations. The range of threat is likely to expand as automation reduces the need for expertise or effort.
- **Precision:** Attackers will take advantage of the opportunity to craft more precise attacks, by using deep-learning analytics to predict victims' attack surfaces and game their defence methods.
- **Stealth:** Attackers will exploit AI in order to evade detection and elimination: to be "stealthy". A range of evasion attacks in which malware evolves to bypass security controls have already been shown to be feasible.[45] [46] [47] [48] [49] [50] [51]

Opportunities for defenders

While it creates clear opportunities for attackers, AI also has real potential to enhance the speed, precision and impact of operational defence, and support organizational resilience.[53] AI-enabled defences are being researched and developed, and AI is also being used to support human defenders by augmenting and automating tasks usually performed by analysts (e.g. threat triage). These approaches are becoming increasingly deeply integrated into defensive responses within the cybersecurity ecosystem.[54] The global value of AI in cybersecurity is predicted to reach $46 billion by 2027.[55]

As described, AI could be used by an attacker to predict the defender's moves. For defenders, an improved analytical ability to predict threat actors and their attack strategies could enable better orchestration of defensive moves. This gamification is part of an accelerating arms race between AI attack and defence methods: Despite the promise of AI-based defences, it has already been shown that some can be circumvented by adversarial AI-based attacks. For example, intelligent agents have been developed, capable of manipulating malware to bypass machine learning-based defences),[56] [57] [58] and attacks against machine learning-based security systems are becoming more prevalent.[59] In fact, the community should explore the value of automating security policies, detection and mitigation more broadly, using AI.

AI attacker-defender balance

Reconnaissance

AI looks at and learns from social media profiles at scale

AI accurately replicates communication styles of trusted contacts

Creates convincing impersonation messages

Intrusion

AI crafts spear-phishing emails based on reconnaissance intel

Identifies vulnerabilities by autonomously scanning and fuzzing the perimeter

Rapidly locates ideal initial footholds, discovers ephemeral devices

C2 establishment

AI learns regular pattern of activity for the network

Malware auto-configures to replicate "normal" behaviours

C2 connections made in periods of high activity to blend in with the noise

Privilege escalation

AI creates list of keywords based on infected device's documents, messages and data, and creates realistic permutations and potential passwords

Credentials breached in seconds

Lateral movement

AI autonomously harvests target accounts and credentials

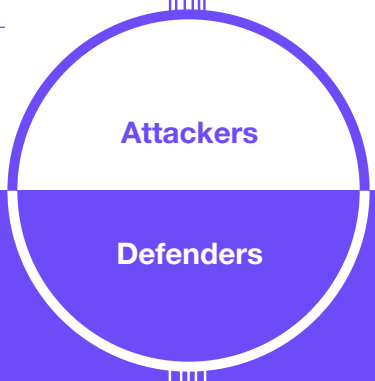
Calculates optimal path established to reach desired destination

Speed of movement drastically increased, no C2 channel required

Mission accomplished

AI decides which material is relevant, e.g. identifies compromising material based on context and exfiltrates to incriminate users

Exfiltrates relevant material only – reducing data transfer volumes thus becoming more stealthy



Improving security posture

Identifying and managingcode and hardware vulnerabilities[60]

AI-enabled re-programming to secure vulnerable environments[61 62]

Dynamic threat detection

Dynamic defences that can identify novel and evolving threats (unlike traditional detection methods based on matching historical patterns)

Autonomous detection and identification of malware, network anomalies and intrusions, spam and botnets, next-generation antivirus[63 64 65 66 67]

Proactive defence

Refinement of cyber deception to proactively create environments that are difficult for attackers to operate in[68 69]

Fast response and recovery

Automatic real-time responses to interrupt and contain machine-speed attacks

Enriched analytics to support human investigation and response

Potentially faster recovery from incidents, for example, through the use of self-regenerating networks to reinstate pre-compromise states

Attribution

Using the pattern-recognition and analytical capabilities of AI in the forensic analyses underpinning cyber attribution[70 71 72]

Expanded attack surface and manipulating the algorithm

AI-driven systems and processes are quickly becoming part of the vital assets of major enterprises, performing increasingly critical functions with decreasing human oversight. This is expanding the scale and criticality of the attack surface that could be exploited through adversarial AI. Adversaries will seek to manipulate or disrupt the processes of organizations, and the infrastructure relied on by society, by altering the integrity of algorithms and of the data that feeds them.[73] [74] [75] Some AI algorithms have already been shown to be open to manipulation and data-poisoning by attackers.[76] [77]

As these algorithms are used in increasingly critical functions, this could have grave consequences[78] (including physical harm, as autonomous cyber-physical systems emerge).[79] Furthermore, there is a risk that the decisions made based on complex probabilistic algorithms and huge quantities of data could lack "explainability", leaving the leaders accountable for them unable to verify or justify their correctness, or identify subversion of them.

Attackers will be able to apply AI to get more value from stolen data, and also to create more harm by using it to refine cyberattacks. In a world in which the quality of AI algorithms' training and accuracy is increasingly important, data becomes an enabler and has much greater economic value because of what it allows its owner to do; data is therefore likely to be increasingly heavily targeted.

What is truth?

As digitally manipulated videos, images and audio ("deepfakes") become increasingly sophisticated, convincing and difficult to distinguish from reality,[80] and also more widespread particularly as the technologies for creating them become more accessible,[81] there is a risk that "the truth" will become increasingly difficult to establish. Actors may take advantage of the opportunity to generate realistic and finely targeted fake news and manipulated messaging, distorting public perception of the truth and altering political or economic outcomes.[82] [83] Uses in disinformation campaigns have already been seen.[84] [85] It is likely that deepfakes may become a tool in ransomware attacks aimed at individuals.

Deepfakes may also be exploited to create new cyberattack vectors. For example, voice-mimicking software has allegedly already been used in a major theft.[86] Targeted manipulation of victims to carry out an attacker's goals may become increasingly convincing and effective as the underlying technologies develop.

Challenges and required action

Ongoing evolution of the right defensive tools

It is not yet clear where the balance between AI-enabled attackers and defenders will lie. To mitigate the risk of the advantage lying with cybercriminals and other malign actors, it is critical that the cybersecurity community quickly prepares to combat fast-emerging AI-enabled attackers, by continuing to evolve technologies and operational capabilities that can match their pace, dynamism and sharpened predictive capabilities (as well as building the defences to address new forms of threat such as deepfakes).[87] [88] [89] While traditional (non-AI) risk controls will form an important baseline, this likely means using faster and more dynamic AI-enabled defences.

It is critical that investments continue to be made in developing the right AI-enabled defences. Investment must be driven by an accurate understanding of the emerging adversarial model and resulting critical gaps in defensive capability. An example of a potential capability gap is the use of segregation-based defences, the effectiveness of which could be altered if autonomous malwares can be placed inside air-gapped or otherwise segregated systems without the need for continuous attacker control.[90] Focused industrial and academic research is needed to support this activity and develop the right research agenda. Drawing the growing research and experiential evidence possessed by organizations out into the wider ecosystem could enable a better understanding of the adversarial model as AI-enabled adversaries increasingly operate in the wild. This would create a stronger foundation for the improvement of tools and knowledge for the defensive community.

In developing these defensive approaches, there is a need to consider how to mitigate the potential harms of an emerging arms race. Aggressive AI-driven strategies of defenders could cause opponents to respond more aggressively.[91] Furthermore, attackers might benefit from advances made by defenders to improve their own capabilities. For example, while research into the use of machine learning to identify "normal" network behaviour benefits anomaly detection by defenders, it could also be exploited by attackers to identify how to "blend in".

Addressing systemic risk: collaborative operational security

The consequences of security compromise or a failure in the autonomous decision-making occurring in one part of the ecosystem will be increasingly systemic, with the potential to affect other organizations and important societal functions as the ecosystem becomes more interconnected. Collaborative operational security approaches will be needed to ensure the resilience of the ecosystem as a whole to the advancing threat from AI. There is a need to ensure that information-sharing approaches evolve to be effective against emerging algorithmic threats, for example.

Building defensive capacity

The threat of AI-enabled attackers, who will target a wide range of actors, could mean that an increasing number of participants in the digital environment fall further behind in terms of their ability to defend against it. Many actors could be left unable to access new sophisticated and costly AI-enabled defences. It is important to consider how to build the capacity needed to support actors in defending their part of the ecosystem and contributing to collaborative defensive efforts.

- **Incentivizing defensive technology adoption:** Government and enterprise leaders will need to identify methods of incentivizing equitable and affordable access to key existing and emerging defensive technologies in the market.
- **Best practice guidance:** There is a need for operational frameworks that guide cybersecurity practice – methods of automated detection, response and investigation that are tailored to the emerging AI-enabled threat landscape and defensive opportunities.
- **Skills, education and communicability:** Board engagement on these issues will be critical in ensuring that organizations make the necessary investments. There is a need to educate leadership sufficiently on the complexities of AI and ensure that the issues are communicable at board level.

Secure defensible algorithms

As a critical dependence on the output of AI algorithms develops across industry, it will be increasingly critical to ensure their integrity: that their outputs are correct and unbiased, and that they have not been subverted by attackers. The community has not yet fully developed the necessary approaches for assuring the properties of fairness, adversarial robustness and explainability that must underpin trust. There is a danger that leadership will find themselves accountable for the decisions made by algorithms without a full understanding or assurance of their security properties or even their functionality.[92]

To support the development of secure, defensible algorithms, there is a need to develop security principles for AI. The requirements will need to be identified and codified through collaborations between government, organizations, technology suppliers and academia. Adoption of secure development practices will need to be incentivized, which may require supporting standardization and regulation, some of which is already under development.[93] [94] [95] Principles that need to be covered include:

- **Secure design:** AI systems need to be hardened against adversarial manipulation and disruption techniques.[96] [97] They also need to be explainable, to enable those responsible for algorithmic decisions to verify their integrity.[98] [99] [100]
- **Life-cycle management:** Algorithms need to be vetted rigorously and dynamically, especially given the constant evolution of models as new data is ingested.[101] Version control will be needed for dynamic AI models
- **Incident management:** Those responsible for the outputs of AI algorithms will need to be able to detect when algorithms have been manipulated, respond to mitigate the harm this could cause, and recover to a state of algorithmic integrity.

Quantum computing

05

Rapid progress is being made in the development of quantum computers. As this technology matures, it has the potential to drive transformational changes across industry and society. Quantum computing also poses a number of risks that must be addressed to ensure that security concerns do not threaten uptake.

There is still time to mitigate these risks before they arise. Individual organizations need to start considering their ability to transition to quantum safety, and many are doing so. There are also distributed risks that require collective action in multiple sectors and jurisdictions.

Business leaders and governments need to ensure that they understand the technologies and the risks and are prepared to act quickly if the full transformative value of quantum technologies is to be realized.

Significant investments are being made in quantum research and development by major technology corporations, national governments, and VCs. A technological arms race is developing that has the potential to unlock trillions of dollars of value within the global economy

Quantum arms race

Quantum computing is one of the most strategically important technologies that will emerge in the next 5–15 years. It may well launch a technological revolution and bring great opportunity. Quantum computers make use of the laws of quantum physics to process information, in principle enabling types of information-processing tasks that cannot feasibly be achieved using classical computers. As quantum computers work alongside classical computers, a set of computational problems could become tractable for the first time.

