



مجلس الأمان السيبراني  
CYBER SECURITY COUNCIL



# Cyber next 50

Securing the UAE's 2071 vision

October 2023

KPMG Lower Gulf



**We are not just living for today or tomorrow, we are living to secure the future of our grandchildren, not just our children.**



**Sheikh Mohammed  
bin Zayed Al Nahyan**  
President of the  
United Arab Emirates

**Determination, strategy and vision for the future are our real resources in the quest for excellence and success.**



**Sheikh Mohammed  
bin Rashid Al Maktoum**  
Prime Minister of the  
United Arab Emirates

# Contents

1 Executive summary

2 Scope and approach

3 A cyber security retrospective

4 Megatrends

5 Imagine if...

6 Global cyber security themes in 2071

7 Securing the UAE's vision

8 Appendices

# Executive summary

The United Arab Emirates Cyber Security Council collaborated with KPMG to explore the future of cyber security over the next 50 years. Our research focuses on the myriad issues arising from the adoption of information technology and highlights the current trends that are expected to impact our lives in the upcoming decades. These megatrends include demographics, climate change, health challenges and energy consumption.

The world's population is expected to reach 9.7 billion by 2050<sup>1</sup>, bringing unique societal risks to different regions. Climate change driven by greenhouse gas emissions is also impacting food security and contributing to population displacement and the degradation of ecosystems. In addition, health challenges such as antimicrobial resistance and longer life expectancies are increasing pandemic risks and adding more pressure on healthcare systems. With global energy consumption expected to increase by 50% by 2050<sup>2</sup>, the importance of renewable sources and energy efficiency is also increasing in the face of rising costs and climate pressures.

Despite these risks, some technological and scientific solutions offer hope for a better future. In most cases, however, technology advances are neutral and can

bring advantages or disadvantages depending on how society embraces them. The technological innovations expected to shape our future include artificial intelligence, hyper connectivity, bio engineering, quantum computing, space technology, robotics, smart manufacturing, augmented reality and nuclear fusion.

KPMG experts therefore reviewed the social, economic and political trends of today, as well as future information technology trends, creating a set of "Imagine if" scenarios that explore the potential socio-political implications of technological advances. These scenarios were grouped into themes covering virtual worlds, robotics and artificial intelligence, the impact of omniscience, the integration between people and machines and the implications of our long-term reality.

The UAE is already positioned as the happiest place to live in the Arab world<sup>3</sup>, according to the latest UN World Happiness Report 2023. By 2071, quality of life and happiness will be increasingly determined by a safe and secure hybrid physical and digital world where citizens can freely socialize, work and play. In addition, the UAE's Digital Economy Strategy, which was launched in April 2022, seeks to double the contribution of the digital economy to the UAE's gross domestic product (GDP) from 9.7% in 2022 to 19.4% by 2032. It also aims to enhance the position of the UAE as a hub for digital economy in the region and globally.

The UAE is already a leading player when it comes to cyber safety: it ranks within the top five countries worldwide in the Global Cyber Security Index of the International Telecommunication Union (ITU) of the United Nations. Tailoring the UAE's legislation in the cyber security domain in preparation for the next 50 years will require an evolution towards a legislative framework that approaches humans, AIs and a combination of the two increasingly consistently.

In addition, the UAE's position of delivering humanitarian aid regardless of religion, race, color or culture is laudable. In the future the definition of humanitarian aid will likely evolve to include 'cyber security aid', as cyber-attacks increasingly have real world consequences for those less fortunate and able to deal with such attacks.

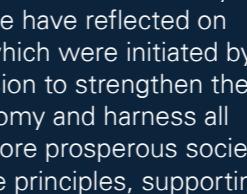
In our vision of the future, KPMG experts hypothesize that developments in immersive virtual reality will blur real life and fiction, with businesses thriving in the virtual world and data becoming the new money. Robots will seamlessly integrate into our lives, from personal care to military systems, while AI will be able to predict and shape the future. Hyperconnected sensors will also grant unprecedented omniscience and machines may develop the capability to read human thoughts and manipulate our DNA. To prolong the human lifespan, the rich and powerful will consider cloning, genetic manipulation and transferring memories to AI. Finally, with a focus on integrity, transparent supply chains will emerge, and cyber security will become an even more important part of national defense.

New models providing higher abstraction levels of permitted interactions between people and AI systems will be required, in addition to the need of new licensing frameworks. Cyber operations are expected to become more automated, forming partnerships between security professionals, AI tools and the decision-making systems that support them.

Fifty years since its founding, the UAE has evolved into a hub of dynamism, a symbol of perseverance and a happy and cohesive society. As the nation recently celebrated its golden jubilee, we have reflected on the ten 'Principles of the 50', which were initiated by the UAE government with a vision to strengthen the union, build a sustainable economy and harness all possible resources to build a more prosperous society. We are eager to embrace these principles, supporting the nation in the next 50 years and beyond.

that improve the country's ability to deal with advanced forms of fakery, deception, manipulation and criminal activity in the information space.

It has been a privilege to witness the UAE's rapid transformation over the years, and we look forward to contributing to its continued advancement in cyber innovation.



**HE Dr. Mohammed  
Al Kuwaiti**

Partner  
Head of Cyber Security  
United Arab Emirates  
Government



**Timothy Wood**

Head of Cyber Security  
KPMG Lower Gulf

# Imagine if ...

To bring the future to life, we have developed a series of "Imagine if" themes which are subdivided into hypothetical scenarios as follows:

## Reality and fiction blur

The creation of virtual worlds



We couldn't differentiate truth and fiction



People become lost in the virtual world



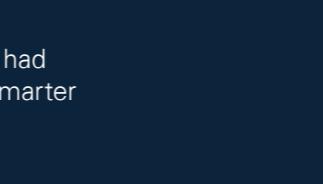
Data was money

## The power of the machine

The rise of robotics and artificial intelligence



Robots had become ubiquitous



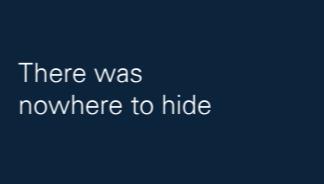
Machines had become smarter than us



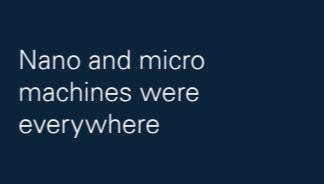
Machines could predict the future

## The impact of omniscience

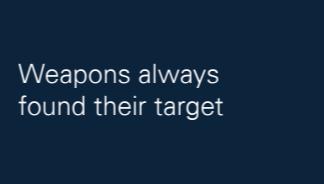
A world of networked sensors and effectors



There was nowhere to hide



Nano and micro machines were everywhere



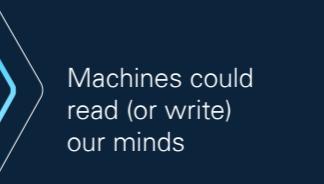
Weapons always found their target

## The new hybrid

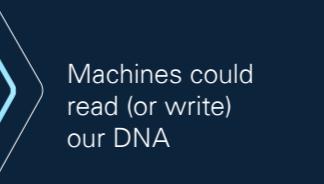
A coming together of people and machines



Machines anticipate our every need



Machines could read (or write) our minds



Machines could read (or write) our DNA

## Life, but not as we know it

What will the long term really bring?



People and machines became one



Tomorrow we never die



Each of the 'Imagine if' themes consider the possible sociopolitical implications of technological trends.



## Reality and fiction blur

- Commerce will dominate the virtual world with many new business streams focusing on the immersive experience
- Real world scenes and people will be replicated and manipulated in real time
- Data will become the new money



## The power of machines

- We imagine robots becoming accepted in every aspect of our lives, including personal care and military systems
- AI will be able predict and shape the future



## The impact of omniscience

- Hyperconnected sensors and nano and micro machines will become mainstream, allowing omniscience for states and corporations
- Weapons will likely be able to find their targets anywhere at an exceedingly high speed



## The new hybrid

- We foresee machines developing the ability to read people's thoughts
- Machines may sequence, analyze and write human DNA
- Integration between humans and technology will become widespread

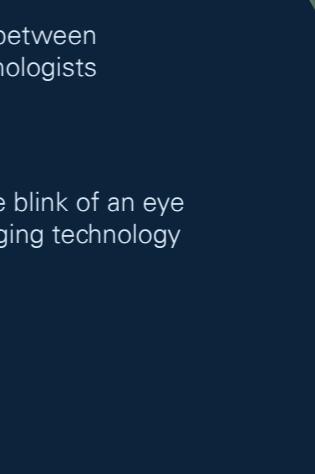
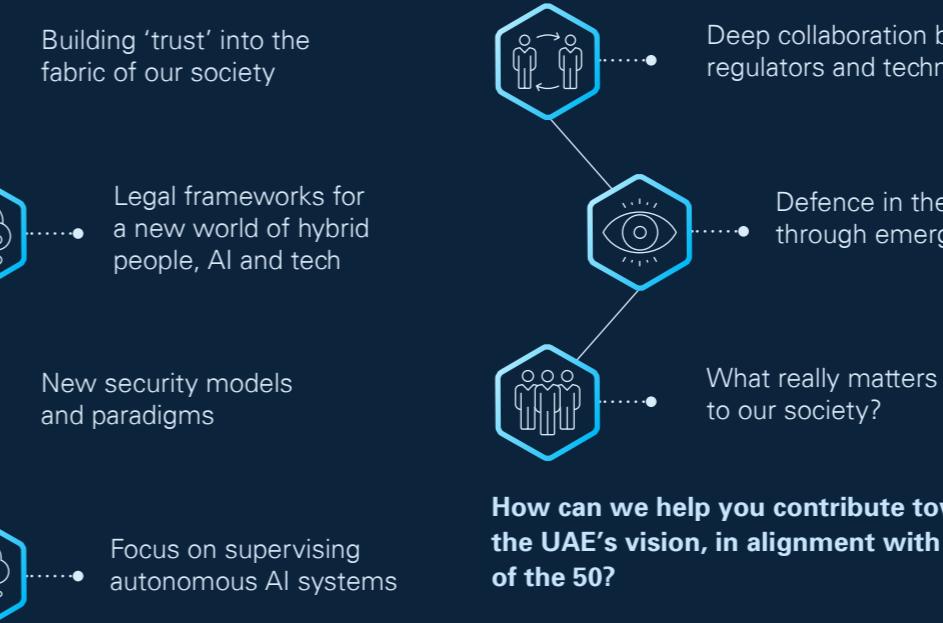
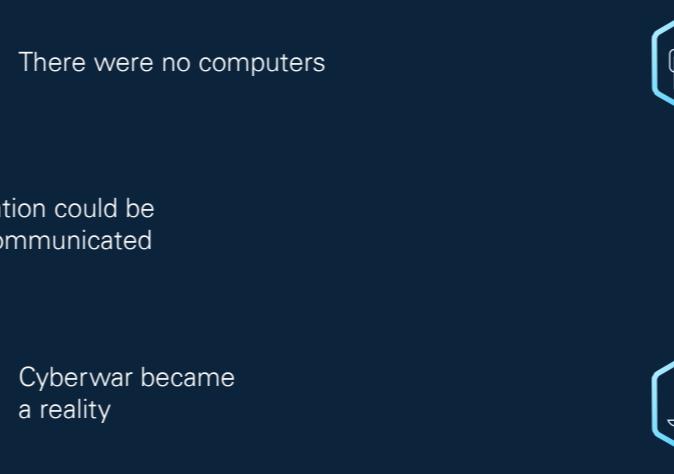
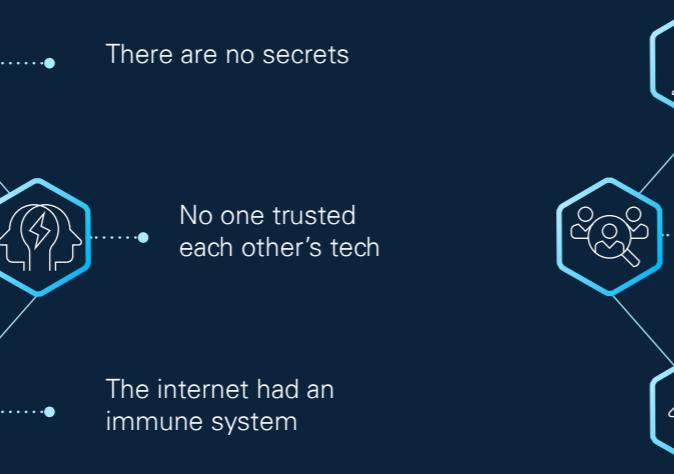


