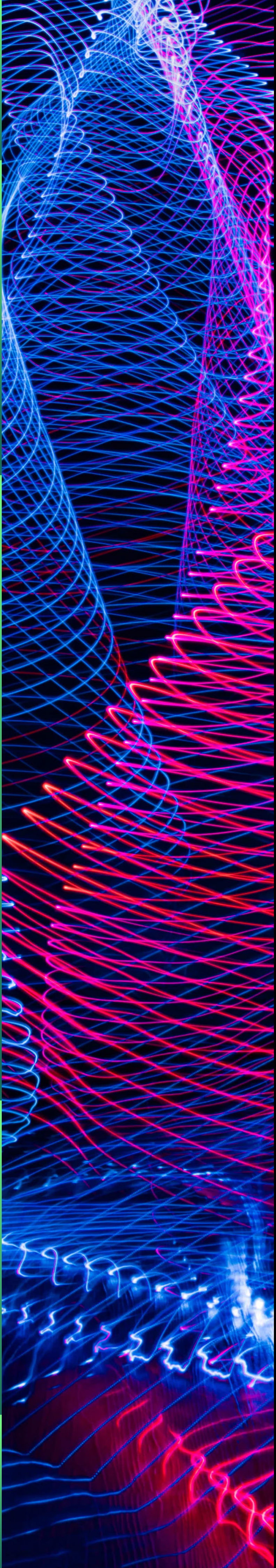


مؤســـسة دبي للمســـــــتقبل
DUBAI FUTURE FOUNDATION

IN COLLABORATION WITH

شرطة دبي
DUBAI POLICE

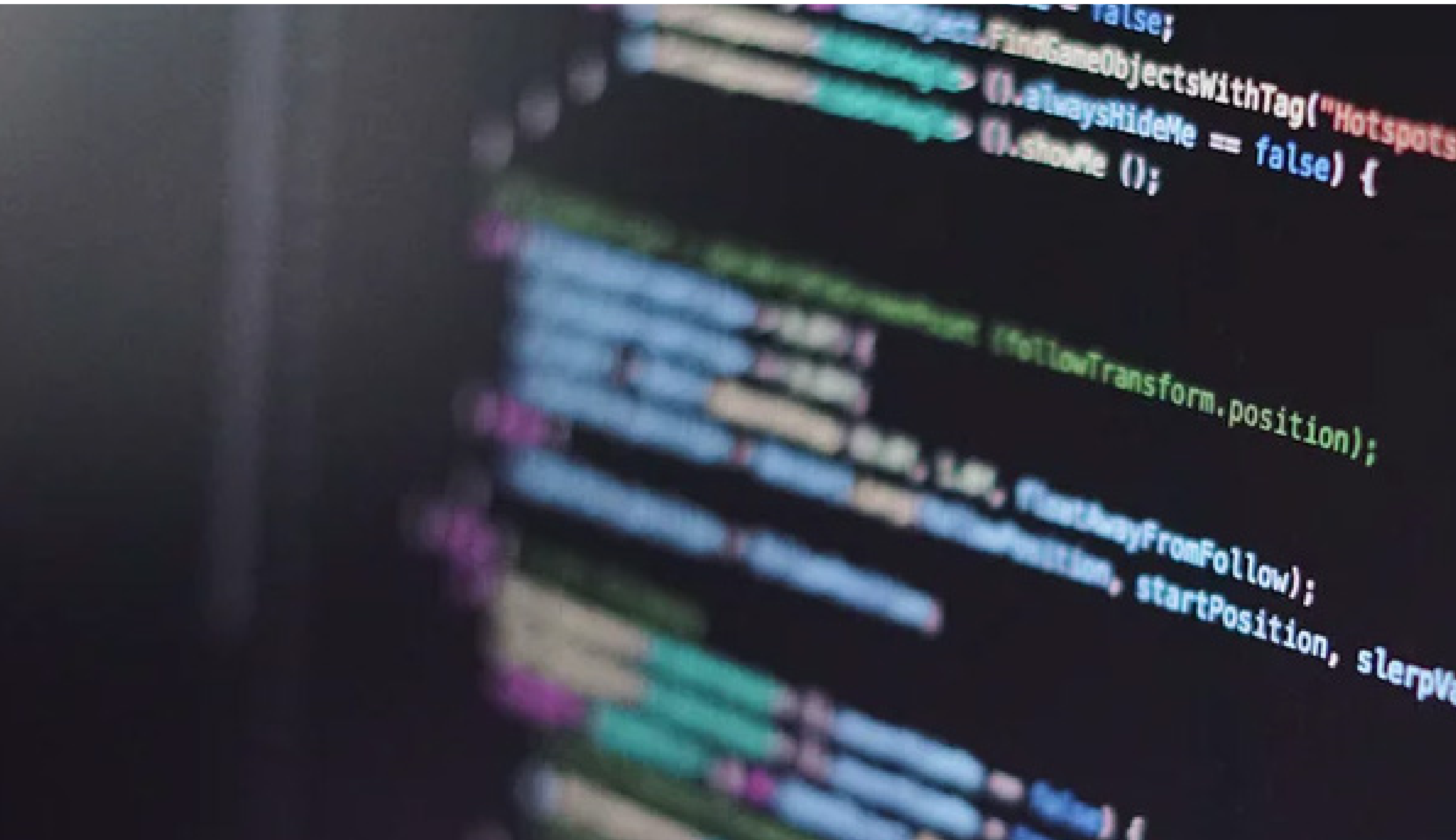
THE DIGITISATION OF CRITICAL INFRASTRUCTURE

BANKING AND FINANCIAL SERVICES SECTOR SCENARIOS OF RISKS AND RESILIENCE

DUBAIFUTURE.AE

Last year the worlds of business and government were shaken when it discovered that Orion, a popular software produced by an American company called SolarWinds, had been hacked. This was because SolarWinds provides network-monitoring and other technical services to hundreds of thousands of organisations, including most Fortune 500 companies and government agencies around the world. The attack gave hackers remote access to an organisation's networks, making it possible to steal confidential information. What was most shocking about the hack was not its occurrence, but the month that passed before it was discovered.

At least six US government departments, including energy, commerce, treasury and state, were breached as well as the National Nuclear Security Administration's networks. The media reported that dozens of security and technology firms, as well as non-governmental organisations, outside the US were also affected, in Canada, Mexico, Belgium, Spain, the United Kingdom, Israel and the United Arab Emirates.



```
false;
FindGameObjectsWithTag("Hotspots
().alwaysHideMe = false) {
().showMe ();
(followTransform.position);
floatAwayFromFollow);
startPosition, slerpV
```

Such threats are not new, and in fact the world faces numerous threats on a continuous basis, both in the form of natural disasters and human-made ones. From natural catastrophes such as raging fires, floods, and hurricanes, to global pandemics, terrorism and supply-chain failures, the nature and scale of threats that face societies have been increasing in magnitude. But when such threats affect the critical infrastructure upon which the welfare of societies depend, the impact of such threats becomes aggravated. This is particularly so when much of our critical infrastructure has or is transitioning into the digital space already. Future planning plays a vital role in addressing risks and incorporating the ability to respond to unforeseen disruptive events. Organisations should therefore adopt future thinking to enhance preparedness against their vulnerabilities in time of crisis.

This brief is a joint effort by the Future Foresight and Decision-Making Support Center at Dubai Police and the Dubai Future Foundation that focuses on the rising threats emanating from cyber-crime and their potential implications for the banking and financial sector in the Emirate of Dubai. The banking and financial sector is an essential and vital component of the critical infrastructure of any modern society. As such, it forms the focus of this brief, which examines four assumptive scenarios of cyber-attack incidents and two potential responses. This provides a wider lens for the key institutions in the critical infrastructure to look forward and prepare better for a secure and resilient future. This brief is a first in a series of six that addresses different sectors as they relate to the critical infrastructure.

WHAT IS **CRITICAL INFRASTRUCTURE?**

Critical infrastructure (CI) includes the facilities and services that are important to maintain the operations of a society and an economy. It is defined as “those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government”.[1] As such, it plays a key role in the functioning of our economy and in the public welfare of society.

