2022

EDITION

GLOBAL CYBERSECURITY FORUM

RETHINKING THE GLOBAL CYBER ORDER



Global Cybersecurity Forum

ORGANIZED BY

الهيئة الوطنية للأمن السيبراني

National Cybersecurity Authority

2022
EDITION
GCF



UNDER THE PATRONAGE OF
THE CUSTODIAN OF THE TWO HOLY MOSQUES,
KING SALMAN BIN ABDULAZIZ AL SAUD



HIS ROYAL HIGHNESS

MOHAMMED BIN SALMAN BIN ABDULAZIZ AL SAUD

CROWN PRINCE AND PRIME MINISTER

CONTENT

ABOUT GCF 008

2022 EDITION 012

PROCEEDINGS 022

KEY TAKEAWAYS 108

GLOBAL COLLABORATION 122

KNOWLEDGE HUB 150



ABOUT GCF

Global Cybersecurity Forum

ABOUT THE **GLOBAL CYBERSECURITY FORUM**

During the Kingdom of Saudi Arabia's G20 Presidency, the Global Cybersecurity Forum (GCF) was launched in February 2020 as an action-oriented platform aiming to contribute to a more resilient and safer Cyberspace for all.

Recognizing the importance of raising cybersecurity resilience at a global level, and the imperative for international collaboration among diverse stakeholders and countries to accomplish this goal, the GCF was established to create a space for global cybersecurity stakeholders to collaborate and act to the benefit of all. The GCF's aim is to expand global cybersecurity dialogue, tackling the most challenging and critical topics and moving beyond discussions of a technical nature to the strategic socioeconomic and geo-political issues that cybersecurity is a part. ■














2022 EDITION

2022 EDITION
RETHINKING THE GLOBAL CYBER ORDER

In 2022, returning to an in-person event once again, the GCF set out to raise its ambitions. The 2022 edition welcomed over 9000 participants from 117 countries. 127 of the world's best cyber minds contributed to diverse perspectives across 41 content-rich sessions. Under the theme, Rethinking the Global Cyber Order, the Forum catalyzed socioeconomic impact, spearheaded multilateral collaboration, and advanced progress on key issues. ■


Global
Cybersecurity
Forum

Sub-themes for 'Rethinking the Global Cyber Order'

The GCF 2022 program was designed to substantively advance global cooperation. A broad range of compelling topics were mapped across five sub-themes to ensure a cohesive and probing program under its guiding theme, 'Rethinking the Global Cyber Order'.



Geo-cyber Evolution

The first sub-theme, geo-cyber evolution, focused on understanding the evolving international cyberspace order. Sessions explored issues such as geo-technological competition and conflict and opportunities for a stable and peaceful cyberspace. ■



Disruption Frontier

Under the second sub-theme, disruption frontier, sessions mapped current and future cybersecurity threats, exploring future technologies as potential solutions. ■



Cyber Economics

The third sub-theme, cyber economics, looked at the economics-based dynamics that influence behavior in Cyberspace, with a focus on the collaborative, proactive actions, market forces, incentives, and economic governance can shape Cyberspace. Sessions also looked at means for reducing the economic incentive for cybercrime. ■



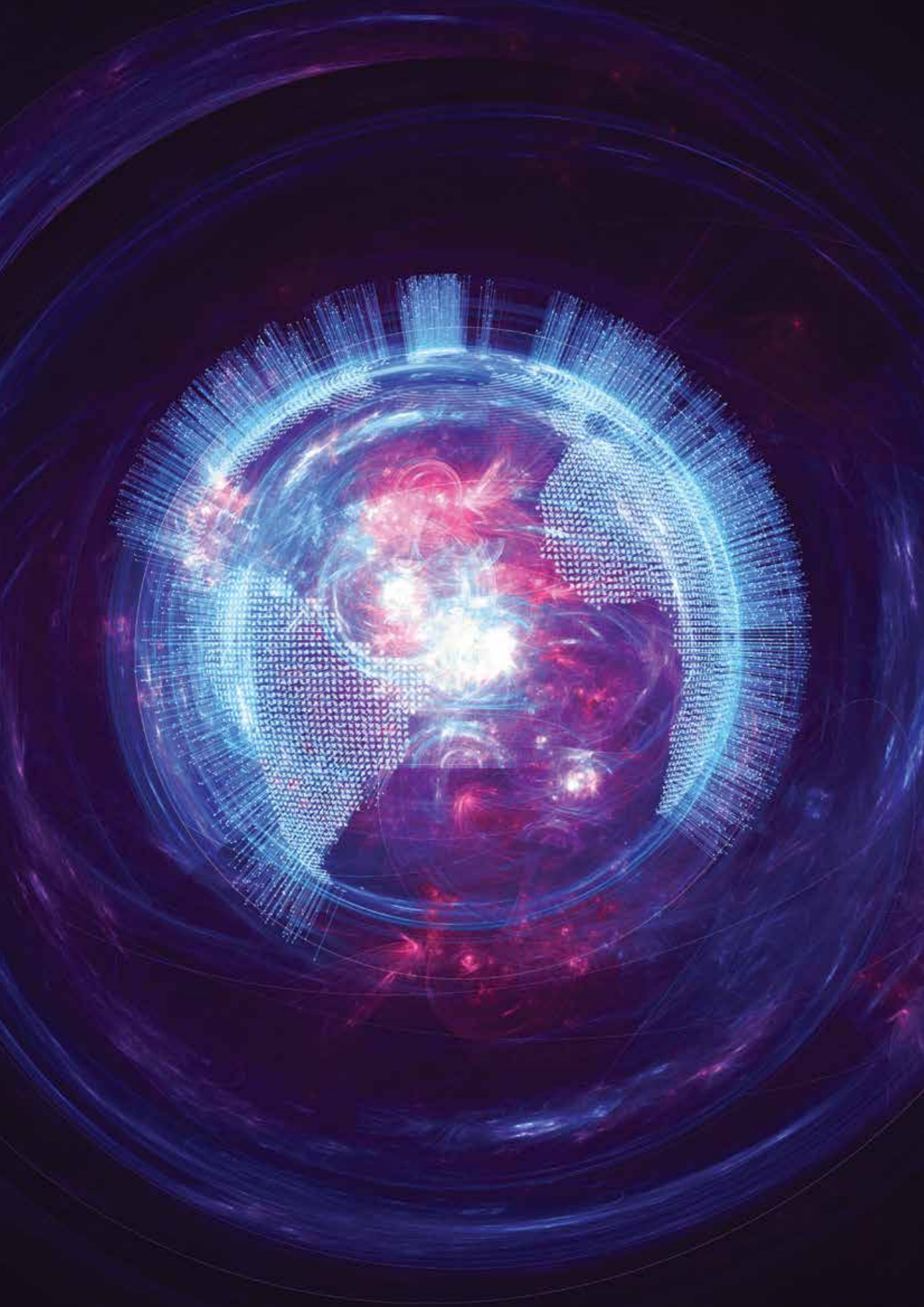
Future of Cyber Work

To examine the human dimensions of cybersecurity and how it intersects with the workforce, the fourth sub-theme, future of cyber work, featured sessions on how to attract, retain, and foster highly skilled talent through understanding challenges and incentivization, and the different dimensions of competition. ■



No One Left Behind

The final sub-theme, no one left behind, sought to bridge global cyber divides and ensure that cybersecurity benefits and supports all people and societies. Sessions identified key challenges women face in cybersecurity and how to ensure children globally can safely benefit from the opportunities presented by Cyberspace. ■



Opening Speech from **His Royal Highness Prince Faisal bin Bandar bin Abdulaziz, Governor of Riyadh**

Distinguished attendees,

On behalf of the Custodian of the Two Holy Mosques King Salman bin Abdulaziz Al Saud, I am honored to open the 2022 edition of the Global Cybersecurity Forum.

We warmly welcome you to Riyadh and wish you success in your endeavors to achieve the goals of this Forum.

Esteemed guests,

The cybersecurity sector is witnessing rapid development and increasing challenges, which makes international collaboration more urgent than ever before. Under Vision 2030, the Kingdom has strived to achieve developmental, social and economic progress in all fields, not least in cybersecurity. His Royal Highness Prince Mohammed bin Salman bin Abdulaziz, Crown Prince and Prime Minister of the kingdom of Saudi Arabia, has provided significant attention and support to cybersecurity, which has resulted in the Kingdom ranking second place internationally in the Global Cybersecurity Index of 2021.

In the first edition of this forum, His Royal Highness Prince Mohammed bin Salman announced two global initiatives to protect children in Cyberspace and empower women to contribute effectively to cybersecurity; a reflection of His Royal Highness' commitment for the Kingdom to deliver benevolent initiatives to the world and his interest in cybersecurity as one of the priorities of our time.

Finally, I call on all partners around the world to work with the Global Cybersecurity Forum to reach a safe and stable Cyberspace that enables growth and prosperity for all.

I thank you for your presence and wish everyone success at this Forum. ■

His Royal Highness Prince Faisal bin Bandar bin Abdulaziz,
Governor of Riyadh




Global
Cybersecurity
Forum

Opening Speech from
H.E. Majed bin Mohammed Al-Mazyed, Governor of the National Cybersecurity Authority, Saudi Arabia

Your Excellencies,
Ladies and Gentlemen,

Good morning... and good evening to those of you who are watching us from other continents.

Welcome to Riyadh and welcome to the 2022 edition of the Global Cybersecurity Forum.

We have gathered the brightest minds in the sector from over 110 countries with a simple yet ambitious theme in mind: Rethinking the Global Cyber Order.

The world is evolving rapidly across many industries, and Cyberspace is not exempt from these shifting realities. If we want to prevent the crystallization of a global cyber order that is unsecure, unstable, and where the most vulnerable are unprotected, we must find new ways of collaborating. We have a responsibility to imagine a cyber order that is based on our shared values of peace, tolerance, and prosperity.

A Cyberspace that respects different cultures and values, together with our global aspirations for progress and innovation. An equitable Cyberspace where all nations – at every stage of development – are empowered to advance and prosper.

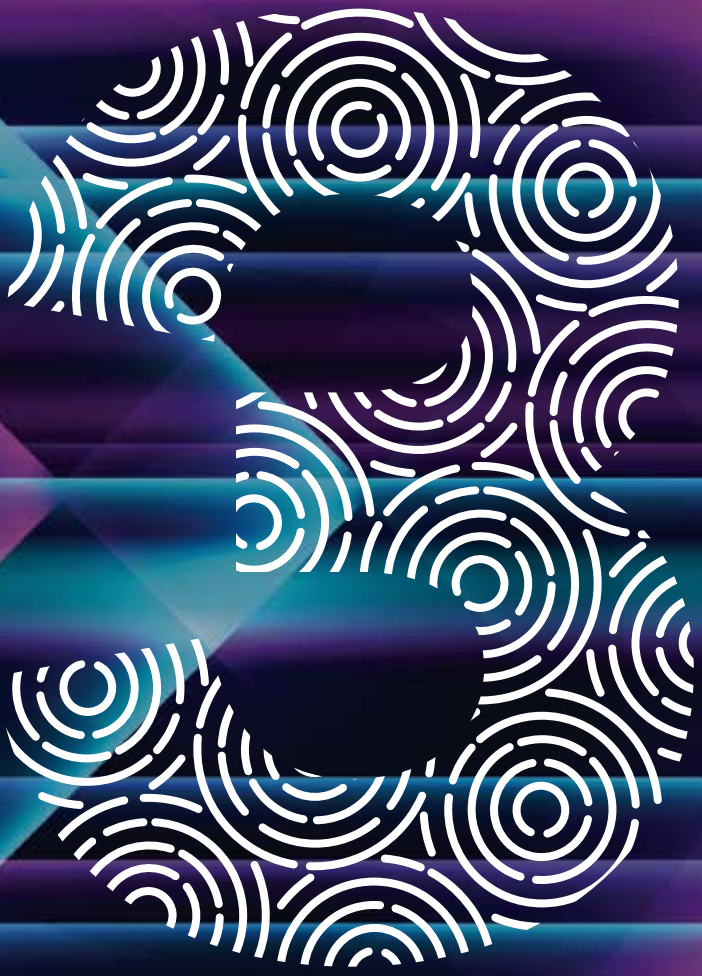
An inclusive Cyberspace where all segments of society are able to contribute and feel protected and supported. In hosting the Global Cybersecurity Forum, Saudi Arabia aims to plant the seeds of discussion, collaboration, and ingenuity that will help rethink the global cyber order in a way that is more just, resilient, safe, and secure.

GCF is a platform for partnership opportunities to grow, develop and reimagine the future of the cybersecurity sector and beyond. It is a space for new perspectives that drive collaboration, innovation, and investment across industries, and where we push knowledge boundaries, advance dialogue, and shape the global cybersecurity agenda.

Now, as we get started with our program, I hope that you will find the forum's rich agenda over the next two days insightful and inspiring. We look forward to working with all of you to deliver on our collective ambitions and bring global partners behind our common cybersecurity goals. Together, we can shape a Cyberspace that reflects our shared values and aspirations, driving prosperity for the benefit of all people around the world.

Thank you ■

H.E. Majed bin Mohammed Al-Mazyed,
Governor of the National Cybersecurity Authority, Saudi Arabia



PROCEEDINGS

Rethinking the Global Cyber Order, Why? (1/2)

| **Michio Kaku** Professor of Theoretical Physics, **City University of New York**
| **Shyam Saran** **Former Foreign Secretary, India**
| **Mary Aiken** Professor of Cyberpsychology and Chair of the Department of Cyberpsychology, **Capitol Technology University**
| **John Defterios** (Moderator) – Former CNN Emerging Markets Editor and Professor of Business, NYU Abu Dhabi

The panelists opened the first session of the 2022 Edition of the Global Cybersecurity Forum, addressing three of the five sub-themes of the Forum – Disruption Frontier, Geo-Cyber Evolution and No One Left Behind. The discussion covered several emerging cybersecurity threats that require a new level of global coordination and collective response. All states are facing rapidly transforming cyber environments with unfamiliar and emerging ecosystems and unknown and often hostile actors. A key element, quantum computers, is ushering in a new era of cybersecurity. Quantum computers are powerful enough to negotiate their way through cyber walls that are designed to protect the most important aspects of an organization or states security systems.

"In the future, historians will view digital computers like an abacus, obsolete. Digital computers will be phased out. The web, the cloud will be Quantum... Quantum will take over everything."

Michio Kaku





Panelists also addressed the critical threats states and individuals face by online anonymity. This invisibility means that one's actions undertaken online may no longer have consequences. To fully understand human behavior in Cyberspace, grasping how negative behavior impacts individuals when online is crucial. The impact of technology on children's development was emphasized to ensure no one is left behind online, where children and women can be targeted disproportionately.

In conclusion, panelists agreed that today's cybersecurity challenges are borderless, global and constantly evolving. Global collaboration and preparedness through a framework similar to those used for trade issues or arms control could be a solution. Governments need to educate their citizens to be prepared for the challenges of dealing with ever more complex developments like artificial intelligence and quantum computers. States themselves and companies need to reinforce their protection systems to be prepared for the quantum computing threats of tomorrow, which makes collaboration more imperative as states seek to maintain harmony. ■

"People do things online that they would not do in the real world, particularly young people. They take risks online that they would not typically take."

Mary Aiken

"I would like to say to all those who are gathered here that, in all the deliberations that you would be involved in, may sometimes seem to be torturous, may sometimes seem to be extremely complex. But I don't think we should ever forget what our first Prime Minister Jawaharlal Nehru said at the United Nations in terms of this collaboration, that it is far better to sweat for peace, rather than bleed in war."

Shyam Saran

Keeping the Lights On

Amin Nasser CEO, **Aramco**



In his introductory remarks, Amin Nasser, stressed that the importance of cybersecurity to the energy sector cannot be overstated. The energy industry as a whole, and Aramco in particular, has long been a target for attackers. While attacks were typically physical in the past, the danger is now compounded with the threat of cyberattacks in the form of ransomware or damage to critical energy infrastructure. Nasser noted, "The energy industry has an obvious vulnerability, namely the sector's dependency on legacy systems, many of which were built long before cyber attacks were ever considered a risk." Any significant disruption of energy flow through either physical attacks or cyberattacks would have devastating consequences.

"To help put the stark reality of cybersecurity into perspective, we must never forget that cyber attackers only need to be successful once to cause major damage. While to prevent such, we on the other hand, must be successful every single time."