## Life, but not as we know it

- Developments in medical devices and neural implants will lead to the integration of computers and humans for fashion, medical and warfare purposes
- Neural implants will be able to help with neurological diseases
- The rich and powerful will find ways to prolong life through cloning, genetic manipulation and transferring their memory to AI

## The future of cyber security itself

Extrapolating from the 'Imagine if' hypotheses, we have identified key actions which we can take to bring this future to life. The report explores six possible disruptors to the world as we know it:



**How can we help you contribute towards securing the UAE's vision, in alignment with the principles of the 50?**

## Securing the UAE's vision

While we can never predict what life will be like in 2071, we can begin to see patterns of potential challenges. In the publication, we delve into a variety of themes to understand the actions we can take to prepare for headwinds and ensure a safe, secure tomorrow.



# Scope and approach

We were invited by the United Arab Emirates Cyber Security Council to explore the future of cyber security, and what the landscape may look like when the UAE celebrates its Centennial in 2071. An opportunity to pause, step back from the challenges of today, and look at how the world might change and evolve over the coming decades.

It is always dangerous to seek to predict the future with certainty, so we chose to take a different approach. The seeds of tomorrow can be found today, even when looking beyond 20 years. We also considered the last 50 years and asked ourselves what lessons we can draw from that past.

From these strategic trends, drawn from a wide range of futurists, we have created sets of plausible, but by no means certain, "Imagine if" scenarios. These scenarios explore the potential impact of technology advances on our society, and some of the dilemmas which those technologies may pose in terms of social impact, cyber security and privacy.

We then grouped these "Imagine if" scenarios into themes, and from each theme we begin to extract the key challenges in how society may choose to adopt those technologies. These set the scene for an analysis of the major security and privacy issues,

and in turn for an analysis of how the UAE may better understand those issues and shape the adoption of such technologies for the good of society.

There is no single view of the future in this report; that would be presumptuous and unrealistic. There are many futures that might emerge from the trends and scenarios we set out. We have choices ahead and we owe it to the generations to come to make those choices carefully.

**"The power of scenarios lies in their ability to compel us to venture beyond the familiar and confront challenging inquiries. How do we steer clear of dystopian trajectories, optimize outcomes for humanity, and harness technology as a benevolent force? The responsibility to make these choices and shape our shared destiny rests with us."**

**Akhilesh Tuteja**  
Global Cyber Security Leader  
Partner, KPMG in India

# A cyber security retrospective

The 1970s were the digital decade characterized by advances in digital devices, along with major automation of telecommunication through digital switching technology. The seeds of a personal computing, email and mobile phone revolution were planted. Success came with the adoption of flexible digital technology, miniaturization and automation. The 70s brought key theoretical underpinnings for computer security in the form of the Bell-LaPadula model and the foundations of modern asymmetric cryptography in the form of the RSA algorithm.

**The 80s** were the computer decade with advances in hardware, software and graphical user interfaces. The office automation tools of today were born. The key successes of this decade came through computerization, speed of processing, and the advantages of technology spanning business and home usage. We saw hacking begin to scale often with mischief rather than criminality in mind. The early internet was a more innocent place. The internet worm spread in 1988, one of the early examples of self-replicating malware. Early computer viruses had made their appearance on the scene and antivirus software was born.

**Into the 90s** and the software decade began. More powerful operating systems were penned, the search engine was created, and the world wide web was born. Growth was one of the key lessons from the 90s, the ability to rapidly scale a technology through rapid adoption with minimal infrastructure. Software was a perfect fit. The 90s was also a time of globalization as the internet grew beyond its cradle in the United States. It brought the

scaling of the cyber security industry, the growth in Chief Information Security Officer (CISO) roles and the first evidence of a state cyber espionage operation in the form of Moonlight Maze. It seemed that the time of innocence were drawing to an end.

That theme of networking continued into the 2000s – the arrival of the smartphone, the birth of the app, and a rapid upgrade of mobile telecommunication infrastructure into 3G and then 4G. Early virtual reality technologies came and went. The key themes were mobility, the app and rise of the concept of access from anywhere – the start of our always-on world. There was a proliferation of worms and other self-propagating malware, including Conficker in 2008. The computer security community was coming of age although the focus was on the basics of patching, early firewall technologies and malware prevention.

**The 2010s** were the information era. Social media services which had appeared in the 2000s began to have massive impact. Public cloud infrastructure

began to appear along with software as a service. Organizations were able to scale in new ways. The decade opened with the discovery of STUXNET, the first malware to target operational technology. We saw a rapid expansion in organized cyber crime including the proliferation of ransomware enabled by crypto-currency. Cyber security became a profession with regulators demanding enhanced protection measures for critical infrastructure. Privacy legislation matured. Security operations were born, along with national cyber security strategies and centers.

It seems too early to be certain what will follow in **the 2020s**. This is a time of hyperconnected and enmeshed information businesses, of manipulation of the information, and of power projection through cyberspace. It is also becoming the decade of artificial intelligence, as AI raises a host of moral questions and may transform our workforce forever. But the decade is still young.

# A cyber security retrospective (continued)

Before we start on a journey into tomorrow,  
let's pause to look back over the last 50 years.

1970s



1980s



1990s



2000s



2010s



2020s



What's  
next?

# Pride in our past: a brief history of the UAE

Focusing on the United Arab Emirates, we see a massive transformation over the decades since the Union was formed in 1971. A transformation which has mirrored that seen around the world, with a particular emphasis in the early years on energy, transportation, logistics and infrastructure investments. More recently, the country's leadership has had the foresight to promote and invest in strategic areas such as digitization, artificial Intelligence, next-gen broadband connectivity and the space sector, paving the path for UAE to adopt digital technologies at a rapid pace.

Currently, the UAE is one of the world's most technologically advanced countries, with the digital economy contributing 4.3% to the GDP<sup>6</sup> — and more growth on the horizon. The UAE has bolstered digital capabilities by improving IT infrastructure, increasing the speed of internet services, and promoting the use of smartphones and electronic payment systems. Cyber security is at the heart of the technology, AI and fourth industrial revolution.

## Starting in 1971

The rulers of Abu Dhabi, Dubai, Sharjah, Ajman, Fujairah and Umm Al Quwain proclaimed the creation of the new state...



1973

Emirates airline launched

1981

The dirham was introduced as the UAE's currency

1985

The Gulf Cooperation Council was formally launched in Abu Dhabi

2004

President registered in the population register and ID card system, triggering the official launch of this national program, the largest technological program in the Middle East Region

2006

His Highness Sheikh Khalifa Bin Zayed Al Nahyan becomes President of the UAE

2009

2013

Abu Dhabi becomes home to International Renewable Energy Agency (Irena) Launch of the Dubai Metro, the world's longest automated driver-less train system and the first Metro in the Gulf region

2014

2017

UAE announces the creation of the UAE Space Agency to supervise the Mars mission

2018

2019

2023

KhalifaSat makes history as the first satellite built on UAE soil reaches space

2019

2023

2023



# The megatrends

**What might the next 50 years of cyber security bring? The megatrends shaping our world include:**

## **Demographics**

The world population is projected to reach 9.7 billion by 2050. Changing demographics bring challenges ranging from ageing populations, declining fertility rates and increased debt/taxation burdens in some economies; to infrastructure and educational challenges in the rapidly growing and urbanizing populations in sub-Saharan Africa and South Asia.

The UAE's population is predicted to grow to 10.9 million in the next 20 years<sup>4</sup>, with Dubai's population doubling, following a post-pandemic immigration wave. Factors such as economic diversification and attraction of foreign workers will largely contribute to the population increase.

## **Climate change**

Currently implemented policies are predicted to result in further global warming of 2.8 degrees over the period leading up to 2100, with a diminishing window for global action which might limit that warming to 1.5-2 degrees.<sup>5</sup> Changes in climate are

predicted to lead to food security issues, population displacement and ecosystem degradation – as well as creating potential flash points for conflict. The UAE is taking measures to tackle the growing threat of extreme temperature and drought caused by climate change. It has outlined multiple initiatives to balance the short term gains from fossil fuels with the existential imperative arising from climate change.

## **Health challenges**

Growing antimicrobial resistance linked to increased risk of cross-infection of human populations with animal pathogens associated with increasing population density and mobility, lead to increased pandemic risk. Longer life expectancies lead to growing pressures on healthcare systems associated with diabetes, cardiovascular disease, cancer and chronic respiratory diseases.

The Centennial 2071 project aims to place the UAE as the best country in the world by 2071, with superlative healthcare. The country's 2071 healthcare agenda focuses on medical tourism, telemedicine, AI and cloud technology in healthcare and regulation for the use of e-health.

Of course, technology trends will be a major determining factor in the world we find ourselves in. Some will help us tackle the challenges above, while others may have more complex implications which will change our lifestyles forever. The fourth industrial revolution is in its infancy, and may be long past by the time we reach 2071.