Critical infrastructure comprises, but is not limited to, energy, water systems, transport, agriculture, telecommunications, healthcare, food, banking finance, and emergency services both in the public and private sectors.[2] Governments in various countries define CI on the basis of national contexts and priorities. In Dubai, the critical infrastructure compromises the following sectors with examples of CI organisations for each sector:

EMERGENCY SERVICES	Dubai Corporation for Ambulance Services.
TRANSPORTATION	Road and Transport Authority, Dubai Airports, Dubai Bus, Dubai Taxi, and Dubai Metro, and Dubai ports.

[1] Jahier, Khan. (2014). Critical Infrastructure Protection within NATO. Civil-Military Planning and Support Section, Operations Division. Retrieved 17 October 2020, from: http://www.cipre-expo.com/wp-content/uploads/2014/02/Khan-Jahier-NATO-CIPwithin-NATO.pdf

[2] Radvanovsky, R. S., & McDougall, A. (2018). Critical infrastructure: homeland security and emergency preparedness. CRC Press.

FINANCE	Dubai's International Financial Centre, Department of Finance, banks, finance companies, investment and commercial banks, money changers, and Central Bank of the UAE.
ENERGY	ENOC
ELECTRICITY AND WATER	DEWA
ICT	Dubai Smart City, Dubai Internet City, Telecommunications Regulatory Authority, telecommunications companies (Du and Etisalat).
HEALTHCARE SERVICES	Hospitals, clinics, pharmacies, Dubai Health Authority, Dubai Healthcare City.
PUBLIC SAFETY	Dubai Police and Dubai Civil Defense.

Other countries, such as the United States, add further categories to CI such as commercial facilities, which include a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

CRITICAL INFRASTRUCTURE IS RAPIDLY DIGITISING

Digital technology is disrupting the different components that make up the critical infrastructures of countries. The digitisation of transactions, flows, and stocks has made it possible for connected devices and hardware to exchange information with each other across socio-technical ecosystems. This has allowed organisations, especially those operating in the critical infrastructure space, to deploy automated and intelligent communication and self-monitoring systems with the ability to analyse and diagnose issues without the need for human intervention. More specifically, digitisation has changed the design of critical infrastructure to support the following principles: [3, 4]

CONNECTIVITY
systems and machines are connected through publicly owned infrastructure that use different technologies.

MAINTAINABILITY
The ability to work without any human intervention and management should also be sufficient for continuous updates to take place to keep up high-security standards.

SECURITY
high security standards are required to protect against cyber-attacks.

PROTECTION
Technologies should be used to protect the components of the critical infrastructure.

[3] https://www.cisa.gov/commercial-facilities-sector.

[4] SolidRun. (2020). Digital Transformation in Critical Infrastructure Networks. Retrieved 17 October 2020, from: https://www.solid-run.com/wp-content/uploads/2020/09/whitepaper-digital-transformation-whitepaper.pdf

THE BENEFITS OF DIGITISATION FOR CRITICAL INFRASTRUCTURE JUSTIFY THE POTENTIAL RISKS

Around the world, governments have been quick to recognise the benefits of digitisation and data-driven innovations for the provision of sustainable and resilient level of services to their citizens. In Dubai, His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister and Ruler of Dubai has pointed out that “The digital economy is a major catalyst in the growth and development of our new economic sectors and enhancing our competitiveness in the global market and in the future economy”. Digital transformation of critical infrastructure provides important benefits: [5, 6]

DECREASED COMPLICATIONS

Digitising critical infrastructure reduces the complexity of managing and provisioning IT infrastructure. It provides a cost-effective approach to plan, customise, implement, and maintain IT infrastructure.

MORE EFFICIENT WORKFLOWS

Infrastructure digitisation creates the basis for more efficient workflows. When each task within a workflow can have separate needs, teams can have control over how servers or other infrastructure are managed. It also reduces the need for large teams to do a lot of manual work to get started with product development. It also helps save on staffing costs: through machine-to-machine and system-to-system communication, data is shared across multiple systems located anywhere in the infrastructure without any human involvement.

[5] Calsoft Inc. (2020). 5 Key Benefits of Infrastructure Automation. Retrieved 17 October 2020, from: https://blog.calsoftinc.com/2020/05/5-key-benefits-of-infrastructure-automation.html

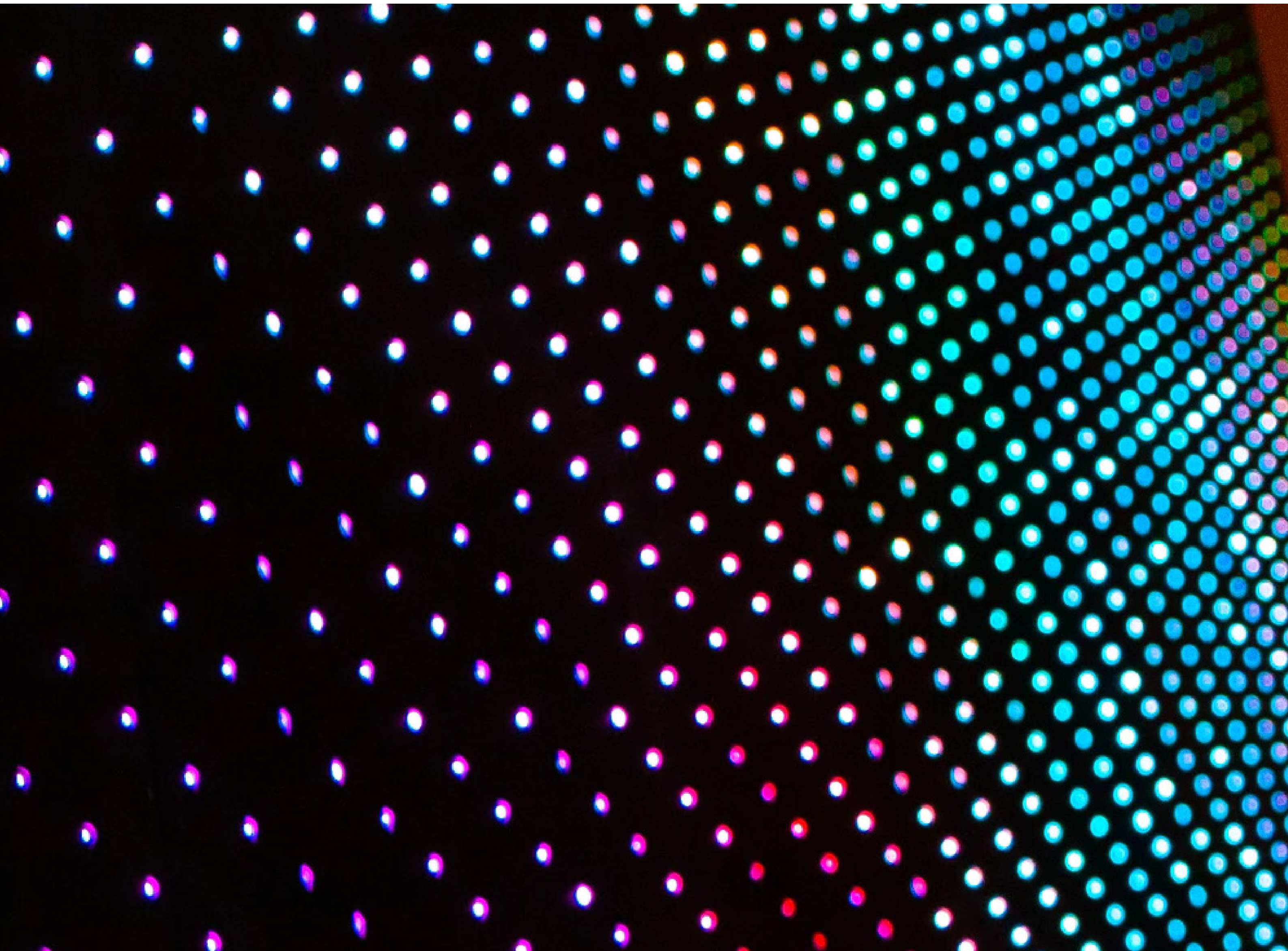
[6] SolidRun. (2020). Digital Transformation in Critical Infrastructure Networks. Retrieved 17 October 2020, from: https://www.solid-run.com/wp-content/uploads/2020/09/whitepaper-digital-transformation-whitepaper.pdf

FASTER DELIVERY

Infrastructure automation controls the process of IT provisioning and this reduces the time (and effort) needed to set up the underlying infrastructure. Teams can get started with building products sooner and bring them to the market faster, overtaking the competition and meeting the customer demands effectively.