Amin Nasser



Nasser emphasized that, for this reason, Aramco and other companies must put in place strong cybersecurity standards independently, particularly in the areas of safety, operational excellence and environmental excellence. However, individual action is not enough where Nasser emphasized, "fighting against cyber-attacks is not something that individual companies can do on their own." Collaboration across borders, industries, and in the public and private sectors is necessary to tackle these cyber threats. Aramco has taken a lead on such initiatives by partnering with the Saudi Arabia National Cybersecurity Agency and the World Economic Forum to support adaptation of best practices and principles for cyber resilience globally.

Keeping the Lights On

| **Jeremy Jurgens** Managing Director, **World Economic Forum**
| **Dr. Saad Alaboodi** CEO, **SITE**, Saudi Arabia
| **Christophe Blassiau** SVP Cybersecurity and Global CISO, **Schneider Electric**
| **Robert Putnam** Global Manager Cybersecurity Products and Services, **ABB**
| **Sasha Qadri** (Moderator) – Journalist

The panel's discussion emphasized that today, energy is the fuel for the prosperity of all other industries and this fuel needs to be protected. Therefore, the energy sector and cybersecurity are inextricably linked as they directly impact the global economy, national security, and humanity.

The greatest cyber threat within the energy system is disruption, which can have catastrophic consequences for citizens, societies, and economies. One of the most significant risks contributing to this threat is the exposure of Operational Technology (OT) assets to the internet. Another contributing factor to cyber threats is complacency. Individuals and companies often fail to understand and model the risk present in critical infrastructure and therefore do not mitigate it, while human error significantly contributes to cyber incidents.

Panelists noted that because of the proliferation of cyberattacks on energy infrastructure, there is a critical need to develop standards and a systematic methodology of evaluating energy infrastructure, particularly risk modelling. Organizations should also incorporate cybersecurity governance, as well as increase awareness training to reduce human error.



"There are some really fundamental governance principles that need to be put in place within organizations, the training needs to be put in place and just addressing some of these foundational elements such as complacency through better training, better awareness is a kind of first line of defense, even before you come up with the technology approaches which are continually evolving."

Jeremy Jurgens

"The awareness has gone from 'I am air gapped, how can anyone possibly penetrate my facility and do something nefarious', to – there are plenty of examples out there [of attacks]. It's moved from an inconvenient truth to an undeniable reality."

Robert Putnam

$10

billion – to be spent on cybersecurity in oil and gas sector by 2025

(Source: Global Data, 2022)



In concluding remarks panelists agreed that governments could nudge the energy sector out of its complacency by developing and enforcing regulatory standards, and driving the progression of a global cybersecurity framework. The framework should highlight the roles, responsibilities, and accountability of actors within the ecosystem. When it comes to the private sector, there is a need to improve industry-wide collaboration in Cyberspace and for all actors in the ecosystem to collaborate, execute, and deliver results for the global cybersecurity problems of today. ■

"There are three main commonalities that connect the cybersecurity domain with the energy domain. Both the energy and cybersecurity sectors have direct impact on the global economy, national security and human lives."

Dr. Saad Alaboodi

$5

trillion – Market size of ICT

(Source: Sun News Online, 2019)

A Cyber War Deterred?

| **Dr. Khalid Biyari** Assistant, Minister of Defense for Executive Affairs, **Ministry of Defense**, Saudi Arabia
| **Rajesh Pant** National Cyber Security Coordinator, **National Security Council Secretariat**, Government of India
| **Robin Geiss** Director, **United Nations Institute for Disarmament Research (UNIDIR)**
| **Rebecca McLaughlin-Eastham** (Moderator) – TV Anchor & MD, RME Media

Panelists discussed that defense and deterrence take a different form in Cyberspace to traditional warfare given the complexity of the cyber domain. On one hand, there is a distinct opportunity for people working in cybersecurity defense to capitalize on many of the concepts that have been successful in the military. One such method may be through offering clear thresholds for acceptable actions. On the other hand, Cyberspace presents a unique set of challenges when it comes to deterrence and disarmament. The lines in cyberspace are blurred and actors are often anonymous.



"Today, the tech field is far ahead of the policy field. We have processes for cyber. In Geneva, we have a process for AI and robots on the battlefield and so on and so on. But again, that's a bird's eye perspective. All the synergies that these technologies will have -- that needs to be better understood. It is a race."

Robin Geiss



Panelists discussed that given the lack of clarity around traditional deterrence in the evolving space of cybersecurity, the arms race of the 21st century spans across not just the military, but also across economic, scientific, and technological domains. There is a global race to bring military processes up to machine speed. The international community, already overwhelmed with many unique crises, must also be prepared to confront the challenges presented by a cyber arms race.

Concluding the discussion, panelists agreed that future threats include the convergence of many different technologies, including cyber-AI, advancements in robotics, advancements in sensors, cameras, and even smaller batteries. The impact of this convergence remains to be seen, especially how these developments may shape military processes and future battlefields, including prospects for future conflict prevention. ■

"Any national strategy has to cover all aspects of the cyber ecosystem. Governance has to be there, [as well as] risk compliance, the audits, the education and awareness, and your defense posture. Everything has to be covered"

Rajesh Pant

"Things are accelerating as governments, organizations and corporates are accelerating to build their defenses. Hackers and cyberspace criminals are gaining access to better computing capabilities and more clever approaches, and it is a race. The only thing you can do as corporate or government is to ensure you have the best people, best trained staff, put them in the right environment so that can really excel."

Dr. Khalid Biyari

The Rising Tide

Dr. Khaled Al-Dhaher Vice Governor for Supervision and Technology, **Saudi Central Bank (SAMA)**
Prof. Isa Ali Ibrahim **Minister of Communications Digital Economy**, Federal Republic of Nigeria
Olayan Alwetaid Group CEO, **stc group**
Abdulrahman Al-Fageeh Acting CEO, **Saudi Basic Industrial Corporation (SABIC)**
Alex Liu Managing Partner and Chairman, **Kearney**
Ramia Farrage (Moderator) – Senior Producer and Presenter, Forbes Middle East

Panelists emphasized that the continuous rise of cybercrime is driven by multiple factors, such as the accelerating pace of digitalization, the increasing complexity caused by disruptive technologies, and the rising financial incentives of executing cyberattacks and cybercrime. With the unprecedented rise in cyberattacks, cyber economics or the cost of cybersecurity and cyberattacks is now at the forefront. There is a growing need to truly understand the financial impact of cyberattacks.

Panelists noted that today the costs and financial impact of a cyberattack are multilayered and can be grouped as tangible or intangible. Tangible costs include elements such as investment in protection, prevention, and detection capabilities and services. Intangible costs include brand or reputational damage, the psychological impact of cyberattacks, and the disruption of services to customers. In addition to these costs, cybercrimes and attacks greatly undermine the public trust in the digital

"There's a role for public-private partnerships, communication, and forums like this between competitors in the country, multi-domestic collaboration with the G20 and other government-to-government bodies to have common standards on how to look at and unify criminals and criminality and identity."

Alex Liu





economy and can lead to mistrust between producers, suppliers, and consumers.

In conclusion, the panelists agreed that in order to tackle these issues, there is an urgent need for proactivity to ensure continuity of services and enhance trust in the system. Governments may shift their focus to developing standards and guidelines, while providing adequate budgets for protection and prevention. Additionally, significant investment by governments in technology and capability development may help to ensure a whole-of-government focus on prevention, detection, and protection. At the organizational level, businesses can also take important steps, including focusing on risk audits, penetration testing, public-private partnerships, and cybersecurity awareness and training. ■

"There is a need for us to try to attain cyber security maturity and most importantly to have cybersecurity immunity where the cost of the attack is more expensive than the damage to be done by the attack."

Isa Ali Ibrahim

"Investing in technology alone, without having the right governance, without having the right capabilities that enable the use of technology to detect, prevent, and protect, will not be sufficient."

Dr. Khaled Al-Dhaher

"We need to address the root causes of cyberattacks as they affect us in two ways. The first is on a macro-economic level, undermining the public's trust in digital services. On the other hand, it deepens and widens the divide between the suppliers and producers".

Abdulrahman Al-Fageeh

"Being an infrastructure provider, we monitor and protect against a lot of types of attacks. The way we are looking at it is simple. This is a fight that can only be won by investing in our own protection systems and that is what we are doing."

Olayan Alwetaid

$10.5

trillion – Annual cybercrime costs by 2025

(Source: Boise State University Study)

Every 4.2

seconds a new malware is released

(Source: G Data)

Ensuring Resilience and Interoperability While Integrating Diversity

| **Ursula Owusu-Ekuful** **Minister for Communications and Digitalization**, Republic of Ghana
| **Göran Marby** President and CEO, **ICANN**
| **John Defterios** (Moderator) - Former CNN Emerging Markets Editor & Professor of Business, NYU Abu Dhabi



The panel discussed how African countries face critical challenges as they seek to enhance cybersecurity capabilities in their respective nations. The main challenges are providing universal internet access and tackling the rising costs of security. With some African regions unable to access the internet, their participation in critical developments for the fourth industrial revolution is limited.

Panelists noted that African nations are struggling to build resilient systems on their own and there is not as much focus on the African continent or the global south. As cybersecurity is increasingly becoming a whole-of-society undertaking, all nations are as vulnerable as the most vulnerable actor in the ecosystem. Countries cannot progress independently unless all countries make progress.

In conclusion, panelists noted increased collaboration as a clear path forward, particularly for nations looking to capacity-building programs. Developed nations should place greater emphasis on

"We recognize that we in the technical community didn't do everything right from the beginning. We built something global with the internet but what we didn't do well was to turn the global into local. Each country has the right to their own internet. We need to further develop this so that people can use their own language, keyboards and narratives to be able to interact on the internet."

Göran Marby



providing support for less developed nations, as it is in their best long-term interest to ensure everyone is prepared to deal with a potentially catastrophic cyber-event. Another potential solution is collective internet governance led by international organizations - these organizations can provide resilient and interoperable systems that can in turn protect everyone. ■

"We're not asking for favors, we're asking to be seen as part of the global internet community, treated as such, and assisted in our weak points and our vulnerabilities to also come up to speed with the rest of the world. Because we may ultimately prove to be the salvation of the global internet community going forward."

Ursula Owusu-Okuful

No Nation Left Behind

| **Abdullah Alswaha** **Minister of Communications and Technology,** Saudi Arabia
| **Khumbudzo Ntshavheni** **Minister of Communications and Digital Technologies,** South Africa
| **Doreen-Bogdan Martin** Secretary-General, **International Telecommunication Union (ITU)**
| **Rebecca McLaughlin-Eastham** (Moderator) – TV Anchor and Managing Director, RME Media

Panelists noted one third of humanity has never connected to the internet. This striking figure highlights the urgency with which the cybersecurity ecosystem must focus on ensuring no one is left behind. No single stakeholder in the ecosystem can ensure universal connectivity on their own. To realize the full potential of the digital economy requires collaboration and interaction across entities and geographies. It requires countries to develop connectivity programs and partner with others around the globe.

Panelists agreed that a crucial facet of increasing connectivity is ensuring the safety and security of everyone online, particularly the most vulnerable. Energy security, food security and supply chain disruptions are among critical items at the top of the world's risk register, and often putting cybersecurity on the backburner.

"I think what's concerning and a space where we need to focus ... is the gaps that we see with developing countries, so developed countries are advancing, but developing countries are falling further behind and so we have to focus on strengthening the capacity in particular in least developed countries."

Doreen-Bogdan Martin





Governments must work together and treat cybersecurity as a top priority. One way forward is the development of global and regional frameworks centered around universal access, inherent security, and standardization.

Panelists emphasized that for a truly secure global Cyberspace, focus is needed on developing the capabilities of the least developed countries who are unable to advance their cybersecurity sector due to a lack of expertise. Countries around the world, particularly ITU member states, can work in partnership to develop capacity building support globally. In an interconnected, interdependent world, continuous adaption and collaboration provides the best opportunity for cybersecurity for all.

In conclusion, panelists suggested that moving forward, countries place additional focus on universal connectivity, developing a skilled cybersecurity workforce, and sustainable digital transformation. Achieving this would require investments in training and upskilling, developing standardized frameworks at the global and regional level, and fostering a culture of collaboration and engagement across all sectors. ■

"... And last but not least we need more collaboration because today a cyber threat could be the next digital pandemic."

Abdullah Alswaha

3.5
million unfilled cybersecurity jobs
(Source: Boise State University Study, 2021)

8.4
billion passwords compromised in the RockYou 2021 data breach
(Source: Teiss)

Incentive Reinvention

Craig JONES Cybercrime Director, **INTERPOL**

Elvira Tejada De La Fuente Chamber Prosecutor of the **Supreme Court**, Head of the **Cybercrime Unit, State Attorney General's Office,** Spain

Marco Gercke Director, **Cybercrime Research Institute**

Rawan Radwan (Moderator) – Deputy Section Head, Arab News



Panelists discussed several key challenges on the topic of cybercrime policing, in particular a disparity in policing standards with varying cybercrime laws in different countries or, in some cases, no laws at all. In some cases, laws are drafted with acute local focus within communities and so do not properly reflect the transnational nature of many cybercrimes. As the role of policing is to protect communities, this makes sense, but this policing model falls short when dealing with transnational crime. This means there is now a critical imperative to develop international standards related to cybercrime law enforcement globally.

"Preventing cyber criminals is a must. Not only on the national and state levels, but also there must be a framework for collaboration in preventing such attacks on private sectors, SMEs, and individuals."

Elvira Tejada De La Fuente



Panelists discussed that to reach this end goal, states could engage in the complex and collective process of building international standards through transnational conventions. Progress has already been made within the United Nations for negotiations on a new cybercrime treaty, but this requires focus, effort and time. However, these processes represent the necessary evolution of cybercrime policing.

In conclusion, panelists agreed that despite the many challenges in this area, there is reason to be encouraged. Countries have used multilateral and international organizations to drive progress on cybercrime and this dialogue continues amongst many states, including smaller states, in order to make progress and establish international consensus on a topic that affects the police functions of all nations. ■

"Law enforcement is not equipped at this moment in time to deal effectively with transnational crimes such as cybercrime. Yes, it can deal with commodity-based crimes such as drugs or human trafficking, because that's the policing model working in that physical space. Once you spread that out across the globe, there are different priorities."

Craig JONES

Securing the Energy's Supply Chain

H.R.H Prince Abdulaziz Bin Salman Al-Saud Minister of Energy, **Ministry of Energy**, Saudi Arabia

Rima Maktabi (Moderator) – London Bureau Chief, Al Arabiya News Channel



H.R.H Prince Abdulaziz Bin Salman Al-Saud emphasized that the energy sector faces the most serious threats and potential ramifications of a critical cyberattack. There are particular vulnerabilities in the context of Saudi Arabia's energy system, which encompasses oil and gas refining, chemicals, power, distribution, transmission, pipelines, and vendors. The Kingdom must prepare for any and all attacks that may occur and cannot become complacent with recent cybersecurity successes.

The Kingdom has goals to become a leading exporter of electricity and hydrogen and cannot afford to be exposed to such attacks without being well equipped to defend against them. While Saudi Arabia is making tremendous progress in the domain of cybersecurity, every sector must continue to prepare for the next potential threat.



Every industry must collaborate in bringing an end to the challenge. H.R.H Prince Abdulaziz Bin Salman Al-Saud noted, "We need to be humbled by the fact that it's been an endeavor over the last four or five years. But I believe that there is permeating culture that we all need to work with each other and congregate on the best possible practices that can be available." It is also important to engage the country's youth to fight against cybercrime, and in particular young women. Women continue to take a lead on cybersecurity efforts in Saudi Arabia and must be supported in their efforts to drive forward the Kingdom's leadership in this area. ■

"Cyber attacks are a great danger that have to be attended to collectively. Every industry should collaborate in bringing an end to this challenge."

H.R.H. Prince Abdulaziz Bin Salman Al-Saud

Safe Children in Cyberspace

Powered in Collaboration with unicef

- **Dr. Albert Antwi-Boasiako** Ag. Director-General, **Cyber Security Authority,** Republic of Ghana
- **Sanjay Wijeskera** Director Programme Group, **UNICEF**
- **Natasha Jackson** Head of Public Policy and Consumer Affairs, **GSMA**
- **Prof. Amanda Third** Co-Director, **Young and Resilient Research Centre, Western Sydney University**
- **Afrooz Kaviani Johnson** (Moderator) – Child Protection Specialist, UNICEF

Panelists emphasized that the internet was not designed with children and young people in mind. This means children are exposed to a myriad of risks online, ranging from cyber bullying to sexual exploitation. Children, who form approximately a third of those online, do not fully understand the mechanics of the internet.