## **Artificial intelligence**



The advent of artificial general intelligence following the rapid development of AI and the extension of domain specific applications over the next decade.

## **Hyper connectivity**



Development of network infrastructure enabling greater bandwidth and massive interconnection of devices, supporting further development of the internet of things, ubiquitous sensors and effectors.

## **Bio engineering**



Developments in medical devices and implants (including neural links and advanced prosthetics), in the sequencing and manipulation of the genome for good and for bad, and in the synthesis of tailored therapeutics.

## **Quantum computing**



The development of quantum computing disrupting the current digital computing model and providing massive increases in computing power, linked to developments in quantum secure communication.

## **Space technology**



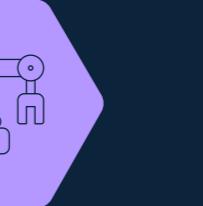
The race for space continues with increased access and reduced launch costs, establishment of interplanetary presence for humankind, more sophisticated autonomous space missions; but also risks from space debris fields and counter-space operations.

## **Robotics**



A broad set of advances in which robots become more sophisticated and ubiquitous in all spheres of life from high risk industrial and military applications, through advanced swarming drones, to anthropomorphized robots for personal care and miniaturized surgical robotic devices.

## **Smart manufacturing**



The continuing development of 3D printing technologies and the ability to provide highly tailored and personalized manufacturing systems, linked to just in time delivery models.

## **Augmented reality**



The creation of high fidelity non-intrusive augmented reality systems and highly immersive virtual reality environments, linked to the potential developments in neural implants and neural stimulation technologies.

## **Nuclear fusion**



The growing availability of nuclear fusion including micro reactor developments resulting, along with growth in renewables, in fundamental changes in the dependence on oil and gas based energy sources.



# Imagine if...

To bring the future to life, we have developed a series of "Imagine if" scenarios which consider the possible sociopolitical and cyber security implications of technological trends.

## Reality and fiction blur

# Imagine if... we couldn't differentiate between truth and fiction

Augmented reality



Artificial intelligence



**"Where do we draw the line, or what happens in the case of a one-way migration from the physical to the virtual world? Considering the nature of these questions it is not unlikely that philosophy will gain relevance in the field."**

Prasad Jarayaman

Americas Cyber Security Leader  
Partner, KPMG in the US

The first of our groups of "Imagine if" scenarios explores the creation of virtual worlds, the value we attach to assets in these worlds, and our ability to differentiate reality from synthetic experience.

By 2071, developments in immersive virtual reality, deep fake and behavioral manipulation technology have blurred reality and fiction. In this world it has become impossible to be certain that the constructs you are immersed in are real or fictional. Real world scenes can be replicated and manipulated in real time, convincing replicas of people can be constructed and interacted with. The uncanny valley has been crossed.

Truth was always subjective, but in this new world people have few ways of differentiating truth and fiction, and a greater willingness to believe what they wish of "facts". Group think leads to self-reinforcing echo chambers of increasingly extreme views, fed by both self-selection of content and by algorithms which emphasize the exceptional. The Internet becomes polyinstantiated with many separate instances.

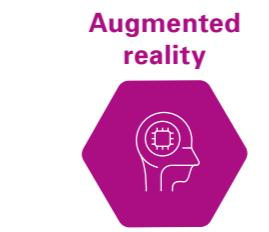
Societies must find new ways of maintaining trust and of constraining the extremes of reality manipulation as well as providing tools to allow people (or machines) to do so. Some authorities take advantage of this to provide immersive control environments, others create definitive sources of trusted information but are tempted to manipulate those truths.

The concept of trust becomes increasingly important, as does securing "reality". Crime finds many ways of manipulation by social engineering, but so too do states and corporates as they seek to control the narrative and to influence the behaviors of populations. The authenticity of information becomes paramount with a need for robust mechanisms for detecting tampering and forgery. Automated filtering and suppression of certain types of information become routine. Privacy concerns dominate as fake personas are created and real personas manipulated. Legal frameworks around the protection of personal images evolve but struggle to keep pace with AI-driven manipulation.



Reality and fiction blur

## Imagine if... people became lost in the virtual world



Augmented  
reality

Bio  
engineering



Virtual reality technology has continued to develop with retina tracking, miniaturization of VR systems and improved haptic feedback. Augmented reality has also found widespread usage. New business models have developed in the virtual world around provision of tailored customer experiences, new modes of interaction and ways of heightening stimulation. Large scale collection of personal and behavioral data is commonplace, as firms seek to provide highly tailored and addictive modes of interaction.

Cyber security challenges develop around the protection of virtual assets and the access controls in virtual worlds, as well as fine grained controls over permitted interactions between objects including avatars.

Virtual assets become increasingly valuable as people (and firms) tailor their experiences and avatars. Fraud, blackmail, extortion and bribery find new manifestations. Law enforcement and legal frameworks fight to keep up with the pace of innovation.

Privacy becomes a major issue as the ability to collect and manipulate personal data grows. Norms on the protection of personal spaces in the virtual world from interference and intrusion must also evolve.

**"The digital economy race belongs to those governments which can balance cybersecurity prerequisites and economic growth. Striking this equilibrium entails crafting regulations and safeguards that empower businesses to flourish while ensuring resilience in the face of ever-evolving cyber threats. Forward-looking governments must invest in innovative technologies, adopt agile strategies, and foster a culture of vigilance to secure a prosperous and digitally robust future."**

**H.E. Yousef Hamad Al-Shaibani**  
Director General, Dubai Electronic Security Center

Reality and fiction blur

# Imagine if... data was money

**By 2071, data has become the new money and people are paid for how their data is used, transformed and manipulated. Rights to use data have become a major corporate asset, alongside more conventional balance sheet entries. People are remunerated for micro-transactions on data.**

In the future, the rights to acquire and exploit data on the characteristics and behavior of individuals has become a major commodity. Even if individuals do not provide data directly, it can be easily inferred through sophisticated analytics.

Augmented reality



Hyper connectivity



Different societies adopt very different models over the rights of people (and potentially AIs) to control how such data is exploited. It is also possible that data will no longer remain the main currency and will be surpassed by the AI analysis algorithm running on the data. Privacy regulations will evolve as they try to deal with this complexity, with many commercial pressures to exploit data for advantage, leading to innovation ahead of regulation and evolution of societal norms.

Cyber crime will find ways to derive personal data in novel ways and use that to good effect to exploit and manipulate individuals. Will individuals be able to track their personal data and understand how it is being used and abused by those criminal groups?



# The power of the machine

## Imagine if... robots had become ubiquitous

**"If machines had complete control,  
what do we lose? If you have beaten  
creativity, genius-ness and the  
adaptability of society, do we all  
become sheep?"**

**James Mabbott**  
KPMG Futures Partner,  
KPMG in Australia



The second of our groups of "Imagine if" scenarios focuses on the development of robotics and artificial intelligence, and what this might mean for our society.

**By 2071, patterns of labor have changed with many manual tasks now undertaken by robots, and many personal services professions have been reshaped as robots take on care roles. Maintenance and manufacturing have become robotic activities.**

There are fundamental questions over the norms governing how such robots are used, and the limitations on their interactions with human beings. The potential for manipulation of robots has led to higher standards for the cyber security and safety of devices which directly interact with us or whose manipulation can have lethal consequences.

During the first and second industrial revolutions, machines merely coexisted with humans as basic tools or operated independently. The third industrial revolution marked a shift toward dynamic cooperation, where humans and machines temporarily shared workspace and resources. With the advent of Industry 4.0 and advanced information technology, the human-machine relationship is expected to evolve according to the 5C model: Coexistence, Cooperation, Collaboration, Compassion, and Coevolution.

The rapid advancement of technology has opened the possibility, either now or in the near future, for machines to attain a level of intelligence that allows them to perform tasks or missions without specific, predefined instructions. Consequently, the trajectory of human-machine interface technology is shifting from being primarily an informational system to automation and, ultimately, to autonomous agents.





## The power of the machine

# Imagine if... machines became smarter than us

Artificial  
intelligence



**By 2071, developments in artificial intelligence had resulted in sentient machines and general intelligence. Machines have already started to excel in specific disciplines, for instance, empowering sustainable secure technology with low carbon emissions. AI has begun to reshape our world, changing the nature of work. Effective exploitation of AI has created competitive advantage in many areas for nations and corporations.**

The sophistication of AIs has disrupted our society. At best we establish a beneficial partnership with AIs, at worst they have a potential for social disruption akin to the industrial revolution as people are disenfranchised and discarded.

The frameworks to oversee and monitor the application of AI must evolve quickly and will inevitably involve oversight of AIs by other AIs. Societal debates over the limits of AI capability and

the moral complexities of their application will lag the evolution of the technology itself.

Legal debates on the corporate status of AIs and their agency in acting on behalf of people continue, along with responsibility for harm caused by the use of AI technology.

The application of AI technology has the potential to create a new arms race. Some regimes will use AI to reinforce their national security and advantage; other societies will collaborate to innovate around AI but will struggle to establish regulatory norms given the pace of technology development.

Organized crime will exploit the technology through adversarial AIs, but so will nation states in defending their interests. The AI to AI interactions will outpace the ability of people to understand and constrain their interactions and emergent behaviors.

**"Instilling trust in AI models involves proactively ensuring smart systems are built responsibly and following international standards that protect the privacy and security of nations and governments."**

**Eng. Ahmed Bin Saeed Al Sayyah,**  
General Manager,  
Electronic Government Authority

The power of the machine

# Imagine if... machines could predict the future

By 2071, machines are able to predict the actions of individuals and social groups with high levels of confidence, as well as identifying how and where to intervene to shape that future.

Fundamental questions arise over the frameworks which govern the operation of artificial intelligences as they arrive at the point where they can effectively manipulate humanity through observation of our behavior and control over aspects of our information space and virtual world, through politics and through religion.

Will AIs develop independent thought and free will... and will our reactions be determined by the interventions of AIs themselves? Does humanity retain free will and creativity in this brave new world? The third of our groups of "Imagine if" scenarios focuses on examples on omniscience and omnipotence in this new world enabled by technology.

Quantum computing



Artificial intelligence



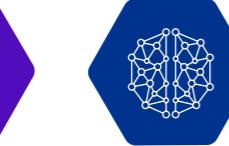
## The impact of omniscience

# Imagine if... there was nowhere to hide

**Power in this new reality sits with those who can intervene in the real and virtual worlds at scale, at speed and in unexpected ways."**

**David Ferbrache**  
Global Head of Cyber Innovation,  
KPMG International

Space technology



Hyper connectivity



Artificial intelligence



**By 2071, hyperconnected sensors are deployed across smart cities, supported by advances in small satellite technology and drones. This surveillance grid, linked to sophisticated AI, allows omniscience for the state (or corporation). The scope of such technology is vast: e.g. population censuses could be carried out through IoT. The collection and fusion of personal data allows many inferences to be made over our human behavior.**

Patterns of crime have changed in this new surveillance environment with physical assaults, robberies and property crimes being capable of rapid detection and policing. New forms of crime have emerged including

deception and exploitation of the sensor grid, along with recourse to crime in the virtual world with sophisticated cyber concealments.

