T20
SAUDI ARABIA 2020
THINK

POLICY BRIEF

HEIGHTENING CYBERSECURITY TO PROMOTE SAFETY AND FAIRNESS FOR CITIZENS IN THE POST-COVID-19 DIGITAL WORLD

Task Force 11

COVID-19: MULTIDISCIPLINARY APPROACHES TO COMPLEX PROBLEMS

Authors
MUHAMMAD KHURRAM KHAN, STEFANIE GOLDBERG, PAUL GRAINGER, BHUSHAN SETHI

موجز السياسة

زيادة الأمن السيبراني لتعزيز السلامة والإنصاف للمواطنين في العالم الرقمي بعد انتهاء جائحة فيروس كورونا المستجد (كوفيد-١٩)

فريق العمل الحادي عشر

جائحة فيروس كورونا المستجد (كوفيد-١٩): نُهج متعددة التخصصات لمعالجة المشكلات المعقدة

المؤلفون

محمد خرام خان، ستيفاني غولدبرغ، بول غرينجر، بوشان سيثي

ABSTRACT

COVID-19 has disrupted life. With every G20 nation having experienced stay-at-home orders, citizens are relying heavily on digital technology to live, work, learn, access information, and connect with each other. Previous patterns of proximity are unlikely to return, and virtual communications will increasingly become a permanent fixture of life. But as reliance on technology intensifies, so does the opportunity for threat actors to carry out cybercrimes or distribute disinformation to the detriment of personal or civic life. This is distinct from cyber warfare or data harvesting. The G20 should generate international protocols to help protect citizens from such malicious activities.

لقد أدَّت جائحة فيروس كورونا (كوفيد-١٩) إلى تعطل مظاهر الحياة الطبيعية. فمادامت كل دولة من دول مجموعة العشرين قد خضعت لطلبات البقاء في المنزل، فإنّ المواطنين يعتمدون بشكل كبير على التقنيات الرقمية من أجل العيش والعمل والتعلم والوصول إلى المعلومات والتواصل مع بعضهم بعضًا. ومن غير المرجح أن تعود أنماط الحياة السابقة في ما يتعلق بالتقارب، وستصبح الاتصالات الافتراضية عنصرًا ثابتًا في الحياة بشكل متزايد. ولكن مع ازدياد الاعتماد على التقنية، تزداد الفرصة لدى الجهات المُهَدِّدَة بارتكاب جرائم السيبرانية، أو توزيع معلومات مضللة على حساب الحياة الشخصية أو المدنية. ويختلف هذا عن عمليات الحرب السيبرانية أو جمع البيانات. لذا، يجب على مجموعة العشرين وضع بروتوكولات دولية للمساعدة في حماية المواطنين من هذه الأنشطة الخبيثة.

CHALLENGE

One of the biggest unexpected consequences of the COVID-19 pandemic—and the large number of business and school closures associated with efforts to curb the virus—has been the rapid increase in technological transformation (Iansiti and Richards 2020).

When G20 nations declared stay-at-home orders, businesses, healthcare providers, and educational institutions rapidly deployed virtual operating models and individuals went online to connect and partake in daily activities. A greater portion of the global population is now reliant on the internet for information and to complete personal and financial transactions (CPG, FMCC & Retail 2020). But this increased reliance on technology also comes with heightening cybersecurity threats (Pipikaite and Davis 2020). Trends show an uptick in cyber attacks being carried out amidst the pandemic across two categories:

1. The spread of fake news or mis/dis information intended to undermine governments or consumer trust. Many accounts of fake news emerged for example, in Italy, including one claim that a vaccine was available for purchase for 50 Euros (Reality Check Team and BBC Monitoring 2020). In the UK, conspiracy theories circulating on the internet claimed that the onset of 5G networks propagated the coronavirus, which led to vandalism of cell towers (Satariano and Alba 2020).