Currently, there are major engineering challenges to building hardware and software that can realize the theoretical potential of quantum computing. It is generally thought that some applications of quantum computing may become practical at scale in around a decade, although timeline predictions vary. The timeline may be shortened.[102] [103] [104] Significant investments are being made in quantum research and development by major technology corporations, national governments and venture capitalists.[105] [106] [107] A technological arms race is developing that has the potential to unlock trillions of dollars of value within the global economy.[108] [109]

Quantum algorithms have the potential to bring about major advances and transformative benefits in a range of use cases across industry.[110] [111] [112] [113] [114] For example, quantum could be applied to molecular simulation, accelerating drug discovery[115] and materials science,[116] [117] could solve complex optimization problems in financial services[118] [119] and aerospace,[120] and could improve AI capabilities.[121] Early versions of quantum-computing services are already being offered by a small pool of companies[122] [123] that are beginning to engage clients to collaborate on creating the algorithms needed to realize the niche benefits that are already achievable or are likely to be so in the near future.[124]

The full extent of the transformations that may be achievable as quantum computing matures is not yet understood, but it is clear that this technology has the potential to create great shifts in value creation. Nations, sectors and organizations that are not able to reap its benefits risk falling behind the progress made by others.

Broken cryptography and broader risks

The most significant implications of the quantum arms race are already being felt by the global cybersecurity community.

Disrupting cryptographic infrastructures

The principal cybersecurity risk is posed by the impact quantum computing will have on currently widely adopted asymmetric cryptography. A sufficiently powerful and error-corrected quantum computer would solve some of the classical mathematical problems on the intractability of which many of these cryptography methods rely.[125] [126] It would therefore have the potential to break the cryptographic security on which enterprises and the wider digital economy rely.

Quantum timeline and the risks to cryptography

Superposition

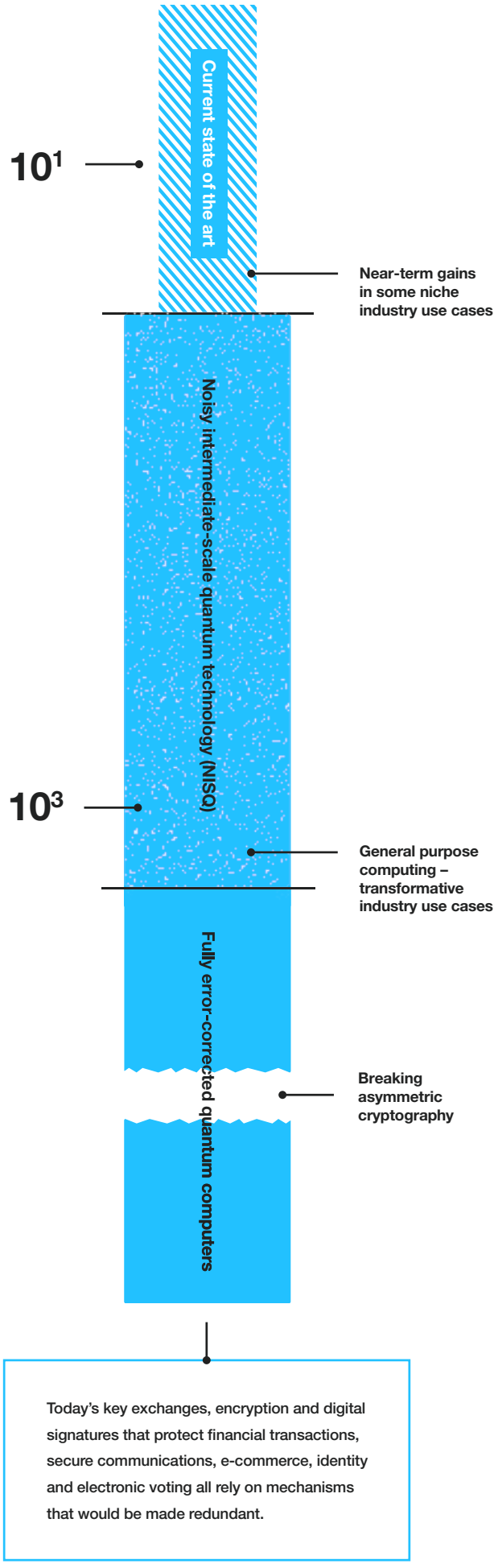
Superposition describes a particle's ability to exist across many possible states at the same time. So the state of a particle is best described as a superposition of all those possible states.

Entanglement

Quantum entanglement refers to a situation in which two or more particles are linked in such a way that it is impossible for them to be described independently even if separated by a large distance.

Observation

Superposition and entanglement only exist as long as quantum particles are not observed or measured. "Observing" the quantum state yields information but results in the collapse of the system.



Both classical and quantum cryptographic solutions that are resistant to this threat ("quantum-safe") are emerging, e.g. through the standardization process for post-quantum cryptography run by the US National Institute of Standards and Technology (NIST).[127] [128] A number of implementation challenges are yet to be resolved, however.[129] [130] [131] [132] [133] It is not yet fully understood how quantum cryptography will affect the balance between attackers and defenders, nor how this will play out commercially or politically.[134] [135]

If quantum computers were to become capable of breaking asymmetric cryptography before the digital ecosystem had achieved the necessary transition to quantum safety, it would create significant cybersecurity risks for individual organizations. Businesses and governments could be left unable to ensure the confidentiality, integrity and availability of the transactions and data on which they rely, if they or the organizations and suppliers that they depend on were not prepared.[136] [137]

There are also several shared infrastructures that depend on the collective application of quantum-vulnerable cryptography. This includes the interconnected systems and interdependent business models of the industrial internet of things (IIoT), and the distributed-ledger technologies being rolled out across a range of industrial applications. In many cases, "ownership" of these shared infrastructures is highly distributed, and it is not necessarily clear who is responsible for ensuring that they are made quantum-safe.

'Download now, decrypt later'

The potential future quantum threat to cryptography is relevant to the risk decisions being made today. There is a "download now, decrypt later" risk for datasets with extended periods of sensitivity: data that exists now could be harvested by adversaries for decryption in the future. Similarly, there is a risk to systems being rolled out today with long lifespans (e.g. satellites, transport and industrial control systems), which could be in operation for decades.

Novel and secondary security risks arising from broader economic and industrial transformation

As industry use cases for quantum computing emerge, organizations will need to consider how they start to adopt quantum into their business models in order to retain competitive advantage. Adoption is likely to create new security dilemmas, however.

As organizations face a need to outsource quantum computations on their most valuable IP to third-party services, they could face risks of adversarial interference. There is also a risk that unintended functionalities arising from quantum algorithms that are inherently biased, or that have been manipulated by adversaries, could go undetected by the organizations liable for them. This could be due to a lack of personnel with quantum expertise. It could also be due to technical explainability and verification challenges for complex, non-deterministic quantum algorithms (a subject of ongoing research).[138] While verifying the results of many quantum algorithms will be straightforward, there may be cases where the reverse operation for verification is difficult.

Wider security issues will emerge. It is likely that quantum computing will be misused for malicious purposes. Criminals will seek to access quantum services, exploiting their computational power to advance cyberattack capability. There are also potential parallels with dual-purpose technology in the context of the proliferation of weapons of mass destruction, e.g. through the use of quantum computing to develop weaponized pathogens.

For nations to reap the full potential benefits of quantum, it is critical that a workforce is built that has sufficient expertise to develop secure quantum hardware and algorithms, and maintain their security operationally

It is not only activity with malicious intent that will be a concern. As with all new technologies, there will be disruptive applications found for quantum computing to create new economic advantages for particular parties (for example, optimizing financial-trading strategy, which could be disruptive to markets and economic processes).

Geopolitical risk and equitable access

Quantum technology has the potential to be game-changing for national security. Currently, some national governments are putting significant investment into the development of sovereign quantum technologies and skills, and several countries are placing quantum technologies on their lists of controlled goods.[139] The potential concentration of the first sovereign quantum capabilities (technologies and experts) in a small number of advanced nations has geopolitical implications.

As with all new technologies that raise the bar in terms of competitiveness, there is a global risk that competition and protectionism will interfere with international collaboration and equitable access. This could act as a major barrier to unlocking the full potential economic and societal benefits of quantum technology to the wider economy, and widen asymmetries in terms of security and industrial capability. If equitable access to the technologies is not ensured, nations that have sovereign quantum capabilities may use them to create a strategic advantage, while other nations fall into "quantum poverty".

Challenges and required action

The potential impacts of quantum on cybersecurity may still be further away than the effects of other technologies examined in this report; yet as the development of the technology accelerates, the near-term actions taken individually and collectively to prepare for it become increasingly important. While the quantum risk is understood within parts of the technical community, and defensive solutions are emerging, further attention from enterprise and policy leadership is needed.

Guidance and education on the quantum security risk for enterprise leaders

Enterprise leaders will need to be able to address the risks to their organization, in particular, to:

- Assess the materiality of the quantum threat to cryptography to the organization's assets, supported by accurate inventory and understanding of asset lifespan
- Ensure that the cryptographic estate is adequately managed and that plans are in place for the transition to quantum-safe cryptography within a suitable timeline[140]
- Consider all other security risk controls that may be weakened in the face of an attacker with quantum computing power (all controls that rely on complexity of computation as an integrity guarantee should be considered)
- Account for the organization's dependencies – the corresponding activities of its business-to-business (B2B) product and service providers – in assessing risk
- Make decisions on whether to embrace the potential benefits of adopting quantum computing into the business model, supported by an understanding of the potential security risks and how to mitigate them (which could include the use of quantum-based mitigations)[141]

There is a considerable challenge in persuading senior leadership to invest in a problem of this nature, particularly when there is still so much uncertainty about what the material impacts will be and when they will occur. A vital step will be building "quantum literacy" at an enterprise leadership level, educating leaders on the development of quantum technology and the potential benefits and risks it could create for their organization. A set of principles or taxonomy that can guide enterprise leaders (facing a variety of

circumstances) in deciding how and when to invest in preparing for quantum risks and opportunities would also be valuable.

Identifying and addressing distributed risk

For some shared infrastructures and interdependent sectors, the actions taken to achieve quantum safety will need to be coordinated between multiple parties. Where there is distributed governance and ownership, it may be unclear who is responsible for driving this transition. There would be value in a sector-by-sector analysis to identify where distributed parties need to act collectively to address the threat, and whether the responsibility for driving this transition needs to be assigned.

Developing quantum securely

National governments and industry will need to work together on their investment strategy for developing sovereign quantum capability, given the significant national strategic advantages that those with more mature capability are likely to have (similar to the current contention over the provision of 5G services by a small pool of nations).[142] [143] As quantum programmes develop, it will be critical that their security dimensions are regularly revisited, and that the emergence of risk is monitored by the responsible bodies.

For nations to reap the full potential benefits of quantum, it is also crucial that a workforce is built that has sufficient expertise to develop secure quantum hardware and algorithms, and maintain their security operationally. Given that quantum is complex and classically counter-intuitive, there will inevitably be a widening skills gap unless investments are made in establishing education and training at scale. Consortia are forming to accelerate development and identify workforce needs.[144]

Revisiting governance principles

In the face of the upcoming quantum transition and potential future threats, the right set of standards, governance principles and regulation will need to be embedded into the frameworks that organizations use to make risk decisions. Work on developing the relevant technical standards and quantum-proof algorithms is already underway,[145] but there has been less progress on identifying the necessary governance principles for incentivizing the actions that need to be taken by organizations and their suppliers.