Some societies establish complex expectations over privacy, including the creation of spaces safe from surveillance, constraints on the collection and processing of surveillance data, and penalties for misuse. In other societies, state or corporates dominate through benevolent and malevolent use of such information advantage. Global norms around privacy seem to be illusive and culturally dependent.



## The impact of omniscience

# Imagine if... nano and micro machines were everywhere

Robotics



Smart manufacturing



**By 2071, nano and micro machines are commonplace, and capable of salvaging power from their environments. They have a wide range of roles from micro drones; microscopic sensors and nanopropes; to micro effectors able to interact with the human body.**

Ubiquitous surveillance becomes possible using insect sized micro drones, allowing highly covert applications as well as providing resilience through sheer numbers. Micro devices become commonplace in medical applications allowing both internal investigations and diagnostics, while also opening up the possibility for highly targeted micro surgical and medical interventions.

Micro devices also find roles in repairing and maintaining smart cities augmenting and supplementing robot deployed in maintenance roles. The implementation of sophisticated swarm algorithms allows these devices to self organize to carry out complex and intricate tasks. Suddenly it seems that these inter-networked machines are everywhere.

These devices pose new security challenges given the limited power budget available to secure their communications links, and limited onboard processing available. The swarm control algorithms and potential for emergent behaviors raises new questions over the verification of the reliability and integrity of those devices.

## The impact of omniscience

# Imagine if... weapons always found their targets



**By 2071, weapons have become smart and can find their target anywhere at any time, down to finding a single person in the crowd at speeds faster than the blink of an eye. Weapons range from hypersonic missiles, to swarming drones, to tailored bio-weapons.**

Many weapons systems will integrate sophisticated AIs into their operation – whether robotics, avionics or vetronics. The cyber security of military systems has become key to national security, with the military investing increasing funds into engineering cyber security defenses, and to developing offensive cyber and electronic warfare techniques designed to disrupt adversary defense and offensive systems.

Conventional patterns of warfare are changing beyond recognition, as too are the ways that power is projected by nation states and other actors. National advantage attaches to those states (and other non-state groups) who can demonstrate an ability to rapidly develop and acquire new weapon technologies, as well as being prepared to think in unconventional ways about the way those technologies are used.

The “hacking” of military weapon systems leads major incidents, with cyber attacks also risking escalation of conflict situations. The Laws of Armed Conflict (and associated international norms) struggle to keep up with the evolution of weapon systems.



The new hybrid

# Imagine if... machines anticipate our every need

**"Not only could machines become indistinguishable from humans, but technology could change what DNA is and how humans operate. The societal and cultural implications here are massive and profound."**

**Caroline Rivett**

Global Life Sciences Cyber  
Leader Partner, KPMG in the UK

Hyper connectivity



Artificial intelligence



Our fourth group of "Imagine ifs" explores the interaction between people and machines, and how it sets the scene for a possible convergence between the two.

**By 2071, personal assistants can anticipate our every need and make sure those needs are met before we even realize we have them. Personal assistants oversee our interactions with the internet and the virtual world, assist us in getting the best from those worlds and safeguard us in our interactions.**

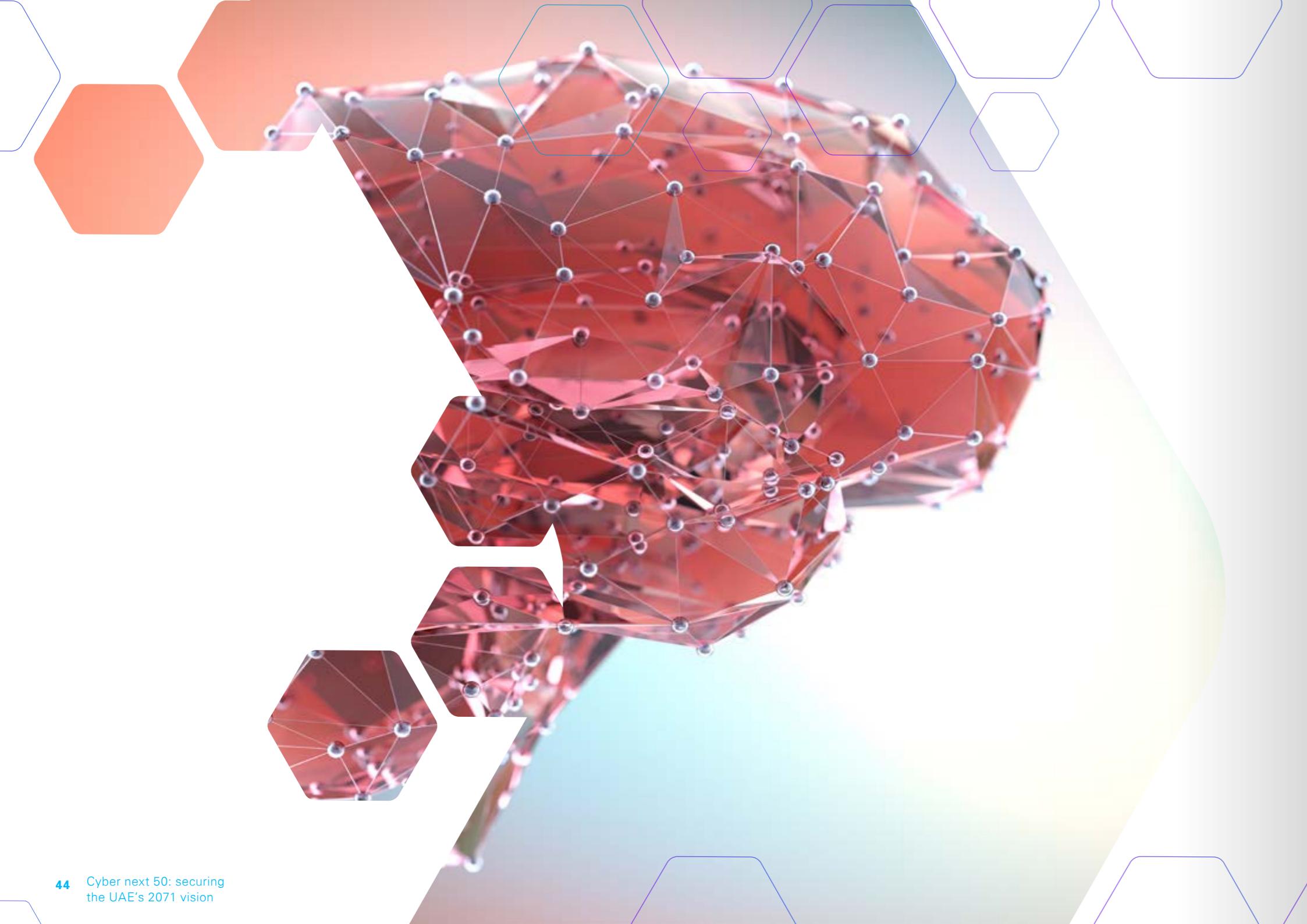
Personal assistants become intimately linked to our lives. A balance has to be struck between the commercial advantages to the provider of the assistant and the independence of that assistant in meeting our needs. This space will be increasingly regulated as societal concerns develop over the biases shown by such assistants.

Privacy concerns will also develop over the extent of data collected and maintained by such assistants, as well as the complexities of determining the extent of the agency which can be shown by such assistants particularly when anticipating our future requirements.

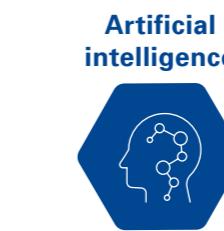
Cyber crime will find ways to manipulate such assistants both to steal personal data, but also to defraud the individuals supported by those assistants. Nevertheless, these assistants will play a key role in preventing crime against their owners by implementing sophisticated fraud prevention algorithms.

Over time we move from a model of protecting end points and computer systems to one of protecting the lifestyle and interests of an individual.





The new hybrid  
**Imagine if...  
machines could read  
(or write!) our minds**



**By 2071, machines have developed the ability to read our thoughts through micro observations of our expressions, through neural implants or monitoring of brain activity. Stimulation of the brain, initially developed for medical purposes, has found broader application for pleasure and ultimately to allow machines and people to directly interact.**

The societal norms around such technologies remain ill developed. Medical devices include sophisticated implants based on direct neural stimulation to suppress neurological abnormalities, to allow sensory experiences, and to provide motor interfaces for prosthetics. Military applications of such technology have also proliferated allowing augmentation of human performance and interactions with robotics and exoskeletons.

The commercialization of such technology has created a market for human augmentation, as well as tempting states to employ such technology for control of its people including the extremes of criminal behaviour and perhaps more abhorrent viewpoints.

The cyber security of such implants is of paramount importance given their ability to directly manipulate individuals, as well as potential access to the human mind and insights on our most private thoughts and intentions.

Criminal groups will find ways of exploiting brain stimulation as a new narcotic for the masses, leading to new patterns of addiction and new tech enabled crimes.

The new hybrid

# Imagine if... machines could read (or write!) our DNA

**By 2071, machines can quickly sequence and analyze DNA, and then write new DNA to transform our gene sequence or manufacture tailored proteins. Nanopore technology helps sequence millions of bases. Gene splicing selectively modifies human RNA/DNA. Fast protein synthesis technologies have also advanced.**

Norms over the use of such technologies are slow to develop and societal debates over the acceptable norms of generic manipulation continue. Rich individuals and "rogue" states will test the boundaries. We are entering a time of designer humans, but also a time of medical advances which act to extend life and hold back ageing.

Hyper connectivity



Artificial intelligence



DNA data has become ubiquitous with such data readily acquired leading to derivation of highly sensitive information on generic disease and modelling of biological characteristics. Privacy concerns over such data have grown given the potential for exploitation, for targeting of individuals and even for engineering of biological weapons tailored to their genome.

The manipulation and tampering with genetic engineering systems creates significant risks – and may lead to creation of tailored bio weapons or lethal modification of medical systems/processes.



It's life but not as we know it

# Imagine if... people and machines became one

**"If the aging process is reduced or reversed, it is a completely different world. Who is going to control how long we live, and what impact will this have on the world?"**

**Nashikta Angadh**  
Risk Consulting Partner,  
KPMG in South Africa



Our last group of "Imagine ifs" is perhaps the most challenging, and asks us to consider whether our definitions of life itself will remain unchanged by 2071, or whether perhaps our world will be very different indeed.