2. Criminal cyber activity such as phishing, malware distribution, and ransomware attacks often carried out by money launderers, cyber terrorists or other organized crime groups aimed at exploitation (e.g., financial, sexual). Phishing is one of the most common and most productive hacking tricks of cyber criminals. Reports have shown that 32% of corporate data breaches and 78% of cyber-espionage operations are caused by phishing emails (Verizon 2020). During the pandemic, cyber criminals have taken advantage of the public's fear surrounding the virus by targeting phishing attacks via fraudulent World Health Organization (WHO) emails to retrieve sensitive information (WHO n.d.). One leading global technology platform observed around 18 million daily malware and phishing emails related to COVID-19 in April 2020. This was in addition to more than 240 million COVID-themed daily spam messages (Kumaran and Lugani 2020). The sharp rise of video conferencing apps has also enticed hackers to launch online scams. A recent study found that over 6,576 fake and impersonating phishing domains have been registered for a popular video conferencing app since January 2020 (Tidy 2020).

Unfortunately, these attacks target not just individual users. Large-scale organizations, financial institutions, universities, and hospitals are also becoming victims of sophisticated and coordinated cyber attacks. According to PwC's Digital Trust Insights

Pulse Survey, 61% of Chief Information Security Officers (CISOs) surveyed have seen an increase in the incidence of phishing attacks related to COVID-19. Furthermore, 50% have seen an increase in compromised business emails (PwC 2020).

These are attempts to mislead citizens or rob them of their assets. This activity is different from state sponsored cyber-warfare and data harvesting (an area where emerging COVID-19 contact tracing apps are especially susceptible). These are also potential abuses of technology and should be the subject of separate studies.

Factors contributing to the increase in cyber attack incidents during the pandemic include displacement, opportunism, proliferation, susceptibility, and hostility, as shown in Figure 1 (Auld and Smart n.d.; Dickie 2020).

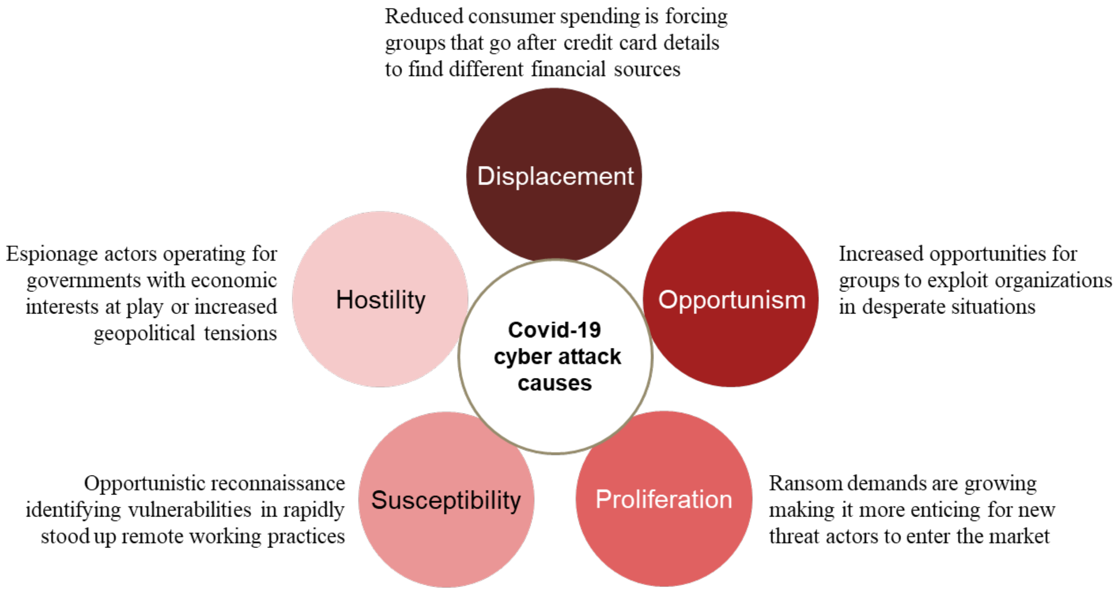

Reduced consumer spending is forcing groups that go after credit card details to find different financial sources
Displacement
Espionage actors operating for governments with economic interests at play or increased geopolitical tensions
Hostility
Covid-19 cyber attack causes
Opportunism
Increased opportunities for groups to exploit organizations in desperate situations
Opportunistic reconnaissance identifying vulnerabilities in rapidly stood up remote working practices
Susceptibility
Proliferation
Ransom demands are growing making it more enticing for new threat actors to enter the market

Figure 1: **What caused the increase in cyber incidents during COVID-19?**
Source: **PwC UK, 2020**

Social distancing measures will likely remain the norm for the foreseeable future. It is probable that physical interactions will continue to be discouraged and the use of digital platforms will expand. The number of transactions through artificial intelligence (AI) is expected to proliferate, putting consumers further at risk. Falling victim to a cyber scam has very real physical, financial, and emotional consequences that can be particularly devastating for digitally vulnerable populations (i.e., the digitally unaware who lack resources, infrastructure, or skills to improve their digital and/or cyber literacy, making them a potential target for manipulation). The G20 has a collective responsibility to mitigate these risks and protect citizens from these potentially devastating dangers.