The practices that should be adopted by individual organizations will need to be clarified (e.g. the reasonable treatment of data in light of the “download now, decrypt later” risk), with sufficient emphasis placed on them to ensure that they become a part of the appropriate incentivization mechanisms (e.g. B2B requirements and insurance). Regulators and governments will need to consider at what point they should be starting to mandate action in order to ensure that any risks to the public good are adequately addressed.

It will be critical to ensure that there is the right level of alignment between technical standardization and governance efforts around the world, to avoid divergence hampering international collaboration or the operations of international organizations. There is also a need to manage the full range of global governance principles (e.g. promoting the ethical use of quantum resources) required as quantum technology rolls out (an approach similar to the global technology councils that emerged to manage AI[146] may be required, for example).

Equitable access to quantum capability

Quantum technology has the potential to create significant and far-reaching benefits. It is important to ensure that there is equitable access to the technology across the world in order to unlock these benefits, and to avoid widening asymmetries in security and industrial capability between nations. Prominence has been given to the quantum risk to cryptography and its security implications, and there is a risk that this will inhibit broader access. Governments will need to work together to ensure that the right balance is struck between recognizing the potential benefits of enabling equitable access to quantum capability and being realistic about the associated risks.

Digital identity

06

Ensuring robust and secure digital identity is vital to enabling online and increasingly offline transactions. At present, however, there exist numerous different views on how digital identity systems should be implemented, resulting in a divergent range of global approaches.

There is a need to develop a system that enables interconnectivity and mutual assurance and trust between different approaches, in order to support economic and social transactions in a way that allows local relying parties to make risk-based decisions. Furthermore, this system must protect individuals' privacy and be able to do so across national boundaries.

Some of the same approaches that exist in the physical world, such as those used to assure passport integrity, need to be applied in the digital world. Greater collaboration is required in order to better understand the wide range of current differing approaches. Consideration also needs to be given to how to deal with the threats posed in a distributed environment, noting that some of the participants in that environment may be motivated to abuse their privileged positions.

Heterogeneous approaches across the globe

Establishing a robust and globally interoperable approach to digital identity management is critical to realizing the potential economic and societal value of the digital ecosystem in the next 5–10 years. By getting digital identity right, there is the potential to solve existing security and privacy challenges, facilitate a low-friction global market, support the digital transformation of existing services, and create opportunities for businesses and public services to unlock new value by offering new types of trusted services (e.g. in transport, commerce and finance).[147] [148] [149] Interoperable identity-management systems, while not comprising the entirety of the solution for economic and social inclusion globally, are a necessary precondition.[150] [151]

It is widely agreed that the way in which identity is currently managed within the digital ecosystem is suboptimal. Weak identity management is exacerbating cybersecurity issues and is at the root of many forms of cybercrime,[152] [153] while the lack of interoperability between isolated solutions is acting as a barrier to unlocking value.

The reimagination of digital identity is ongoing. There have been efforts by various national governments and regional bodies, as well as industry-led efforts, to implement digital identity management approaches.[154] [155] [156] The specialist identity community has established principles;[157] [158] [159] supporting technologies exist;[160] [161] [162] [163] and identity solutions are being implemented in new use cases.[164] [165] Significant challenges will have to be faced in terms of implementing identity systems and supporting technologies, incentivizing actors to play their part in the emerging identity ecosystem, and ensuring that parts of the global population are not excluded.

Competing paradigms and investments in a diverse range of solutions (due in part to differing contexts across countries, sectors and companies) have created a fragmented landscape of identity approaches. Achieving the level of interoperability needed to support transactions across multiple sectors and jurisdictions is, and will continue to be, challenging. These issues are being examined and addressed by the relevant communities.[166]

Digital identity, if managed in the right way, could clearly form an important part of the security and privacy solution, helping to address challenges, including some of those arising from other emerging technologies (e.g. strong authentication guarantees could help mitigate the risk of AI-based impersonation). There are security and trust challenges, however, that need to be addressed as the next-generation digital identity ecosystem emerges. The community should recognize that business and digital services are becoming increasingly entangled. Total trust of identities from heterogeneous systems is unrealistic, but zero trust is likely insufficient to support the desired transactions. Federated identity systems are needed, which share and project sufficient trust across supply chains to deliver services. Therefore, the community will need to find a global model for *transitivity of trust*.

Security risks to digital identity systems

As next-generation identity systems emerge, society will build up an increasing dependence on using them in critical applications.[167] [168] The high-value identity ecosystem is likely to be heavily targeted. Increasingly sophisticated threat actors will capitalize on the opportunity to exploit vulnerabilities in its component parts (e.g. authentication devices and mechanisms,[169] [170] access-management, communications and databases) and the actions of users in order to take over accounts, subvert transactions and harvest sensitive data, for example. Criminals will seek to abuse the system for financial gain, and various actors within the digital identity ecosystem (e.g. industry identity providers and governments) may seek to exploit their position to gain economic or political advantage, both overtly and covertly.

Threats to the ID ecosystem: threat groups and motivations

THE INSIDER
Intentional or unintentional

Motivation: Grudge, financial gain

Trusted and able to subvert access controls, physical security management, software development processes, configuration and asset management. Agents for other threat groups

COMPETITORS
Competition or rivalry

Motivation: Competitive advantage

Engagement of third party to undertake attacks on their behalf, use of insiders (recruitment and placement)

NATION STATE
Espionage and sabotage

Motivation: Political and economic advantage

Large-scale espionage including account takeover, defeat of authentication systems, infrastructure attacks, tracking and surveillance. Impersonation and construction of legends

ORGANIZED CRIME
Global, difficult to trace and prosecute

Motivation: Financial advantage, potentially opportunistic

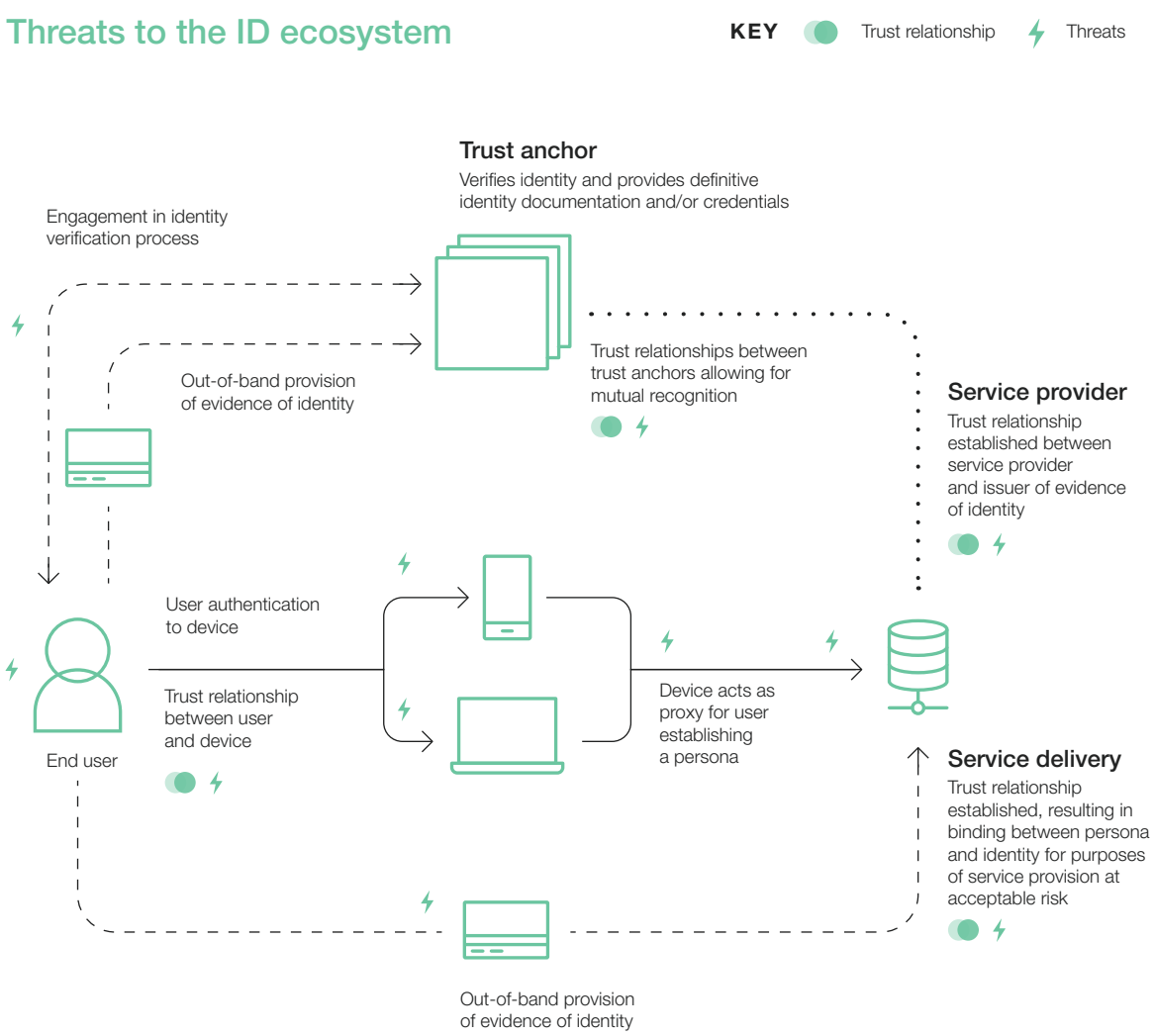
ID theft at large scale using stolen personal data. Account takeovers. Reuse of credentials. Defeat of authentication systems. Man in the middle attacks. Fake identity documents

HACKTIVISTS
Attention or popular causes

Motivation: Dynamic and unpredictable, potentially issue-motivated

Impersonation and account takeover. Defeat of authentication systems

Threats to the ID ecosystem



The risks to the security of emerging identity systems can be considered in terms of their **confidentiality, integrity and availability**.

- There will be a major **confidentiality** risk to the large amounts of personal information managed by identity systems (including personally identifiable information [PII], and biometric, behavioural and locational data). Minimizing the risk to this data will be critical.

- There is a risk that the **integrity** of the identity ecosystem will be subverted, reducing the confidence of participants in it. For participating actors, there are challenges to establishing the integrity of the components they depend on (particularly in cases where there is a trust deficit), and establishing their competence in protecting their part of the ecosystem against abuse.

- There is an **availability** risk: that attackers will attempt to prevent access to or use of identity infrastructure. If the infrastructure does not have the necessary resilience and fallback modes, then attacks on the availability of systems on which services depend critically could have grave consequences. Achieving resilience will be particularly challenging in those elements of society where infrastructure (both technical and governance) is weak.

Defenders will face new cybersecurity challenges associated with building a secure identity ecosystem and ensuring its integrity on an ongoing basis. Compromise will have increasingly severe and systemic impacts, and undermine the trust between actors that is necessary for the system to operate effectively.