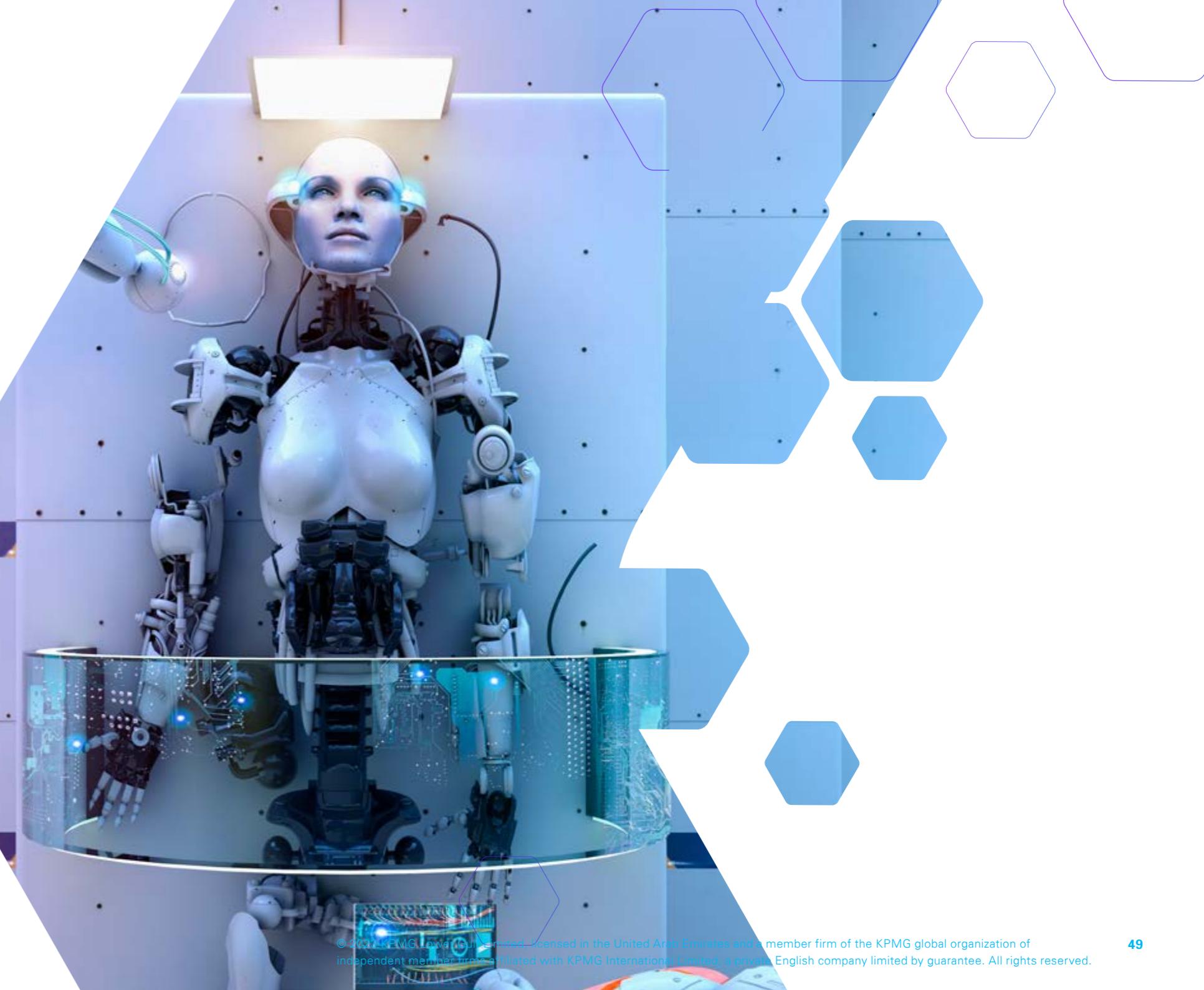
**By 2071, developments in medical devices and neural implants led to integration of computers and human beings... for fashion, for medicine, for warfare. Sophisticated prosthetics have replaced and augmented human limbs. Neural implants have helped deal with neurological disease, brought sight to the blind and sound to the deaf. Some have succumbed to the attraction of embedding co-processors in their brains, perhaps they had no option. Fashion trends come to embrace machine technology implants.**

The limits of machine augmentation become a societal debate. Cure moves to become improvement – as both neural implant and prosthetic

technologies develop. The military seeks combat advantage, but so too might those with financial resources to buy such capabilities. Medical devices become increasing sophisticated and increasingly interventionist – and with that comes increasing dependency or even addiction.

Debates around the limits of machine augmentation continue, but it seems inevitable that some states (and corporates) will push those boundaries further while regulation lags. As people (augmented by technology) cross borders, what are the implication of those movements and migrations?

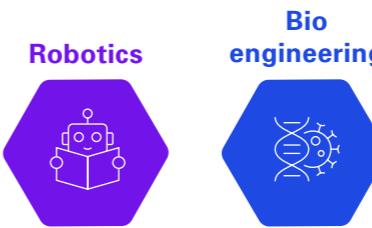
The cyber security of machine implants is a growing concern as such devices become the target for exploitation. Privacy becomes the right to freedom from unauthorized intrusion into lives – in a world where machines and people fuse. The hacking of machine implants has growing real world consequences on lives and welfare, and there is no option to be off the grid when medical implants depend on continuous monitoring.





It's life but not as we know it

## Imagine if... tomorrow we never die



**By 2071, the richest and most powerful of people have found ways to prolong life whether through cloning, through genetic manipulation or by transferring their memories and personalities to artificial intelligences or robots.**

Fundamental questions arise over what it means to be human and the extent to which an artificial being or a clone can genuinely embody the personality and persona of a living person. As families seek to capture the essence of loved ones to allow interactions after death, and individuals seek an immortality of sorts, then the line between life and death will start to blur, raising fundamental questions in law and in religion.

Of course, there will be questions over the extent to which clones and avatars can continue to act on behalf of their deceased person, and quite what this means for inheritance and the rights of descendants of that individual. Who has the rights to the image and persona of a deceased person, or are such rights vested in the clone?

There will be concerns over the integrity of the process of transference as well as the cyber security of the clone or avatar itself, and the extent to which it can be manipulated in its new form.

If such transference becomes acceptable to society then this will have fundamental implications for the structure and stability of society itself, as the concept of aging and death changes.

# The future of cyber security itself

Of course, cyber security itself will evolve as a discipline, and so too will the actions of states and organized crime in planning and carrying out cyber attacks. In addition, there could be nations with no armies where sensors and network nodes become the main protectors, and PPPs (public private partnerships) jointly own all infrastructure. We have used a similar lens to postulate the cyberwar disruptors and the cyber security disruptors:

**"Ownership of the information space is the ultimate source of power. If the Internet ecosystem became unhackable it would certainly help reduce our dependency on cyber security"**

**Major General Dr. Mubarak Saeed bin Ghafan Al Jabri,**  
Assistant Under-Secretary for Support and Defence Industries, Ministry of Defence

## The cyberwar disruptors



There are no computers anymore

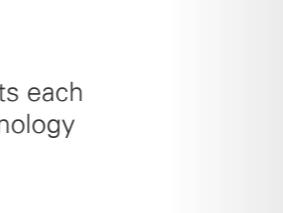


A nation can be excommunicated

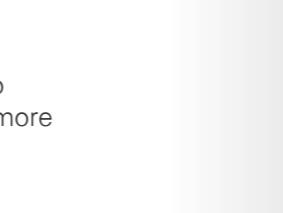


Cyberwar has become a reality

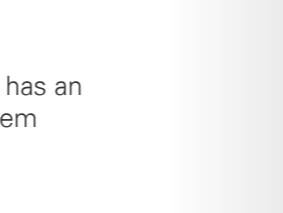
## The cyber security disruptors



No-one trusts each other's technology



There are no secrets anymore



The internet has an immune system





The future of cyber security itself

## Imagine if... there are no secrets anymore

Quantum computing



**By 2071, developments in quantum computing have undermined the security of all encryption algorithms for those with access to state of the art quantum technology – but perhaps quantum technologies have also enabled tamper evident communication channels which allow complete confidence in the privacy of such communications. Maintaining a quantum technology advantage becomes a national security advantage.**

In this new world much that which was secret is no longer so for those people and organizations whose data has been collected over time. Suddenly historic diplomatic and technology secrets are known. Less

sophisticated organizations find themselves under surveillance. Intellectual property and sensitive research can be harder to protect, and countries find ways to re-innovate technologies based on stolen secrets.

Alternatively, people can be more confident in the detection of eavesdropping and may find new ways to protect their most sensitive communications going forward using quantum key distribution and quantum entanglement.

Either way, quantum technologies become a source of national competitive advantage, and the world divides into the haves and have nots.

**"Given the rapid advancement of technology, and its influence to predict the possible futures for cyber security. We owe it to our future generations to empower them with the skills and knowledge to harness the opportunities and cope with any implications that may arise."**

**H.E. Nour Ali Al Noman,**  
Director of the e-Government  
Department

The future of cyber security itself

# Imagine if... no-one trusted each other's tech

**By 2071, no country is prepared to trust technology unless it is produced by an ally or they have visibility over the production processes. There have been too many cases of hidden functionality. Technology supply chains have become more transparent with greater emphasis on the verification of the integrity of those supply chains. Blocks of nations have brought production back on-shore for key components.**

The world has become more polarized with existing divisions between power blocks becoming more severe leading to concerns over the trust in components and systems sourced beyond national borders, fueled by greater use of supply chain attack techniques by state and proxy organized crime groups. This has led to onshoring of key technology production activities.

Hyper connectivity



Disruptive event



Developments in smart manufacturing have opened up the possibility of manufacturing closer to destination, although of course demanding high levels of security around both manufacturing operations and the protection of sensitive intellectual property.

Security models which are robust in the face of untrusted hardware and software components attract greater attention, along with continued improvements in the monitoring of anomalous system behavior associated with exploitation of untrusted components.

Tensions between open markets with minimal barriers to movement of goods and services, and the national security implications of dependencies on externally provided systems have continued to grow with little international consensus on common approaches.





The future of cyber security itself

## Imagine if... the internet had an immune system

Hyper connectivity

Disruptive event



**By 2071, the internet has developed immunity against many cyber attacks, able to restructure and adapt to attacks, to counter attackers and to fight back. The internet has become a more resilient system of systems reflecting its criticality to modern society.**

There is little consensus on who controls “the internet” with nations taking different approaches to exerting sovereignty over that network and defending “their” parts of the global network. Many parts of the internet are now able to rapidly counter malicious activity, reacting within milliseconds. Sometimes the attacking bots react with equal speed. Responses range from protective blocking to automated counterattacks aimed at permanently destroying those systems.