PROPOSAL

More broadly, the short-term non-health consequences of the pandemic have come about because of the dislocations to the economy. Disrupted supply chains, a recalibration of values, collapse of some business sectors, and the insolvency of businesses have led to unemployment, underemployment, and the redundancy of certain skills. This reinforces poverty, thereby reducing demand, and creating a recessional cycle. Poverty weakens the individual's ability to establish protective digital systems. The G20 can play an active role in helping establish protections that are economical and cost effective for consumers and citizens. To protect people, networks, and supply chains worldwide, international protocols and basic education on cybersecurity are needed. Furthermore, they should be updated regularly as new forms of technology and new threats emerge (e.g., contact tracing apps for COVID-19).

Longer term, there is likely to be a shift in consumer attitudes and behaviors. Enhanced collective social consciousness will increase calls for more transparency and action from multilateral corporations and protections from governments. These apply across a range of social issues, such as safety measures, health outcomes, unemployment, education, and racial discrimination. These attitude changes will impact and influence how consumers engage in the online world. Therefore, the G20 should reflect these post-pandemic attitude changes in the development of cybersecurity protocols, educational materials, and measurements. Furthermore, the G20 can benefit from including cybersecurity protections in the broader suite of protections that are likely to be enforced for vulnerable populations that have been disproportionately impacted by COVID-19 (e.g., around education, employability, health etc.).

More specifically, the G20 should focus on four interrelated policy recommendations aimed at protecting citizens from cybersecurity threats. First, establish a multilateral framework for cybersecurity regulations and protocols. Second, agree on a clear definition of cyber literacy and educate citizens on the topic. Third, develop a cyber index to measure collective progress. Finally, broaden the community and skills capacity of cybersecurity professionals.

1. A G20 multilateral framework for cybersecurity, regulations and protocols.

While consumer education is important, relying on human behavior alone is not sufficient (Jang-Jaccard and Nepal 2014). As more consumer data gets stored, and as citizens increasingly conduct their daily life in the online world (Donahoe et al. 2017), G20 protocols should be established so that a set of international regulations can be applied when malicious practices occur. These should encourage prevention as well as reactive security. The G20 should sponsor a Task Force of experts in cybersecurity from both the public and private sectors, appointed with the approval of member nations. This Task Force should develop a framework for basic cybersecurity and establish a set of international regulations or protocols to be incorporated into national regulatory systems. These regulations should require that technology providers and the businesses who leverage them are implementing the right systemic controls to prevent attacks and, in the event that a breach does occur, they take appropriate remedial action. The implementation and enforcement of such regulations will help to safeguard investments in cybersecurity within organizations even as they face weakening balance sheets due to the pandemic (Morgan, Huang and Trinh 2019).

Specific actions the G20 should take include:

- Review the responses to cyber attacks that have occurred in recent years, and the literature stemming from these (Harmon and Ivashina 2020);

- Conduct a scan of existing cybersecurity regulations (both international and jurisdictional) to identify where regulations fall short in requiring technology providers and other public and private sector businesses to protect digitally vulnerable populations;

- Agree on and authenticate a common set of global regulations and/or stronger local regulations that are relevant to cybersecurity; and

- Liaise with appropriate national and regional regulatory bodies and work with them to influence international corporations operating across the G20 to further adhere to these regulations. These should include both the technology providers and the businesses and institutions using systems and platforms to engage with customers/end-users, such as banks, healthcare providers and universities.