Panelists agreed that any solutions or interventions developed to improve cybersecurity for children should be done by incorporating the unique perspectives of children. These children-centered solutions should be

"A child's perspective and ingenuity should be brought to the table and youth should no longer be viewed as only a vulnerability."

Gitanjali Rao via pre-recorded message





created on the principle of viewing children as key stakeholders and not just a vulnerability. To achieve this, governments, private sector, NGOs, and the entire ecosystem should come together to first understand the needs of children.

In conclusion, panelists asserted that a whole-of-government approach with research backed insights is needed in the development and execution of frameworks, policies, and regulations. An example of this approach is the National Child Online Safety Framework which is being developed by the Kingdom of Saudi Arabia together with UNICEF and the Young and Resilient Research Centre. However, governments cannot work alone. The private sector, particularly internet and platform providers, have a key role in creating an enabling environment for children. There is a need for providers to focus on the experiences children have while interacting with their platforms and services. Children's perspectives and needs must be incorporated during the design phase to ensure every child has access to safe and reliable digital technology. There is also a need for adults to be better role models for their children at home. Increased awareness at all levels of the ecosystem will help to protect children as they connect online. ■

"So whilst we in the room here today might work very, very hard. It is the children of the next generation who will take on those challenges, so we need to start investing in them and growing them now ... engaging children makes our interventions more effective here and now, today."

Prof. Amanda Third

20%

percentage of children in Africa and Southeast Asia experienced sexual exploitation and abuse online in the past year

(Source: End Violence)

Cooperation as an Imperative to Tackle Cybercrime

Major General Dr. Ahmed Naser Al-Raisi President, **INTERPOL**

Rima Maktabi (Moderator) – London Bureau Chief, Al Arabiya News Channel



Major General Dr. Ahmed Naser Al-Raisi emphasized during the discussion that crime has effectively become borderless within the cyber domain, and conventional approaches to tackling criminal activity no longer work in today's interconnected landscape. As a result INTERPOL focuses on providing member states with a key platform for cooperation, information sharing, and joint action.

Al-Raisi noted that INTERPOL's transnational priorities include neutrality, information sharing and operational support. Tackling cross-border crimes requires a close exchange of information and a collective commitment to preventing criminal activity. Specifically, usage and contribution to INTERPOL's 19 databases has aided in identifying both perpetrators and victims of cybercrimes. INTERPOL provides additional operational support, including investigative support, field operations, and domestic capacity building to provide states with the resources necessary to prevent and protect against cybercrime within their jurisdiction.

"If I have information about a crime in another country or continent, this information will be necessary for those countries. If we have an information database where we can exchange this information, even if there is no diplomatic relationship, this information is important for the protection of citizens, residents, companies, and society as a whole from the calamity of cybercrime which is greatly increasing year on year."

Dr. Ahmed Naser Al-Raisi



Looking to the future, Al-Raisi suggested that progress in the cyber domain requires a clear framework of standards for collaboration. As there is no simple solution to stopping crimes, a framework grounded in cross-border collaboration and information exchange will allow nations and multinational organizations to most effectively utilize the resources needed to prevent contemporary crimes. Most importantly, such a framework will further establish the principle that no nation can be left behind in the global fight against cybercrime. Internally, INTERPOL may additionally seek to develop into a digital-first organization to be proactive in their approach to global cybercrime. ■

$10.5

trillion – expected global cost of cybercrime by 2025, representing the greatest transfer of economic wealth in history

(Source: Cybersecurity Ventures)

Distributed Ledger Technology (DLT) – Opportunity or Obstacle?

Dr. Craig Wright Founder and Chief Scientist, **nChain**

Ramia Farrage (Moderator) – Senior Presenter and Producer, Forbes Middle East



Dr. Craig Wright noted that blockchain and emerging technologies like Distributed Ledger Technology (DLT) face widespread criticism driven by misinformation. When people consider these technologies, they consider tradable assets that are speculative or involve gambling. They do not consider the benefits, including data integrity, the use of transferring funds, and the ability to have micro payments. On the topic of micro payments, Wright emphasized, "My goal this decade is next year to get into the millions of transactions a second publicly, but by the end of the decade, to get to in the order of five to 10 million transactions per second on a public blockchain that will be at a cost of under a 1,000th of a cent." Generally, people are only focused on bitcoin tokens and not necessarily the blockchains that correlate with those tokens. However, blockchain can play an important role in opening markets and advancing security apparatuses for governments and corporations alike.



Dr. Wright highlighted that as a key example of DLT implementation for security, threshold signature technology has unique benefits for national security councils to ensure a deep level of protection over working files. This technology gives users clear information on the status of their files and alerts to any changes being made. It also allows users to pinpoint the exact moment where a hacker has accessed a system - these real-time updates give users the ability to start rectifying the situation without delay.

Dr. Wright noted that central bank digital currencies have the potential to open up new pathways of international trade for nations. Ubiquitous national digital currencies would allow states to trade independently globally, without having to first go through Swift or any other controls. ■

The Cybersecurity Market

Sheikh Salman bin Mohammed Al Khalifa CEO, **the National Center for Cybersecurity,** Kingdom of Bahrain
Eugene Kaspersky CEO, **Kaspersky**
Fahad Al-Jutaily CEO, **sirar by stc**
Rawan Radwan (Moderator) – Deputy Section Editor, Arab News

Panelists discussed the shifting cybersecurity threat landscape alongside the market and regulatory landscape. Governments and private corporations may seek to alter their operations to increase preparedness and standardize response protocols to adapt more effectively to the threats of tomorrow.

Panelists noted three clear cybersecurity trends in 2022: increase in cybercrime and cyber threats; the changing nature of the industry, and the shifting behavior of nations. First, cyber criminals are now more organized than ever and have expanded their attacks from consumers and individual organizations to unprecedented numbers of large-scale industrial level attacks as "Ransomware as a Service" offerings complete with customer support. Secondly, the industry

"The world is now shifting from the traditional Castle, where they trust everything inside their parameters and moving towards something called "zero trust" where they trust nothing in their network unless they know who the users are and their privileges."

Sheikh Salman bin Mohammed Al Khalifa





is transforming and adapting to the increasing threat level by incorporating new concepts and technologies for enhanced security at all levels, including improved identity management and zero trust networks. Lastly, more and more states are now developing and implementing policies focused on data privacy and data sovereignty increasing the regulatory requirements that all ecosystem players must adhere to.

In conclusion, panelists agreed that countries and companies can focus on a number of key actions to better navigate cyberspace. First is the imperative to design new systems based on the principles of cybersecurity, this requires all scenarios to be accounted for and tested during the development of all products and services. Secondly, sector entities can shift their focus to investing in emerging technologies and capability building. Investments and budgets should happen in consultation with cybersecurity teams alongside conducting security audits to identify the most critical areas for investment. Lastly, governments can support the ecosystem by developing robust policies and regulations that standardize and harmonize services and products to ensure an adequate level of cybersecurity is maintained across the ecosystem. ■

"We speak about security for small businesses, even enterprises, we can balance the risks, we can estimate the damage from a successful cyber attack. In case of critical systems, the damage could be unlimited. The damage could be the size of the national economy, so the security doesn't compensate the risk, so we need to introduce something new."

Eugene Kaspersky

Cyber threats are getting much more complicated. The bad guys are smarter, but at the same time, there are more demands from the markets. Now we have to protect individuals, businesses of different size, industrial sector, and critical infrastructure."

Fahad Al-Jutaily

The Topography of Cyber Threats

| **Eng. Nezar Alomar** Deputy Governor, Cyber Technologies and Operations, **National Cybersecurity Authority,** Saudi Arabia
| **Helmut Reisinger** CEO EMEA & LATAM, **Palo Alto Networks**
| **David Kanamugire** Chief Executive Officer, **National Cyber Security Authority (NCSA),** Rwanda
| **Pierre Yves Jolivet** Vice President, Cyber Defense Solutions**, Thales Group**
| **Chris Gibson** Executive Director, **Forum of incident Response and Security Teams (FIRST)**
| **Chris Fox (Moderator)** – Technology Presenter, BBC

Panelists discussed that the attack surface in cyberspace is increasing at a drastic pace and is being accelerated by five major drivers. The first is geo-politics where the international community has seen a major increase in global cyber competition and state driven attacks. The second driver is digital transformation, wherein businesses are becoming increasingly digitalized with IT and OT assets interacting more than ever before. The third driver is software vulnerabilities, as the majority of coders and programmers are using open-source components which leads to malicious content being disseminated rapidly. The fourth driver is the shift to online operations triggered by the COVID-19 pandemic. The fifth driver is the hackers themselves with more organized, sophisticated, and automated attacks than ever before.

"One thing that we try to tell our people is cyber cannot be a technology issue. It's like thinking that COVID is a clinical issue. It is an economic issue. It's a whole-of-society issue, and a coordinated response is what is needed."

David Kanamugire





The growing complexity of Cyberspace and cyberattacks accentuates major problems facing the ecosystem. Cyber poverty has emerged as one key issue. Significant parts of the world lack the financial resources and the capabilities necessary to bolster their cybersecurity. At the organizational level, this includes public services, NGOs, charities, and SMEs. The divide will continue to widen as more technological advancements such as AI and quantum computing emerge.

In conclusion, panelists agreed that governments and organizations should invest in and develop solutions that can help protect the ecosystem. First, there should be emphasis on zero trust architecture with zero exceptions. Secondly, as the world moves to the cloud, there is a need to enable organizations to enhance protection from the code to the cloud. Third, there is a need to integrate AI and emerging technologies in all aspects of cybersecurity, cloud security and data privacy. However, there is still room for governments to do more. As David Kanamugire emphasized, "One thing that we try to tell our people is cyber cannot be a technology issue. It's like thinking that COVID is a clinical issue. It is an economic issue. It's a whole-of-society issue, and a coordinated response is what is needed." National cybersecurity agencies should coordinate at the ecosystem level, focusing on operational cooperation, information sharing, joint capability development across all entities and awareness strategies of best practice to enhance security. ■

"Cyber poverty to me is a big, big issue. It's not regional, it's not government, it's not political. It cuts across sectors, verticals, markets, regions, and countries."

Chris Gibson

Cybersecurity of Critical National Infrastructure

Eng. Nadhmi Alnasr CEO, **NEOM**



Eng. Nadhmi Alnasr emphasized that with technology becoming more integral to managing critical national infrastructure (CNI) at scale, and artificial intelligence becoming a key component of automation at all levels, attackers are developing new ways to breach CNI systems. Eng. Alnasr noted, "The fastest growing and most dangerous of these attacks have one thing in common, they are enabled by AI, the same technology which is helping to achieve more efficiency and effectiveness." This means, NEOM and the Kingdom must work to ensure the security of water, electricity, emergency services, and other critical infrastructure points that maintain safe, secure, and robust communities.



NEOM hopes to drive progress for its own security, but also for that of the Kingdom at-large and the rest of the world. Saudi Arabia is working towards self-healing critical national infrastructure, which would be able to spot the first signs of attack and neutralize them before the first symptoms would be visible in the physical world. These solutions define NEOM's future-forward approach.

Eng. Alnasr stressed that NEOM plans to have central connectivity across multiple critical infrastructure networks. It is not possible to respond automatically in all security scenarios as human accountability needs to be preserved for key decisions impacting critical national infrastructure. In turn, NEOM plans to implement a full role-based cognitive control solution that allows decision makers to provide cognitive security operations in place of AI when necessary. Eng. Al Nasr added, "All these capabilities that we are designing, planning, and hopefully implementing in NEOM will be in a single integrated and cognitive solution that will allow us to create a safe, inclusive, and progressive society free from the silent threats of the cyber pandemic." ■

"A different kind of global pandemic is occurring every day, without most of us noticing what's happening around us. This is a cyber pandemic, with seemingly endless variants and versions, which can have damaging and long-lasting consequences."

Eng. Nadhmi Alnasr

Promoting Internet Security – Best Practices

Powered in Collaboration with ICANN

- **Dr. Chafic Chaya** Regional Manager of Public Policy and Government Affairs, Middle East, **RIPE NCC**
- **John Crain** SVP, Chief Technology Officer, **ICANN**
- **Dr. Hanna Kreitem** Senior Advisor, Internet Technology and Development – MENA, **Internet Society**
- **Baher Esmat** (Moderator) – Regional Vice President for Stakeholder Engagement in the Middle East, and Managing Director for the Middle East and Africa (MEA) Regional Office, ICANN

Panelists discussed how the internet has become a critical part of life in all its aspects. This dependence on the internet has made its security a universal concern. By design, the internet has always relied on a trust-based model between providers and users, today with the evolution and revolution of the internet, the need for built-in security systems is paramount.

Panelists agreed ecosystem entities need to work together to protect Cyberspace. Many global organizations provide access to best practices, research, training, and measurement data to this end. Cybersecurity and internet security is a whole-of-ecosystem endeavor and governments and private sector organizations can research, identify, and strive to become a part of these organizations and alliances to utilize the benefits and resources that they offer.

"I would love to see those that are thinking about how to use regulation to actually talk to the other parts that are doing the network technology so that we can make sure that when we try and regulate technology, we don't break it at the same time."

John Crain





In conclusion, panelists noted that a key element to creating a safer internet is collaboration and coordination. Collaboration between governments, technical communities, and other critical stakeholders is necessary for information sharing and for implementing best practices. These efforts have already proved successful for the rollout of IPV6 networks in the Gulf region. As Dr. Chafic Chaya noted, "The region is one of the most successful regions in deploying IPV6 because of the great efforts and collaboration between the internet community and the government and regulators." Governments and private sector entities can also focus on developing regulations and products that are based on collaborative research with stakeholder involvement. Governments should also coordinate across the multiple agencies operating in the ecosystem - both entities developing regulations and those responsible for ensuring connectivity to ensure an internet which is open, secure, and trustworthy. ■

Divergent Futures

Powered in Collaboration with KEARNEY

Gwenda Fong Assistant Chief Executive, Strategic Planning & Digital Readiness, **Infocomm Media Development Authority (IMDA),** Singapore
Pano Yannakogeorgos Clinical Associate Professor and Program Director, **New York University, Center for Global Affairs**
Rudolph Lohmeyer (Moderator) – Partner, Kearney



The long-term future of the global cyber order is deeply uncertain. Looking out to 2030, a wide range of potential future cybersecurity environments is plausible. This uncertainty is driven by factors including the unstable tension between market forces and governance institutions, intensifying great power rivalry – both geopolitical and geotechnological, and the fate of individual digital sovereignty as our lives are increasingly pervaded by technology. Will markets become increasingly well-governed or will regulation fail to keep pace with innovation? Will leading powers become more deeply locked in escalatory national security competition and conflict, or will stable and balanced international order emerge? Will individuals as both citizens and consumers gain new forms of control over their personal data or will their digital sovereignty be overrun? To manage this degree of uncertainty requires systematic consideration of the full range of potential future scenarios, or alternative futures, and

"The first step in the pathway is to identify what we want the world to look like. We might all agree, we might disagree. But all of these scenarios presented today are frightening because they look a lot different for us. It's about thinking of what we want the world to look like and how we can achieve that."

Pano Yannakogeorgos



identification of the strategies that prove most robust across them. In this session, three global experts applied this approach to identify a robust set of pathways for advancing multilateral collaboration on cybersecurity.

This session centered on exploration of three scenarios depicting alternative 2030 cyber orders. The first 2030 scenario, "Surveillance Rivals," is characterized by starkly divided geopolitical blocs with divergent regulatory models, particularly with respect to data. The second 2030 scenario, "Transnational Titans," is a future shaped by powerful private sector actors, thriving innovation, and strong, but unequal economic growth. The third 2030 scenario of "Disintermediated Government" is a world defined by pervasive applications of distributed ledger technology in which large volumes of economic exchange occur beyond the visibility of government. For each of the three scenarios, panelists were asked to identify the pathways of multilateral collaboration on cybersecurity most likely to hold the greatest potential for meaningful progress.