Challenges and required action

The global digital identity ecosystem will be distributed and heterogeneous. Mitigating security risks within the end-to-end system will be a challenge, yet it is necessary in order that its users (relying parties and individuals) have confidence in how the system as a whole operates, and its providers have confidence that the infrastructure they are interacting with is trustworthy. The need to secure the ecosystem will need to extend to edge cases, and ensure that parts of the global population are not excluded.

If security challenges are not adequately addressed, confidence in the digital identity ecosystem will be dented, which could prevent its full potential value being unlocked. Senior leaders will need to act in order to achieve a resilient and secure digital identity ecosystem, and the security community has a vital role to play in this.

Assurance, trust and transparency

For digital identity solutions to be trusted and taken up, there is a need for assurance and transparency between actors in terms of the security and resilience of their different components.[171] Actors participating in identity transactions have to be able to accurately understand the extent to which the end-to-end process is trustworthy, and to make informed decisions on whether to implement additional assurance mechanisms to make up for trust deficits (where their confidence in the integrity of the process is limited). Of course, it is ultimately up to the relying parties to determine the degree of additional assurance required, but greater consistency in the way in which these requirements are articulated and understood will reduce friction and enable interoperability on a greater scale.

Much progress has been made in developing security approaches and standards for identity systems that are self-contained, and for guiding aspects of the requirements of identity management, such as identity proofing, how to assure authentication, and biometric security.[172] [173] [174] [175] [176] [177] Examples of nationally and regionally defined performance standards exist, supporting the validation of transactions that require varying levels of trust (while avoiding inappropriately costly demands).[178] [179] Comprehensive criteria do not, however, yet exist for the distributed identity ecosystem, and differing policy considerations and business drivers are leading to a lack of interoperable approaches and trust across sectors and businesses.[180]

It is important to avoid circumstances in which false assumptions about the security of systems used to support identity management could lead to suboptimal security of the services that leverage them (as has already happened with the use of SMS to support the authentication of users for financial transactions).[181] Creating transparency around the security attributes (and inherent weaknesses) of systems within the identity management ecosystem will help industries seeking to develop innovative yet fit-for-purpose services.[182]

Shared and interoperable governance frameworks

A governance framework (standards, certifications) that is globally defined, or at least mutually recognized and interoperable, is needed, in order to create transitivity of trust through a common understanding of assurance levels. To promote trust between the various components of an identity ecosystem that is distributed globally, base levels of cybersecurity should be defined for those running identity systems and processes in order for them to participate – analogous to the global participation standards that exist in the aviation industry's standards and practices (ICAO SARPs) or the payments industry's data security standards (PCI DSS), for example.

These base levels need to include both technical requirements for the secure design of components of identity solutions, and process-assurance requirements. The base level will need to ensure that privacy is protected and may need to provide end users with the ability to exercise control over how their identity is being processed and shared. Consent about the use of personal data relating to identity needs to be meaningful and revocable.

Business and policy incentives have to be established, to drive the various ecosystem participants to meet these requirements and ensure that secure solutions are not priced out of the market. Incentive models need to support interoperability and innovation,

and to be underpinned by an understanding of how liability is assigned for assuring security in the various components of the ecosystem. Market forces – B2B contractual terms and insurance models – will play an important role in driving security behaviours, and certain regulation may be required to resolve conflicts of interest. There have been successful examples within the security community of industry groups convening to establish principles and incentivize participants to meet them; existing initiatives such as the Charter of Trust might be leveraged or their methods drawn upon.[183]

Promoting further approaches to creating transparency, such as developing open code and making use of existing trust networks, may be beneficial. Some industry players have convened to form trust-based alliances, e.g. the FIDO Alliance[184] and DID Alliance.[185]

Convening actors

As divergent approaches to digital identity become entrenched in the digital activities of varying nations and organizations, there is a need to convene actors to examine the interoperability issue and drive the development of the requisite governance frameworks and incentive models to secure the identity ecosystem. The roles of various actors – government, the private sector, civil society and important industry players (e.g. banks, telecommunications service providers and major technology companies) – need to be established.

Highlighting compelling use cases for digital identity where security and transitivity of trust are important could drive a greater level of design and policy collaboration between actors, despite differences in approach and philosophy globally. The COVID-19 crisis may be a compelling use case, since many of the longer-term ways of managing the crisis may depend on digital identity – although the extreme nature of the COVID-19 crisis could inadvertently lead to overly autocratic solutions that are not aligned with the widely recognized ideals of privacy, user-centricity and decentralization. Economic and political drivers may provide further suitable use cases (e.g. cross-border identification and economic inclusion).

Collaborative operational security

The operational-security community will need to be able to protect the distributed, heterogeneous and complex identity ecosystem against fraud and abuse, and respond to limit the impact of compromise. This will require new approaches and collaborative action.

The specialist security community will need to be engaged in assessing the end-to-end security of the identity ecosystem as it emerges, and remediating vulnerabilities in it. It is also important that, as these technologies are rolled out, the security community considers how to secure them against potential future threats (e.g. how to address the need for quantum-proof cryptography across distributed components).

A number of existing approaches to operational security will be challenged in distributed identity systems, and new technologies and operational methods will be needed. This includes approaches to detecting, tracing and countering fraud and abuse (capabilities that are well established for closed environments, but are less well understood for distributed environments). Approaches to modelling systemic-level threats that can account for actors with varying levels of privilege and motivations will be needed, as well as new approaches to efficiently sharing threat information and “stress signals” with the relevant actors.

The right operational security community, which can collaboratively reduce the attack surface and respond rapidly to incidents, will have to be created. There is a need to establish how to incentivize the various players across sectors and jurisdictions to contribute to collaborative fraud and abuse detection and mitigation, information and threat-signal sharing, vulnerability and update management, and incident response. It will be important that sufficient cybersecurity capacity is built to support actors in contributing to these activities.

Conclusion

The Future Series: Emerging Technology and Systemic Risk programme was launched to answer the single question:

Will our individual and collective approach to managing cyber risks be sustainable in the face of the major technology trends taking place in the near future?

The work has concluded that, while progress has been made in improving cybersecurity across the ecosystem, the increased complexity, pace, scale and interdependence shown by our forward look at technological trends will overwhelm many current defences. At the same time, the scope of our cybersecurity activities beyond systems and networks must significantly expand in consideration of growing integrity concerns – for example, in the information layer and the integrity of AI algorithms. New cybersecurity tools are required, as well as an understanding of how to deploy these new solutions effectively at pace throughout global systems. Without interventions now, it will be difficult to maintain the integrity and trust in the emerging technology on which future global growth depends.

New systemic risks are being created – for example, the concentration risk associated with dependence on a small number of major ecosystem providers, and the cascade risks associated with increased entanglement of IT-enabled business processes. These risks cannot be addressed by organizations acting alone. Policy interventions are required that encourage collaboration and accountability on the part of both businesses and governments.

Enterprise leaders need to think in terms of assuring the integrity and resilience of the interconnected business and social processes that sit on top of an increasingly complex technology environment – rather than cybersecurity being simply an issue of protecting systems and networks. Organizations need to keep abreast of how new technologies will affect their exposure to cyber risk and ensure that the necessary mitigations are put in place to keep risk within a tolerable and sustainable level. Leaders need the ability to plan more strategically for emerging risk so they can ensure that the organizations that deliver the most critical infrastructures do not suffer failures that are catastrophic for societies. We need to develop a shared global understanding of how emerging technologies could expose our systems to new attack surfaces.

Managing cyber risk within organizations is already a major leadership challenge. The costs for enterprises are increasing – building and maintaining cybersecurity capability is expensive, and the return on investment is uncertain. The risks associated with cyberthreats are often opaque, and it is difficult to calibrate the right nature and scale of investment in cybersecurity. Regulatory requirements are increasing and are often different among jurisdictions, and there is a risk that divergent approaches to tackling cybersecurity will act as a strategic barrier to cross-border data flow and e-commerce. Current approaches to supply-chain cybersecurity assurance are broken: Friction is being introduced by the need to provide security attestation, which does not necessarily give the level of assurance required, thus diverting resources away from more effective cybersecurity capacity investments.

These challenges are exacerbated by the continued failure of the community to tackle the problem at source. Many incidents are caused by a small number of cybercrime groups that face limited consequences for their actions. There is still a lack of credible deterrence.

Will our individual and collective approach to managing cyber risks be sustainable in the face of the major technology trends taking place in the near future? The answer is "yes", if we succeed in galvanizing collective action across the broad community of stakeholders involved:

- The **security and technology community** needs to prioritize interventions to improve the collective response that will be essential to cybersecurity operations and controlling new cyber risk effectively within business and critical national infrastructures.

- **Industry and government leadership** need to drive a set of policy actions that incentivize the take-up of security solutions, and that underpin greater trust and transparency between different components of the ecosystem: to clarify issues of liability; to reduce friction in current assurance and regulatory models; and to promote international business and trade in data and digital services.

- Finally, interventions are required from the **international community** to ensure that security issues are addressed in such a way that the benefits of emerging technology are inclusive, with particular regard to the needs of developing countries and the need for collective efforts to reduce cross-border cybercrime.

Security and technology community

The community needs to collaborate to identify the emergent gaps that are opening up in defensive operational capabilities and design, develop and deliver effective solutions:

1. New models and enriched information-sharing frameworks need to be developed to deliver situational awareness and facilitate real-time and automated defence in the face of increasingly complex technology environments. These need to be effective across national boundaries as well as throughout supply chains, recognizing divergent national security and regulatory regimes, and must be respectful of personal privacy.

2. Security principles and tools need to be developed to protect AI and advanced machine learning assets, and in tandem protect the privacy of individuals where personal data is being processed.

3. The community needs to convene to develop the security model for quantum computing that encompasses the integrity of algorithms and the secure integration of quantum into hybrid computing environments.

Actions are required to identify which parts of the ecosystem have an individual and collective dependence on cryptography, in addition to other security functions that rely on the complexity of computation, which is potentially threatened by quantum computing. This will require urgent action, both to identify the systemic nature of the risk and also to govern the management of it.

4. There needs to be a convening of security and business experts to establish how the quantum cryptography issue will affect end-to-end distributed business processes and who should take responsibility for mitigating the risk.

Capacity in the workforce will need to be developed to ensure that new approaches to operational defence can be delivered across the ecosystem.

5. Existing cybersecurity skills and education programmes need to be reviewed and enhanced to ensure that they reflect the impact of emerging technologies. These need to be made available globally.

The technical and security community needs to promote security standards that can help ensure

interoperability throughout the enterprise functions, including not only technology standards but also regulatory standards and appropriate enabling infrastructure development (e.g., private networks). This is true for all systems, but is most pressing in the digital identity environment due to its heterogeneous and distributed nature, and the need to ensure trust and privacy throughout the systems.

6. Global interoperability trust standards for next-generation digital identity systems are required that enable projection of trusted identity and personal privacy across heterogeneous systems and jurisdictions in order to support trade.

Industry and government leadership

New education, guidance and governance tools are required for enterprise leadership to address the security impact and risk associated with the use of emergent technology within their organizations and in the wider operational environment. This is essential in order to enable leaders to promote an agenda of increased and meaningful security, and to ensure solutions are developed that protect organizations and better prepare leaders for when significant incidents occur.

7. Enterprise leaders need tools for making decisions on how best to prepare for emerging risks. Greater transparency over incidents and their impacts will improve leaders' collective response.