Areas requiring urgent attention are:

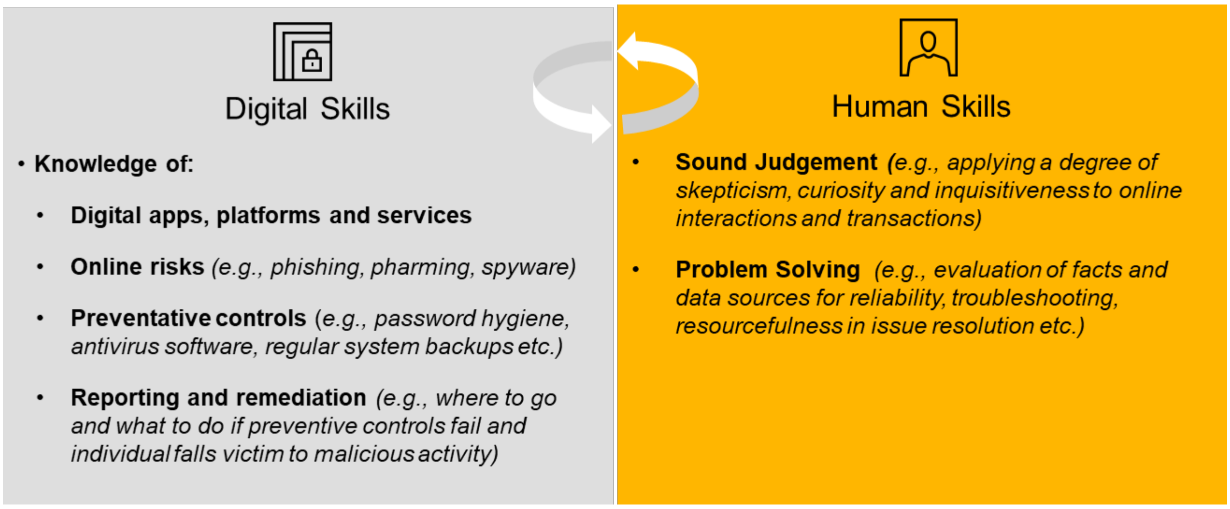
- The security of online data,
- Privacy of the individual in cyberspace,
- Guidelines and protocols on safety issues, and
- Encouraging the development of low-cost security.

The establishment of the Task Force will reinforce existing international efforts to reassure citizens that their online transactions are reasonably secure (Twomey 2018).

2. A G20 cyber literacy definition and sponsorship for the development of educational materials.

Basic awareness and education regarding cyber risks are required to help protect citizens from experiencing the potential hardships that could result from a cyber scam or attack. The G20 countries should agree on a common definition of cyber literacy and develop educational materials that cultivate basic cyber literacy, particularly among digitally vulnerable populations. These efforts should build upon existing recommendations that call upon the G20 to play a role in developing a standardized digital financial literacy definition and programs that promote digital financial education (Morgan, Huang and Trinh 2019; Shull, Twomey and Yoo 2017; Twomey and Martin 2020). Furthermore, they should align with the UN Secretary General's Roadmap for Digital Cooperation, which was recently announced as a result of the pandemic accelerating digitization (United Nations 2020).

The G20 could look to incorporate two dimensions into the standardized definition of cyber literacy: digital skills and human skills as shown in Figure 2.



Digital Skills

- **Knowledge of:**
  - **Digital apps, platforms and services**
  - **Online risks** *(e.g., phishing, pharming, spyware)*
  - **Preventative controls** *(e.g., password hygiene, antivirus software, regular system backups etc.)*
  - **Reporting and remediation** *(e.g., where to go and what to do if preventive controls fail and individual falls victim to malicious activity)*

Human Skills

- **Sound Judgement** *(e.g., applying a degree of skepticism, curiosity and inquisitiveness to online interactions and transactions)*
- **Problem Solving** *(e.g., evaluation of facts and data sources for reliability, troubleshooting, resourcefulness in issue resolution etc.)*

Figure 2: The Digital and Human Dimensions of Cyber Literacy

Source: **PwC analysis**

Once there is a common definition of cyber literacy, educators could be invited to submit educational packages that seek to build cyber literacy among digitally vulnerable citizens by:

- Building awareness of cyber risks and appropriate preventative controls,
- More broadly improving digital acumen, and
- Linking these skills with the development of applicable human skills.