Similar algorithms work to detect and counter “misinformation” and police the information space. The internet itself is also more resilient and able to self-heal, reconfiguring to deal with system failures and outages.

The international norms on acceptable countermeasures are elusive - as is clarity on the rights of state, company or private individuals to take such actions. Some aim to exploit the responses of the network (and its controlling AIs) to achieve their own ends – effectively creating an autoimmune response.

**“The transformative power of machine learning has enabled the development of autonomous systems that operate much like a human being, employing neural networks for learning, fending off attacks, and overcome challenges.”**

**H.E. Engineer Mohammed Ibrahim Al Zarouni,**  
Deputy Director General of the Authority for the Information and Digital Government Sector

The future of cyber security itself

# Imagine if... a nation could be excommunicated

**By 2071, a nation can be excommunicated from cyberspace – whether by cyber attack, by severing submarine cables or jamming satellite comms. While comms have become more resilient and diverse, and less susceptible to single point failure – we have become more and more dependent on high bandwidth and low latency links.**

Nations have developed a range of offensive cyber (and conventional attack) techniques aimed at disrupting the infrastructures of other countries. In response nations have also taken steps to diversify their access using a mix of space and terrestrial communications infrastructure, while also increasing their resilience to attacks from the wider internet.

Hyper connectivity



Disruptive event



Some nations have chosen to firewall themselves off from the global community, in part to control the flow of information (and counter narratives) into their nation, and in part to ensure they are resilient to action by other countries to sanction or excommunicate them.

The interaction between physical geography and internet connectivity remains complex, with natural choke points remaining in the infrastructure which supports our digital world. The protection of those choke points become strategic to many nations.

**"AI capabilities enable nations to protect their online space as cybercrimes know no borders."**

**H.E. Engineer Khalid Al Shamsi**  
Director General of Umm Al Quwain Smart Department





The future of cyber security itself

## Imagine if... cyberwar became a reality

Hyper connectivity

Disruptive event



**By 2071, cyberwar has become commonplace as nations build out their attack capabilities, and cyber attacks have significant real world consequences on infrastructure and on human lives. Every nation (and some corporations and terrorist groups) has invested in developing offensive cyber capabilities as well as exploring their integration with other conventional military capabilities.**

While nations continue to disagree on the definition of cyber war and the norms of international behavior around such "conflicts", the impact of offensive cyber attack has become only too real. Groups have developed ways of manipulating the information space of targets to advantage, as well as degrading and manipulating cyber-physical systems. The line between peace and war, if such a line ever existed, has long since disappeared. Countries could transition from war to peacetime or vice versa

overnight due to the cyber deterrence MAD (Mutually Assured Destruction) model.

Nations struggle to define escalation criteria and frame adequate responses to offensive action, and the use of offensive cyber attack becomes normalized. AI systems play a key role in the orchestration of offensive action at scale and in the defense against such attacks.

Greater emphasis is placed on the design of systems resilient to attack and ensuring systems can degrade gracefully under attack. Cyber security has become synonymous with national security, as nations strive to adapt conventional concepts of power and defense to a very different environment.

The pace of attack and response continues to pick up, leaving little time to de-escalate a situation with consequences which can go far beyond cyberspace.

The future of cyber security itself

# Imagine if... one day there were no computers

**By 2071, an electromagnetic pulse (nuclear EMP or solar coronal matter ejection) disrupts and destroys much of the IT infrastructure we have come to rely on, and suddenly there are no computers. Our digital world has become hyperconnected and potentially fragile to low probability but high impact events.**

Nuclear proliferation continues with many more countries having the capability to launch ballistic delivery systems capable of detonating an exo-atmospheric nuclear burst and causing a major electro magnetic pulse. Concern remains over the potential for a Carrington event such as the geomagnetic storm which impacted the earth in 1859. Either event would be highly disruptive to our digital world, and in particular to our vital space systems.

Hyper connectivity



Disruptive event



Nations struggle to create the case to invest in resilient infrastructure capable of surviving such events, although some choose to make that investment in protecting their most sensitive national security and defence functions, although the disruption of the broader internet would still create massive impacts on society.

Will we see such an event play out? And what would be our response after such an event would we build a different world... and would it be based on carbon or silicon?





# Global cyber security themes in 2071

**"Co-existing with machines as another life form which we must cooperate with, in a form of a partnership, naturally leads itself to policies, rights and violations in terms of how you treat machines and how machines treat us"**

**H.E Ohood Ali Shehil,**  
Director General of Ajman  
Digital Government

We have set out many "Imagine if" scenarios, each raising their own sets of cyber security, privacy and implementation issues. While we can never predict what life will be like in 2071, we can begin to see patterns of potential challenges.

We can foresee developing themes around the augmentation of reality; the development of artificial intelligence; the convergence of human and machine; and perhaps even the potential for human life being supplanted by our silicon children.

Technology offers great potential to tackle some of the challenges humanity currently faces, enabling economic development, helping tackle health challenges and our ageing society, and even ultimately extending life itself.

Political issues will of course play into this complex environment and we can expect nations to seek competitive advantage in the adoption of technology, to harness technology for military and national security purposes, and in a world where geopolitical tensions seem to be on the rise – we also risk cyberwar.

Our hyperconnected and technology enabled world will also be vulnerable to disruption whether by extreme manmade or nature events (such as EMP) or by cyber warfare.

It seems clear that cyber security will remain a challenge in any new world we can envisage, but what are the key implications of this new world?

# Building 'trust' into the fabric of our society

**"We should not assume that anything that exists today will be the case in 50 years. How truth will be harnessed, and the distortion of truth, is a very significant issue. We may very well create a reality which is not true."**

**Roni Michael**  
Partner, KPMG in Israel



Trust will become a key theme in the future. In a world where truth and fiction blur, knowing who or what can be trusted will become more important than ever. Frameworks for digital trust will become an increasingly important part of corporate governance including appropriate transparency mechanisms.

Societies will arrive at very different political settlements over the degree to which the state (or indeed commerce) can shape and control the narratives provided to its people. Within our interconnected global world these worldviews will come into conflict, and international norms will become increasingly important, but also elusive. While consensus can be generated over the most



extreme forms of fakery, deception and criminal activity – this will not extend to more nuanced social, religious or political content. Additionally, the trust frameworks will need to stay agile with the speed at which information manipulation will be possibly aided by the spread of AI and computing power.

Legal frameworks will need to further evolve to deal with new forms of information manipulation, for example deep fake to manipulate political discourse, requiring a principles based approach which focuses on the intent rather than the mechanism. Legal frameworks will need to address the constantly evolving digital landscape for their continued relevance and embed mechanisms to navigate the speed of technological advancements.

# Legal frameworks for a new world of hybrid people, AI and tech

**"Co-existing with machines as another life form which we must cooperate with, in a form of a partnership, naturally leads itself to policies, rights and violations in terms of how you treat machines and how machines treat us."**

**Caroline Rivett**  
Global Life Sciences Cyber  
Leader Partner, KPMG in the UK



The rapid development of AI technology will lead to key questions over the legal personality of AI systems, their ability to exercise agency on behalf of companies and people, on the liability of the manufacturer of AI for its behaviors and actions, and ultimately on the framework of controls which will govern and limit the freedom of action of such AIs.

While it will be tempting to craft legal frameworks which are specific to AIs, these will increasingly be challenged as people and AIs begin to converge. Ultimately a legal framework will be required which is agnostic over whether the entity concerned is a person, and AI or a hybrid of both.



Conventional legal constructs such as theft, assault or even murder will be stretched to apply to the virtual world. In doing so there will be major societal debates around how emotional trauma in that virtual world equates to assault in the real world, as well as to the protection of intellectual property and assets in that virtual world.

Global commerce will need to navigate these different regulatory and legal frameworks to remain effective, and will likely find the differences increasingly difficult to reconcile. Perhaps companies need a chief philosophy officer now.

# New security models and paradigms

**"If the motivations of cyber criminals move beyond monetization extraction activities to manipulation or even control over peoples' lives, will we then need MDR (managed detection and response) for the body?"**

**James Mabbott**  
KPMG Futures Partner,  
KPMG in Australia

C

Security models will seem increasingly outdated, focusing as they do on the protection of the confidentiality, integrity and availability of data. We will aim to build new models which provide a higher level abstraction of the permitted interactions between entities – whether people or AI systems.

Imagine a virtual reality in which your avatar is interacting with content provided by others. What can they know about you and in how much detail, how much of your behavior can they profile, how can they interact with you, and what would you find unacceptable and offensive in their behaviors? As they collect data about you, how can you control the uses to which that data is put, how can you be



# Focus on supervising autonomous AI systems

D

rewarded for its exploitation and use, can you request it is revoked, amended or corrected in real time?

Our concept of privacy will move beyond controlling the collection and processing of information about us, towards a broader concept of managing intrusion into our lives and controlling how those interactions occur. All of which implies a more sophisticated way of establishing permissible interactions between you and other entities, but also monitoring whether those boundaries have been violated or breached. How will access control operate when the accesses we are discussing are to our thoughts, our emotions and our every behavior?

New licensing frameworks will also be required for autonomous systems, whether AIs operating in cyberspace or robotic manifestations of those AIs in the real world. We can expect greater obligations to be placed on manufacturers to take responsibility (and liability) for the behavior of such systems. This will trigger both greater focus on the design of such systems, but also the creation of limiter systems to supervise the behavior of AIs drawing lessons from the safety community in their use of safety instrumented systems. The sophistication of these limiters will grow as moral dilemmas develop around the use of AI.



# Deep collaboration between regulators and technologists

**"The most informed regulators of technology will win, creating an environment where innovation for the good of humanity can prosper."**

**H.E. Mohamed Hayee Al Kaabi**  
Acting Director General, Abu Dhabi Digital Authority

This co-evolution is needed to be able to assess the potential societal impact of technologies, and to keep that impact assessment updated as the technology finds new, and often unexpected, applications.

There is an advantage in creating models for such regulatory engagement, building on the experiences of many nations such as Singapore and the UK in the design of regulatory sandboxes which promote this dialogue and allow the practical testing and trialing of technologies.

These regulatory sandboxes will also help expose issues where there may be more fundamental societal debates early, as well as helping nations

frame their response to the adoption of new technologies. Regulation will also need to flex and evolve in tandem with technologies, and there is benefit in considering the long view when framing such regulation.

Lastly, early engagement also allows us to anticipate the need for supervisory (Suptech) and regulatory technology (Regtech) to be developed which can help oversee the application of new technologies and provide confidence in their secure application.