REDUCED ERROR

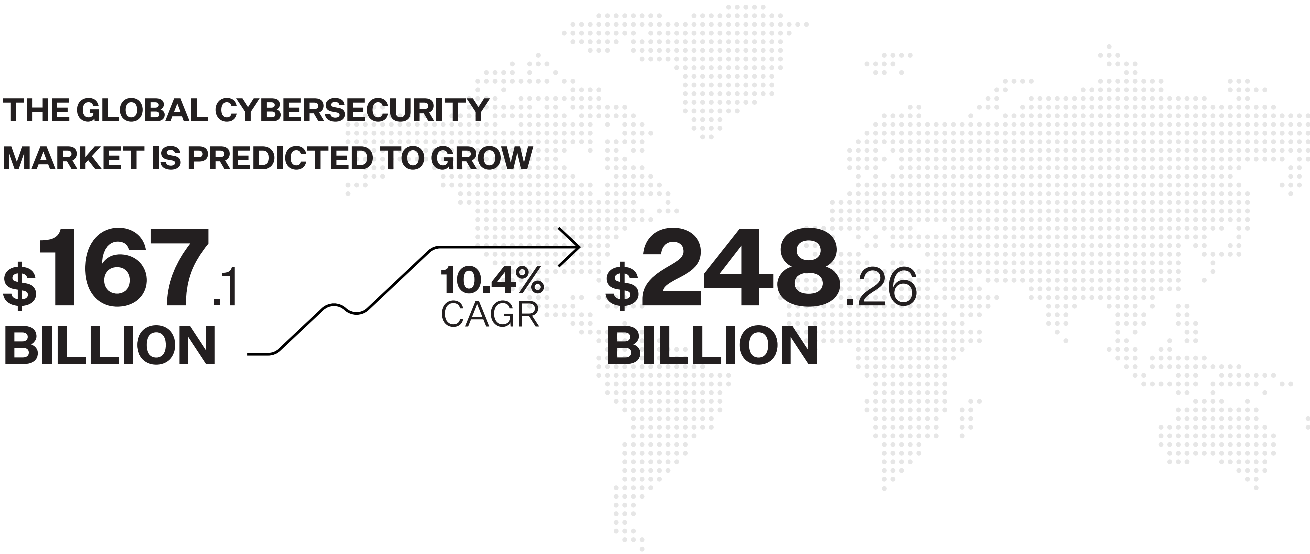
Infrastructure automation reduces the error rate related to manual provisioning of servers. Since all the necessary infrastructure is provisioned automatically, without any human interference, it reduces the chances of error while empowering IT teams to focus on tasks that are mission-critical for the organisation.



DE-RISKING THE DATA-DRIVEN CRITICAL INFRASTRUCTURE

Dubai is a world-leading city that is a pioneer of the use of modern technology with the aim of improving living standards and quality of life. His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister and Ruler of Dubai has affirmed that “our next priorities are developing the contribution of the digital economy to our national economy, consolidating smart infrastructure in the country, enhancing digital readiness, and ensuring business continuity in the UAE under any circumstances”.

Many of Dubai’s services are already digital – from applying for residency visas to paying for parking fines – where much can be done from the touch of one’s mobile device. As all aspects of CI are digitised, risks and threats of cyber sabotage and manipulation grow in parallel. This is reflected in the market for cyber-security products and services. The global cybersecurity market is predicted to grow from $167.1 billion in 2019 to $248.26 billion by 2023, attaining a 10.4% Compounded Aggregate Growth Rate (CAGR).[7]



THE GLOBAL CYBERSECURITY MARKET IS PREDICTED TO GROW

$167.1 BILLION

10.4% CAGR

$248.26 BILLION

[7] https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#558174da381d

Governments are taking notice too. The 2019 US President’s budget included $15 billion for cybersecurity, a $583.4 million (4.1 percent) increase over 2018. The US Department of Defense (DoD) was the largest contributor to the budget. The DoD reported $8.5 billion in cybersecurity funding in 2019, a $340 million (4.2 percent) increase over 2018.[8]

ADDRESSING THE THREE ELEMENTS OF RISK

Risk is the function of three elements: the threats to which an asset is susceptible, the vulnerabilities of the asset to the threat, and the consequences. While cyber-security deals with prevention, insurance deals with recovery.

To build resilience is to build preparedness for what to do when threats or hazards strike. A “hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed”.[9] Vulnerability is a “physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard”. Consequences are the “effects of an event, incident, or occurrence”.[10] Resilience is therefore about protection and response during a crisis and after it.

[8] https://cybersecurityventures.com/cybersecurity-market-report/

[9] Department of Homeland Security, 2010.

[10] Ibid.

THE **FOUR DIMENSIONS** OF RESILIENCE

There are four dimensions to resilience that are identified in the research[11]

TECHNICAL RESILIENCE

this refers to the ability of the organisation's physical system to perform properly when subjected to a crisis.

ORGANISATIONAL RESILIENCE

this refers to the capacity of crisis managers to make decisions and take actions that lead to a crisis being avoided or at least reducing its impact.

ECONOMIC RESILIENCE

this refers to the ability of the entity to face the extra costs that arise from a crisis.

SOCIAL RESILIENCE

this refers to the ability of society to lessen the impact of a crisis by helping first responders or acting as volunteers.

Big data and information systems increasingly play a key role in each of these four elements of resilience. A system failure due to human error, natural disaster, or sabotage may affect each of them. What if the designated safety design and construction built into police and law enforcement information systems broke down? What if the emergency power generators failed as they did in the 2011 Fukushima Daiichi nuclear disaster in Japan? What if the crisis team and top management ability to meet and coordinate was undermined due to a cyber-attack? What if the crisis managers were not prepared for the nature of the crisis as it proved to be the case in the COVID-19 crisis?

[11] Labaka et al. in Technological Forecasting & Social Change 103 (2016) 21–33.

BANKING AND FINANCIAL SERVICES ARE ESSENTIAL COMPONENTS OF DUBAI'S CRITICAL INFRASTRUCTURE

In 2019, Dubai ranked 8th in the world as a global financial leader (up from 15th place in 2018), ahead of all other GCC locations.[12] In the same year, there were a total of 22 licensed banks in the country. The UAE banking industry is the biggest in the region, home to nearly one-third of the GCC's banking assets. As one of the country's two financial centres in the country, Dubai has established itself as an integral component of the global financial services system with vibrant onshore and offshore markets.

The Department of Economic Development's Economic Outlook Report for 2019 indicates that Banking, Insurance and Capital Markets, and the financial services sector, was the third largest contributor to Dubai's real GDP in 2018, generating value added of AED 40.4 billion in constant prices or 10.2 percent of the total. The sector indirectly facilitates other economic activities through the extension of loans and credit.

Dubai-based Emirates NBD is the second-largest bank in the country, the largest in the emirate, and the third-largest in the GCC, claiming approximately 20% of the national loan portfolio. Dubai Islamic Bank (DIB), is the largest Sharia-compliant institution in the UAE, as well as the world's second-largest Islamic bank. Dubai hosts a domestic stock exchange, Dubai Financial Market and an international capital market, Nasdaq Dubai.

[12] https://dubaided.gov.ae/ded_files/Files/Reports/rep_2019/DER2019_EN_Report_f4.pdf

Nearly 90% of the UAE's financial assets are held by locally owned institutions. Much of the remainder is managed by the 38 foreign institutions licensed to operate. A larger number of foreign institutions operate from the Dubai International Financial Centre (DIFC) – the offshore financial services free zone that is one of the key pillars underpinning the emirate's reputation as a regional financial centre. Around 100 foreign banks have established a presence in the free zone.[13] The non-banking financial sector is small (around 20 finance companies licensed by the Central Bank of the UAE [CBU]) accounting for approximately 1.4% of UAE banking system assets.