Across the responses, several robust themes emerged. First, panelists agreed that for smaller countries entering the digital domain, bilateral and multilateral partnerships are urgent imperative in even more competitive cyber landscape. Panelists agreed that states must address disparities between domestic legal frameworks, particularly with respect to the secure design of emerging technologies to enhance harmonization of security protocols. As Ms. Gwenda Fong highlighted, "Singapore has rolled out a cybersecurity labelling scheme for IoT devices which means that we have a certain set of standards by which we can reach and assess IoT devices regardless of where they come from and regardless of who manufactures them, so with such an objective assessment scheme in place, it encourages manufacturers to basically produce things that are secure by design." Across all three scenarios, it was clear that that at the level of national policy, states would benefit from taking an approach that supports regulations to impose more costs on private sector actors which do not manage their cybersecurity correctly. Finally, panelists suggested that governments have a range of emerging opportunities to develop a new generation of partnership models between governments, private sector actors, scientists and innovators, all whom have a shared interest in a more stable and secure global cyber order. ■

Singapore has rolled out a cybersecurity labelling scheme for IoT devices which means that we have a certain set of standards by which we can reach and assess IoT devices regardless of where they come from and regardless of who manufactures them, so with such an objective assessment scheme in place, it encourages manufacturers to basically produce things that are secure by design."

Gwenda Fong

The Future is Female

Powered in Collaboration with BCG

| **Monique Morrow** Senior Distinguished Architect, Emerging Technologies, **Syniverse**
| **Nathalie Rivat** VP System Engineering, **Fortinet**
| **Shoaib Yousuf** Managing Director and Partner, **Boston Consulting Group**
| **Rebecca McLaughlin-Eastham** (Moderator) – TV Anchor & MD, RME Media

Panelists discussed the lack of team diversification in the cybersecurity profession, noting the unique benefits gender diversity would bring to successfully countering evolving threats.

Panelists addressed how diverse teams bring more innovation and have proven to be more efficient. However, artificial targets or quotas for hiring women into the profession are not sufficient - tokenism will not solve the problem. Instead, teams must go further to dismiss the "filter bubble" of viewpoints that don't look or think in the same way. Organizations must change team mentalities across every level and work with human resources departments to do so.

75%

of the cybersecurity workforce is male

(Source: World Economic Forum, 2022)





In conclusion, panelists agreed that in the future, the industry must work to change the media portrayal of a stereotypical male cybersecurity professional. To inspire women to start careers in cybersecurity, it is crucial to highlight successful female role models. Governments can also play a role in highlighting the magnitude of the problem and investing in education programs for women in cybersecurity. This is an area of strength in Saudi Arabia with demonstrated leadership. As Mr. Shoaib Yousuf emphasized, "I never thought about [women in cybersecurity] because nobody pressured or asked me to think about it. It was under the patronage of His Royal Highness the Crown Prince, he was the one who actually thought about it, and started directly at the kingdom leadership level that we need to have women empowerment." ■

"What we need to do is partner with HR. This is really important. When people say we don't find the women, they're not looking hard enough."

Monique Morrow

Move Fast and Break Things

| **Oliver Tavakoli** Global CTO, **Vectra AI**
| **Peter Sund** CEO, **Finnish Information Security Cluster**
| **Seena Amidi** Managing Director of EMEA and Board Member, **Plug and Play**
| **Basmah M. Aljedia** (Moderator) – General Manager, Cybersecurity Industry & Local Content Development, National Cybersecurity Authority, Saudi Arabia

Panelists discussed that as one of the fastest growing sectors in terms of cybersecurity, venture capital firms are placing their investments in the cyber defenses of tomorrow. The cybersecurity market is constantly innovating because of the adversarial nature of the threat. For this reason, venture capital firms are continuously seeking out entrepreneurial actors who may best adapt to the evolving threat landscape.

Panelists noted that successful entrepreneurs are recognized as the exception. While there is a clear need for innovation and business development in the cyber domain, investments across sectors are down. Still, strong interest exists in cybersecurity investments in particular due to regulators alerting all companies to the broad need

$2

trillion – market opportunity for cybersecurity technology and service providers

(Source: McKinsey)





for development in this space - innovators must be able to meet this continuous demand. As noted by Oliver Tavakoli, "the cybersecurity market is always going to have to innovate because we're effectively in an adversarial game. So, unlike most things, you can't simply say we're going to do 10 years of cybersecurity and then be done with it. Our adversaries constantly are changing the game, [and so] we are constantly changing our attack surface by adopting new technologies."

In conclusion, panelists noted that a crucial challenge moving forward will be bridging the gap between cybersecurity talent and the business world in terms of inspiring entrepreneurship. In order to further strengthen the global cybersecurity market, it is important to encourage talented engineers to develop business ideas that can in turn become profitable. Engineers must consider the customer problem that they will solve and be inspired to take the steps necessary to solve it. ■

"Bringing confidence for the future is important, it was wisely said that you don't know what next year will bring. By understanding that it's not only about adapting but shaping the business environment, together we can leverage the power of the many. We want to think carefully of what role data must play and what future we want to envisage."

Peter Sund

The Race for Quantum Supremacy

Powered in Collaboration with ITU

Visa Vallivaara Senior Scientist, **VTT Research Centre of Finland**
Charles Lim Global Head of Quantum Communications and Cryptography, **JPMorgan Chase & Co**
Simon Sinisha Patkovic VP Quantum Safe Solutions, **IDQuantique**
Bilel Jamoussi Chief of the Study Groups Department, **ITU Standardization Bureau (TSB)**
Chris Fox (Moderator) – Presenter, BBC

Panelists discussed the power of quantum computing, which represents a revolutionary new age in the development and innovation of computing technology. With this comes a remarkable range of benefits – including the power to instantaneously process data that would take years to process with a traditional computer. However, it also poses a number of risks, particularly for actors in the cybersecurity domain.

Panelists agreed that progress is already being made in international collaboration on the issue. Standards are an important aspect of innovation as they frame discussions and offer a safe platform for all stakeholders to share best practice and work to solve common problems. Some of these efforts are facilitated by ITU, hosting workshops, webinars and training. Mr. Bilel Jamoussi emphasized,

"The scientific breakthroughs are so vast that quantum computing in a way goes beyond commercial domain and starts becoming a geostrategic and geopolitical item, whereby the countries are looking for a quantum computer to help them reset the geopolitical map of the world."

Simon Sinisha Patkovic





"Standards offer a safe ground or a platform for all the stakeholders to come together and share their best practice or their solutions towards a common problem. In the case of ITU over the past couple of years, we had more than 300 individual experts from 180 different organizations and 43 different countries come to our study groups to develop protocols on quantum technology."

In conclusion, panelists agreed that migration and security will be major challenges for the transition towards quantum computing. Quantum computers have the ability to crack existing encryption algorithms, so heightened security in the quantum age becomes imperative. Potential security measures include quantum key distribution, which encrypts algorithms using the physical properties of photons. Without the technology of quantum key distribution, data stored in data centers could be vulnerable for quantum computers to attack. Migration will also be a challenge, as learning new systems is time-consuming and complex. ■

"Standards offer a safe ground or a platform for all the stakeholders to come together and share their best practice or their solutions towards a common problem. In the case of ITU over the past couple of years, we had more than 300 individual experts from 180 different organizations and 43 different countries come to our study groups to develop protocols on quantum technology."

Bilel Jamoussi

Fierce Competition

| **Flavio Aggio** Chief Information Security Officer (CISO), **World Health Organization (WHO)**
| **Adrian Victor** General Director, **National Institute for Research and Development in Informatics - ICI**, Bucharest
| **George Patsis** CEO, **Obrela Security Industries**
| **Sasha Qadri** (Moderator) – Journalist



Panelists noted that the cybersecurity talent market is facing a critical issue: supply is not meeting demand. The problem is two-fold, entities are seeking to hire cybersecurity engineers with expertise and experience for specific positions, but crucially need to increase and expedite the volume of recruitment due to the continuous increase in demand. Governments, IGOs, and NGOs face a challenge in their own recruitment as they cannot afford to compete with salaries that the private sector provides to attract talent.

Panelists agreed that candidates must have passion, energy, and integrity to be successful, but more importantly they must match the culture of the hiring entity to ensure retention. As Mr. Flavio Aggio highlighted, "I think the most important element for me is the flexibility, the soft skills, the communication skills, the people skills from cybersecurity professionals, the techniques you can teach or you can acquire, but it is much more important to have talents that really care

"Talent is what differentiates your product with others. And when you make the right choices, your product becomes the best, sooner or later. So talent acquisition and talent retention are the most important objectives for any CEO's business plan."

George Patsis



about the organization and understand the culture." There is an extra emphasis on hiring engineers with strong soft skills and leadership potential. To attract candidates, organizations must ensure the job description matches with individuals' competencies. For example, those with strong soft skills must be aligned to managerial or client-facing roles that match this skill set.

In conclusion, panelists agreed that moving forward, cybersecurity organizations will be able to leverage technology to aid the talent shortfall, although organizations should be aware of the risks evident when replacing humans with automation. Organizations may also look towards relevant IGOs to provide training and support. If necessary, organizations can buy services or leverage outside consultants for personnel support. ■

"I think the most important element for me is the flexibility, the soft skills, the communication skills, the people skills from cybersecurity professionals, the techniques you can teach or you can acquire, but it is much more important to have talents that really care about the organization and understand the culture."

Flavio Aggio

21%

Longer to fill cybersecurity roles than other IT roles in the US

(Source: Cyber Seek)

Geo-Technological Competition and Conflict

Powered in Collaboration with ORF

Dr. Beyza Unal Head of Science, Technology and International Security Unit, **UN Office for Disarmament Affairs (UNODA),** New York

Sunjoy Joshi Chairman and Chief Executive, **The Observer Research Foundation (ORF),** New Delhi

Ramia Farrage (Moderator) – Senior Presenter and Producer, Forbes Middle East

Panelists discussed how the current digital revolution has ushered in a new age of competition between government and research and development in the private sector. New questions have arisen regarding the proper level of regulation needed to support innovation. Governments must contend with the rising importance of private sector actors in the field of tech innovation and strike a balance to maintain their own control over national activity.



"Many times states are basically trying to manage the unintended consequences of many of the actions which these private actors have taken. So things have already spun out of control. That is where the real threat to state sovereignty really comes, when the state is an artifact."

Dr. Beyza Unal



Panelists agreed that developments of the digital revolution that governments and private sector actors need to prepare for include quantum computing, blockchain and digital currencies, and biotechnology. These developments present potential points of conflict between the state and society surrounding data security and citizen privacy.

In conclusion, panelists noted that the future of tech governance requires anticipatory governance, multi-stakeholder engagement, and enhanced regulations and controls. Mr. Sunjoy Joshi emphasized the growing threats of competition between the "three P's," the planet, people, and prosperity. Mr. Joshi emphasized, "They do not work in alignment, whether states address them with a cooperative system, or even individuals make choices which affect planet, people, and prosperity. The choices are always queued. The choices are political." Governments must instead work across sectors and borders to ensure cooperation and preparedness. An additional focus on governance through international forums like the United Nations can assist in ensuring increased cooperation between all relevant actors. ■

"They do not work in alignment, whether states address them with a cooperative system, or even individuals make choices which affect planet, people, and prosperity."

Sunjoy Joshi

Rethinking the Global Cyber Order, Why? (2/2)

Ian Goldin Professor of Globalization and Development, **University of Oxford**
Andreas Ekstrom Award Winning **Journalist, Author, and Digital Futurist**
John Defterios (Moderator) – Former CNN Emerging Markets Editor & Professor of Business, NYU Abu Dhabi



$812k
average ransomware payout in Q1 2022
(Source: Sophos)

The opening session of day two of the GCF saw Ian Goldin and Andreas Ekstrom address two of the five Forum sub-themes – Cyber Economics and the Future of Cyber Work. The panelists discussed that in an age of hyper globalization, states must find new pathways for multilateral engagement in the cyber domain to get to the heart of the potential of cyber commerce, to control cyber threats, and to train the workforce of the future. As the number of attacks has increased exponentially in recent months, states must take swift action to protect critical vulnerabilities.

Panelists agreed that society cannot overlook the human element of cyber issues, from unknowing individuals opening phishing emails to

"I will always take diplomacy over war, I will always take culture over ignorance. I will always take a conversation rather than a shout. So we need to look at the best sides of ourselves to build the world we truly want to live in."

Andreas Ekstrom



companies hiring the top cybersecurity talent. In addition, countries and organizations must collaborate to protect critical infrastructure in an age of increased digitalization. Ian Goldin noted, "Globalization also has effects on cyber rules and the global cyber order. There must be a mutual understanding and respect of each other's rules, such that states can understand the differences and can work across them." While total global harmony in the cyber domain may be an unrealistic dream, increased mutual cooperation is increasingly realistic and something states must focus on working towards.

In conclusion, panelists noted that this process requires increased investments in the sector, partnerships between public and private sector entities, and slow but steady progress. Governments must consider engaging in continuous discussions and continuous educational efforts to move forward with collective security goals. Additionally, states are falling behind the curve in the amount of money invested in cybersecurity, to be prepared for the next major attack, increased investments in resources and capabilities are needed rapidly. ■

"Our health systems, including our interactions with our bodies, have become more digitalized. It will percolate through every aspect of our lives. You don't want someone to hack into your body. You don't want someone to hack into your bank account. You don't want to hack into your water supply or energy supply or anything else. Everything becomes vitally important to be protected, and predictable. It's a huge opportunity [for collective action]."

Ian Goldin

Shaping Markets

- **Dr. Mohamed Al Kuwaiti** Head of **Cyber Security, United Arab Emirates Government**
- **Paul Griswold** Chief Product Officer, Cybersecurity, **Honeywell**
- **Francois Candelon** Managing Director and Senior Partner, **BCG Henderson Institute**
- **Fabien Rech** Senior Vice President EMEA, **Trellix**
- **Rebecca McLaughlin-Eastham** (Moderator) – TV Anchor & MD, RME Media

Panelists discussed that innovation in the cyber domain is largely driven by customer needs and the threats that customers and clients are facing. The reactive nature of the current cyber market will pose significant challenges as cyber threats continue to evolve. Governments and the private sector must develop new ways to work more closely and effectively together to advance the future of the cyber order.

Panelists agreed that critical issues plaguing the current cyber market include a lack of talent diversity, a lack of resources, and a restricted flow of information between private sector actors and governments. In order to attract talent and achieve greater diversity, the cybersecurity sector must change public perceptions of cyber defenders or cybersecurity professionals. Instead of being seen as a



"It's not only partnering, it's not only exchanging information, it's the hand-in-hand, shoulder-to-shoulder working on many of [those issues] from an operational perspective as well as from a technical perspective."

Dr. Mohamed Al Kuwaiti



less attractive field of work, cyber defenders should be viewed as 'fire fighters' of cyber threats.

Additionally, governments must focus on investing in resources necessary to protect critical national infrastructure. And to encourage greater information exchange, governments and civil society must strengthen public-private partnerships through multilateral platforms, allowing proactive two-way communication.

In conclusion, panelists emphasized that partnerships and education should be a top priority for governments. As emphasized by Dr. Mohamed Al Kuwaiti, "It's not only partnering, it's not only exchanging information, it's the hand-in-hand, shoulder-to-shoulder working on many of [those issues] from an operational perspective as well as from a technical perspective." Partnerships must include multilateral discussion and exchange of information, but must also involve hands-on collaboration between governments, international organizations, and the private sector to work towards solutions. As Mr. Francois Candelon highlighted, "I think maybe it's just a dream, but I feel that as we're playing cops and robbers, if we are not able to collectively sit together and to find standards, it will become very complex to deal with all the new threats that we are facing." Enhanced cybersecurity education will also encourage a culture of awareness and inspire the next generation of cyber talent. ■

"I think maybe it's just a dream, but I feel that as we're playing cops and robbers, if we are not able to collectively sit together and to find standards, it will become very complex to deal with all the new threats that we are facing."

Francois Candelon

Pervasive and Insecure

- **Mary O'Brien** General Manager, **IBM Security**
- **Ben Miller** Vice President of Services, **Dragos Inc.**
- **Victoria Coates** Senior Fellow for International Relations and National Security, **The Heritage Foundation**
- **Lothar Renner** Managing Director, **Cisco Security, EMEA**
- **Dr. Albert Antwi-Boasiako** Ag. Director-General, **Cyber Security Authority,** Republic of Ghana
- **Sasha Qadri** (Moderator) – Journalist



Panelists discussed as adversaries become more creative with the timing and locations of cyberattacks, tracking and monitoring security capabilities and preparedness levels is critical. Many organizations put too much trust in their current equipment and personnel, leaving gaps for attackers to exploit. Complacency and human error continue to present the greatest threat for governments and corporations in the current cybersecurity risk landscape.

Panelists noted that outdated equipment and complex supply chains are two key elements which leave corporations and governments vulnerable targets. Many entities, particularly in industrial settings, continue to use outdated hardware and software that provides

"It's not unusual for some of our customers to have equipment that was, you know, built 50 years ago, and it's working. But it's working and running on outdated obsolete operations and on patchable operating systems."