# Defence in the blink of an eye through emerging technology

**"The UAE's progress in the field of cybersecurity, aligned with UAE Centennial 2071, promises to safeguard the nation's digital landscape and enable secure progress into the next decades."**

**H.E. Omar Sultan Al Olama**  
Minister of State for Artificial Intelligence, Digital Economy and Remote Work Applications

As cyber attack tooling becomes increasingly automated and sophisticated, including harnessing AI technologies to plan and conduct both reconnaissance and actual penetration and exploitation of systems; this will be matched by increasing use of sophisticated data analytics within the cyber security community to detect and rapidly counter cyber attacks. This will result in an extension of current active defense models being developed by nations to block cyber attacks into more active enterprise, sector and national countermeasures and even automated retaliation measures.

Cyber operations will become increasingly automated forming a partnership between security professionals and the AI tooling and decision making systems which support them. Cyber defense

systems will extend to cover not just the technical compromise of systems, but also counters to more sophisticated manipulation of AI systems (adversarial AI) and also the information space in the real and virtual worlds.

New "system level" defensive models will be developed which provide a framework for integrating data together across the community, and also enable distributed "immune system" models of defense in which multiple countermeasures and response systems operate in a co-ordinated way to counter and disrupt attacks. This will raise fundamental questions over the control of the internet (and newer virtual worlds), and the ways in which nations seek to moderate and limit access to "their" element of these environments.

# What really matters to our society?

In this new world, authority structures can find many ways to enforce their will on people and the choices which societies and their governments make on freedoms and acceptable behaviors will be a major differentiator between nations. States will take very different paths and there will be increasing tensions when those different societal models meet in cyberspace – international consensus may be illusionary and economic power will come into play as nations seek to achieve technology advantage and with that impose their worldview on others.

The very concept of the nation states will continue to shift and evolve – as too will the balance between corporate power built on trade and commerce, the power of the state based on geographic control, and the power of other groupings based on ideology.

In this world of change, opportunities exist for the nations who can create environments in which innovation and legislature co-evolve with a clear vision for the future. We can choose to create an open, free and transparent digital world. Our choices will drive the patterns of investment as well as the migration of skilled labor whether human, hybrid or machine.

G



# Securing the UAE's vision

The UAE has outlined the principles upon which it will build leading up to its centennial year in 2071. These principles chart the strategic roadmap for the UAE's new era of economic, political and social growth – from strengthening the union and institutions to placing digital, technical and scientific development at the heart of its economic development.

They will act as guidelines for all institutions in the UAE as the country approaches a new phase of development over the next five decades. They are part of the 'Projects of the 50' campaign, and are as follows.

## The principles of the 50

### 01. Strengthening the union

The key national focus shall remain the strengthening of the union, its institutions, legislature, capabilities and finances.

### 04. Human capital

The main future driver for growth is human capital: developing the educational system, recruiting talent, retaining specialists and continuously building skills.

### 07. Embracing innovation

The digital, technical and scientific excellence of the Emirates will define its development and economic frontiers.

### 10. Peace and stability

Calling for peace, harmony, negotiations and dialogue to resolve all disputes is the basis of the Emirates' foreign policy.

### 02. The best economy

We will strive over the upcoming period to build the best and most dynamic economy in the world.

### 05. Neighborly ties

Good neighborliness is the basis of stability. The geographical, social and cultural position of the country in its region is the first line of defence for its security, safety and its future development.

### 08. A defined set of values

The core value system in the Emirates shall remain based on openness and tolerance, the preservation of rights, the rule of justice and the law.

### 03. A robust foreign policy

The Emirates' foreign policy is a tool that aims to serve our higher national goals, the most important of which is the Emirates' economic interests.

### 06. A hub of excellence

Consolidating the reputation of the Emirates globally is a national mission for all institutions. The Emirates is one destination for business, tourism, industry, investment and cultural excellence.

### 09. Humanitarian aid

The Emirates' foreign humanitarian aid is an essential part of its vision and moral duty towards less fortunate peoples.

# Action points for implementation

With the roadmap for the future of the UAE clearly defined, how can cyber security leaders best contribute to this roadmap, given the context of potential global themes identified for 2071? We delve into each principle to explore how it can bring a better cyber future for the country.

## The First Principle

### **Strengthening the union**

Tailoring the UAE's legislation in the cyber security domain in preparation for 2071 will require, over the coming decades, an evolution towards a legislative framework that approaches humans, AIs and a combination of the two increasingly consistently. In addition, the legislative framework will need to be applicable across both the physical and virtual worlds as the distinction blurs over time. The Cyber Crime law published in 2021 will evolve over the coming decades to cover these changing dynamics, as legislation increasingly adopts a principles-based approach to defining criminal activity as technology-based approaches become rapidly outdated due to the velocity of technology change.

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*



## The Second Principle

### **The best economy**

To create the best and most dynamic economy in the world by 2071, the UAE's cyber security capabilities, ecosystem and partnerships will need to mirror this position as highly dynamic and adaptive to the rapidly changing technology landscape.

Traditionally, cyber security regulation is seen as holding back the very progress that it should be enabling. Over the coming decades, UAE regulators and technology companies should work hand in glove, working in sandbox environments where regulatory and operational cyber security requirements are iteratively explored. Technology partners in AI, Cloud, IoT the Metaverse and other emerging technologies can be integrated into a highly flexible and collaborative regulatory model; one which enables rapid adoption of technologies across the UAE ecosystem.

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*



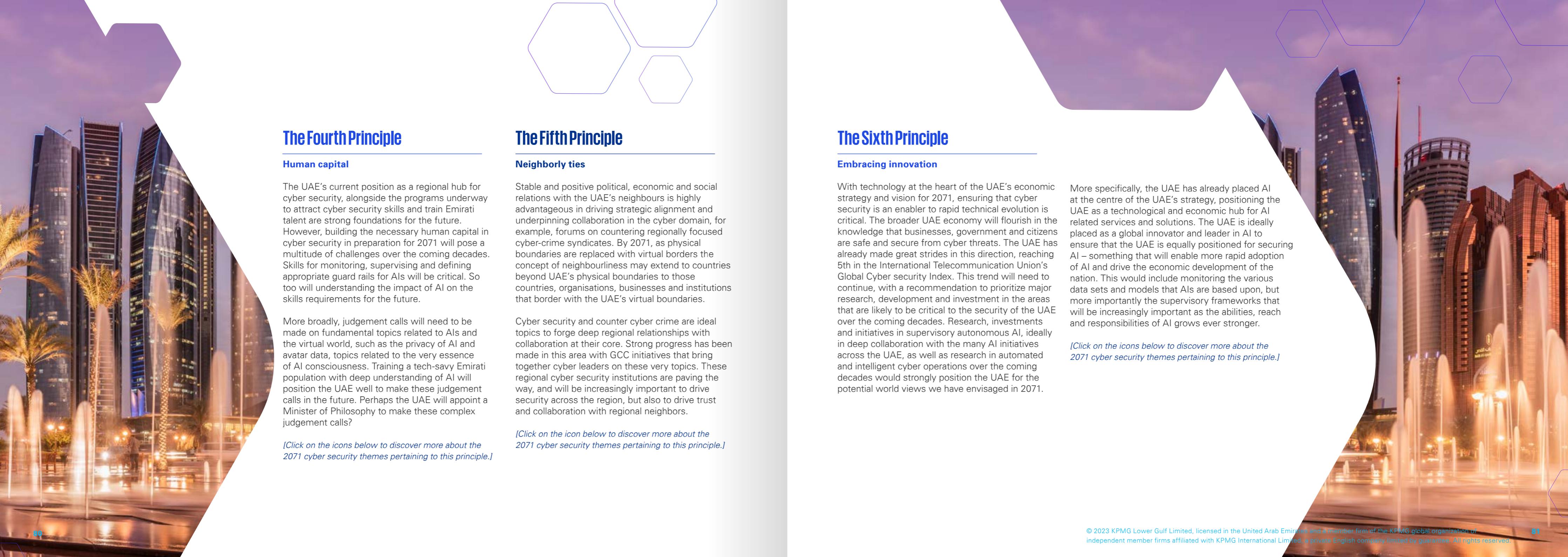
## The Third Principle

### **A robust foreign policy**

The UAE is already positioned as the happiest place to live in the Arab world, according to the latest UN World Happiness Report 2023. By 2071, quality of life and happiness will be increasingly determined by a safe and secure hybrid physical and digital world where citizens (human, hybrid and AI) can freely socialize, work and play. In this future world, the UAE will increasingly need to focus on identifying and holding to account information manipulation and deepfakes by cyber criminals and external state actors that will look to use this hybrid world for strategic and economic advantage.

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*





## The Fourth Principle

### Human capital

The UAE's current position as a regional hub for cyber security, alongside the programs underway to attract cyber security skills and train Emirati talent are strong foundations for the future. However, building the necessary human capital in cyber security in preparation for 2071 will pose a multitude of challenges over the coming decades. Skills for monitoring, supervising and defining appropriate guard rails for AIs will be critical. So too will understanding the impact of AI on the skills requirements for the future.

More broadly, judgement calls will need to be made on fundamental topics related to AIs and the virtual world, such as the privacy of AI and avatar data, topics related to the very essence of AI consciousness. Training a tech-savvy Emirati population with deep understanding of AI will position the UAE well to make these judgement calls in the future. Perhaps the UAE will appoint a Minister of Philosophy to make these complex judgement calls?

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*

## The Fifth Principle

### Neighborly ties

Stable and positive political, economic and social relations with the UAE's neighbours is highly advantageous in driving strategic alignment and underpinning collaboration in the cyber domain, for example, forums on countering regionally focused cyber-crime syndicates. By 2071, as physical boundaries are replaced with virtual borders the concept of neighbourliness may extend to countries beyond UAE's physical boundaries to those countries, organisations, businesses and institutions that border with the UAE's virtual boundaries.

Cyber security and counter cyber crime are ideal topics to forge deep regional relationships with collaboration at their core. Strong progress has been made in this area with GCC initiatives that bring together cyber leaders on these very topics. These regional cyber security institutions are paving the way, and will be increasingly important to drive security across the region, but also to drive trust and collaboration with regional neighbors.

*[Click on the icon below to discover more about the 2071 cyber security themes pertaining to this principle.]*

## The Sixth Principle

### Embracing innovation

With technology at the heart of the UAE's economic strategy and vision for 2071, ensuring that cyber security is an enabler to rapid technical evolution is critical. The broader UAE economy will flourish in the knowledge that businesses, government and citizens are safe and secure from cyber threats. The UAE has already made great strides in this direction, reaching 5th in the International Telecommunication Union's Global Cyber security Index. This trend will need to continue, with a recommendation to prioritize major research, development and investment in the areas that are likely to be critical to the security of the UAE over the coming decades. Research, investments and initiatives in supervisory autonomous AI, ideally in deep collaboration with the many AI initiatives across the UAE, as well as research in automated and intelligent cyber operations over the coming decades would strongly position the UAE for the potential world views we have envisaged in 2071.