Education materials should be peer reviewed in a process overseen by a T20 Task Force. The Task Force should be asked to:

- Formulate a G20 statement that establishes an agreed minimum standard of basic cyber literacy and security awareness for everyday transactions.
- Define various digitally vulnerable populations and determine the different types of cybersecurity risks that each population is most susceptible to as they increasingly engage in the digital world. Examples of digitally vulnerable populations include:
  - Digitally unaware populations shopping and managing their finances online for the first time;
  - Children engaging in virtual technology, unsupervised, for prolonged periods of time for distance learning or entertainment;

  - Patients sharing confidential health information during a telehealth visit;
  - Disadvantaged communities disproportionately subjected to disinformation with the potential to lead to civic disruption;
  - Small business owners attempting to crowdfund donations through digital finance platforms; and
  - Middle- and low-income households sharing a single or few device(s) amongst several household members.

- Ensure that the educational packages are easily digestible, updated as necessary when new technology and/or threats emerge and tailored to the risks associated with specific digitally vulnerable populations. Initially these cyber literacy educational packages should cover:

  - Dangers to be aware of and signs to look out for when engaging with technology and digital tools in private and working life;
  - Risks and potential hardships that can follow security breaches, such as stolen identity, hacked bank accounts, lost savings;
  - Steps to take in the event of suspected hacking or being taken advantage of by cyber criminals;
  - How to fact check and report on suspicious or “fake news”; and,
  - Information on preventive cybersecurity controls designed to suppress the likelihood and potential impact of cyber threats, including policies, tools, standards, processes, and procedures. To keep data safe and secure from cyber perpetrators, online users should adopt cyber hygiene practices and preventive controls. The basic and suggested preventive measures include the use of strong passwords, firewalls, antivirus software, and multi-factor authentication.

Once produced, the G20 should encourage open sharing of these educational materials across member nations using channels that are easily accessible for digitally vulnerable populations and simple to navigate. The G20 could also encourage the private sector, including technology platform providers, to assist in the effort of raising consumers’ cyber literacy levels by embedding educational information into systems and applications. While this may require increased spending in the short-term to develop educational materials, savings will likely result in the longer-term.

3. A G20 index to measure collective progress toward achieving a safer cyber world.

The G20 should establish a working group with stakeholders from cybersecurity organizations, civil society, law, policy, and academia to develop an index to measure the efforts aimed at protecting consumers and their data and assets from cyberattacks. This working group can develop a baseline and track designated periods of time. This working group may collaborate with the International Telecommunication Union (ITU), which manages Global Cybersecurity Index (GCI), to measure the cybersecurity commitment of countries at the global level. It could also harness their experience and influence on the cybersecurity industry (ITU 2019). The index could include both leading and lagging indicators such as (but not limited to):

- Number of individual incidents reported to authorities,
- Number and magnitude of data breaches and consequential impacts,
- Number of successful versus prevented phishing expeditions and number of individuals impacted by the former,
- Percentage of population considered to be digitally vulnerable,
- Percentage of population with a basic degree of cyber literacy, and
- Quality of educational materials linked to short and long-term educational outcomes.

The G20 cyber experts working group should also coordinate with relevant regulatory bodies to encourage public and private sector companies to disclose the relevant information needed to establish the baseline measures and complete these disclosures at regular intervals. Companies should share practices amongst one another.

4. A G20 task force to build a broader community of cybersecurity professionals.

There is an increasing demand for workers in dedicated cybersecurity roles and the need for cyber skills and knowledge more broadly within the business community, in both public and private sectors. In its 2019 annual report, Cybersecurity Ventures predicted that there will be 3.5 million unfilled cybersecurity jobs across the globe by 2021, a 2.5 million increase in unfilled positions from 2014 (2019) and this demand is accelerating because of COVID-19. According to Gartner research, there has been a 65% increase in demand for cybersecurity jobs in the U.S. between February and April

2020 (Gartner n.d.). Similarly, India saw 30% growth in cybersecurity job searches over almost the same period (Press Trust of India 2020).