Like in most advanced economies, banks play a central role in the lives of people. The UAE Central Bank operates among other things the UAE Funds Transfer System, the UAE Direct Debit System and most importantly, the Wages Protection System (WPS). The latter is an electronic salary transfer system that enables employees to be paid via banks, bureaux de change and financial institutions. Any interruption of these services risk creating hardships for individuals and businesses.

[13] https://oxfordbusinessgroup.com/overview/forward-bound-increased-profits-and-stable-liquidity-fuel-expansion

According to FCSA,[14] almost 90% of the people in the UAE make use of digital banking channels and up to 100% make use of ATMs for their banking transactions. This signifies an elevated level of dependency on digital services. In addition, a high percentage of them use mobile banking. Digital branches, electronic wallets, and other contactless services are all on the rise. UAE and Dubai banks are also pioneering the use of 'open banking' where data is shared between multiple, unrelated entities. This is to allow for the creation of single platforms where customers can fulfill a variety of needs. The integration of services into single platforms is seen as the cornerstone of digital banking.[15] While such data-driven innovations enhance customer experience, they also create security difficulties and increased vulnerabilities arising from potential cyber-attacks and cyber-sabotage (Box 1).

IN THE UAE

90%

of the people make use of digital banking channels

100%

make use of ATMs for their banking transactions.

[14] Federal Competitiveness and Statistics Centre https://fcsa.gov.ae/en-us/Lists/D_Reports/Attachments/16/StatisticsUnlocked3en-v04.pdf

[15] https://assets.kpmg/content/dam/kpmg/ae/pdf/uae-banking-perspectives-2020.pdf

SCENARIOS OF VULNERABILITIES: **WHAT IF A CYBER-ATTACK ON THE BANKING AND FINANCIAL SYSTEM TOOK PLACE?**

Cyber-attacks on the banking and financial system of a country have a ripple effect on the entire functioning of society. The interconnectivity and interdependency between the banking system and business, economic and social institutions, means that an attack on one or more institutions can result in significant adverse effects to public health or safety, economic security, and national security as well.

Technical systems are designed and built in a way to prevent such a cascading effect from happening. Nevertheless, such attacks continue to happen annually.

FIVE TYPES OF CYBER-ATTACKS ON BANKING AND FINANCIAL INSTITUTIONS*

1

Deletion of critical data
Compromise of the availability of data critical for the accurate and effective functioning of payments, clearing and settlement processes through data deletion.

Manipulation of critical data
Compromise of integrity of data critical for the accurate and effective functioning of payments, clearing, settlement processes through data manipulation.

Disruption of critical industry-wide services
Disrupted availability of critical payments, clearing, and settlement services of multiple institutions for an extended period of time.

Fraudulent transactions
Initiation of fraudulent transactions leveraging critical payments infrastructure.

Theft of critical non-public information
Compromised confidentiality of industry-critical non-public information for use in insider trading, market manipulating action, or intelligence gathering.

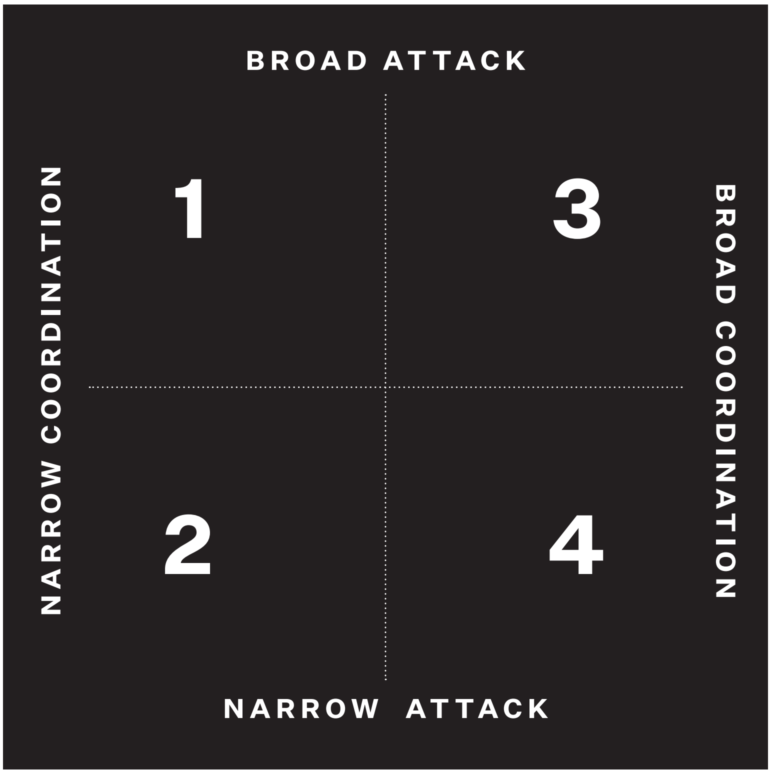
*Source: DTCC/OliverWyman, 2016

HOW MIGHT WE RESPOND?

Cyber-attacks range from narrow attacks on one or two targeted organisations to broad attacks on multiple organisations with the aim of bringing an entire system to a halt. Narrow attacks can result in substantial damage to the targeted organisation and its immediate stakeholders. Broad attacks can have wide ranging consequences on the entire ecosystem.

The extent of the damage is determined by the response coordination level. An uncoordinated response can result in a narrow attack creating widespread damage; while a well-coordinated response can help limit the damage from a broad attack.

IN THE FOLLOWING SECTION WE EXPLORE THE TWO RESPONSES UNDER 4 SCENARIOS.



Narrow Coordination Under Two Scenarios: **BROAD AND NARROW ATTACKS**

NARROW COORDINATION UNDER TWO SCENARIOS:

BROAD AND NARROW ATTACKS

1

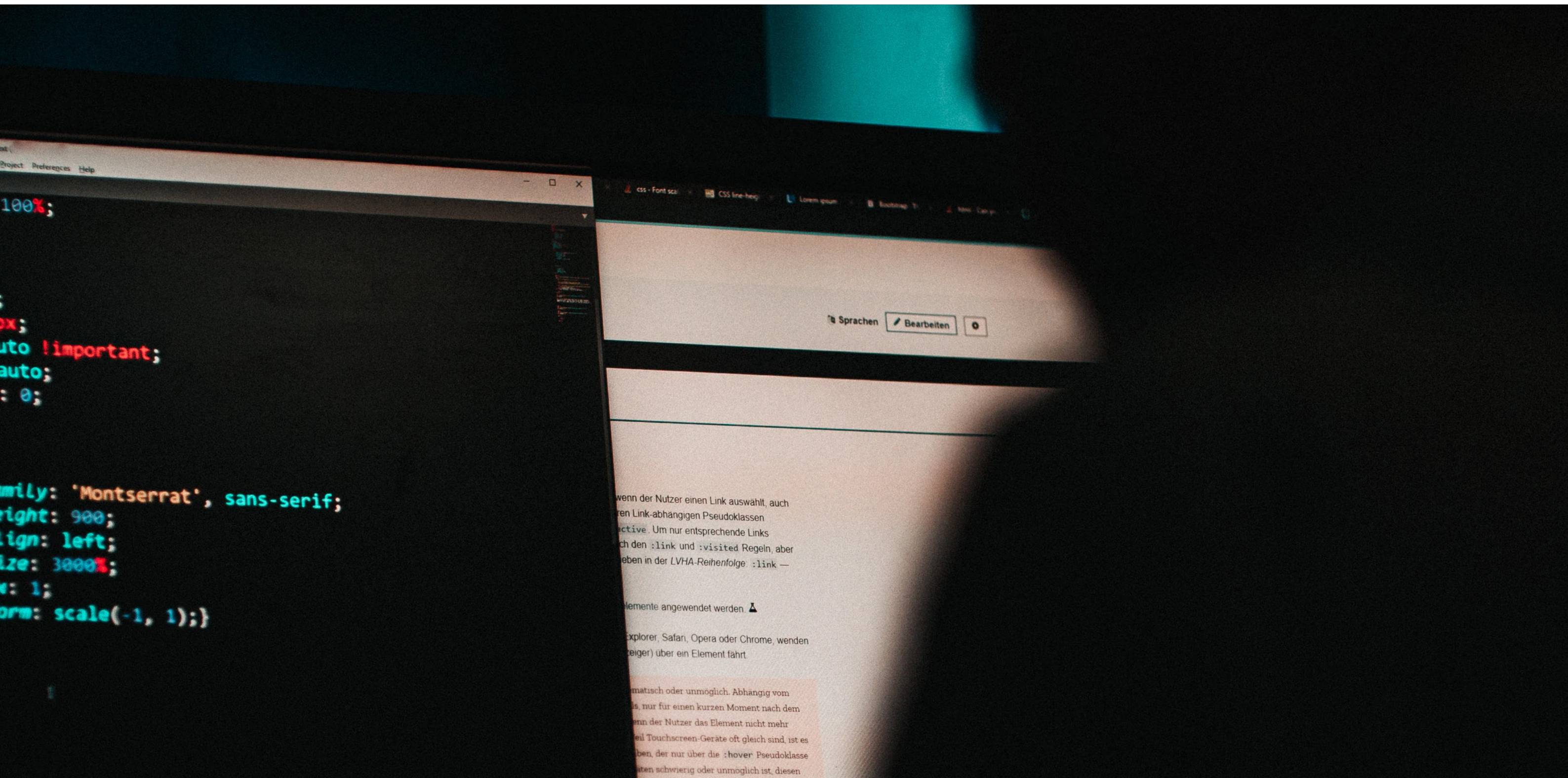
In this scenario, there is a broad attack on the banking and finance system that brings a majority of business to halt. However, the attack is only confronted initially with a narrowly coordinated response. The narrowness of coordination is the result of lack of readiness and preparation among institutions at all levels. There has been very little advance awareness, training or coordination between key institutions regarding what to do and how to respond to such a threat. There is therefore little knowledge of the technical design and architecture of the different security systems at different key institutions, little knowledge of who to call, correspond and coordinate with at the government level, and little awareness of the extent of the threat, the nature of the risk, and the potential range of loss.