Mary O'Brien



weak defenses. Mary O'Brien noted, "It's not unusual for some of our customers to have equipment that was, you know, built 50 years ago, and it's working. But it's working and running on outdated obsolete operations and on patchable operating systems." Entities must keep stock of their equipment and have better awareness of when it is time to proactively begin replacing old equipment to increase protection. Supply chains present an additional challenge, as hostile actors have increasingly targeted smaller suppliers with less sophisticated cybersecurity systems. This weaponization of supply chains has the potential to create a chain reaction, disrupting global production and the potential to cost billions of dollars in damages.

In conclusion, panelists agreed that governments and corporations must consider zero-trust as both a critical tool and mindset about cybersecurity. Organizations should consider a zero-trust paradigm, wherein they assume they are constantly being breached and internal and external actors are consistently verified. This mindset is increasingly necessary as threats continue to evolve. ■

"You can have huge defenses around your business and the supply chain and have all kinds of sophisticated means of looking to block and tackle. But what we've learned is that there's always a way in and the adversary will get in. So, it's important to have the capability to actually track what the adversary is doing."

Lothar Renner

Cybersecurity at the Heart of the Next Gen Telco

| **Bocar Alpha BA.** CEO & Board Member, **SAMENA Telecommunications Council FZ LLC**
| **Jabiri Kuwe Bakari** Director General, **Tanzania Communications Regulatory Authority**
| **Konstantinos Masselos** President, **Hellenic Telecommunications & Post Commission (EETT)**
| **Chris Fox** (Moderator) – Television Presenter, BBC



Panelists discussed that traditional telcos face unique hurdles in adapting to the challenges of tomorrow. Telcos must adapt to becoming public-facing cybersecurity organizations, particularly considering developments in 5G network rollouts. In this regard, next generation telcos must have the most advanced cybersecurity capabilities across industries and sectors.

Panelists identified critical issues on the path to 5G network implementation, including data safety, regulation and consumer protection. Network implementation is complicated by companies in different countries having vastly different security standards. Introducing comprehensive implementation standards may help to ensure heightened security in an increasingly digitalized world. As Konstantinos Masselos emphasized, "The most critical point is to have universal standards and certification schemes. So equipment that complies with standards and certification schemes is qualified to be used in our network, and in turn this will allow us to use equipment from different vendors from different countries."



In conclusion, panelists agreed that governments and telcos may consider closer cooperation to implement widespread cybersecurity standards for 5G network implementation. With a wide range of regulators and member states involved, reaching a consensus is a major challenge but simultaneously presents the greatest opportunity for progress moving forward. Another opportunity for future cooperation involves pushing the frontier of cybersecurity into outer space, with greater coordination over satellite operations. Bocar Ba noted, "In terms of technological innovation, our possibilities are limitless. Next year at the GCF what we may have to look at is the convergence of two businesses, the business as we know it today and the [space economy]." Telcos must be prepared to push forward progress on each of these fronts to adapt to the shifting cybersecurity landscape. ■

2.7

billion – number of people globally that are still not connected to the internet

(Source: United Nations, 2022)

AI for Child Protection

Powered in Collaboration with WeProtect GLOBAL ALLIANCE

Irakli Beridze Head, Centre for Artificial Intelligence and Robotics, **UNICRI, United Nations**
Yalda Aoukar Co-founder and Managing Partner, **Bracket Capital**
Lt. Col. Dana Humaid Director General, International Affairs Bureau, **Ministry of Interior,** United Arab Emirates
Laura Taddei Director of Business Affairs , **BenevolentAI**
Iain Drennan (Moderator) – Executive Director, WeProtect Global Alliance



Panelists discussed that as more people of all ages gain access to the internet each year, issues of security and privacy, abuse, and exploitation become prevalent. As Yalda Aoukar emphasized, "These platforms where children and adults are mixing in a predominantly unmoderated environment are really hunting grounds for predators." Artificial intelligence (AI) represents one key technology that may be used to fight child sexual abuse online. Most of the time, resources are scarce when it comes to AI investment. However, education and training programs, as well as multi-stakeholder collaboration provide avenues for increased AI application in protecting vulnerable populations online.

Panelists agreed that while child safety online is a significant challenge of the digital age, there is reason to be encouraged with recent developments. States have increasingly engaged in multi-stakeholder collaboration and partnership on the safety of AI application online. The Global Partnership on AI is one avenue for

"Artificial intelligence is not a silver bullet. Obviously it is not going to solve all problems. The silver bullet is all of you here. The silver bullet is the multi stakeholder collaboration. It's for all of us to contribute into finding the solution."

Irakli Beridze



cooperation between states and the private sector. AI initiatives provide a common framework for protection while simultaneously allowing for adequate human oversight.

In conclusion, panelists agreed that governments can work to enshrine in law AI rights for children alongside international regulations that are both flexible enough to integrate new digital threats and agile enough to fight the current threats of today. Governments may seek to establish legislation for safety by design protocols for video games and mobile applications. AI can be a force for good in the fight to protect children online, but it can also present its own dangers. Countries can be more proactive in their efforts to regulate the application of AI for internet safety. ■

24%

of video gamers are under the age of 18 in the USA

(Source: Statista, 2022)

Shaping the Global Cybersecurity Agenda

Powered in Collaboration with ITU

Marco Obiso Chief, AI Digital Networks and Society Department, **International Telecommunication Union (ITU)**
Vanessa Copetti Cravo Telecommunication Regulation Expert, Cybersecurity Technical Group, **ANATEL**
Howard Taylor Executive Director, **Global Partnerships to End Violence Against Children**
Andrea Rigoni (Moderator) Senior Partner, EU Digital Policy Director, Deloitte Risk Advisor

Panelists discussed the interconnected and borderless nature of Cyberspace and the unique and pervasive challenges countries are experiencing in developing regulations and managing the emergence and spread of harmful and untested technologies. We are in the era of "Global Technology", where technologies are not limited or controlled by one country or region and are available for everyone to access and use, for better or worse - and this includes children. More children are increasingly unsupervised online without clear guidance from parents and guardians and are operating in an environment developed for adults and are put in situations where their safety and protection may be compromised. The ecosystem needs to work together to change this and create a safer Cyberspace for children.

Panelists addressed the multiple challenges governments, communities, and the private sector are facing in their drive to protect children online. The first challenge is centered around the collection and dissemination of data and evidence to enhance research capabilities and bring perpetrators to justice. The second challenge is a top-down commitment of leadership across the ecosystem, from government, the private sector,

"This [child sexual abuse online] is a problem, which goes across borders quite often ... the victim is in one country, the perpetrator is in a second, the material is hosted in the cloud or on a platform in the third, and there could be a fourth or a fifth jurisdiction, so that's why we need this international engagement."

Howard Taylor









policy makers, regulators, and technology companies. Strongly committed leaders can help take actions and create the sense of urgency around the issues of child online protection that is clearly missing at the moment.

In conclusion, panelists agreed that as we move ahead governments and the private sector need to become active in this battle. The Cyberspace ecosystem, especially governments, need to consider children as critical national infrastructure and develop strategies, policies, regulations, and awareness initiatives through a holistic child lens. Governments also need to work with the private sector for a whole-of-ecosystem approach. Vanessa Copetti Cravo noted, "You need concrete action on the ground. It is a call for action. You know we cannot go another year saying it's important. We all agree we have to protect children; they are our most valuable asset." As a first step, all stakeholders need to join existing global platforms and alliances striving to protect children in Cyberspace as only through global cooperation can the internet become safe for children. ■

Mind the Gap

Powered in Collaboration with BCG

- **Olga Botero** Co-Founder and Chair, **Seccuri Inc**
- **Juliette Wilcox CMG** UK Cyber Security Ambassador, **His Majesty's Government** (UK Government)
- **Anamaria Meshkurti** Head of Marketing, Communication and Engagement, **Fongit**
- **Stefan Deutscher** (Moderator) – Partner and Associate Director, Cyber Security and IT Infrastructure, BCG

Panelists discussed that while the demand for skilled cybersecurity talent is growing globally, only 25 percent of the current workforce is female. The gender gap in the cybersecurity workforce is exacerbated by women earning on average 20 percent less for the same roles as their male peers (Infosecurity Magazine).

Panelists noted that the hurdles which prevent women considering cybersecurity as a career includes the negative media representation of cybersecurity experts. The emphasis on the negative or hostile aspects of the cyber professional as "up to no good" also can discourage women from entering the field. " Additionally, the media fail to highlight women making immense progress in the sector, which deprives young girls of positive role models to look up to. Additionally, the perception of young students and professionals is that cybersecurity is an extremely technical field with limited application of soft skills or non-technical degrees, further discouraging young people from entering the field or seeking a job.



"When you close your eyes and you think of a CEO, of a coder, of an engineer, do you see a man, or do you see a woman? I always saw men for a long time, so this is the normal for me. Normalizing is that when we start to see as many women as men when we say the words coder, programmer, engineer. And this of course starts at home, starts at school, when we are being formed in the beginning years of our life, but also in the media."

Anamaria Meshkurti





25%

cybersecurity jobs held by women

(Source: Cybersecurity Ventures, 2021)

In conclusion, panelists emphasized that governments, private sector, and the media need to create opportunities for and work toward encouraging girls to pursue a career in Cyberspace. The media needs to highlight the positive aspects of Cyberspace and identify and market female role models in the industry, while also creating awareness of the various non-technical jobs and pathways in the sector. A key area of focus for governments and the private sector is the development of platforms, events, and programs which enable young students to connect with and network with professionals who can support them as mentors. Lastly, on an ecosystem level, there is a need to remove the challenges that women face in the profession. A strong focus on retention through initiatives around flexible working hours and opportunities to return to the profession after a break can prove instrumental. ■

Hacking the Mind of a Cybercriminal

| **Mary Aiken** Professor of Cyberpsychology and Chair of the Department of Cyberpsychology , **Capitol Technology University**
| **Marco Gercke** (Moderator) – Director, Cybercrime Research Institute

Mary Aiken highlighted that cyber behavioral science adds a new dimension to tackling cybercrime. In order to have full coverage of resilience and response mechanisms, law enforcement officials and private entities must combine the technical aspects of cybersecurity with the behavioral aspects of criminality. A deeper understanding of how individuals function online will allow for the creation of more effective prevention and protection strategies. In particular, the behavior of children online must be an area of greater focus for governments and the private sector. Aiken noted, "We are letting our children go online, a huge number every day around the world and often for the first time in this environment, which was built for adults, it was not built for children. It is unsafe for children, and we are just letting that happen... We need a sense of outrage about this."



To apply behavioral science most effectively to the shifting cyber landscape, Aiken highlighted that it is crucial to understand the various personality traits and differing actions of individuals online. To prevent risk-taking action from children in particular, law enforcement agents may consider looking within their jurisdiction to understand how



young people are growing up and living in Cyberspace. Aiken noted, "We want our young people with their incredible tech skills to head into a career in cybersecurity or cyberpsychology, to look towards Vision 2030 and make a fantastic contribution to that. But if they get sidetracked into delinquent behavior or risk taking or exposing themselves to extreme content, they may damage themselves in a way that they will not fully participate in their career." As human behavior can change once online, awareness of individual actions will help prevent a pathway to criminal behavior and instead inspire young people to be a force for good. Additionally, in the case of ongoing criminality, law enforcement officials can use individuals' personality traits to stage a more effective intervention. In this case, strategies will depend upon the relevant traits of the criminal. A functioning psychopath may respond to emotional effects differently from another individual, so the method of intervention will have to change.

In conclusion, Aiken emphasized that entities must consider the growing threat of ransomware being provided as a black-market service. Ransomware, like other forms of criminality, has lowered the barrier of entry to cybercrime. Individuals that do not have advanced tech skills can still hire other criminals from the internet and create real-world threats and consequences. Law enforcement agencies around the world must be prepared to prevent and control these new threats. ■

"We have to be positive about the future. We have to be positive about tech. You know, technology in itself is neither good nor bad. It is either used well or poorly by humans."

Mary Aiken

FinTech: Catalysts for Transformation

| **Issam Abousleiman** Regional GCC Director, **World Bank**
| **Martin Boer** Senior Director, Regulatory Affairs, **Institute of International Finance (IIF),** Washington
| **Sasha Qadri** (Moderator) – Journalist

Panelists discussed the issue of the financial services sector being one of the most cyber attacked sectors globally. As country and company borders are increasingly blurred with the rise of global fintech services, adversaries are using new tools to attack personal data and assets.

Panelists emphasized that fintech services are rapidly evolving and driving financial innovation. In such a transforming sector, entities must be alert to cybercriminal activity impacting both codes and physical infrastructure. Steps must be taken proactively and with global cooperation to protect vulnerable services. Even as the financial industry is largely based on trust, entities must still adopt a zero-trust mentality both internally and externally to effectively prevent threats. As Issam Abousleiman emphasized, "The important part of zero trust is actually meaning that you have to have 100% trust in people, systems, and protocols necessary to make it happen.

"Financial inclusion, the idea of giving people access and their own authority to be able to take their own financial services under their own control has been really important. But on the flip side, when you give people all these new tools, it also creates cyber hazards. It makes a broader cyber vector that the adversaries can attack and breach."

Martin Boer





Zero trust is probably misleading." Additionally, governments have an important role to play in enhancing regulations and encouraging higher standards of cybersecurity protection for fintech firms. Likewise, they must work with firms to establish clearer definitions of terms like "cyber incidents" to apply more uniform response mechanisms.

In conclusion, panelists agreed that Fintech firms can work to strengthen the relationship between themselves and third-party vendors in order to enhance resilience across the board. Martin Boer noted, "It's still really important to do your due diligence to have constant communication back and forth. Because if you're offshoring your risk, your customer data, your internal processes, or your money, then you want to make sure that it's secure." As fintech firms are only as strong as the weakest link in the global digital bank transaction chain, one attack could disrupt activity for many firms, causing financial ruin. Increased cooperation to reduce financial stability risk should be a top priority of fintech firms and governments in the future. ■

Trust in Emergent Technologies

Amandeep Singh Gill **United Nations Secretary General Envoy on Technology**

Rudolph Lohmeyer (Moderator) – Partner, Kearney



Amandeep Singh Gill noted that due to the divided nature of the world today, we see different sets of technologies being developed globally giving rise to a diverse landscape of emerging technologies. Within this landscape, a small subset of technologies will undoubtedly be more decisive for the future compared to others. Technologies such as artificial intelligence, big data, et cetera are likely to have a lasting impact on society.

Gill emphasized that these emerging technologies have two sides. On one hand, they can help realize our potential as a society through the acceleration of the achievement of the Sustainable Development Goals (SDGs), "New technologies will come and they will be disruptive... So, we need a touchstone, we need some kind of a guiding light that helps us navigate this uncertain future... There is the SDGs, that should be our guiding light." On the other hand, they are giving rise to

"I think we need more public goods, digital public infrastructure, digital public goods, that kind of level the opportunity for entrepreneurs of all sizes. Level the opportunity for the wider public to benefit from the digital transformation, to access government services at low cost and more equitably."

Amandeep Singh Gill



a myriad of regulatory challenges in Cyberspace. There are still gray areas around the norms and rules of Cyberspace and a lack of global consensus on the applicability of international laws, particularly around attribution, and protection of critical civilian infrastructure. This lack of clarity in Cyberspace, accentuated by emerging technologies, has created a pressing need for collaboration and for working toward narrowing the digital divide. In particular there is a critical human element to increasing cooperation in the domain. Amandeep added, "Technology is not the answer to every problem that we have. It is an enabler and we need to continue to do the hard work on bringing people together... in a nice, human centered way."

In concluding the conversation, Gill emphasized that as a first step to narrowing the divide, there is a need to build digital public infrastructure, and create digital public goods to ensure no one is left behind. Additionally, to better manage emerging technologies, a focus on the societal implications and governance of these technologies right from their inception, design, and R&D stages is needed. At the global level, there is a critical need for multilateral cooperation and opportunities to come together and address the challenges around technology. One such opportunity is the Summit of the Future, which will be held in 2024 and will provide global leaders an opportunity to address issues such as climate change, international peace and security, and emerging technologies. ■

The Security of Algorithms

| **Dr. Kashif Kifayat** Chairman, **National Centre of Cybersecurity,** Pakistan
| **Preetam Maloor** Head of Emerging Technologies Division, **International Telecommunications Union (ITU)**
| **Piotr Ciepiela** Partner, Global Cyber Architecture, Engineering & Emerging Technologies Leader, **EY**
| **Chris Fox** (Moderator) – Technology Presenter, BBC



Panelists discussed computer algorithms being an integral part of our daily lives, from influencing what we see on social media to informing the design of our cities and infrastructure - all the algorithms informing our decisions are built using data.