The G20 can benefit from mobilizing a Task Force (across the T20, B20, and W20) aimed at increasing the number of cybersecurity professionals and broadening the demographic profile of those entering into cybersecurity employment. It should encourage cultural diversity and the employment of women. Currently, female employees represent only 24% of the cybersecurity workforce at the global level (Iqbal and Khan 2019). Bringing together policy makers with technologists, businesses, and women across the G20, this Task Force could:

- Convene a panel of experts in cybersecurity from both the public and private sectors to develop a skills and competency framework for cybersecurity career paths;
- Work with universities to restructure education curricula and skills development funding to provide further emphasis on building cybersecurity skills and cyber literacy (including digital acumen) more broadly;
- Encourage the G20 to promote awareness of available cybersecurity educational and career path opportunities at the national and subnational level;
- Develop a blueprint for incentivizing and encouraging individual citizens to invest in their own education and/or skills building in the cybersecurity field;
- Identify potential mechanisms to attract more women and minorities into the cybersecurity profession;
- Encourage businesses to invest in the reskilling of employees, with a focus on developing digital and cyber skills as well as elevating employees' cyber literacy more broadly (e.g., 68% of CISOs surveyed in PwC's Digital Trust Insight Pulse Survey have increased training and awareness of cybersecurity in their organizations due to COVID-19 (PwC 2020)); and
- Create an international community, which enables businesses and nations to share leading human capital practices in cybersecurity and report on progress over time.

The expansion of the cybersecurity community and promotion of women and minorities into cyber employment will help close the skills gap, improve the diversity of thinking in the field, and generate positive socioeconomic impacts at the local and global levels. Consequently, it will create a safer world online for citizens at large.

Disclaimer
This policy brief was developed and written by the authors and has undergone a peer review process. The views and opinions expressed in this policy brief are those of the authors and do not necessarily reflect the official policy or position of the authors' organizations or the T20 Secretariat.

REFERENCES

Auld, Andy and Jason Smart. n.d. “Why Has There Been an Increase in Cyber Security Incidents During COVID-19?” PwC UK article. Last accessed July 30, 2020. Available at https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html.

CPG, FMCC & Retail. 2020. “COVID-19: The Unexpected Catalyst for Tech Adoption.” The Nielsen Company article. Last modified March 16, 2020. https://www.nielsen.com/us/en/insights/article/2020/covid-19-the-unexpected-catalyst-for-tech-adoption.

Cybersecurity Ventures. 2019. “The 2019 Official Annual Cybersecurity Jobs Report.” Herjavec Group website, October 30, 2019. Available at https://www.herjavecgroup.com/2019-cybersecurity-jobs-report.

Dickie, John. 2020. “The Coronavirus Will Not Change Business for mafia Organisations.” BBC World Service Radio’s ‘Newshour,’ May 26, 2020. https://www.ucl.ac.uk/news/headlines/2020/may/coronavirus-will-not-change-business-mafia-organisations.

Donahoe, Eileen, Melissa Hathaway, James Andrew Lewis, Joseph S. Nye Jr, and Paul Twomey. 2017. “Getting Beyond Norms: New Approaches to International Cyber Security Challenges.” Centre for International Governance Innovation. Special Report. Last updated September 7, 2017. https://www.cigionline.org/publications/getting-beyond-norms-new-approaches-international-cyber-security-challenges.

Gartner. n.d. “Cybersecurity Labor Shortage and COVID-19.” Gartner Research website. Last accessed July 30, 2020. https://www.gartner.com/en/human-resources/research/talentneuron/cybersecurity-labor-shortage-and-covid-19.

Harmon, Mike and Victoria Ivashina. 2020. “Managing the Liquidity Crisis.” Harvard Business Review article. Last updated April 9, 2020. Available at: https://hbr.org/2020/04/managing-the-liquidity-crisis.

Iansiti, Marco, and Greg Richards. 2020. “Coronavirus Is Widening the Corporate Digital Divide.” Harvard Business Review. Last updated March 26, 2020. https://hbr.org/2020/03/coronavirus-is-widening-the-corporate-digital-divide.

International Telecommunication Union (ITU). 2019. Global Cybersecurity Index (GCI) 2018. Geneva: ITU Publications. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Iqbal, Zaheema and Muhammad Khurram Khan. 2019. “Saudi Women in Cybersecurity: Narrowing the Gap of Human Capital Crisis.” Global Foundation for Cyber Studies and Research. White Paper. Last updated January 24, 2019. https://www.gfcyber.org/saudi-women-in-cybersecurity-narrowing-the-gap-of-human-capital-crisis.