At the organisational level, only very few institutions had any pragmatic strategy for how to respond to such an attack. Overall, organisations lacked coordinating units in charge of security issues and therefore lacked systems of monitoring and enforcement. With insufficient or ineffective guidance and governing frameworks information and data at most organisations were kept unsafe.

Consequently, the attack has left long-lasting reputational damage to the institutions in the country. The public have become concerned that senior management in businesses and other organisations have lacked the commitment to maintain adequate levels of data security. There are justified fears that further similar attacks may follow and that they may have to face up to frequent business interruptions.

Economically, the narrow and weak coordination has meant that recovery is taking longer. Larger banks have concentrated on their own recovery, coordinating where possible with other large banks. Smaller banks and their clients have been more exposed. As many of these come from smaller emirates, the economic fallout of the cyber-attack on the banking system has been more severe in the smaller emirates with salaries, pensions, and payments for public contracts all interrupted. The lack of coordination at all levels has meant that there was no single source of information about the incident which allowed rumors to spread among clients and consumers. In some places, there have been runs on banks as customers were not sure whether their funds are safe and whether and when they can access them. Recovery time is unknown and the economic impact is increasing by the hour.

At the societal level, there are fears and rumors of job losses, misused funds, bouncing payments, and loss of critical business information. The elevated level of anxiety and stress in society led those who were able to access their bank accounts to withdraw and transfer funds outside the country via alternative means. There has been an increase in incidents of violence at banks and money transfer services, as well as labour strikes, and even domestic violence. The Police force was overwhelmed with requests to interfere and assist.



NARROW COORDINATION UNDER TWO SCENARIOS:

BROAD AND NARROW ATTACKS

2

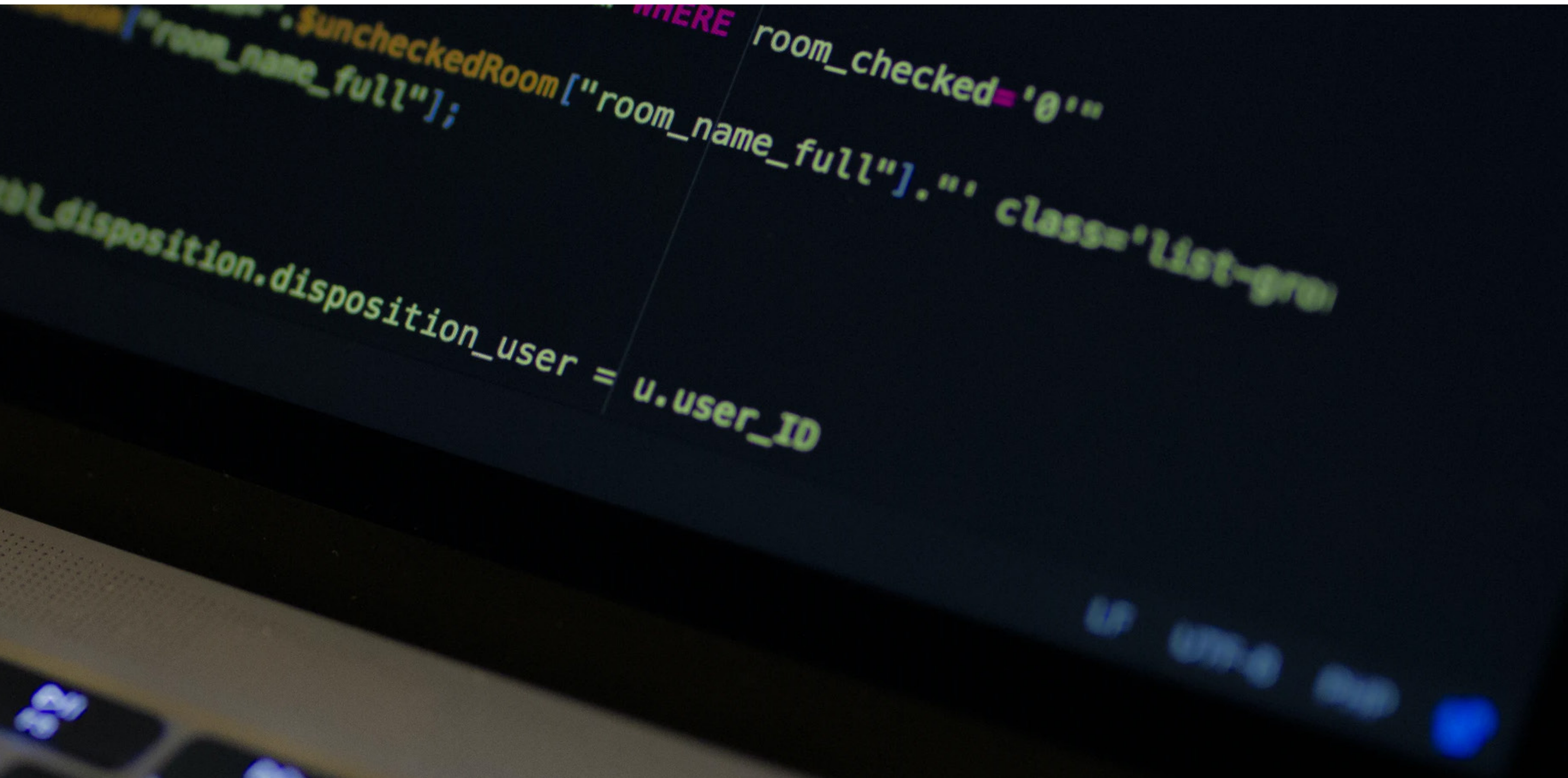
In a second scenario, a narrow attack targets one or two financial institutions in Dubai. As the attack was limited in its targeting, a general sentiment of ‘this wouldn’t happen to us’ prevails among other banking and other institutions in the Emirate. The attack is seen as a result of specific loopholes and vulnerabilities at the target institutions and was therefore seen as nothing that the other institutions needed to worry about.