The increasing entanglement of businesses and supply-chain interdependencies – as well as the growing regulatory and related security attestation processes – is creating an urgent need to deliver a mechanism for ensuring trustworthy and reliable organizational cybersecurity behaviours to underpin confidence across different components of the ecosystem. This is most pressing in areas where there is increasing shared reliance on infrastructure, such as major cloud and shared service providers. This will require the identification of gaps in incentive models and interventions to address them.

8. New and internationally applicable methods for security attestation are required to make governance cost-effective and meaningful. Standard-of-care models will need to be developed to support this and to underpin general confidence in supply chains.

9. Business will need to work with regulators and policy-makers to consider and promote clear responsibility and liability models. These need to be able to operate across international boundaries in order to support trade and reduce unnecessary friction.

10. Regulations and attestations need to reflect the dynamic real-time nature of the underlying technology and risk environment.

International community

The international community needs to develop policy interventions to ensure a level of cybersecurity capacity that will enable global inclusivity. Capacity needs to span all dimensions of cybersecurity, such that cybersecurity does not act as a strategic barrier to the wider adoption of technology and its potentially transformative value to the global economy. The capacity requirements include the need to maintain a skilled workforce and establish assured access to the more complex cyber-defensive capabilities.

11. Countries need to collaborate to provide equitable access to cybersecurity capacity. Frameworks should be developed for identifying national cybersecurity capacity in response to emerging risks, and policy interventions adopted to ensure strategic investments in such capacity can be made. An emerging technology risk register would assist in this process.

Collective action against the known cybercrime groups needs to be significantly enhanced and

interventions designed to close the gaps in collective investigation in order to promote more robust deterrence models for malicious behaviour in cyberspace.

12. Greater emphasis should be placed on the attribution and disruption of threat actors behind cybercrime. This requires increased collaboration between countries, international bodies and the technology businesses that deliver the underpinning infrastructure.

13. International capacity and commitment to combating cybercrime (and other related threats to the integrity of the global digital economy) should be strengthened by the establishment of standards and the effective promotion of legal, regulatory and operational measures.

There are increasing cross-border and cross-sectorial interdependencies between different components of national and international critical infrastructure.

14. An internationally consistent approach to the identification of critical national infrastructure components is required in order to ensure that cross-border risk aggregation is not hidden, and that systemic risk in cyberspace can be properly identified and prepared for.

15. International specialist trade bodies should develop the capacity for identifying emerging technology risks to their sectors and membership communities.

Acknowledgements

Accenture
Christine Leong
Kelly Bissell

Accepto
Shahrokh Shahidzadeh

Access Now
Naman Aggarwal
Brett Soloman

Airbus
Paolo Bianco

Aker
Anders Rimstad

Amazon
Jordana Siegel

Axis Capital
Daniel Trueman
Stuart Quick
Jo Chadha

Bank of America
Naveen Manivannan
Nicole Muryn Clement

Ben Gurion University
Oleg Brodt
Yuval Elovici

Better Identity Coalition
Jeremy Grant

Bill and Melinda Gates Foundation
Kanwaljit Singh

BI.ZONE
Arina Pazushko
Dmitry Samartsev

British Telecom
Kevin Brown
Ryan Parker
Andrew Lord

Carnegie Mellon University
Nicolas Christin
Giulia Fanti

Checkpoint
Sharon Schusheim
Gil Messing

City of Amsterdam
Baron Ger
Lies Alderlieste-de Wit

Cognite
Jakob Eide

Credit Suisse
Clayton Chandler
Martin Clements
Claude Honegger

Cujo AI
Einaras von Gravrock
Santeri Kangas
Indre Deksnyte

Darktrace
Nicole Eagan
David Palmer
Maximilian Heinemeyer
Kitty O'Neill

Deloitte
Andrew Morrison
Chris Verdonck
Colin Soutar
Matt Caccavale

Department for Digital, Culture, Media and Sport, UK
Hannah Rutter
Elizabeth Marsh-Rowbotham

ENISA
Evangelos Ouzounis
Ioannis Agrafiotis

Equifax
Ahmad Douglas
Jamil Farshchi
Lauren Wagner

Ericsson
Brian O'Toole

Europol
Phillip Aman
Nicole Samantha van der Meulen

FIDO Alliance
Andrew Shikiar

Forcepoint
Nicolas Fischbach
Nico Popp

Fortinet
Alan Sanchez
Phil Quade

Garrison Technologies
David Garfield
Henry Harrison

Global Identity Foundation
Paul Simmonds

GSMA
Amy Lemberger
David Rogers

Hewlett Packard Enterprise
Kirk Bresniker

Huawei
Bob Xie Zhijun

Iberdrola
Agustin Valencia
Gil-Ortega

IBM
Emily Ratliff
Jerry Chow
Nick Coleman

Imperial College, London
Sir Peter Knight

Iron Mountain
Kimberly Anstett

IOT Security Foundation
John Moor

KPMG
James Wilhelm
Ravi Jayanti
Hans-Peter Fischer
Orvil Keimig
David Ferbrache

KPN
Paul Slootmaker

Kudelski Security
Andrew Howard

Maersk
Andrew Powell

Mastercard
Peter Allwood
John Beric
Paul Trueman

McKinsey & Co.
James Kaplan
Henning Soller

MITRE
Irv Lachow

NHS Digital
John Noble

NIST
Katerina Megas
Carl Williams

Nokia
Antero Paivansalo

Office of National Intelligence
Christopher Brookes

Organization of American States
Belisario Contreras

Oxford Quantum Circuits
Ilana Wisby

Palo Alto Networks
Danielle Kriz
Greg Day

Proximus
Fabrice Clement

PwC
Grant Waterfall
Alexandre Amard

Queens University Belfast
David Crozier
Máire O'Neill

Quintessence Labs
Vikram Sharma
Jane Melia

Renault
Diego Baldini

Research ICT Africa
Gabriella Razzano

Ripjar Technologies
David Balson

Salesforce
Jim Alkove

Saudi Aramco
Muhanad Shahat
Bandar Al-Mashari
Ali Al-Amri

Saudi Aramco
Daniel Cuthbert
Daniel Barriuso
Fredrik Hult

Shape Security
Shuman Ghosemajumder

Swiss Telecom
Phillippe Vuilleumier
Marco Wyrsch

Team8
Nadav Zafrir
Bob Blakely

Telefonica
Patricia Diez Munoz
Pablo Alarcon Padellano
Sofia Bravo Arocha

Telenor
Anders Arnes

The German Marshall Fund of America
Sam duPont

University of Waterloo
Michele Mosca

University of Oxford
Michael Goldsmith

University of Surrey
David Birch

Wipro
Josey V George

Contributors

University of Oxford

Sadie Creese,
Professor of Cyber Security,
Department of Computer Science,
University of Oxford

Jamie Saunders,
Oxford Martin School Fellow,
University of Oxford

Louise Axon,
Research Associate in
Cybersecurity, University of Oxford

World Economic Forum

William Dixon,
Head of Future Networks
and Technology

Jordynn McKnight,
Design Lead

Jean-Phillipe Stanway,
Designer

Alison Moore,
Editor

Charles Phillips,
Editor

Karolis Strautniekas,
Folio Art Illustrator

Steering Committee Members

Nick Coleman,
Chief Security Officer of Payments,
Mastercard

Greg Day,
Vice-President and Chief Security
Officer EMEA,
Palo Alto

Dave Ferbrache,
Global Head of Cyber Futures,
KPMG

Endnotes

1 "The Global Risks Report 2020", World Economic Forum, January 2020: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (link as of 9/10/2020).

2 K. Schwab, "The Fourth Industrial Revolution: What It Means and How to Respond", World Economic Forum, January 2016: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ (link as of 9/10/2020).

3 S. Creese, R. Hannigan et al., "Foresight Review of Cyber Security for the Industrial IoT", Lloyd's Register Foundation, July 2020: https://www.lrfoundation.org.uk/en/news/cybersecurity-foresight-review/ (link as of 26/10/20).

4 "Transformative IoT: Beyond Connectivity", GSMA: https://www.gsma.com/iot/beyond-connectivity/ (link as of 9/10/2020).

5 "The Role of ICT in Reducing Carbon Emissions in the EU", BT, May 2016: https://www.bt.com/bt-plc/assets/documents/digital-impact-and-sustainability/our-approach/our-policies-and-reports/ict-carbon-reduction-eu.pdf (link as of 9/10/2020).

6 B. Ekholm and J. Rockström, "Digital Technology Can Cut Global Emissions by 15%. Here's How", World Economic Forum, January 2019: https://www.weforum.org/agenda/2019/01/why-digitalization-is-the-key-to-exponential-climate-action/ (link as of 9/10/2020).

7 "Foresight Review of Robotics and Autonomous Systems', Lloyd's Register Foundation, October 2016: https://www.lrfoundation.org.uk/en/news/foresight-review-of-robotics-and-autonomous-systems/ (link as of 9/10/2020).

8 "Rethinking the Value Chain: A study on AI, Humanoids and Robots", KPMG, 2018: https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/09/rethinking-the-value-chain.pdf (link as of 20/10/2020).

9 N. Joshi, "How AI Can and Will Predict Disasters", Forbes, March 2019: https://www.forbes.com/sites/cognitiveworld/2019/03/15/how-ai-can-and-will-predict-disasters/ (link as of 9/10/2020).

10 "Digital Transformation of Industries: Healthcare Industry", World Economic Forum in collaboration with Accenture, January 2016: http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/wef-dti-healthcarewhitepaper-final-january-2016.pdf (link as of 9/10/2020).

11 "Future of Food: Harnessing Digital Technologies to Improve Food System Outcomes", World Bank, April 2019: https://www.worldbank.org/en/topic/agriculture/publication/future-of-food-harnessing-digital-technologies-to-improve-food-system-outcomes (link as of 9/10/2020).

12 R. Dongoski, "Digital Agriculture: Enough to Feed a Rapidly Growing World?", Ernst & Young, April 2018: https://www.ey.com/en_gl/digital/digital-agriculture-data-solutions (link as of 9/10/2020).

13 "Global Lighthouse Network: Insights from the Forefront of the Fourth Industrial Revolution", World Economic Forum, December 2019: http://www3.weforum.org/docs/WEF_Global_Lighthouse_Network.pdf (link as of 9/10/2020).

14 "Identification for Development (ID4D) 2019 Annual Report", World Bank, 2019: http://documents.worldbank.org/curated/en/566431581578116247/pdf/Identification-for-Development-ID4D-2019-Annual-Report.pdf (link as of 9/10/2020).

15 "5G PPP Phase 1 Security Landscape", 5G PPP Security Working Group, 2017: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf (link as of 9/10/2020).

16 "An Introduction to Network Slicing", GSMA, 2017: https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf (link as of 9/10/2020).

17 M. Patel, D. Sabella, N. Sprecher and V. Young, "Mobile Edge Computing: A Key Technology Towards 5G", ETSI White Paper, p. 16, September 2015.

18 "Setting the Scene for 5G: Opportunities & Challenges", International Telecommunication Union (ITU), 2018: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-E.pdf (link as of 9/10/2020).

19 "The 5GCAR EU Initiative Demonstrates Future Wireless Vehicular Communication', 5GCAR (EU), June 2019: https://5gcar.eu/wp-content/uploads/2019/06/Final_Demonstration_PressRelease.pdf (link as of 9/10/2020).