Jang-Jaccard, Julian and Surya Nepal. 2014. “Survey of Emerging Threats in Cybersecurity.” Journal of Computer and System Sciences 80, no. 5: 973-93. https://doi.org/10.1016/j.jcss.2014.02.005.

Kumaran, Neil and Sam Lugani. 2020. “Protecting Businesses Against Cyber Threats During COVID-19 and Beyond.” Google Cloud. Last updated April 16, 2020. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond.

Morgan, Peter J., Bihong Huang and Long Q. Trinh. 2019. “The Need to Promote Digital Financial Literacy for the Digital Age.” T20 Japan Policy Brief. https://t20japan.org/policy-brief-need-promote-digital-financial-literacy.

Pipikaite, Algirde and Nicolas Davis. 2020. “Why Cybersecurity Matters More Than Ever During the Coronavirus Pandemic.” World Economic Forum. Last updated March 17, 2020. https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity.

Press Trust of India. 2020. “Covid-19 Disruption Side Effect: Rise in Cybersecurity Jobs in India.” Business Standard article. Last updated June 15, 2020. https://www.business-standard.com/article/companies/covid-19-lockdown-side-effect-rise-in-cybersecurity-jobs-in-india-120061501450_1.html.

PwC US. 2020. “Digital Trust Insights Pulse Survey.” Survey results. Accessed July 30, 2020. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/pwc-covid-19-ciso-pulse-survey.html.

Reality Check Team and BBC Monitoring. 2020. “Coronavirus: Italy Sees Rapid Spread of Fake News.” BBC News article, March 12, 2020. https://www.bbc.com/news/world-europe-51819624.

Satariano, Adam and Davey Alba. 2020. “Burning Cell Towers, Out of Baseless Fear They Spread the Virus.” New York Times article. Last modified April 10, 2020. https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html.

Shull, Aaron, Paul Twomey, and Christopher S. Yoo. 2017. “Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-Stakeholder Community.” Faculty Scholarship at Penn Law. Accessed July 30, 2020. https://scholarship.law.upenn.edu/faculty_scholarship/2014.

Tidy, Joe. 2020. “Google Blocking 18m Coronavirus Scam Emails Every Day.” BBC News article. Last updated April 17, 2020. https://www.bbc.com/news/technology-52319093.

Twomey, Paul. 2018. “Toward a G20 Framework for Artificial Intelligence in the Workplace.” Centre for International Governance Innovation, CIGI Papers No. 178, July 2018. https://www.cigionline.org/sites/default/files/documents/Paper%20No.178.pdf.

Twomey, Paul and Kristen Martin. 2020. “A Step to Implementing the G20 Principles on Artificial Intelligence: Ensuring Data Aggregators and AI Firms Operate in the Interests of Data Subjects.” G20 Insights. Last updated June 11, 2020. https://www.g20-insights.org/policy_briefs/g20-principles-artificial-intelligence-data-aggregators-ai-firms.

United Nations. 2020. “Roadmap for Digital Cooperation.” United Nations. Report of the Secretary-General, June 2020. https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

Verizon. 2020. “Data Breach Investigations Report (DBIR).” Reporting link. Accessed July 30, 2020. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

World Health Organization (WHO). n.d. “Beware of criminals pretending to be the WHO.” Webpage. Accessed July 30, 2020. Available at https://www.who.int/about/communications/cyber-security.

APPENDIX

Global Foundation for Cyber Studies and Research (GFCyber) is an independent, nonprofit and non-partisan think tank. It conducts research studies, contributes policy publications, and provides advisory and intellectually indulges on various aspects of classical, contemporary, and modern cybersecurity topics. The foundation aspires to bring together experts from diverse backgrounds with key interests and expertise from the intersection of cyber policy and technology. Please visit their website for more details: http://www.gfcyber.org.

PwC's purpose is to build trust in society and solve important problems. PwC is a network of firms in 157 countries with 276,000 people who are committed to delivering quality in assurance, advisory, and tax services. PwC refers to the PwC network and/or one of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

AUTHORS

Muhammad Khurram Khan
Global Foundation for Cyber Studies and Research

Stefanie Goldberg
PwC US

Paul Grainger
UCL

Bhushan Sethi
PwC US

t20saudiarabia.org.sa