The development of new technologies brings great opportunities – but also the potential for security breaches and potentially devastating cyberattacks. In the lead up to the 15th G20 summit in Riyadh, GCC countries are evaluating their own readiness to cope with future cyber intrusions. Improving cybersecurity in the region will require the public and private sectors alike to acknowledge the danger of these threats – and to allocate adequate funds to fight them.

Gulf Monitor | Yossi Mekelberg | Cybersecurity

One of the key agenda items for the next G20 summit in Riyadh, scheduled for the end of 2020, will be to discuss the opportunities and challenges of new technologies. The aim is to "adopt long-term and bold strategies to utilise and share benefits of innovation."[1]However, the age of naiveté that sees information technology as a silver bullet bringing about cost-free economic development and prosperity is well and truly over.

Instead, significant resources are now being invested in cybersecurity and "cyber resilience" to protect individuals, and private and public institutions – in other words the state and the nation as a whole – from cyber intrusions to full-blown cyberattacks. So, it is no surprise that the next G20 meeting, while exploring the transformative uses of technological innovation for the benefit of humanity, will be particularly focused on ensuring protection from cyber criminals.

Progress vs. vulnerability: A troubling trade-off

There is an inherent correlation between the ambition to become a leader in the digital world and the apparent vulnerability to a wide range of cyber threats. For GCC states pursuing economic diversification, technology plays a central role: For instance, one of the objectives of Saudi Vision 2030 is to transform 10 cities across the kingdom into smart cities starting with, Makkah, Riyadh, Jeddah, Al Madinah, and Al Ahsa.

In the neighbouring UAE, an objective was set of 50% of government transactions to use blockchain platforms within the next three years, hoping to make savings in the region of $3bn.[2]And, the entire

GCC region has embarked on polices to unlock the possibilities offered by Big Data.[3]

It is reasonable to expect that cyberattacks, whether for political or economic objectives, will increase in frequency as the economies of the GCC states become increasingly digitalised. Experts warn that mounting an cyberattack is incredibly easy even for novice hackers due to users' lax approaches to cybersecurity. And while some attacks may be relatively benign and merely irritating, others are capable of devastating crucial services and utilities to the point of complete paralysis.

A malicious software attack in 2012 on the disaster prevention computer systems at an industrial facility of the Saudi oil company Aramco served as a wake-up call.[4]The malware corrupted tens of thousands of hard drives, shut down employee email, destroyed data and damaged almost three-quarters of the company's IT infrastructure – a level of destruction that alarmed the country's leaders enough for them to order the development of a coordinated cyber resilience framework.[5]

In the summer of 2019 Bahrain reported several cyber breaches: in July hackers shut down several systems of the Electricity and Water Authority. And in August cyber intrusions occurred in systems of the National Security Agency, the Ministry of Interior and the First Deputy Prime Minister's office. Not surprisingly, Iran was mentioned as the likely culprit in both cases, leading experts to wonder whether this was a signal to the rest of the GCC countries that they too are vulnerable to such attacks.

Ensuring safety in cyberspace

The effectiveness of the steps taken by the GCC countries to develop the resilience of state institutions and business sectors is reflected in their ranking in the Global Cybersecurity Index (GCI). The index assesses the preparedness of countries to combat cyberattacks under five pillars: legislation, technical and organisational capabilities, capacity building and cooperation with other stakeholders. GCC countries come top in the Middle East and rank highly globally for their commitment to cybersecurity.[6]

In Saudi Arabia, the Council of Economic and Development Affairs has been tasked with setting up the necessary mechanisms and measures to implement a cyber-resilience system and to monitor its progress through coordinated efforts among all relevant stakeholders.

In a signal of the issue's increasing importance, the National Cyber Security Centre was removed from the purview of the Ministry of Interior and now reports directly to the King’s Office, and at the beginning of 2020 Saudi Arabia hosted the Global Cybersecurity Forum – the first event of its kind – which attracted more than 1,200 participants and 140 speakers.

Dubai, Bahrain and Qatar have similarly developed their own cyber-resilience strategies. These plans require organisations in the public and private sectors to enable IT system continuity, disaster recovery and wider business continuity.[7]

Measures taken range from benchmarking, comparing cybersecurity in the Gulf with other leading countries, and adapting it to specific conditions in each of the GCC’s countries. The complexity of the legal, organisational and capacity-building required to deal with the main cyberthreats of fraud, espionage, terrorism, violation of privacy and defamation have led to prolonged consultations, but also the results set by the decision makers.

Guarding against an evolving threat

With most of the world’s interactions, including business and commerce, government activities, communications, education and entertainment, being conducted online amid the outbreak of the coronavirus pandemic, the steps taken by the GCC countries will reassure users and investors.

However, governments and authorities must continue to work to ensure strategies and measures are sustainable and can adapt to meet the rapidly evolving nature of cyber threats.

The GCC’s cyber strategies face three main challenges: first, ensuring that cybersecurity regulations across the region are uniform in scope and implementation; second, combatting complacency and ensuring that cybersecurity guidelines are followed with no exceptions; and last, allocating adequate resources to anticipate threats.[8]

As it stands, there is a tendency to invest more in developing new technologies than in defending them. In the coming years, a major challenge will be to match resources – both tangible and perceptual – to current and future threats. This will not happen unless there is increased awareness of the daily threat of cyberattacks; adequate legislation to adapt and respond to the fast-changing nature of technological developments; and the formation of national regulatory bodies that can coordinate domestic and international action against emerging cyberthreats.

Yossi Mekelberg is a professor of international relations and the faculty lead on outreach projects at Regent's University, London, and a senior consulting research fellow with Chatham House's MENA programme. His interests include politics of the Middle East, Israeli politics, the Middle East peace process, international relations theory and US foreign policy towards the region. Yossi is a consultant at Castlereagh Associates.

Sources:

[1] G20 Saudi Arabia 2020, Agenda, https://g20.org/en/g20/Pages/agenda.aspx

[2] Yigal Chazan, "UAE continues to drive the Arab world's tech ambitions", Arabian News, https://www.arabianbusiness.com/startup/404777-uae-continues-to-drive-the-arab-worlds-tech-ambitions

[3] "Big Data in the GCC", https://www2.deloitte.com/jo/en/pages/about-deloitte/articles/revolution/big-data-gcc.html

[4] Ellias Groll, *Cyberattack Targets Safety System at Saudi Aramco*, Foreign Policy, https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/

[5] Kate Fazzini, "The Saudi oil attacks could be a precursor to widespread cyberwarfare — with collateral damage for companies in the region," CNBC, 22 September, 2019, https://www.cnbc.com/2019/09/21/saudi-aramco-attacks-could-predict-cyber-warfare-from-iran.html

[6] Global Cybersecurity Index 2018 and 2019, ITU https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx; and https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[7] Dubai Cyber Security Strategy, https://desc.dubai.ae/res/wp-content/uploads/DCSS-EN.pdf; Bahrain Cyber Security Strategy, https://perma.cc/RSL4-FPJA

[8] James Shires and Joyce Hakmeh, "Is the GCC Cyber Resilient?", Chatham House Briefing Paper, March 2020, file:///C:/Users/ymeke/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/CHHJ8019-GCC-Cyber-Briefing-200302-WEB%20(3).pdf