20 "Transformative IoT: Beyond Connectivity", GSMA: https://www.gsma.com/iot/beyond-connectivity/ (link as of 9/10/2020).

21 IoT Cybersecurity Alliance: https://www.iotca.org/ (link as of 9/10/2020).

22 Charter of Trust: https://www.charteroftrust.com/ (link as of 9/10/2020).

23 Open RAN Policy Coalition: https://www.openranpolicy.org/ (link as of 9/10/2020).

24 "IoT Cybersecurity Certification", Cellular Telecommunications Industry Association, April 2020.

25 Interagency International Cybersecurity Standardization Working Group (IICS WG), “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)”, National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8200, November 2018: doi: https://doi.org/10.6028/NIST.IR.8200 (link as of 9/10/2020).

26 Report from an expert panel chaired by Carl Bildt, “Calling the Shots: Standardization for EU Competitiveness in a Digital Era”, October 2019: https://kreab.com/brussels/wp-content/uploads/sites/26/2019/10/etsi-report-a4-v9.pdf (link as of 9/10/2020).

27 Organisation for Economic Cooperation and Development: Working Party on Security and Privacy in the Digital Economy, “Roles and Responsibilities of Actors: Governance of Digital Security in Organisations and Security of Digital Technologies”, OECD Digital Economy Papers 248, December 2018: doi: https://www.oecd-ilibrary.org/science-and-technology/roles-and-responsibilities-of-actors-for-digital-security_3206c421-en (link as of 9/10/2020).

28 “Good Practices for Security of IoT: Secure Software Development Lifecycle”, European Union Agency for Cybersecurity, 2019: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1 (link as of 9/10/2020).

29 United Kingdom’s Multi-stakeholder Advisory Group on Cyber Issues, “Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015”, United Nations, 2019: https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf (link as of 9/10/2020).

30 “Connected and Autonomous Vehicles: The Future?”, UK Parliament Science and Technology Committee, March 2017: https://publications.parliament.uk/pa/ld201617/ldselect/ldsctech/115/11502.htm (link as of 9/10/2020).

31 “California Consumer Privacy Act”, State of California – Department of Justice – Office of the Attorney General, 2018: https://oag.ca.gov/privacy/ccpa (link as of 9/10/2020).

32 “The Directive on Security of Network and Information Systems (NIS Directive)”, Shaping Europe’s Digital Future – European Commission, 5 July 2016: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (link as of 9/10/2020).

33 “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”, National Institute of Standards and Technology, April 2018: doi: 10.6028/NIST.CSWP.04162018 (link as of 9/10/2020).

34 K. Grace, J. Salvatier, A. Dafoe, B. Zhang and O. Evans, “When Will AI Exceed Human Performance? Evidence from AI Experts”, Journal of Artificial Intelligence Research, vol. 62, pp. 729–754, 2018.

35 “Worldwide Spending on Artificial Intelligence Systems Will Be Nearly $98 Billion in 2023, According to New IDC Spending Guide”, International Data Corporation, September 2019: https://www.idc.com/getdoc.jsp?containerId=prUS45481219 (link as of 9/10/2020).

36 X. Mou, “Artificial Intelligence: Investment Trends and Selected Industry Uses”, International Finance Corporation (World Bank Group), September 2019: https://www.ifc.org/wps/wcm/connect/7898d957-69b5-4727-9226-277e8ae28711/EMCompass-Note-71-AI-Investment-Trends.pdf?MOD=AJPERES&CVID=mR5Jvd6 (link as of 9/10/2020).

37 “Gartner Survey Reveals Leading Organizations Expect to Double the Number of AI Projects In Place Within the Next Year”, Gartner Newsroom Press Releases, July 2019: https://www.gartner.com/en/newsroom/press-releases/2019-07-15-gartner-survey-reveals-leading-organizations-expect-t (link as of 9/10/2020).

38 “Foresight Review of Robotics and Autonomous Systems”, Lloyd’s Register Foundation, October 2016: https://www.lrfoundation.org.uk/en/news/foresight-review-of-robotics-and-autonomous-systems/ (link as of 9/10/2020).

39 “McAfee Labs 2020 Threats Predictions Report”, McAfee Blogs, 5 December 2019: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-2020-threats-predictions-report/ (link as of 9/10/2020).

40 T. C. King, N. Aggarwal, M. Taddeo and L. Floridi, “Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions”, Sci Eng Ethics, vol. 26, no. 1, pp. 89–120, February 2020: doi: 10.1007/s11948-018-00081-0 (link as of 9/10/2020).

41 M. Brundage et al., “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation”, 2018: https://arxiv.org/abs/1802.07228 (link as of 9/10/2020).

42 N. Kaloudi and J. Li, “The AI-Based Cyber Threat Landscape: A Survey”, ACM Comput. Surv., vol. 53, no. 1, pp. 1–34, May 2020: doi: 10.1145/3372823 (link as of 9/10/2020).

43 “AI-Augmented Attacks and the Battle of the Algorithms”, Darktrace, 2019: https://futurecio.tech/ai-augmented-attacks-and-the-battle-of-the-algorithms/ (link as of 9/10/2020).

44 J. Seymour and P. Tully, “Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter”, Black Hat USA, vol. 37, 2016: https://www.slideshare.net/cisoplatform7/weaponizing-data-science-for-social-engineering-automate-e2e-spear-phishing-on-twitter (link as of 9/10/2020).

45 “Sophos 2020 Threat Report”, Sophos, December 2019: https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf (link as of 9/10/2020).

46 H. S. Anderson, J. Woodbridge and B. Filar, “DeepDGA: Adversarially-Tuned Domain Generation and Detection”, in Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security, 2016, pp. 13–21.

47 H. S. Anderson, A. Kharkar and B. Filar, “Evading Machine Learning Malware Detection”, Black Hat USA, p. 6, 2017.

48 H. S. Anderson, A. Kharkar, B. Filar, D. Evans and P. Roth, “Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning”, 2018: https://arxiv.org/pdf/1801.08917.pdf (link as of 9/10/2020).

49 L. Tong, B. Li, C. Hajaj and Y. Vorobeychik, “Feature Conservation in Adversarial Classifier Evasion: A Case Study”, 2017: https://arxiv.org/abs/1708.08327v1 (link as of 9/10/2020).

50 W. Xu, Y. Qi and D. Evans, “Automatically Evading Classifiers: A Case Study on PDF Malware Classifiers”, presented at the Network and Distributed System Security Symposium, San Diego, CA, 2016: doi: 10.14722/ndss.2016.23115 (link as of 9/10/2020).

51 uvasrg/EvadeML, UVa Security Research Group, 2020.

52 “Innovations of AlphaGo”, DeepMind Research Blog, 10 April 2017: https://deepmind.com/blog/article/innovations-alphago (link as of 9/10/2020)

53 G. Press, “AI Stats News: Humans Plus AI 20X More Effective In Cybersecurity Defense than Traditional Methods”, Forbes, November 2019: https://www.forbes.com/sites/gilpress/2019/11/07/ai-stats-news-humans-plus-ai-20x-more-effective-in-cybersecurity-defense-than-traditional-methods/ (link as of 9/10/2020).

54 L. Columbus, “10 Charts that Will Change Your Perspective of AI in Security”, Forbes, November 2019: https://www.forbes.com/sites/louiscolumbus/2019/11/04/10-charts-that-will-change-your-perspective-of-ai-in-security/ (link as of 9/10/2020).

55 “Artificial Intelligence (AI) in Cybersecurity Market Worth $46.3 billion by 2027 – Exclusive Report Covering Pre and Post COVID-19 Market Estimates by Meticulous Research”, GlobeNewswire News Room, 19 June 2020.

56 H. S. Anderson, A. Kharkar and B. Filar, “Evading Machine Learning Malware Detection”, Black Hat USA, p. 6, 2017.

57 H. S. Anderson, A. Kharkar, B. Filar, D. Evans and P. Roth, “Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning”, 2018: https://arxiv.org/pdf/1801.08917.pdf (link as of 9/10/2020).

58 “Cylance Antivirus Products Susceptible to Concatenation Bypass”, Carnegie Mellon University Software Engineering Institute, CERT Coordination Center, CERT/CC Vulnerability Note VU#489481: https://www.kb.cert.org (link as of 9/10/2020).

59 “Sophos 2020 Threat Report”, Sophos, December 2019: https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf (link as of 9/10/2020).

60 F. Wu, J. Wang, J. Liu and W. Wang, “Vulnerability Detection with Deep Learning”, in 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, December 2017, pp. 1298–1302: doi: 10.1109/CompComm.2017.8322752 (link as of 9/10/2020).

61 V. Murali, L. Qi, S. Chaudhuri and C. Jermaine, “Neural Sketch Learning for Conditional Program Generation”, 2018: http://arxiv.org/abs/1703.05698 (link as of 9/10/2018).

62 M. Nye, L. Hewitt, J. Tenenbaum and A. Solar-Lezama, “Learning to Infer Program Sketches”, 2019: http://arxiv.org/abs/1902.06349 (link as of 9/10/2020).

63 A. J. Saleh et al., “An Intelligent Spam Detection Model Based on Artificial Immune System”, Information, vol. 10, no. 6, p. 209, June 2019: doi: 10.3390/info10060209 (link as of 9/10/2019).

64 D. Berman, A. Buczak, J. Chavis and C. Corbett, “A Survey of Deep Learning Methods for Cyber Security”, Information, vol. 10, no. 4, p. 122, April 2019: doi: 10.3390/info10040122 (link as of 9/10/2019).

65 C. D. McDermott, F. Majdani and A. V. Petrovski, “Botnet Detection in the Internet of Things Using Deep Learning Approaches”, in International Joint Conference on Neural Networks (IJCNN), July 2018, pp. 1–8: doi: 10.1109/IJCNN.2018.8489489 (link as of 9/10/2019).

66 C. Yin, Y. Zhu, S. Liu, J. Fei and H. Zhang, “An Enhancing Framework for Botnet Detection Using Generative Adversarial Networks”, in International Conference on Artificial Intelligence and Big Data (ICAIBD), 2018, pp. 228–234.

67 C. Yin, Y. Zhu, J. Fei and X. He, “A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks”, IEEE Access, vol. 5, pp. 21954–21961, 2017: doi: 10.1109/ACCESS.2017.2762418 (link as of 9/10/2020).

68 J. Pawlick, E. Colbert and Q. Zhu, “A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy”, ACM Comput. Surv., vol. 52, no. 4, pp. 1–28, September 2019: doi: 10.1145/3337772 (link as of 9/10/2020).

69 S. Fugate and K. Ferguson-Walter, “Artificial Intelligence and Game Theory Models for Defending Critical Networks with Cyber Deception”, AIMag, vol. 40, no. 1, pp. 49–62, March 2019: doi: 10.1609/aimag.v40i1.2849 (link as of 9/10/2020).

70 M. Taddeo and L. Floridi, “Regulate Artificial Intelligence to Avert Cyber Arms Race”, Nature, vol. 556, no. 7701, p. 296, 2018: https://www.nature.com/articles/d41586-018-04602-6?amp;amp (link as of 9/10/2020).