The panel stressed that multiple challenges have surfaced in the development and use of algorithms and the data on which they are based. At the top of this list is data integrity, data illusion, and data security. It is no surprise that when an algorithm is provided with poisoned data, all results become unreliable and sometimes may cause harm in the real world. Another challenge is the historical lack of understanding and concern for security during the developmental stage of most algorithms in use today. Dr. Kashif Kifayat emphasized the root of most security concerns, noting, "When we were developing computer networks and the internet, they never thought security was the problem. So then they developed all these algorithms and security was not embedded in them... so it's very hard actually to fix this problem. They're trying to fix it every day and they are creating more vulnerabilities."



In conclusion, panelists agreed that to overcome these challenges, a first step is to train developers to focus on security by design. Developers need to fully understand and account for the vulnerabilities they may inadvertently create during the initial design stage of the algorithms. For governments, there is a need to better regulate emerging technologies by involving innovators, policymakers, and all stakeholders in the ecosystem during the development of regulations. As Preetam Maloor emphasized, "We're going to leverage the expertise in these groups to help build these resources for AI readiness. So this is going to be our first big step in helping these numbers add up." Governments need to establish a baseline level of control over algorithms and ensure regulators have access to the algorithms and AI being used by the public particularly through social media platforms. For the private sector, there is a need to renew the emphasis on data security and establish strict controls over data integrity. Technology companies and entrepreneurs also need to ensure that the data being used to develop algorithms is a representative sample to ensure reliable decision making. Lastly, there is a need to leverage the benefits AI has to offer. The whole cybersecurity ecosystem must actively embed algorithms and AI in their defenses as this can significantly improve threat detection and prevention capabilities. ■

"When we were developing computer networks and the internet, they never thought security was the problem. So then they developed all these algorithms and security was not embedded in them... so it's very hard actually to fix this problem. They're trying to fix it every day and they are creating more vulnerabilities."

Dr. Kashif Kifayat

Post Quantum Cryptography

Powered in Collaboration with ETRI

| **Sang-Yoon Chang** Associate Professor, **University of Colorado**, Colorado Springs
| **Sylvain Guilley** General Manager and CTO, **Secure-IC**
| **Dr. Godfrey Gaston,** Cybersecurity Innovation Consultant
| **Kim Ik Kyun** Assistant Vice President, Cyber Security Research Division, **Electronics and Telecommunications Research Institute (ETRI),** Korea
| **Sasha Qadri** (Moderator) – Journalist

In the discussion panelists noted that with the anticipated development of quantum computers in the coming decades, post-quantum protection will soon be an expected standard, not just an idea. Quantum computers will have the power to attack systems that are considered untouchable in the present-day and it is not too early to start planning for the age of quantum computing.

Panelists agreed that while no quantum computer exists today that can create - or solve - this problem, preparedness is a necessity as protocols must begin to transition to this new computing standard. For example, important information and data that exists today and may be considered safe in current conditions can be invaded once quantum computers exist. Organizations need to take steps now to protect this data before it is too late.

"I think we're pretty clear that this is going to be an area where there's going to be billions spent. If you're entrepreneurially minded, if you're thinking in that sort of area, if you're looking to invest, I think finding companies or finding new research institutes, universities, and people who have expertise in this area, I think this this has got to be absolutely key."

Godfrey Gaston





In conclusion, panelists stressed that companies must also be prepared with expertise in this area. Post quantum cryptography represents a clear market for security issues but also for business opportunities for highly skilled cryptographers. Due to the highly technical nature of quantum cryptography, potential hires must be experts, which presents challenges for companies looking to increase protection. As Sang-Yoon Chang noted, "The first thing I would do is hire somebody, to get that expertise to prepare for the post quantum era. I would hire an applied cryptographer that can actually not only understand the ciphers, but also help with the implementation and integration of the system." Private sector actors must be prepared to align on specific standards. As organizations like the National Institute for Standards and Technology (NIST) begin work today on models for post quantum standardization, it is the responsibility of private sector entities to gain familiarity with these models and start to develop a plan. ■

Metrics for Success

Powered in Collaboration with DQInstitute

Global Standards for Digital Intelligence

Dr. Yuhyun Park Founder, **DQ Institute**
Mark Zelman Consultant, **World Bank**
Sri Chandrasekaran Senior Director, **IEEE Standards Association**
Chris Fox (Moderator) – Technology Presenter, BBC



In the discussion panelists agreed that in an environment where more children gain internet access each day, not enough is being done on the national or international level when it comes to awareness or protection mechanisms. DQ Institute's 2022 Child Online Safety Index (COSI), released at GCF, notes that the international community currently lacks the infrastructure necessary to ensure that children can be safe and prosper online.

Speakers highlighted that there are a number of critical missing links when it comes to protecting children online. First, there is a lack of collaboration and coordination on the specific issue from governments and ICT corporations in particular. Due to this lack of cooperation, there is no universal agreement yet on what safety for children online should even look like.

Second, public awareness is lacking. Parents are susceptible to thinking their child is the exception and is always behaving safely online. However, as statistics

DQ Institute reveals results of 2022 Child Online Safety Index



73%

– percentage of children that have experienced a cyber risk, according to the DQ Institute 2022 Child Online Safety Index

(Source: DQ Institute)

"A lot of parents gave their power over to technology because they feel like they don't know about technology or their kids know better. But if you think about it, social media is a recent development. If you're new, children are new to this technology, too. So don't give up and don't give the power over to technology."

Dr. Yuhyun Park

show, protecting children online is everyone's problem. ICT companies need to ramp up their efforts to protect young people online but so do individuals and families. Lack of awareness of negative behavior cannot remain an excuse. Finally, there is an urgent need for more assessment frameworks for technologies, as entities and governments currently fail to align on even basic standards such as the age of a "child" online. As Sri Chandrasekaran noted, "Once we have these measures in place, where there's a standard, there's assessment frameworks, the indexes are properly defined, there might still be some variation between our region's adoption, but the standards will be flexible enough to do that. Then for people to accept the technology, whether as a parent or as a regulator or as a government body, it becomes much easier."

In conclusion, panelists agreed that ICT corporations and families must begin to think of the digital environment through the lens of a traditional "net-zero" environmental mentality. By treating cyber activity like sustainability, achieving net-zero cybercrime becomes a whole-of-society goal to rally behind. Governments must play a key role in establishing regulations to encourage safety by design principles with companies and must also increase efforts to educate children and their parents on the risks of increased connectivity and best practices for their safety online. ■

"Whole of Society" Cyber Awareness

Powered in Collaboration with unitar United Nations Institute for Training and Research

- **Esa Alsumiri** Member of the **Saudi Shura Council**
- **Alex Mejia** Director, Division for People and Social Inclusion, **United Nations Institute for Training and Research (UNITAR)**
- **Nadezhda Neynsky** Former Foreign Minister of Bulgaria, Former Ambassador to Turkey, Member of 2022 Cohort of Advanced Leadership Initiative (ALI), Harvard
- **Rebecca McLaughlin-Eastham** (Moderator) – TV Anchor and Managing Director, RME Media



Panelists discussed how the pandemic had accelerated a shift online which has exacerbated challenges in the cybersecurity ecosystem with an unprecedented increase in cyberattacks and ransomware. As emphasized by Nadezhda Neynsky, "There is no need to throw bombs or to do something more brutal than to use cybersecurity to destabilize the state, because when you face a cyber attack against the railways structure or against the airport structure, this undermines the efforts of the government to assure security for their citizens." The costs of cybersecurity and cybercrime are continuously on the rise. It is no longer just an issue for governments and big corporations, it impacts citizens just as much because the cost of cybercrime is intimately borne by society.

During the discussion, panelists agreed that as a starting point, there is a need to create a "whole of society" awareness about the true costs of cybercrimes. The costs of cybercrimes can be divided into direct

$9.4

million – average cost of a data breach in the US

(Source: IBM, 2022)

$4.35

million – average cost of a data breach globally

(Source: IBM, 2022)



"There is no need to throw bombs or to do something more brutal than to use cybersecurity to destabilize the state, because when you face a cyber attack against the railways structure or against the airport structure, this undermines the efforts of the government to assure security for their citizens."

Nadezhda Neynsky

costs which includes financial losses, data losses, remediation costs, et cetera, and indirect costs which includes reputational damage, client losses, opportunity costs and productivity losses. Only by truly understanding the costs would the imperative for cooperation and collaboration be clear for everyone involved.

In conclusion, panelists noted that collaboration and cooperation in cyberspace can be best achieved through multilateral platforms. There is a need for states to fully utilize forums such as the UN and GCF. These platforms allow states and stakeholders to raise awareness on cybersecurity issues and ensure government commitments for programs and initiatives such as the Sustainable Development Goals which need to be seen from a cybersecurity and access to technology perspective. Additionally, cooperation at these platforms can also help bridge the rising digital gap by ensuring capability building and knowledge transfer for all participants. ■

Co-Creating the Future of Cyber

| **Purvi Kay** Head of Cyber Security Governance, Risk and Compliance, **BAE Systems PLC**
| **Kevin Emery** Global Director of Cybersecurity, **UL Solutions**
| **Dr. Hazim Almuhimedi** Risk & Compliance Deputy Governor, **National Cybersecurity Authority**, Saudi Arabia
| **Ramia Farrage** (Moderator) – Senior Presenter and Producer, Forbes Middle East



"It's exactly the same transparency, continuous communication and collaboration. Whether government or private sector, we're all aiming for the same goal, right? What we want to do is protect our country, our assets, our people, and economy. So if we can do it together and have that trust and transparency, then we will achieve that goal together."

Purvi Kay

Panelists discussed that neither governments nor tech companies can secure Cyberspace on their own. Private partnership can lead to effective regulations that protect against risk while keeping pace with innovation. Governments and private sector entities must communicate regularly to keep ahead of the next emerging threat.

Panelists agreed that governments may seek to support the creation of specialized entities with a cybersecurity mandate, such as National Cybersecurity Authorities. In this way the mandate of the government (and the newly created entity) is to leverage any existing frameworks

93%

percentage of cyber decision makers that say public private partnerships are vital to national defense, while only 34% believe they're actually effective

(Source: Security Magazine)





for cybersecurity protection, create new ones, and encourage domestic standardization for private sector players. On the flip side, the mandate of the private sector is to hire the best possible engineers and train them to be productive members of the national cybersecurity ecosystem. Both sides must work towards a position of transparent, healthy, and trusted cooperation. Continuous communication is required for a cohesive national prevention and protection strategy.

In conclusion, panelists highlighted that regulators and private sector entities can collaborate on national compliance and technical assessments. By upskilling and utilizing service providers, governments can better understand their cybersecurity capability and identify potential areas of weakness. Dr. Hazim Almuhimedi emphasized, "Service providers for cybersecurity in collaboration with a cybersecurity integrator will help achieve the cybersecurity protection and the minimization of risk that we are hoping to achieve." Clear and transparent information sharing between parties will encourage more effective rapid response and risk management mechanisms. ■

"Service providers for cybersecurity in collaboration with a cybersecurity integrator will help achieve the cybersecurity protection and the minimization of risk that we are hoping to achieve."

Dr. Hazim Almuhimedi

Unleashing the Potential of the Cloud

| **Mark Ryland** Director of the Office of the Chief Information Security Officer, **Amazon Web Services**
| **Abbas Kudrati** APAC Chief Cybersecurity Advisor, **Microsoft**
| **Suliman Alsamhan** Chief Executive Advisor, **SITE**, Saudi Arabia
| **Rawan Radwan** (Moderator) – Deputy Section Head, Arab News

"There's never, you know, unequivocal gain with no loss. But often, the gains outweigh the losses. And I really do think that's true when it comes to cloud technology. There definitely are a few things you need to be concerned about."

Mark Ryland



90%

of companies in US, Canada, and the UK were impacted by ransomware in 2022
(Source: SpyCloud, 2022)

In the session panelists highlighted that the cloud market is growing globally at a rapid pace with providers investing in building their own infrastructure, while at the same time maintaining a commitment to investment in cybersecurity. Cloud technology provides speed and agility to governments and businesses alike as part of their digitalization strategy. While customers retain access to their critical data in the cloud, the lack of physical infrastructure or touchpoints for the customer leads to increased suspicion of data security and privacy.



Panelists emphasized that given its nature, the cloud is particularly susceptible to attack. Incorrect environment configuration can lead to a network invasion and the loss of data. However, the cloud also provides notable strengths that must be leveraged to ensure a more secure cyber society, including speed of data transmission. The cloud itself covers many of the classic security controls that individuals would otherwise need to handle themselves. One such tool, the backup vault block, protects data in an environment where even the most powerful administrator in an organization cannot delete it. Humans must learn to work alongside these tools, yet not rely entirely upon them in the case of a critical cyber threat.

In conclusion, panelists stressed that there can be clearer delineations for responsibility between individuals, the government, and providers. If internet users don't seek to understand roles and responsibilities as a customer and as a provider, the result will be a gray area where the customer assumes that the provider will protect the data, and the provider assumes the customer is taking proactive steps on their own. The governance model and framework for managing the cloud must provide clarity and be designed in a much more secure manner. At the same time, governments must provide education at a citizen level to encourage cloud migration and preparedness. Training is a critical part of these efforts. ■

"...I want to reiterate shared responsibility model. People usually think that when we move data and infrastructure on the cloud, it is the cloud service provider's responsibility. I don't have to worry about security. Yes, Cloud is a new security imperative, but you need to understand the responsibility between the cloud service provider and you as a customer or employee."

Abbas Kudrati

"Today, the cloud provides us with high availability, our ability to move our workloads from one zone to another – to restore these systems in a timely manner. It provides us with better methods to bridge the gaps we have today".

Suliman Alsamhan

Securing Development

| **Mohammed Ben Amor** Secretary General, **Arab ICT Organization**
| **Rodney Taylor** Secretary General, **Caribbean Telecommunications Union**
| **John Omo** Secretary General, **African Telecommunication Union**
| **Masanori Kondo** Secretary General, **Asia-Pacific Telecommunity**
| **Sasha Qadri** (Moderator) – Journalist and Moderator

In the session speakers discussed that Information and Communication Technologies (ICTs) are a critical part of every facet of development from agriculture to health, education to manufacturing. The entire development cycle is interwoven through the development and use of ICTs. This important position makes it necessary to establish sufficient interoperability, security, and trust in ICT systems and services to ensure no aspect of development is compromised. Securing development can be defined as creating sufficient trust and security in ICT systems and services.

Speakers agreed that developing countries with limited resources find it difficult to focus on development of ICT infrastructure and fail to provide opportunities to their citizens in ICT-enabled areas such as education, business, healthcare, et cetera. Even in situations where ICT may be a targeted area for development, countries find it difficult to access funding to invest in ICT infrastructure. Mohammed Ben Amor noted "Until now, if we look to any development institutions or funding institutions, we will not find anyone, anywhere in the word





where cybersecurity is in their plan. So there is a lot of work in order to convince funding institutions to put cybersecurity in [their] priorities." This lack of funding is widening the digital divide globally and even though global institutions where the promotion of ICT development exists, there is still much work to be done.

In conclusion, panelists agreed that as a first step, development institutions must prioritize and underscore the importance of ICTs and by extension cybersecurity in all their programs and projects, while developing countries must focus on the identification and creation of bankable projects. Once developing countries focus on bankable projects, they are more likely to attract financing and grants from financial institutions. It is also the responsibility of developed countries to emphasize cooperation and support developing countries in transfer of knowledge, skills, and capabilities to develop and protect ICT infrastructure. Rodney Taylor noted, "[there is a] shortage in cybersecurity skills, and that shortage is felt most acutely in developing countries... Certainly I would recommend that to address the issue of funding, that perhaps you can first look at international cooperation, technical assistance and so on to help developing countries." Moving forward, the international community can discuss the development of a global cybersecurity fund which can be utilized for cybersecurity and ICT projects in countries with high vulnerabilities or large skills gap. ■

"We in the developing world must also come up with bankable projects, projects that will attract funding, and funding that is sustainable. The projects must themselves be sustainable and have a commercial interest that then attracts lending."