The narrow attack has forced the target institutions to adapt, learn lessons and prepare better for the future. But as they have done so individually, the learning from the attack has been confined to them and not shared with other institutions. In fact, given the narrowly coordinated response, the opportunity to consider a wider response arrangement and a broader coordination among other potential targets in the Emirate has been limited. This has resulted in minimal technical and organisational learning across organisations that are part of critical infrastructure ecosystem.

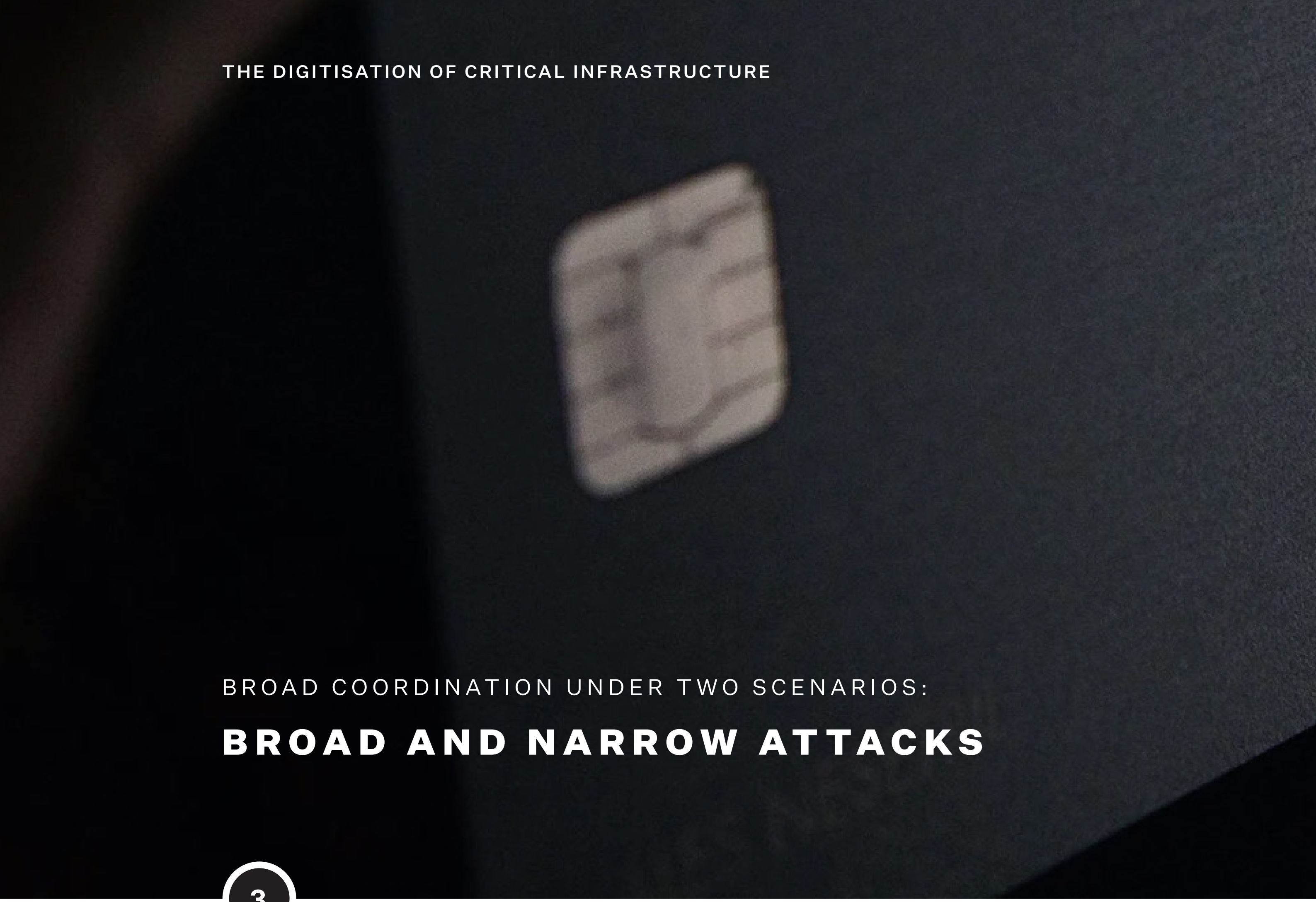
The narrow attack has nevertheless resulted in thousands of businesses and individuals being left out of service with nowhere but the banks themselves to go to. As these have been striving to survey the damage and restore service, they have had no redundant resources to respond to the more immediate needs of affected customers. The narrow coordination has also meant that social and governmental institutions have not been prepared to rush to aid. The lack of information about the depth and breadth of the attack has hampered their ability to provide effective support where needed.

The attack, while narrow in nature, has generated a sense of unease and vulnerability among those directly and indirectly affected by it, both domestically and overseas. Clients who couldn't pay bills or complete necessary transactions had to explain their situations individually and face potential penalties. This has had the effect of reducing trust in the security of the banking system as it has been seen that the onus of security falls on individual banking institutions alone. It has also created the impression that certain banks and financial institutions are better equipped and managed than others in dealing with growing cyber-attacks. Such impressions have led to unhealthy competition between financial institutions around perceived immunity against cyber risks, elevating the level of investment in cyber security technologies beyond optimal levels of efficacy.

Overall, the uncoordinated response has meant that each institution had to foot the bill of security on its own, resulting in a situation that is characterised by higher security costs overall with lower security efficacy for each institution. This is in contrast with the scenario of broad coordination across institutions in the critical infrastructure ecosystem where the costs of security are distributed and the security efficacy is high.



```
WHERE room_checked='0'"
.$uncheckedRoom["room_name_full"]."' class='list-gro
["room_name_full"];
_disposition.disposition_user = u.user_ID
```



BROAD COORDINATION UNDER TWO SCENARIOS:

BROAD AND NARROW ATTACKS

3

In the third scenario, a cyber-attack strikes across the banking and financial system. The attack is quickly detected as there is a centralised alert system in place at the Dubai Cyber-Security Detection and Repel unit, which constantly monitors and flags cyber threats. Most key institutions that are part of the critical infrastructure have rehearsed for such a scenario already. From a technological perspective, they have advanced prediction solutions capable of forecasting threats through data analytics, social media tracking and surveillance, online group chats, political unrests, dark-web and deep web conversation. A cross-institutional emergency team is already in place and knows exactly the steps that need to be taken. There is a high level of awareness among all concerned entities, not only at the level of senior management but at all levels of organisation. Staff feel both competent, and therefore confident, to prevent such attacks from running too long or wreaking havoc through the economy.

The government declares that emergency procedures are activated. Assurance is provided from the highest level of leadership, especially regarding safety of funds and access to essential goods and services.

Coordination takes place between all banks and across critical stakeholders, including the Central Bank, key Government entities, major retailers, credit bureaux, Police Cyber-Crime Unit, key grocery chains and petrol stations as well as medical services. Under the emergency procedures, Emirates ID serves as a temporary payment card for essential products and services (with fixed upper limits).

A pre-validated network of grocery/petrol purchasing points is already in place. Insurance companies announce their readiness for immediate emergency funding. Backup systems at banks and other key institutions are up and running before the spread of any panic.

This broad level of coordination across businesses, government and societal institutions ensures that essential businesses and daily lives go uninterrupted.

A roadmap for how to deal with the situation has been prepared and is ready to be implemented in a highly coordinated manner. There is therefore a consistency in the response across all levels and sectors.

A consistent statement from the Central Bank emphasising their support to the banking system ensures that the public is assured. The Police manage communication with the public about contingency plans, recovery time, and information pertaining to assistance, support and relief plans. As a result, recovery is quick and losses are limited. The reputation of Dubai's governmental and private institutions for resilience and crisis management are strengthened further.

BROAD COORDINATION UNDER TWO SCENARIOS:

BROAD AND NARROW ATTACKS

4

The fourth scenario is like the second, a narrow attack hits one to three financial institutions in the Emirate of Dubai. Only this time, the response is broad and coordinated. The Dubai Cyber-Security Detection and Repel unit at the Dubai Police immediately raised the alert level to red to inform all organisations across the Dubai critical infrastructure ecosystem of the need to activate emergency procedures. The critical infrastructure ecosystem consists of key organisations in key services in the Emirate, including healthcare, social care services, power and water supply, transport, food supplies, and banking and finance. The Dubai Police coordinate a cross-organisational “security fence” platform that stretches across all organisations that are members of the platform. Each organisation has a full-time unit that acts as the point of coordination, monitoring and liaison with the Police.