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*

## The Seventh Principle

### A hub of excellence

The UAE has been strengthening its federal institutions for decades. This is no more evident than in the field of cyber security where numerous federal institutions have been setup to manage cyber crises, define strategies and legislation and operationally protect critical information infrastructure (CII) from harm. By 2071, these institutions will likely look very different to today, taking on a broader and more encompassing role to deter, protect, detect, respond and recover from threats in the hybrid physical and virtual world. Strengthening the remit of federal entities as well as the legislation that they uphold, will cement the position of the UAE as one nation, with a single common framework for protecting the nation from threats.

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*

## The Eighth Principle

### A defined set of values

Openness, transparency and adherence to a free and open internet will be key to our collective global security in 2071.

Collaboration with institutions in the digital domain that drive positive collaboration, trust frameworks and international rules, such as the International Telecommunication Union, will become increasingly important. The UAE is ideally positioned to collaborate with these institutions to develop and adopt new security models that are aligned to this evolving landscape.

*[Click on the icon below to discover more about the 2071 cyber security themes pertaining to this principle.]*

## The Ninth Principle

### Humanitarian aid

The UAE's position of delivering humanitarian aid regardless of religion, race, colour or culture is laudable. Over the coming decades the definition of humanitarian aid will likely evolve to include 'cyber security aid', as cyber-attacks increasingly have real world consequences for those less fortunate and able to deal with such attacks. Furthermore, by 2071 this humanitarian aid may extend beyond the physical, into the virtual world. The UAE is already running capacity building programs to support other nations in building up their cyber security capabilities and programs as well as providing aid to the neediest. These programs can be extended and perhaps merged in the fullness of time to provide cyber security aid to nations that require support.

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*

## The Tenth Principle

### Peace and stability

The UAE has positioned itself as a key cyber security partner in global and regional institutions, including a leadership role in for Cyber Security in the Gulf Cooperation Council and a contributor to the International Counter Ransomware Initiative. In addition, other forums that endeavour to build trust and collaboration, such as the United Nations will becoming increasingly important over the coming decades to ensure that the UAE is well placed to drive peace and harmony in the digital domain.

*[Click on the icons below to discover more about the 2071 cyber security themes pertaining to this principle.]*

# About KPMG

For about 50 years, KPMG Lower Gulf Limited has been providing audit, tax and advisory services to a broad range of domestic and international, public and private sector clients across all major aspects of business and the economy in the United Arab Emirates and in the Sultanate of Oman. We work alongside our clients by building trust, mitigating risks and identifying business opportunities.

KPMG Lower Gulf is part of KPMG International Cooperative's global network of professional member firms. The KPMG network includes approximately 236,000 professionals in over 144 countries. KPMG in the UAE and Oman is well connected with its global member network and combines its local knowledge with international expertise, providing the sector and specialist skills required by our clients.

KPMG is widely represented in the Middle East: along with offices in the UAE and Oman, the firm operates in Saudi Arabia, Bahrain, Kuwait, Qatar, Egypt, Jordan, the Lebanon, Palestine and Iraq. Established in 1973, the Lower Gulf firm now employs approximately 1,780 people, including about 190 partners and directors across the UAE and Oman.

As we continue to grow, we aim to evolve and progress, striving for the highest levels of public trust in our work. Our values are: Integrity: We

do what is right; Excellence: We never stop learning and improving; Courage: We think and act boldly; Together: We respect each other and draw strength from our differences; For Better: We do what matters to meet the changing needs of our clients, we have adopted an approach aligned with our global purpose: Inspiring Confidence, Empowering Change.

Our KPMG IMPACT initiative aims to help clients future-proof their businesses amid times of increasing focus towards issues such as climate change and social inequality. The goal is to help them achieve success across 17 major Sustainable Development Goals (SDGs) and become more resilient and socially conscious.

Fifty years since its founding, the UAE has evolved into a hub of dynamism, an economic heavyweight and a symbol of perseverance. As the nation recently marked its golden jubilee, KPMG Lower Gulf is proud to celebrate its 50th anniversary in the UAE this year.

Our three pillars – exceptional quality of service, an unwavering commitment to the public interest, and building empowered teams – are the foundation of our firm. Over the coming decades, we commit to lending our support to the UAE's journey as it goes from strength to strength: together, for better.



# Acknowledgments

## Working group

**HE Dr. Mohammed Al Kuwaiti**  
Head of Cyber Security  
United Arab Emirates Government

**Timothy Wood**  
Cyber Partner,  
KPMG Lower Gulf

**Briinish Alva**  
Cyber Security Manager,  
KPMG Lower Gulf

**Claire Mulheron**  
Clients and Markets Manager,  
KPMG Lower Gulf

**Lavanya Malhotra**  
Clients and Markets Assistant Manager,  
KPMG Lower Gulf

**William Navarro**  
Clients and Markets Lead Designer,  
KPMG Lower Gulf

**Sandra Sayouri**  
Clients and Markets Graphic Designer,  
KPMG Lower Gulf

**Lea El Essrawi**  
Clients and Markets  
Knowledge Management Associate,  
KPMG Lower Gulf

**David Ferbrache**  
Global Head of Cyber Innovation,  
KPMG International

**Billy Lawrence**  
Global Cyber Security Program Deputy  
Senior Manager, KPMG International

**Leonidas Lykos**  
Global Cyber Security Program  
Associate, KPMG International

## KPMG Global Network

**Akhilesh Tuteja**  
Global Cyber Security Leader  
Partner, KPMG in India

**Alex Holt**  
Global Head of Telecoms and Media  
Partner, KPMG in the US

**Andreas Tomek**  
Global Cloud Security Cyber Leader  
Partner, KPMG in Austria

**Atul Gupta**  
Global TMT Cyber Leader  
Partner, KPMG in India

**Barry Brunsman**  
Global CIO Advisory Leader  
Partner, KPMG in the US

**Bobby Soni**  
Global Tech Consulting Leader  
Partner, KPMG in India

**Caroline Rivett**  
Global Life Sciences Cyber  
Leader Partner, KPMG in the UK

**Charles Jacco**  
Global Financial Services Cyber  
Leader Partner, KPMG in the US

**Cliff Justice**  
Enterprise Innovation Leader,  
KPMG in the US

**Dani Michaux**  
EMA Cyber Security Leader  
Partner, KPMG in Ireland

**Hartaj Nijjar**  
Cyber Leader, KPMG in Canada

**Henry Shek**  
Cyber Leader, KPMG in China

**James Mabbott**  
KPMG Futures Partner,  
KPMG in Australia

**John Anyanwu**  
Cyber Leader,  
KPMG in Nigeria

**Kareem Sadek**  
Risk Consulting Partner,  
KPMG in Canada

**Lekshmy Sankar**  
Cyber Security Director,  
KPMG in the US

**Lisa Heneghan**  
Global Chief Digital Officer  
Partner, KPMG in the UK

**Matthew O'Keefe**  
ASPAC Cyber Security Leader  
Partner, KPMG in Australia

**Mika Laaksonen**  
Cyber Leader,  
KPMG in Finland

**Mina Zaki**  
Cyber Security Alliances  
Associate Director, KPMG in Australia

**Nashikta Angadh**  
Risk Consulting Partner,  
KPMG in South Africa

**Öztürk Taspinar**  
Digital Innovation Leader,  
KPMG in Belgium

**Prasad Jayaraman**  
Americas Cyber Security Leader  
Partner, KPMG in the US

**Ronald Heil**  
Global ENR Cyber Leader  
Partner, KPMG in Netherlands

**Roni Michael**  
Partner, KPMG in Israel

**Sander Klous**  
Data & Analytics Partner,  
KPMG in the Netherlands

**Sylvia Kingsmill Klasovec**  
Global Privacy Leader  
Partner, KPMG in Canada

**Steven Hill**  
Global Head of Innovation  
Partner, KPMG in the US

**Ton Diemont**  
Cyber Security Leader  
for Saudi Arabia  
Partner, KPMG Lower Gulf

**Walter Risi**  
Global IoT Security Leader  
Partner, KPMG in Argentina

**Wendy Lim**  
Cyber Partner,  
KPMG in Singapore

**Wilhelm Dolle**  
Global IGH Cyber Leader  
Partner, KPMG in Germany

## External

**Dr. Edward Amoroso**  
CEO, TAG Cyber

# Sources

1. **World Population Prospects: The 2017 Revision**, published by the UN Department of Economic and Social Affairs
2. **International Energy Outlook 2021**, US Energy Information Administration: <https://www.eia.gov/outlooks/ieo/narrative/introduction/sub-topic-01.php>
3. <https://worldhappiness.report/ed/2023/>
4. <https://u.ae/en/about-the-uae/economy/digital-economy#:~:text=The%20UAE's%20digital%20economy%20contributes,increase%20in%20the%20coming%20period.>
5. <https://worldpopulationreview.com/countries/united-arab-emirates-population>
6. <https://www.unep.org/resources/emissions-gap-report-2022>
7. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
8. <https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/finance-and-economy/digital-economy-strategy>
9. <https://www.mofa.gov.ae/en/mediahub/news/2023/1/21/21-01-2023-uae>

# Contact us



**Timothy Wood**  
Partner, Head of Cyber Security  
KPMG Lower Gulf  
**T:** +971 56 4096 842  
**E:** timothywood@kpmg.com



**David Ferbrache**  
Global Head of Cyber Futures  
KPMG International  
KPMG in the UK  
**E:** david.ferbrache@kpmg.co.uk



**Akhilesh Tuteja**  
Global Cyber Security Leader  
KPMG International and Partner  
KPMG in India  
**E:** atuteja@kpmg.com



**Prasad Jayaraman**  
Americas Cyber Security  
Leader and Principal  
KPMG in the US  
**E:** prasadjayaraman@kpmg.com



**Dani Michaux**  
EMA Cyber Security  
Leader and Partner  
KPMG in Ireland  
**E:** dani.michaux@kpmg.ie



**Matt O'Keefe**  
ASPAC Cyber Security  
Leader and Partner  
KPMG Australia  
**E:** mokeefe@kpmg.com.au

[www.kpmg.com/ae](http://www.kpmg.com/ae)  
[www.kpmg.com/om](http://www.kpmg.com/om)

Follow us on:



@kpmg\_lowergulf

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG Lower Gulf Limited, licensed in the United Arab Emirates, and KPMG LLC, an Omani limited liability company and a subsidiary of KPMG Lower Gulf Limited, a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International. Designed by Creative UAE

Publication name: Cyber next 50

Publication number: 4775

Publication date: 2023