John Omo

Intelligence in Real Time

| **Adrian Colbrook** Strategic Growth Director, **BAE Systems Digital Intelligence**
| **Oliver Väärtnõu** CEO, **Cybernetica**
| **Dr. Christopher Ahlberg** CEO/Co-founder, **Recorded Future Inc.**
| **Dr. Bushra AlAhmadi** Engineering Consultant, **SITE,** Saudi Arabia
| **Sasha Qadri** (Moderator) – Journalist

Panelists discussed how clear, consistent, and reliable information sharing across industries and nations has become more necessary in an increasingly digitalized world. To truly think of cybersecurity as a public good, the international community must be willing to provide access to critical information. However, there is an important balance between open information exchange and privacy protection, especially with intelligence that concerns national security. Striking this balance will be a key imperative for governments in the coming years.

Panelists agreed that with the coming of a new digital age, the sheer amount of data available poses both opportunities and risks. Private sector actors and governments must cooperate to extract meaningful intelligence from the vast quantity of data they have, and, most importantly, they must develop new and safe ways to share this intelligence. Standardized frameworks may prove useful in this case, with examples like the MITRE Attack framework already existing from the American not-for-profit MITRE Corporation. These frameworks provide a pathway for industries to come together and safely share the most important intelligence. There is also the persistent issue of trust, particularly between governments. As highlighted by Dr. Christopher Ahlberg, "Governments over-classify things … this is very common, go to any country in the world, over classification … and that's what we have to stop. Stop classifying what's actually not a secret."



"Governments over-classify things … this is very common, go to any country in the world, over classification … and that's what we have to stop. Stop classifying what's actually not a secret."

Dr. Christopher Ahlberg



In this case, governments must develop more effective methods of selectively sharing some data points while protecting others.

In conclusion, panelists emphasized that private sector entities can work within industry clusters to share data and intelligence more effectively, as set out by pre-existing capacity building frameworks like MITRE Attack. Organizations can also take advantage of the role of AI and machine learning in gaining real-time situational awareness to detect threats. For example, corporations may be able to use AI bots to identify cyber criminals on the dark web before threats surface. On the issue of trust, governments should invest into platforms which use privacy preserving technologies for building privacy and trust into the network natively as this would provide a pathway for open cooperation and information exchange between all actors. ■

"[I believe in] the importance of collaboration in every aspect of cybersecurity, because we're all fighting and defending against the same common adversary, because cybersecurity is a global problem. And we have each and every one of us a role to play to make sure everyone is safe."

Bashra Alahmadi

Pathways to Regional Cyber De-escalation

Powered in Collaboration with MEI@75

Dr. Bassant Hassib Assistant Professor of Political Science, **British University in Egypt**
Steph Shample Non-Resident Scholar, **Middle East Institute**
Mohammed Soliman Manager, **McLarty Associates**
Rebecca McLaughlin Eastham (Moderator) – TV Anchor and Managing Director, RME Media



Panelists discussed how cyber warfare is being treated as an expansion of conventional methods of conflict. Globally, we are seeing a rising trend of cyber warfare due to it being low cost and easy to implement. This trend is also visible in the Middle East and Africa region, where cyber de-escalation and technology management are fraught with complexity and challenges. One of the biggest challenges is the growing digital divide across the region. Gulf countries have been able to make significant progress across all areas of cybersecurity and technology through a robust regulatory environment and attraction of digital/tech powerhouses, while their counterparts in the region are still trying to catch up.

During the discussion, panelists noted that to help bridge this divide, Gulf countries are focused on avenues of capacity building and technical skills transfer and have launched numerous multilateral initiatives in this regard. In fact, the Global Cybersecurity Forum is one initiative which is aimed at uniting and supporting states in the cyber domain. Forums and platforms such as the GCF focus on



international collaboration and help in the dissemination of best practices and ideas. Mohammed Soliman noted, "Tech conversations are taking place away from the old traditional tech hubs. There are a lot of emerging middle powers. Saudi Arabia is one of them. There is the determination. There is the human capital. There is the will to be in that space. And I think that this is the way forward." These initiatives help in bridging the gap across the region, however, there is still significant room for improvement.

Moving forward, multiple pathways for regional collaboration and de-escalation should be explored. As a first step, there is a need to revisit regional frameworks and agreements to further ensure their alignment with international cybersecurity legislations and conventions. Additionally, there is a need for increased clarity on the definitions and provisions in existing regional frameworks and agreements. Lastly, there is a need for the region to increase representation at cybersecurity focused multilateral platforms such as the UN committees and Groups of Government Experts (GGEs). ■

"And that's where policy drives it [awareness] from the top down, and grassroots education spreads the awareness from the bottom up, and then you hopefully meet in the middle."

Steph Shample

The Cyber Corps

| **Almerindo Graziano** CEO, **Cyber Ranges**
| **Andrés Jesús Ruiz** Senior Policy Advisor, Cybersecurity Unit, National Security Department, **Cabinet of the Prime Minister,** Spain
| **Aapo Cederberg** Founder and CEO , **Cyberwatch Finland**
| **Joe Sarno** Senior Vice President for International Sales APJ & Emerging, **Fortinet Inc.**
| **Chris Fox** (Moderator) – Technology Presenter, BBC



Panelists emphasized that building a quality team of cybersecurity defenders requires individuals with leadership skills and a passion for security. However, attracting talent has become a key challenge for cybersecurity teams, and developing and retaining them has proven to be even more challenging. Organizations must become creative in their recruitment and development efforts.

Speakers agreed that one main challenge is the so-called 'talent gap', or the discrepancy between the skills individuals advertise through certifications or resumes and their real-life abilities. As highlighted by Almerindo Graziano, "Certifications today are not based on observable abilities. If you look at the most important certificates in your life, you know, things like driving license, nobody's going to give you a driving license just based on a test that you pass. You have to be able to demonstrate that you can drive a car. But if you are working in the cybersecurity industry, you get a certification for a digital forensic analyst,



penetration tester, but you've never been observed doing one." Due to this common misalignment, organizations are struggling to match job openings with the required skillset. Private sector entities must also realize that hiring talent is only half the battle, and an additional emphasis must be placed on talent development and retention. As so much of the cybersecurity industry is about individual skills, entities must focus on education and the development of an innovative spirit within their organizations.

In conclusion, panelists agreed that in order to act on these challenges private sector entities must focus on developing young talent to be cybersecurity experts given the current gaps in the talent landscape and place a greater focus on attracting women to the cybersecurity sector. The right talent can bring value to an organization regardless of gender, and increased diversity on a team leads to a more productive and happier organization. For this reason, many entities have dismissed traditional resume interviews entirely and instead focus on talent assessments. Entities must also prioritize cyber threat drills and crisis management protocols, particularly in cases of critical national security. Taking these steps will strengthen future resilience and preparedness within organizations. ■

4.7

million – professionals working in the cybersecurity field in 2022

(Source: Fortune)

"The future is digital, right? So cybersecurity is not seen just as a mere technology now, but it's a sustainability issue. And the attack surface is getting bigger and more complex and threats are getting more complex. And this leads to more cyber skills on the market."

Joe Sarno





KEY **TAKEAWAYS**

Key takeaways, insights, and implications

The 2022 edition of the GCF delivered on its ambitions: convening an unprecedented diversity of cybersecurity experts across government, the private sector, academia, international organizations and NGOs and advancing collective action toward a safer and more prosperous Cyberspace for all. The Forum's five sub-themes enabled deep exploration into the most pressing and pertinent Cyberspace issues of the day, and allowed the expert panelist's insights and thought leadership to push knowledge boundaries. In addition to the insights generated by each panel, summarized in the previous pages, the discussion at this year's Forum yielded four critical, cross-cutting themes and a set of particularly salient insights which are summarized over the next pages. ■

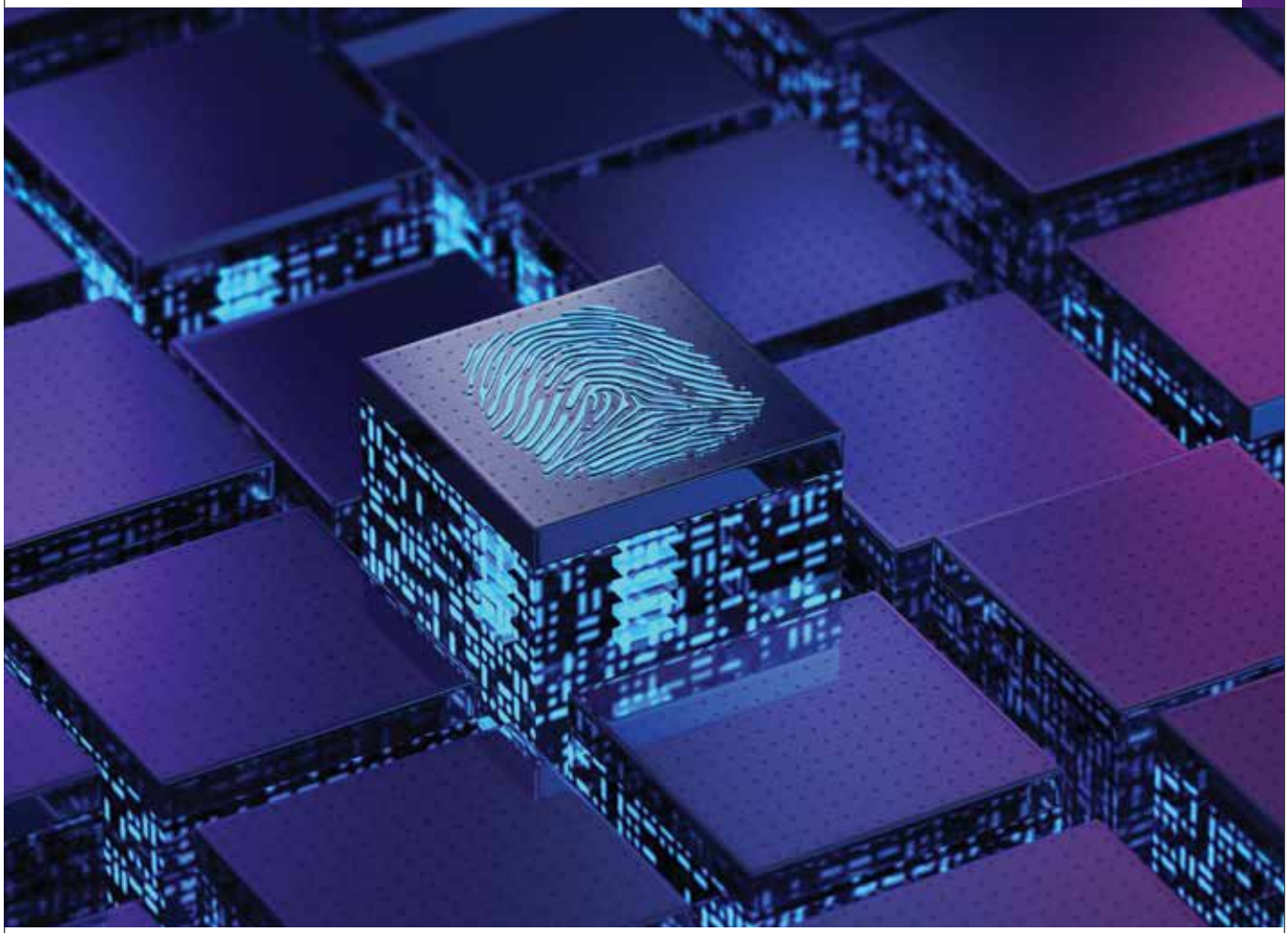


KEY TAKEAWAYS



Takeaway:

1 Radical Change: Preparing for a Structurally Altered Cyber Future



From the first panel, the 2022 edition of the GCF highlighted the extent to which the global cyber order has entered a period of radical change. Speakers explored the key drivers of this transformation, from the sheer pace of technological advancement and the intensifying competition for innovation leadership, to the shifting economic structure of cybercrime and the uncertain future of the digital sovereignty of citizens. Several of these transformations emerged as particularly significant.

1.1 The Quantum Era – Facing the Prospect of Mass Obsolescence

The accelerating advance of quantum computing represents an inflection point that could result in "a new era of cyber insecurity". In the future we are facing the prospect of quantum computers that will be as much as 100 trillion times faster than traditional supercomputers. Those in possession of them would be able to evade the security protocols on which the digital economy currently relies. One possible result, for those who do not adapt with sufficient speed to the Quantum Era, will be the sudden obsolescence of many critical cyber systems. Another possible scenario is the likelihood of a multi-tiered internet in which the highest levels of cybersecurity are only available to the few. ■

■ **KEY TAKEAWAYS**



1.2 Next Generation Diplomacy – Meeting the Challenge of Change

There was wide acknowledgement that traditional diplomacy will prove ill-equipped to meet the demands of the future cyber environment. This will manifest itself in terms of speed, content and approach. In terms of speed, effective cyber diplomacy will require new capabilities to anticipate challenges and shocks and resolve them proactively early in their evolution. In terms of content, the diplomacy required in the future must be characterized by much greater degrees of technical sophistication. Finally, in terms of approach, the diplomatic framework required in the future must be significantly bolder and more collaborative in order to arrive at the optimal solutions needed, rather than being limited to lowest common denominator agreements and slow, incremental progress. ■

Takeaway:

2 Multilateral Collaboration: New Pathways of Collective Action

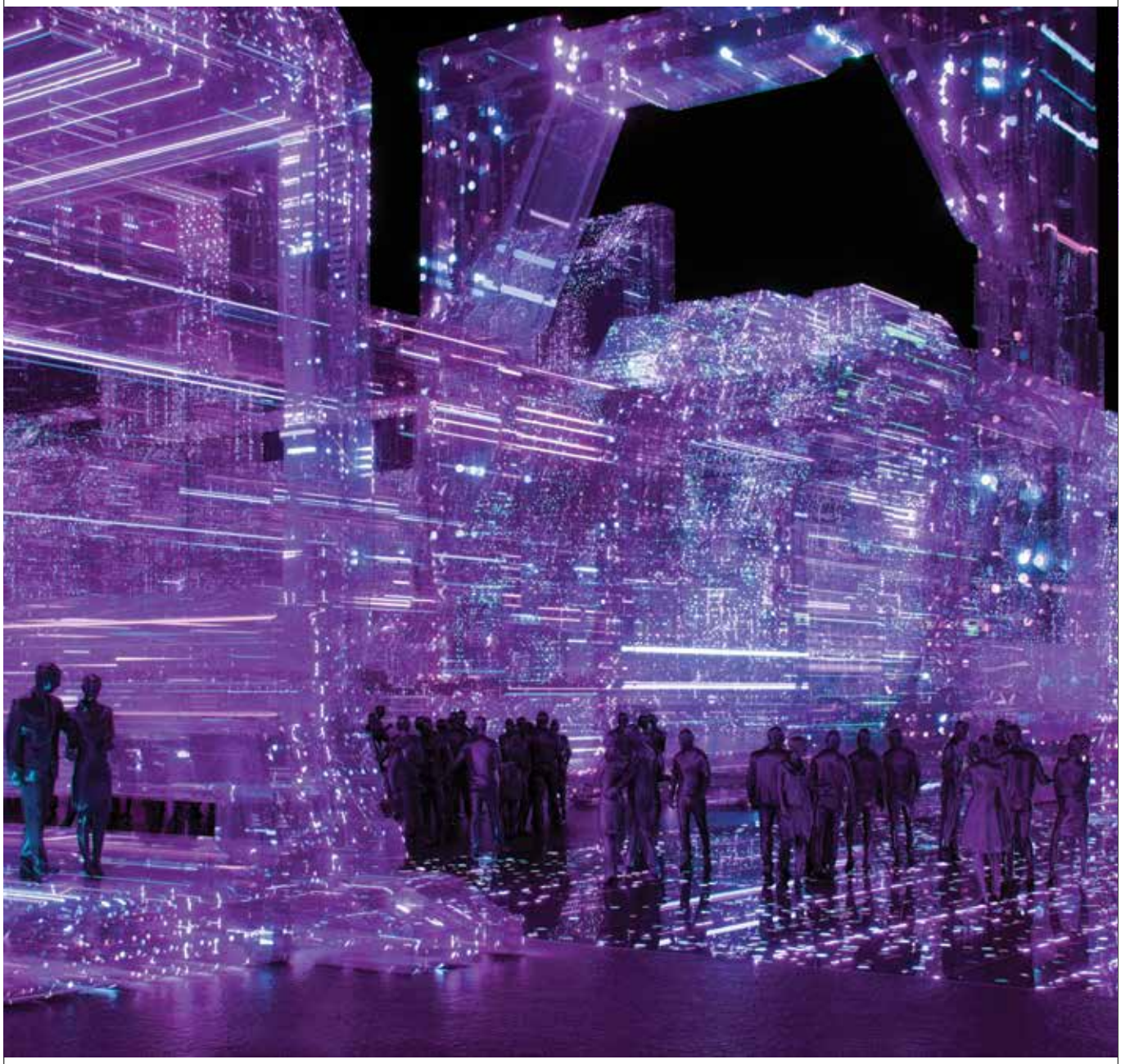
Many forces are shaping the balance of order and disorder in the global cyber landscape. On the side of order, none of these are more important than multilateral collaboration. Across many discussions at this year's GCF, a fundamental reality is that because cyber challenges are transnational and ever-evolving, no one country can achieve comprehensive cybersecurity alone. Alongside this, the competitive nature of the cyber domain and its growing role in government's national security complicate and can limit the scope of substantive collaboration. There was broad consensus that building momentum in multilateral collaboration on cybersecurity requires both strengthening existing institutions and developing new pathways of collective action.