As soon as the affected institution raised the alarm, an alert went to all member organisations to activate their emergency plans. These included a set of actions ranging from immediate communication with clients and partners to activating contingency plans to support vulnerable clients.

Information about the technical nature of the threat is shared and technical experts from across the ‘security fence’ platform were quickly mobilised to provide technical assistance. Both the cost of and the knowledge from the incident are shared. Clients felt appeased and comforted that the situation is in control and that this is an attack on all and not on a vulnerable institution. The wide alert about the attack has meant that clients of the targeted financial institutions found that all key public and private institutions with which they have financial transactions are aware of the situation and have communicated to them the temporary procedures put in place to remedy the situation until the full service is restored. Trust in the system is enhanced, the cost of security and recovery is widely distributed and the value of learning is shared.

HOW MIGHT WE BE BETTER PREPARED?

TECHNICAL VULNERABILITIES

The technical dimension of risk is the capability of physical systems to cope and perform well under a crisis so that they are able to continue to perform their key functions.[16] Technical preparedness therefore revolves around three main themes: prevention, detection and recovery.

Organisations need to be aware that a cyber-attack is taking place or that a vulnerability is identified. Here, prevention through interception is particularly important. If an attack is intercepted and prevented in a timely manner, no further effort is required beyond that point apart from raising awareness about it with the relevant authorities and within a business community.

[16] Ionuţ A. (2018). Improving The Level of Critical Infrastructure Protection by Developing Resilience. Land Forces Academy Review. 23. 237-243. 10.2478/raft-2018-0028.

If interception and detection do not take place in time, then the technical systems should be designed and built in such a way that they allow for a quick damage mitigating response. The focus of the response should be on mitigating the impact of an attack in terms of time and spread.

The technical system should also be designed and built to allow for a quick recovery time. There must be a balance struck between a speedy service resumption and a safe resumption. Alternate processes and back-up applications and geographically diverse data centres could be part of the recovery strategy.

Technical resilience is only possible through a broad coordination between interlinked organisations. A quick recovery at a few organisations may be undermined by a slower recovery elsewhere. Within organisations, there needs to be investment in advanced prediction solutions capable of predicting and forecasting threats through data analytics, social media tracking and surveillance. They need to invest in the skills required to run and modify these systems to achieve a high-level of readiness against imminent cyber-attacks.

WHAT BANKS CAN DO?

There are several methods that banks can adopt in order to create a more safe and secure digital landscape and defend themselves against potential cyberthreats.

ASSESS CLOUD SECURITY

Regularly review your cloud infrastructure to ensure it's up to date. Assess your cloud security's current state compared to security benchmarks, best practices and compliance standards.

MONITOR CLOUD SECURITY

Use a vulnerability management tool to help you automate threat detection and protect against potential threats before they become a problem.

ESTABLISH STRICT ACCESS MANAGEMENT POLICIES

By only providing access permissions to employees who require it, you're ensuring your organisation is well-protected from within –– especially if you employ contractors or part-time workers.

ESTABLISH A DISASTER RECOVERY PLAN

Having a plan in place helps you avoid data loss and allows you to minimise downtime after a disruption. This only works if you back up your data regularly and often.

ENCRYPT DATA

Encrypting your data, and protecting the cryptographic keys, ensures your most sensitive digital assets are always protected –– even if your IT structure is critically compromised.

ORGANISATIONAL VULNERABILITIES

The organisational dimension of risk is the capacity of a organisations to foresee, prepare for, react and adjust to unexpected disturbances.[17] As organisations continue to undergo a digital transformation – using technologies such as cloud services, AI, IoT and so on, they become exposed to new risks and vulnerabilities.

One important aspect of organisational preparedness is increasing awareness among employees of how cyber-attacks can happen and the impact they can have. This can only be done effectively if cyber-security is a coordinated function within and across organisations. Organisations need to develop and adopt a cyber-security governing framework that defines the laws, policies, steps and guidance for organisations on how to manage data, protect it, and respond to risks and sabotage.

Just as the behaviour of one person can undermine the security of an entire organisation, one organisation can also undermine the security of an entire industry. Awareness can only be effective when applied at industry-wide level and coupled with regulation.

[17] Denyer, D. (2017). Organizational Resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management.

Regulation needs to tie protocols and practices together across organisations and at the country level. By design, digital operations are transnational. Organisations need to be aware of security risks and exposure via their transnational supply chains.

WHAT MIGHT ORGANISATIONS DO?

RECRUIT NEW TALENT

The cybersecurity industry is already severely constrained for talent. Organisations operating in the Critical Infrastructure domain need to become creative in where they look for cybersecurity talent. Infrastructure players might look to “cyber-utilities,” for instance, which are industry-aligned working groups that pool information and resources to improve cybersecurity effectiveness for their membership.

FORM A CYBER RESPONSE TEAM

The first hours after the discovery of a cyberattack are the most critical in effectively mitigating losses, and their importance is magnified in the case of attacks against infrastructure where loss of life may be a possible second- or third-order effect. For this reason, selection and training of an incident response team before an incident occurs is key.

CULTIVATE A MINDSET SHIFT ACROSS THE ORGANIZATION

To begin the mindset shift, organisations need to develop a perspective on what a cyberattack would actually look like for them. Cyber war gaming and table top exercises have long been a staple for developing this perspective in corporate environments, and they can be similarly effective for infrastructure. Effective exercise scenarios emulate the actions of timely real-world attackers to impose a series of difficult decisions on the team, creating numerous (and sometimes painful) learning opportunities.

The European General Data Protection Regulation (GDPR) provides a good starting point for data management across borders, but it should be complemented with national and industry specific regulations too. Ultimately, legislation is key for compliance and for putting security prominently on the senior management agenda.

At the level of individual organisations. management needs to recognise the potentially devastating financial losses caused by a cyber-attack, identify critical services, and build a protection strategy as well as a mitigation strategy.

To be effective, organisations need to build partnerships with their key stakeholders around security coordination and risk management to help reduce the impact of any attack. Management needs to be fully aware of the extended boundaries of their security architecture in order to engage with potentially vulnerable stakeholder organisations in their commercial and technical ecosystem.

Organisations should also come together to share experiences. This will make future recurrences less likely as awareness about the full range of vulnerabilities becomes greater.

ECONOMIC VULNERABILITIES

The economic dimension of the risk is the ability of the economy to cope, recover, reconstruct and minimise the aggregate negative impact on social welfare. The longer the interruption of services is, the greater the impact on the economy. One critical aspect in this context is managing fear. Members of the public and businesses will understandably be concerned with the potential length of service interruption and the safety of their funds.

It is imperative therefore that a high-level broad coordination response from key government entities and key economic players, such as the Central Bank and large employers, is in place. Such a high level of effective coordination to counter a national crisis has been on display by the UAE government during the peak of the COVID-19 crisis.

But a cyber-attack on the banking system may cause a more severe crisis over a shorter period of time. With e-payments, ATMs, in-store payments, and inter-bank transfers locally and internationally all interrupted, the economic impact will be acute. In this context, managing fear begins with assuring the public about access to essential goods and services. This assurance should begin by pre-empting any such crisis.

A broad coalition of key government entities and key economic players, perhaps building on the COVID-19 committee, could prepare a joint emergency plan and a response roadmap and communicate them to the public. In the case of such an emergency, all major stakeholders as well as the public are assured that the crisis is under control. Assurance from the highest level of leadership, regarding especially with regards to safety of funds and access to essential goods and services, would be critical.

Contingency funds and funds-dispersing mechanisms are activated. Both the public and small businesses need to be able to continue to have access to funds and payment mechanisms to purchase essential goods and services, including fuel and medical services.

A pre-identified list of potential vulnerable transaction points should be created to allow emergency responders to intervene instantly to keep interruption time to the minimum. These could be drawn from stress-test exercises conducted to determine the extent of vulnerability that characterise a list of pre-identified essential payment systems (for example for hospitals, police, civil defence, among others).