71 E. Nunes, N. Kulkarni, P. Shakarian, A. Ruef and J. Little, “Cyber-Deception and Attribution in Capture-the-Flag Exercises”, presented at the 2012 IEEE/ACM International Conference on Advances in Social Network Analysis and Mining, Istanbul, August 2012.

72 E. Nunes, P. Shakarian, G. I. Simari and A. Ruef, Artificial Intelligence Tools for Cyber Attribution, Springer, 2018.

73 "Know Your Threat: AI is the New Attack Surface", Accenture Labs, 2019: https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf (link as of 9/10/2020).

74 N. Papernot, P. McDaniel, A. Sinha and M. P. Wellman, "SoK: Security and Privacy in Machine Learning", in 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, April 2018, pp. 399–414: doi: 10.1109/EuroSP.2018.00035 (link as of 9/10/2020).

75 M. I. Jordan and T. M. Mitchell, "Machine Learning: Trends, Perspectives, and Prospects", Science, vol. 349, no. 6245, pp. 255–260, July 2015: doi: 10.1126/science.aaa8415 (link as of 9/10/2020).

76 B. Biggio, B. Nelson and P. Laskov, "Poisoning Attacks against Support Vector Machines", 2012: https://arxiv.org/abs/1206.6389 (link as of 9/10/2020).

77 B. Biggio and F. Roli, "Wild Patterns: Ten Years after the Rise of Adversarial Machine Learning", Pattern Recognition, vol. 84, pp. 317–331, 2018.

78 S. Herpig, "Securing Artificial Intelligence", October 2019: https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf (link as of 9/10/2020).

79 "Tencent Keen Security Lab: Experimental Security Research of Tesla Autopilot", Keen Security Lab Blog: https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/ (link as of 9/10/2020).

80 E. Zakharov, A. Shysheya, E. Burkov and V. Lempitsky, "Few-Shot Adversarial Learning of Realistic Neural Talking Head Models", in IEEE/CVF International Conference on Computer Vision (ICCV), October 2019, pp. 9458–9467: doi: 10.1109/ICCV.2019.00955 (link as of 9/10/2020).

81 deepfakes/faceswap, 2020.

82 A. K. Cybenko and G. Cybenko, "AI and Fake News", IEEE Intelligent Systems, vol. 33, no. 5, pp. 1–5, 2018.

83 B. Buchanan, "A National Security Research Agenda for Cybersecurity and Artificial Intelligence", Center for Security and Emerging Technology, May 2020: https://cset.georgetown.edu/wp-content/uploads/CSET-A-National-Security-Research-Agenda-for-Cybersecurity-and-Artificial-Intelligence.pdf (link as of 9/10/2020).

84 G. Chng, "Deepfakes Is an Emerging Threat Vector", RSA Conference, 24 July 2019: http://www.rsaconference.com/industry-topics/blog/deepfakes-is-an-emerging-threat-vector (link as of 9/10/2020).

85 "Faked Pelosi Videos, Slowed to Make Her Appear Drunk, Spread across Social Media", The Washington Post, May 2019.

86 "An Artificial-Intelligence First: Voice-Mimicking Software Reportedly Used in a Major Theft", The Washington Post, September 2019.

87 D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks", in International Conference on Advanced Video and Signal Based Surveillance (AVSS), November 2018, pp. 1–6: doi: 10.1109/AVSS.2018.8639163 (link as of 9/10/2020).

88 S. Kwon, M. Cha and K. Jung, "Rumor Detection over Varying Time Windows", PLoS ONE, vol. 12, no. 1, p. e0168344, January 2017: doi: 10.1371/journal.pone.0168344 (link as of 9/10/2020).

89 J. Zhang et al., "Protecting Intellectual Property of Deep Neural Networks with Watermarking", in Proceedings of the 2018 on Asia Conference on Computer and Communications Security - ASIACCS '18, Incheon, Republic of Korea, 2018, pp. 159–172: doi: 10.1145/3196494.3196550 (link as of 9/10/2020).

90 G. Allen and T. Chan, "Artificial Intelligence and National Security", Belfer Center for Science and International Affairs Cambridge (MA), 2017.

91 M. Taddeo and L. Floridi, "Regulate Artificial Intelligence to Avert Cyber Arms Race", Nature, vol. 556, no. 7701, p. 296, 2018.

92 M. Taddeo, T. McCutcheon and L. Floridi, "Trusting Artificial Intelligence in Cybersecurity is a Double-Edged Sword", Nature Machine Intelligence, vol. 1, no. 12, Art. no. 12, December 2019: doi: 10.1038/s42256-019-0109-1 (link as of 9/10/2020).

93 "ISO/IEC JTC 1/SC 42 – Artificial Intelligence", ISO: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/67/94/6794475.html (link as of 9/10/2020).

94 "Artificial Intelligence Standardization White Paper", China Electronics Standardization Institute, January 2018: https://cset.georgetown.edu/research/artificial-intelligence-standardization-white-paper/ (link as of 9/10/2020).

95 S. Herpig, "Securing Artificial Intelligence", October 2019: https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf (link as of 9/10/2020).

96 "Guaranteeing AI Robustness Against Deception", Defense Advanced Research Projects Agency: https://www.darpa.mil/program/guaranteeing-ai-robustness-against-deception (link as of 9/10/2020).

97 "Securing AI against Adversarial Threats with Open Source Toolbox", IBM Research Blog, 17 April 2018: https://www.ibm.com/blogs/research/2018/04/ai-adversarial-robustness-toolbox/ (link as of 9/10/2020).

98 "Introducing AI Explainability 360", IBM Research Blog, 8 August 2019: https://www.ibm.com/blogs/research/2019/08/ai-explainability-360/ (link as of 9/10/2020).

99 D. Gunning and D. W. Aha, "DARPA's Explainable Artificial Intelligence Program", AI Magazine, vol. 40, no. 2, pp. 66–72, 24 June 2019.

100 "ICO and the Turing Consultation on Explaining AI Decisions Guidance", 20 May 2020: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-and-the-turing-consultation-on-explaining-ai-decisions-guidance/ (link as of 9/10/2020).

101 "Identifying and Eliminating Bugs in Learned Predictive Models", DeepMind, 28 March 2019: https://deepmind.com/blog/article/robust-and-verified-ai (link as of 9/10/2020).

102 F. Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor", Nature, vol. 574, no. 7779, pp. 505–510, October 2019: doi: 10.1038/s41586-019-1666-5 (link as of 9/10/2020).

103 S. Bravyi, D. Gosset and R. König, "Quantum Advantage with Shallow Circuits", Science, vol. 362, no. 6412, pp. 308–311, October 2018: doi: 10.1126/science.aar3106 (link as of 9/10/2020).

104 M. Bayern, "Honeywell Claims to Surpass IBM with the World's Fastest Quantum Computer", TechRepublic, June 2020: https://www.techrepublic.com/article/honeywell-claims-to-surpass-ibm-with-the-worlds-fastest-quantum-computer/ (link as of 9/10/2020).

105 E. Gibney, "Quantum Gold Rush: The Private Funding Pouring into Quantum Start-Ups', Nature, vol. 574, no. 7776, Art. no. 7776, October 2019: doi: 10.1038/d41586-019-02935-4 (link as of 9/10/2020).

106 P. Bajpai, "Quantum Computing: How to Invest in It, and Which Companies Are Leading the Way?", Nasdaq, February 2020: https://www.nasdaq.com/articles/quantum-computing%3A-how-to-invest-in-it-and-which-companies-are-leading-the-way-2020-02-11 (link as of 9/10/2020).

107 P. Smith-Goodson, "Quantum USA vs. Quantum China: The World's Most Important Technology Race", Forbes, October 2019: https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#6bd82d5272de (link as of 20/10/2020).

108 P. Guest, "The Subatomic Age: Asia's Quantum Computing Arms Race", Nikkei Asian Review: https://asia.nikkei.com/Business/Technology/The-subatomic-age-Asia-s-quantum-computing-arms-race2 (link as of 9/10/2020).

109 "Quantum Computing Market to Reach $1 Trillion by 2035", Consultancy.uk, 15 April 2020: https://www.consultancy.uk/news/24361/quantum-computing-market-to-reach-1-trillion-by-2035 (link as of 9/10/2020).

110 "Where Will Quantum Computers Create Value—and When?", BCG, May 2019: https://www.bcg.com/en-gb/publications/2019/quantum-computers-create-value-when.aspx (link as of 9/10/2020).

111 "A Game Plan for Quantum Computing", McKinsey Global Institute, February 2020: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing (link as of 9/10/2020).

112 D. Schatsky and R. K. Puliyakodil, "From Fantasy to Reality: Quantum Computing Is Coming to the Marketplace", April 2017: https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/quantum-computing-enterprise-applications.html (link as of 9/10/2020).

113 "The Growing Potential of Quantum Computing", McKinsey Global Institute, February 2016: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-growing-potential-of-quantum-computing (link as of 9/10/2020).

114 E. P. DeBenedictis, "A Future with Quantum Machine Learning", Computer, vol. 51, no. 2, pp. 68–71, February 2018: doi: 10.1109/MC.2018.1451646 (link as of 9/10/2020).

115 "Will Quantum Computing Transform Biopharma R&D?", BCG, December 2019: https://www.bcg.com/en-gb/publications/2019/quantum-computing-transform-biopharma-research-development.aspx (link as of 9/10/2020).

116 "Quantum Computing and the Chemical Industry", McKinsey & Company, July 2019: https://www.mckinsey.com/industries/chemicals/our-insights/the-next-big-thing-quantum-computings-potential-impact-on-chemicals (link as of 9/10/2020).

117 M. Kühn, S. Zanker, P. Deglmann, M. Marthaler and H. Weiß, "Accuracy and Resource Estimations for Quantum Chemistry on a Near-Term Quantum Computer", J. Chem. Theory Comput., vol. 15, no. 9, pp. 4764–4780, September 2019: doi: 10.1021/acs.jctc.9b00236 (link as of 9/10/2020).

118 N. Stamatopoulos et al., "Option Pricing Using Quantum Computers", February 2020: http://arxiv.org/abs/1905.02666 (link as of 9/10/2020).

119 "Getting Your Financial Institution Ready for the Quantum Computing Revolution", IBM Expert Insights, 2019: https://www.ibm.com/downloads/cas/MBZYGRKY (link as of 9/10/2020).

120 "Airbus Quantum Computing Challenge", Airbus: https://www.airbus.com/innovation/tech-challenges-and-competitions/airbus-quantum-computing-challenge.html (link as of 9/10/2020).

121 V. Havlíček et al., "Supervised Learning with Quantum-Enhanced Feature Spaces", Nature, vol. 567, no. 7747, pp. 209–212, March 2019: doi: 10.1038/s41586-019-0980-2 (link as of 9/10/2020).

122 "Amazon Braket", Amazon Web Services: https://aws.amazon.com/braket/ (link as of 9/10/2020).

123 “IBM Q System One”, IBM: https://www.research.ibm.com/ibm-q/qed/index.html (link as of 9/10/2020).

124 Dario Gil, IBM Research, “The Quantum Era of Accelerated Discovery (presentation)”, May 2020: https://www.youtube.com/watch?v=zOGNoDO7mcU&app=desktop (link as of 9/10/2020).

125 J. Chu, “The Beginning of the End for Encryption Schemes?”, MIT News, March 2016: http://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303 (link as of 9/10/2020).