The crisis governance structure should be clear and visible as it was the case during the COVID-19 response. The response is consistent and assuring. Information is communicated through official channels and concerned entities know exactly what to do in accordance with the plan.

On the economic front, the length of the interruption is a key factor. The longer the attack is, the worse the long-term reputational damage to the economy. In fact, the way a crisis is managed will have a long-term impact on the reputation of public and economic institutions managing the Dubai economy. Trust is the opposite of fear and therefore managing fear is an essential element in preserving trust in the Dubai economy in short and long run.

SOCIAL VULNERABILITIES

Social vulnerabilities are the risks that may affect the ability of communities to effectively deal and cope with emerging threats and challenges. The way a society deals with a crisis is to a great extent judged by the way it alleviates the negative impact on its most vulnerable segments.

Key government entities, social sector organisations and the Dubai Police will need to work together on a pre-emptive plan to mitigate the effect of a large-scale cyber-attack on the most vulnerable segments in society. A starting point would be through pre-emptive awareness. As with other aspects of resilience discussed earlier, service continuity and fear management are the two top priorities.

A pre-identified list of societal segments with extra special needs that would require minimal interruption of access to certain goods and services would have to be in place. A broad back-up plan needs to be created and shared across all key emergency response organisations, including some in the private sector such as logistics companies, private clinics, petrol stations and grocery shops. For example, a list of individuals or people of certain professions could be granted access to goods and services from designated dispersing points without the need to make any payments.

Insurance companies could provide automatic guarantees for non-electronic payments made based on solely showing a plastic bank card and an ID. Such temporary alternative payment facilities should be made and agreed in advance of any such crisis if any to prevent highest level of assurance and mitigation against fear of unnecessary hardships.

Broad coordination in a cosmopolitan place like Dubai and the UAE would require collaborating with and engaging ethnic and nationality clubs, tribal, neighborhoods, and family majalis (plural of majlis) or councils, as well as professional associations. Large employers also play an important role in coordinating response between government entities, banks, large retailers and their employees.

Awareness needs to be managed at the local community, especially for children and parents, and in different languages level. The centrality and consistency of response is not only important to prevent unnecessary fear and anxiety but also to prevent scams and criminal activity that might seek to take advantage of the situation.

LOOKING FORWARD

Dubai's critical infrastructure and its economy are increasingly digitising. As Dubai-based businesses and public service providers continue to build the capabilities necessary to reap the benefits of digital technologies, the risks of cyber-crime will continue to grow in magnitude. The nature of a cyber threat is not dissimilar to that of a pandemic. A cyber-attack on one organisation can quickly turn into an attack on all organisations. Just like a pandemic, cyber risks need to be managed collectively and through broad coordinated planning and action. It is not a task for government to take care of on its own, nor it is a task that concern private sector organisations only. What is needed is a broad cross-sector coordinated framework of action. The following constitute some of the important elements of such a framework.

CALLS TO ACTION!

An attack on one financial institution is an attack on the Dubai critical infrastructure. Whether it is a narrow or a broad attack, the response needs to be broad and coordinated.

FOR GOVERNMENT

There must be a high-level unit in government that is charged with maintaining a broad coordination response across all key government entities and key economic players, including the Central Bank and large employers.

Assurance from the highest level of leadership must be communicated to the public, assuring them regarding access to essential goods and services and safety of funds and personal data.

A pre-identified list of vulnerable groups must be created to allow emergency response to be effective and instant.

The crisis governance structure must be clear and known before any crisis occurs and must be visible during the recovery period.

Information must be communicated and reached through well-known official channels.

The Dubai Police are best suited to coordinate plans and action across all key members of the critical infrastructure organisations.

Government must ensure that security protocols and practices at key institutions in the critical infrastructure domain are linked together across sectors and at the country level.

FOR ORGANISATION IN THE CRITICAL INFRASTRUCTURE DOMAIN

Key providers of essential goods and services must come together to create a Dubai-wide back-up contingency plans that ensure minimal interruption of service and maximum assurance for access to key goods and services.

Organisations must make each other aware that a cyber-attack is taking place or that a vulnerability has been identified.

Organisations must increase awareness among employees of how cyber-attacks can happen and their impact.

Organisations must develop and adopt a cyber-security governing framework at the level of the Dubai-Emirate, one that would define the laws, policies, steps and guidance for organisations on how to manage data, protect it, and respond to risks and sabotage.

Senior management at the various organisations that make up the critical infrastructure ecosystem must develop and adopt full-blown strategies for cyber security.

Organisations must build partnerships with the key stakeholders around security coordination and risk management, not least to make future reoccurrences less likely and less costly.

AT THE TECHNICAL LEVEL

Technical systems must be designed to allow for a rapid response and recovery.

Technical design should allow for a broad security coordination between interlinked organisations.

Organisations must invest in advanced prediction solutions capable of predicting and forecasting threats through data analytics, social media tracking and surveillance.

Organisations must invest in the skills required to run and upgrade technical systems to achieve high-level of readiness against imminent cyber-attacks.

Organisations must map security risks and exposure via their transnational supply chains.

AUTHORS

Dr. Sami Mahroum
Dubai Future Foundation

Fatma Rashid Alaleeli
Dubai Police

Amna Ali Al Boom
Dubai Police

Sheikha Mira Ahmed Al Mualla
Dubai Police

Jasim Mohamed Al Shimmari
Dubai Police

OTHER CONTRIBUTORS

Brigadier Dr. Abdullah Abdulrahman Bin Sultan
Dubai Police

Captain Muhammad Ahmed Almheiri
Dubai Police

Dr. Hossam Elshenkari
Dubai Police

Sumaya Abdulrahman Bin Sultan
Dubai Police

Dr. Patrick Noack
Dubai Future Foundation

LIST OF PARTICIPATING ORGANISATIONS IN THE FIRST WORKSHOP

Central Bank

CDA: Community Development Authority

Dubai Municipality

Dubai Economy: Department of economic development

Digital Society Institute (ESMT, Berlin)

Dubai Chambre

Dubai Gov Hum. Res. Dep. : Dubai Government Human Resources deprtment

DEWA: Dubai Electricity and Water Authority

DHA : Dubai health Authority

Dubai Police

Dubai Future Foundation

DIFC : Dubai International Financial Center

Executive Council

Emirates NBD : Emirates National Bank of Dubai

MOI: Ministry of interior

RTA: roads and transport authority

Smart Dubai

استشراف المستقبل
ودعـــم اتخـــاذ
القـــرار
مركز

Future Foresight
& Decision Making
Support
Center

FUTURE FORESIGHT DECISION MAKING SUPPORT CENTER

The Future Foresight and Decision-Making and Support Center at the Dubai Police conducts future studies aimed at identifying future risks and challenges. The Center applies future foresight tools, in cooperation with other departments and with external strategic partners, to provide visions, ideas, and creative initiatives towards the development and improvement of institutional performance and the future preparedness for events that may pose potential risks and threats to society and public order.

مؤســسة دبي للمســــــــتقبل
DUBAI FUTURE FOUNDATION

ABOUT DUBAI FUTURE FOUNDATION

Launched by His Highness Sheikh Mohammed bin Rashid Al Maktoum, Vice President and Prime Minister of the UAE and Ruler of Dubai, the Dubai Future Foundation was established back in 2016 to play a pivotal role in shaping the future of Dubai, as well as to collectively imagine, inspire and design the city's future in collaboration with the government and private entities within various industries.

Mandated in positioning Dubai as a hub for innovation and a leading city of the future, the foundation's main areas of focus are Future Foresight and Imagination, Content and Knowledge Dissemination, Capacity Building, Future Design and Acceleration, and Future Experiences.

As such, DFF builds bridges between government and private sector, innovators, startups, talents and industry experts, and creates an innovation ecosystem that enables innovations to take shape, promotes global dialogues, builds partnerships and cultivates disruptive mindsets.

dubaifuture.ae research@dubaifuture.gov.ae @dubaifuture

مؤسسة دبي للمستقبل
DUBAI FUTURE FOUNDATION

DUBAIFUTURE.AE