126 P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997: https://arxiv.org/abs/quant-ph/9508027 (link as of 9/10/2020).

127 G. Alagic et al., “Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process”, National Institute of Standards and Technology, January 2019: doi: 10.6028/NIST.IR.8240 (link as of 9/10/2020).

128 H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee and R. Cammarota, “Post-Quantum Lattice-Based Cryptography Implementations: A Survey”, ACM Comput. Surv., vol. 51, no. 6, pp. 1–41, January 2019: doi: 10.1145/3292548 (link as of 9/10/2020).

129 “SAFEcrypto”: https://www.safecrypto.eu/ (link as of 9/10/2020).

130 P. Wallden and E. Kashefi, “Cyber Security in the Quantum Era”, Commun. ACM, vol. 62, no. 4, pp. 120–120, March 2019: doi: 10.1145/3241037 (link as of 9/10/2020).

131 “Implementation Security of Quantum Cryptography – Introduction, Challenges, Solutions [White Paper]”, ETSI, July 2018.

132 G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, “Limitations on Practical Quantum Cryptography”, Phys. Rev. Lett., vol. 85, no. 6, pp. 1330–1333, August 2000: doi: 10.1103/PhysRevLett.85.1330 (link as of 9/10/2020).

133 L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, “Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination”, Nature Photon, vol. 4, no. 10, pp. 686–689, October 2010: doi: 10.1038/nphoton.2010.214 (link as of 9/10/2020).

134 “Quantum Security Technologies [White Paper]’, National Cyber Security Centre, March 2020: https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies (link as of 9/10/2020).

135 “New White Paper Published by the National Cyber Security Centre”, UK Quantum Communications Hub, 1 April 2020: https://www.quantumcommshub.net/news/new-white-paper-published-by-the-national-cyber-security-centre/ (link as of 9/10/2020).

136 “Cryptography in a Post-Quantum World’, Accenture, October 2018: https://www.accenture.com/us-en/insights/technology/quantum-cryptography (link as of 9/10/2020).

137 S. Buchholz, J. Mariani, A. Routh, A. Keyal and P. Kishnani, “The Realist’s Guide to Quantum Technology and National Security (Deloitte Insights)”, p. 20, 2020.

138 “Certified True Randomness Created by CQC”, Cambridge Quantum Computing, 28 July 2017: https://cambridgequantum.com/certified-true-randomness-created-by-cqc/ (link as of 9/10/2020).

139 “U.S. Considers Adding Export Controls on Quantum Technology”, Quantum Computing Report: https://quantumcomputingreport.com/u-s-considers-adding-export-controls-on-quantum-technology/ (link as of 9/10/2020).

140 M. Mosca, “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?”, IEEE Secur. Privacy, vol. 16, no. 5, pp. 38–41, September 2018: doi: 10.1109/MSP.2018.3761723 (link as of 9/10/2020).

141 A. Broadbent, J. Fitzsimons and E. Kashefi, “Universal Blind Quantum Computation”, in 2009 50th Annual IEEE Symposium on Foundations of Computer Science, October 2009, pp. 517–526: doi: 10.1109/FOCS.2009.36 (link as of 9/10/2020).

142 “The Quantum Age: Technological Opportunities”, UK Government Office for Science, 2016.

143 “National Strategic Overview for Quantum Information Science”, US National Science and Technology Council, September 2018: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf (link as of 9/10/2020).

144 “NIST Launches Consortium to Support Development of Quantum Industry”, NIST, 28 September 2018: https://www.nist.gov/news-events/news/2018/09/nist-launches-consortium-support-development-quantum-industry (link as of 9/10/2020).

145 G. Alagic et al., “Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process”, National Institute of Standards and Technology, January 2019: doi: 10.6028/NIST.IR.8240 (link as of 9/10/2020).

146 “Call for a Global Convention on Ethical AI”, UNI Global: http://www.thefutureworldofwork.org/opinions/call-for-a-global-convention-on-ethical-ai/ (link as of 9/10/ 2020).

147 “Reimagining Digital Identity: A Strategic Imperative”, World Economic Forum Community Paper, January 2020: https://www.weforum.org/whitepapers/reimagining-digital-identity-a-strategic-imperative (link as of 9/10/2020).

148 “Passwordless Authentication: The Next Breakthrough in Secure Digital Transformation”, World Economic Forum in collaboration with FIDO Alliance, January 2020: https://www.weforum.org/whitepapers/passwordless-authentication-the-next-breakthrough-in-secure-digital-transformation; http://www3.weforum.org/docs/WEF_Passwordless_Authentication.pdf (links as of 9/10/2020).

149 “Five Key Initiatives”, The Better Identity Coalition: https://www.cbetteridentity.org/five-key-initiatives (link as of 9/10/2020).

150 “Identification for Development (ID4D) 2019 Annual Report”, World Bank, 2019: http://documents.worldbank.org/curated/en/566431581578116247/pdf/Identification-for-Development-ID4D-2019-Annual-Report.pdf (link as of 9/10/2020).

151 “Grant: Financial Services for the Poor”, Bill and Melinda Gates Foundation and Alan Turing Institute, December 2019: https://www.gatesfoundation.org/How-We-Work/Quick-Links/Grants-Database/Grants/2019/12/INV-001309 (link as of 9/10/2020).

152 “High Level Requirements (the Key Stakeholders Perspective on Identity 3.0)”, Global Identity Foundation, September 2019. https://www.globalidentityfoundation.org/downloads/High_Level_(Key_Players)_Requirements.pdf

153 “2019 Data Breach Investigations Report”, Verizon, 2019.

154 “National Digital Identity Programmes: What’s Next?”, Access Now, May 2018: https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf (link as of 9/10/2020).

155 “eIDAS Compliant eID Solutions: Security Considerations and the Role of ENISA”, European Union Agency for Cybersecurity, Report/Study, March 2020: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions (link as of 9/10/2020).

156 D. Paddon, “Canada’s Big Banks Launch Verified.Me Network to Help Prevent ID Theft”, CBC News, 1 May 2019: https://www.cbc.ca/news/business/canada-big-banks-launch-verified-me-network-data-identify-theft-1.5118471 (link as of 9/10/2020).

157 “Identity 3.0 – Principles”, Global Identity Foundation, p. 1, July 2018. https://www.globalidentityfoundation.org/downloads/Identity_30_Principles.pdf

158 J. Beddington, “Foresight Future Identities: Final Project Report”, The Government Office for Science, London, 2013.

159 “Principles on Identification for Sustainable Development: Toward the Digital Age”, Access Now, February 2017: http://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf (link as of 9/10/2020).

160 A. Ma, “Thousands of People in Sweden Are Embedding Microchips Under Their Skin to Replace ID Cards”, Business Insider: https://www.businessinsider.com/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5 (link as of 18/10/2020).

161 P. Dunphy, L. Garratt and F. Petitcolas, “Decentralizing Digital Identity: Open Challenges for Distributed Ledgers”, 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018, pp. 75–78.

162 “Estonia – the Digital Republic Secured by Blockchain”, PwC, 2019: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf (link as of 20/10/2020).

163 Universa, “Russia May Stop Issuing Paper Passports”, Medium, 9 July 2019: https://medium.com/universablockchain/russia-may-stop-issuing-paper-passports-f91a15b34835 (link as of 18/10/2020).

164 Known Traveller Digital Identity, “Unlocking the Potential of Digital Identity for Secure and Seamless Travel”: https://ktdi.org/ (link as of 18/10/2020).

165 “Amazon Go”, Amazon.com: https://www.amazon.com/b?ie=UTF8&node=16008589011 (link as of 18/10/2020).

166 “Reimagining Digital Identity: A Strategic Imperative”, World Economic Forum Community Paper, January 2020: https://www.weforum.org/whitepapers/reimagining-digital-identity-a-strategic-imperative (link as of 20/10/2020).

167 David Birch, “Identity is the New Money”, London Publishing Partnership, 2014.

168 “Discover itsme®: Belgian Digital ID”, European Payments Council. https://www.europeanpaymentscouncil.eu/news-insights/insight/discover-itsmer-belgian-digital-id (link as of 18/10/2020).

169 A. Adler and S. Schuckers, “Biometric Vulnerabilities, Overview”, Encyclopedia of Biometrics, S. Z. Li and A. Jain, Eds. Boston, MA: Springer US, 2009, pp. 160–168.

170 P. Korshunov and S. Marcel, “Vulnerability of Face Recognition to Deep Morphing”, October 2019: http://arxiv.org/abs/1910.01933 (link as of 18/10/2020).

171 Deloitte, “Digital Identity: The Future Core of Trust”, Federal News Network, 29 June 2020: https://federalnewsnetwork.com/future-of-government-cyber/2020/06/digital-identity-the-future-core-of-trust/ (link as of 18/10/2020).

172 P. A. Grassi et al., “Digital Identity Guidelines: Enrollment and Identity Proofing”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63a, June 2017: doi: 10.6028/NIST.SP.800-63a (link as of 20/10/2020).

173 “Information Technology — Security Techniques — Entity Authentication Assurance Framework”, ISO/IEC 29115:2013: https://www.iso.org/obp/ui/#iso:std:iso-iec:29115:ed-1:v1:en (link as of 18/10/2020).

174 FIDO Alliance: https://fidoalliance.org/ (link as of 18/10/2020).

175 "ISO/IEC JTC 1/SC 37: Biometrics", ISO: https://committee.iso.org/home/jtc1sc37 (link as of 18/10/2020).

176 A. K. Jain, K. Nandakumar and A. Ross, "50 Years of Biometric Research: Accomplishments, Challenges and Opportunities", Pattern Recognition Letters, vol. 79, pp. 80–105, Aug. 2016: doi: 10.1016/j.patrec.2015.12.013 (link as of 20/10/2020).

177 E. Newton and C. Soutar, "The Quest to Measure Strength of Function for Authenticators: SOFA, So Good", presented at the RSA Conference, San Francisco, February 2017.

178 "eIDAS Compliant eID Solutions: Security Considerations and the Role of ENISA", European Union Agency for Cybersecurity, March 2020: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions (link as of 18/10/2020).

179 UK Government, "How to Prove and Verify Someone's Identity", GOV.UK: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-proofing-and-verification-of-an-individual (link as of 18/10/2020).

180 K. Megas, P. Lam, E. Nadeau and C. Soutar, "NSTIC Pilots: Catalyzing the Identity Ecosystem", National Institute of Standards and Technology, NIST IR 8054, April 2015: doi: 10.6028/NIST.IR.8054 (link as of 20/10/2020).

181 'SMS-based two-factor authentication is not safe — consider these alternative 2FA methods instead', *Kaspersky Daily*, Oct. 2018. https://www.kaspersky.com/blog/2fa-practical-guide/24219/ (accessed Jun. 17, 2020).

182 A. Drozhzhin, "SMS-Based Two-Factor Authentication Is Not Safe — Consider These Alternative 2FA Methods Instead", Kaspersky Daily, October 2018: https://www.kaspersky.com/blog/2fa-practical-guide/24219/ (link as of 20/10/2020).

183 Charter of Trust: https://www.charteroftrust.com/ (link as of 18/10/2020).

184 FIDO Alliance: https://fidoalliance.org/ (link as of 18/10/2020).

185 DID Alliance: http://www.didalliance.org (link as of 18/10/2020).

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