2.1 Global Governance – Prioritizing Inclusive Cybersecurity

The fundamental importance of the progress being made on cybersecurity in key global governance institutions, particularly at the United Nations was recognized. At the same time, the current geopolitical landscape is impeding progress on a number of fronts. However, important opportunities do remain for driving deeper progress, including at global lending institutions. For many countries, especially in the current global financial environment, access to financing is a primary obstacle to strengthening cybersecurity capacity. By elevating cybersecurity to a development priority, global development institutions can contribute to reducing the digital divide and strengthening the security and inclusivity of the global cyber order. ■

2.2 Securing the Energy's Supply Chain

Energy is the fuel for the prosperity of all other industries and this fuel needs to be protected. The greatest cyber threat within the energy system is disruption, which can have catastrophic consequences for individuals, societies, and economies. Therefore, the energy sector and cybersecurity are inextricably linked as they directly impact the global economy, national security, and humanity. There is a critical need to develop standards and a systematic methodology of evaluating energy infrastructure, particularly risk modeling and improve industry-wide collaboration in Cyberspace and for all actors in the ecosystem to collaborate, execute, and deliver results for the cybersecurity problems the world is facing today. ■



2.3 Capacity Building – Whole-of-Society Support

Across multiple sessions, speakers emphasized the importance of adopting whole-of-society approaches to cybersecurity capacity building. There is an opportunity to move beyond efforts more narrowly focused on supporting government institutions, to approaches that build capacity across society and in the private sector. There was wide consensus that there is both an opportunity and an imperative to provide developing countries with the funding, technical expertise, and resources necessary to strengthen cybersecurity at all levels. Particularly with respect to cybercrime, speakers emphasized that proactively bringing developing countries into cross-border information sharing programs would be an efficient way of advancing global security and stability of the global cyber order. ■

Takeaway:

3 Policy Innovation: Rethinking Enduring Challenges

In the emerging cyber order, challenges will intensify, but so will the opportunities for policy innovation. As digital technology becomes pervasive across society, cyber policy must evolve to include the perspectives of diverse stakeholders. Among the many promising frontiers of policy innovation explored at the 2022 edition of the GCF, three received particular attention:

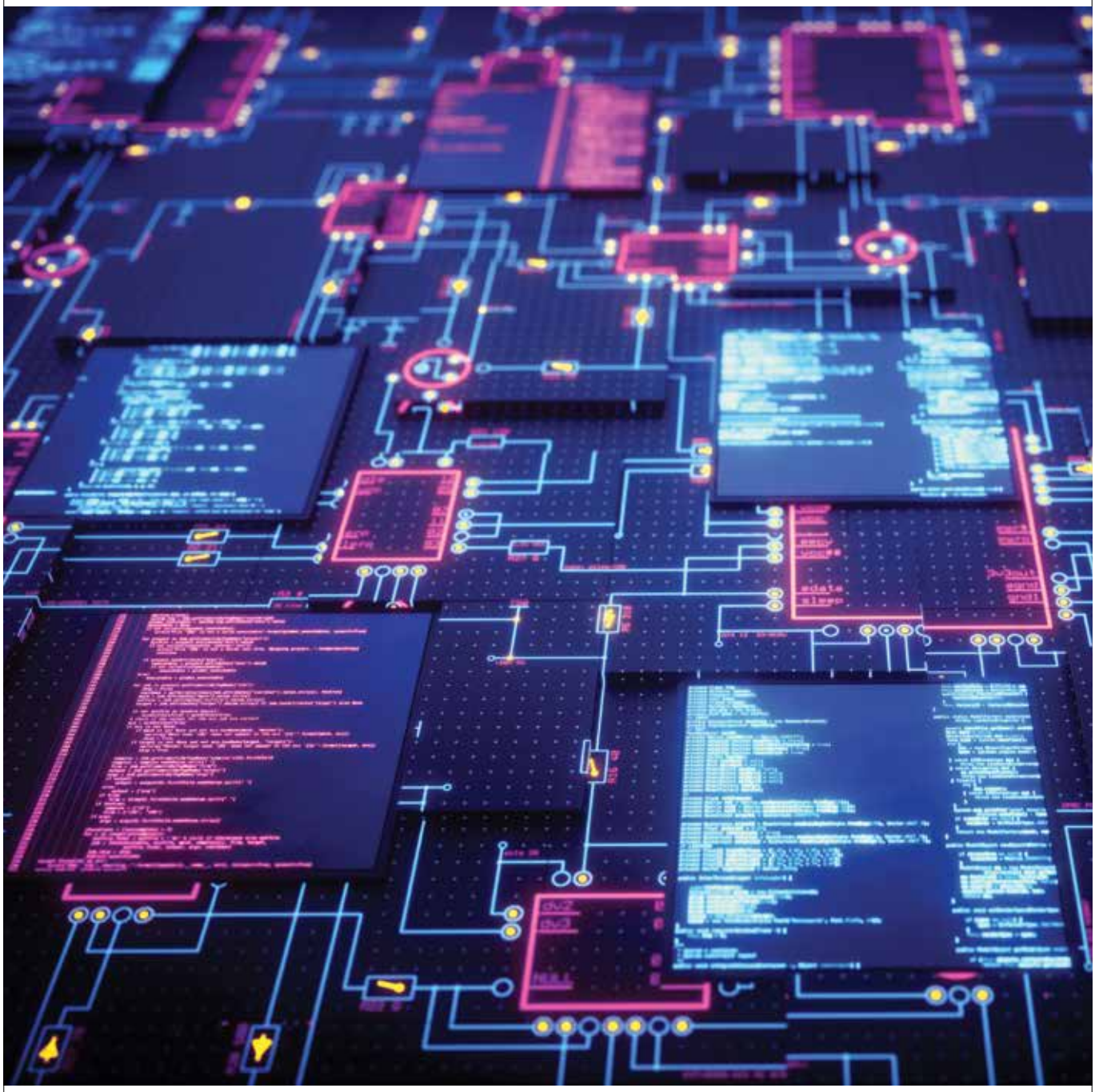
3.1 Vulnerable Populations – Protecting the Future

With each passing day, Cyberspace becomes more deeply intertwined in our lives and those of our fellow citizens. However evidence shows that women and children are targeted disproportionately in Cyberspace and their protection online is an imperative. The developmental impact of technology on children in particular was noted across several discussions. It is estimated that 73% of children have been exposed to cyber risk. In an environment in which ever-more children participate in and rely upon the internet, it is critical to accelerate collaborative policy design and implementation at both the local, national and international level. Governments have an opportunity to increase their focus on creating children-focused, children-centered solutions on the principle of viewing children as not just vulnerable targets, but the stakeholders of the future. A key first step will be for governments, the private sector, NGOs, and the entire ecosystem to better understand the needs of children by collecting, pooling and analyzing anonymized data on children's activity online for research and policy innovation within existing legal frameworks. ■

3.2 Regulation and Innovation – From Tension to Synergy

There was wide consensus that in an age of rapidly emerging technologies, governments and the private sector must work together to find a balanced solution between ensuring incentives for a thriving market-driven innovative environment are fulfilled alongside safeguarding security. The regulatory approaches required to find this balance must be grounded in anticipatory governance and collaborative multi-stakeholder engagement. Emerging technologies represent an opportunity for collaborative innovation in regulation, involving private and public sector innovators with policymakers and citizens through all stages of its development. ■

■ **KEY TAKEAWAYS**



3.3 Future Focused Design – Security-Driven Innovation

Across sessions it was highlighted how critically important the principle of secure-by-design will be in a future characterized by an ever-widening attack surface. The inherent flaws of existing systems are currently due to a lack of understanding and security rigor during system design and development. A key point of consensus was on the urgent need to accelerate training in security-by-design system disciplines with developers and the need to redesign existing systems to ensure cybersecurity by design across all regulations and technologies. ■

Takeaway:

4 Ecosystem Protection and Development

Again and again during the GCF panel discussions, the fundamental importance of applying the lens of complex systems to understand and strengthen the cyber environment was raised. The security of the cyber order will to a large extent be determined by the health of the cyber ecosystem. Readiness for the threats that will characterize the future cyber environment will require a cyber ecosystem that is collaboratively governed, aligned in terms of standards, continuously learning, and rigorously tested. A whole-of-ecosystem approach including cross-sector collaboration will be imperative to develop both the talent and infrastructure needed to maximize resilience in the future. All citizens, not just cybersecurity professionals, should be prepared for the challenges inherent in more complex developments such as the accelerating advance of artificial intelligence and quantum computing. Among the themes discussed at the Forum on the topic of ecosystem protection and development, the following themes emerged:

4.1 Critical National Infrastructure – Preemptive Innovation

As technology becomes more integral to managing critical national infrastructure (CNI) at scale and artificial intelligence becomes a key component of automation at all levels, attackers are continuing to develop new ways to breach CNI systems. For this reason, governments need to reinforce security standards at every level of their national infrastructure supply chain. In the context of the acceleration of the Fourth Industrial Revolution, national infrastructure is only as strong as its weakest link. As a result, governments must drive a whole-of-ecosystem approach centered on cross-sector collaboration, standards alignment and innovation. Self-healing systems represent a particularly promising frontier of innovation in critical national infrastructure protection. These technologies will be increasingly able to detect the first signs of an attack and take neutralizing action before their intended effects are delivered. ■

4.2 Awareness Efforts – Accelerating Diffusion

The overwhelming importance of increasing whole-of-society cybersecurity awareness as a first step toward preparedness was evident. Every stakeholder in the ecosystem has a critical role to play in these awareness efforts – from governments conducting national awareness campaigns, to private sector entities running cybersecurity drills and trainings, to parents educating and discussing the challenges and risks of the digital environment with their children. Speakers discussed that awareness-building must start in school and deepen through the educational journey. Awareness-building is also a critical area in developing economies and capacity building efforts to ensure that the cyber order of the future is inclusively secure. ■



4.3 Workforce Development – Bridging the Gap

Discussions were distinguished by a particular focus on the need for a cybersecurity workforce that can match the growing demand presented by emerging threats. Attracting talent has become a key difficulty for cybersecurity teams, while developing and retaining talent has proven to be even more challenging. There is a persistent mismatch and 'talent gap' between the skill sets required to tackle emerging threats and the skill sets most cybersecurity professionals currently possess. Interestingly, several speakers noted that the proliferation of training certificates has diluted their reliability. As a result, two near-term priorities are suggested: First, building more collaborative, mutually validated official certification systems to reduce the proliferation of unreliable providers. Second, organizations must increase their use of direct testing and expand the implementation of zero-trust architecture. In addition, investing more decisively in cyber education and upskilling can serve both to develop needed capabilities, but also can attract and retain top talent in an ever more competitive labor market. Finally, discussions highlighted the opportunity for government and private sector organizations to reshape the portrayal and resulting image of cybersecurity professionals so as to better attract the younger generation of talent, in particular young women, to the industry. ■

GCF in numbers
Event Highlights

127
Leading & international speakers

117
Countries

41
Content-rich sessions

9,000+
Attendees

GCF in numbers
Event Communications Impact

167M
Total digital impressions

1M+
Livestream views

1K+
Traditional media mentions

1.8M+
Social media engagements

35M
Audiences reached through outdoor advertising

Follow us on

@gcfriyadh

Global Cybersecurity Forum









GLOBAL COLLABORATION

Our Partners

The Global Cybersecurity Forum would like to thank the following partners for their role in supporting the 2022 edition and its success. With the help of our founding, strategic and technology partners, our digital enablers and media partners, we were able to collaborate and Rethink the Global Cyber Order. ■

Founding Partners

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

SITE
الشركة السعودية لتقنية المعلومات
Saudi Information Technology Company


Strategic Partners
aramco
stc
سابك
sabic
Technology Partners
FORTINET
CISCO
paloalto NETWORKS
TREND MICRO
Trellix
Microsoft
Digital Enabler
sirar by stc
Media Partners
euronews.
العربية
alarabiya
ARAB NEWS

Global Cybersecurity Forum Knowledge Partners

For the 2022 edition, the Forum worked with Knowledge Partners comprised of leading international organizations and institutions, to leverage a huge depth of expertise.

Across the two days, Knowledge Partners supported in leading sessions that covered specific topics affecting Cyberspace, including keeping children safe online, ensuring advanced nations accelerate cybersecurity development across the globe, cybersecurity in the quantum era, the benefits of public-private collaboration and improving gender diversity within the cyber workforce. ■



Uniting voices for child protection online

UNICEF, the agency of the United Nations responsible for providing humanitarian and developmental aid to children worldwide, supported the 2022 edition of the Forum by sharing their expertise on child protection in Cyberspace. UNICEF led a key session titled, 'Safe Children in Cyberspace', where discussions covered the urgent need for better protection of children online and the action necessary to deliver children's safety and protection when they roam Cyberspace.

During the event UNICEF and the National Cybersecurity Authority (NCA) of the Kingdom of Saudi Arabia signed a Cooperation Agreement, where the two organizations will collaborate moving forward at the regional and global level on child protection in Cyberspace. ■

"As children's lives are increasingly intertwined with the digital environment, they face risks of violence, exploitation and abuse. UNICEF attended the Global Cybersecurity Forum to engage with technology and cybersecurity leaders to bring children's views and rights to the forefront and motivate action to address those risks and make the internet a safe place for children to learn, socialize and express themselves. At GCF, we also signed a cooperation agreement with the National Cybersecurity Authority of the Kingdom of Saudi Arabia laying the groundwork for collaboration at the regional and global levels on child protection in cyberspace."

– Sanjay Wijesekera, Director of Programme Group, UNICEF



Global expertise for all things Cyber

ITU is the United Nations specialized agency for information and communication technologies. ITU's leadership team participated in a number of sessions across the two days, covering topics from global frameworks for cybersecurity, to the role of AI technology in the cybersecurity sector.

ITU led a session titled, 'The Race for Quantum Supremacy', which explored the potential implications of quantum on cybersecurity for different actors and sectors.

ITU also signed a Framework for Cooperation with the National Cybersecurity Authority (NCA) of the Kingdom of Saudi Arabia, where the two entities will collaborate on the development of Cybersecurity capacity and women's role within the sector. ■



Knowledge sharing with ICANN

ICANN led a session called, 'Promoting Internet Security-Best Practices', that brought together international policy experts to share their personal experiences, methods, processes, and policies in order to identity those most relevant and successful in increasing internet safety. ■

"We were very pleased to participate in the Global Cybersecurity Forum 2022. The Global Cybersecurity Forum provided an excellent venue for us to engage in many valuable discussions and network with key stakeholders and leading players in the field."

Regional Vice President for Stakeholder Engagement in the Middle East, and Managing Director for the Middle East and Africa (MEA) Regional Office, **ICANN**



Frameworks for international Child Online Safety

The DQ Institute is an international think tank that is dedicated to setting global standards for digital intelligence to ensure safety, empowerment, and well-being for all. DQ Institute chose GCF 2022 as the global stage to launch the Child Online Safety Index which surveyed 145,426 children and adolescents in 30 countries over the last three years to identify the risks they face daily whilst using the internet. The index was announced by the institutes founder and CEO, Dr Yuhyun Park.

The panel, 'Metrics for Success', looked at how the worlds digital community currently lacks the infrastructure necessary to ensure that children can be kept safe online and prosper, rather than experience harm. ■

"The DQ Institute was honoured to have launched the 2022 Child Online Safety Index at the Global Cybersecurity Forum this year. Our Index found that worldwide, 73% of 8–18-year-olds have experienced at least one cyber-risk. It is urgent that the private and public sectors work proactively together to develop holistic national policies and Digital-ESG business practices not only to empower today's youth with digital citizenship but also protect those most vulnerable. This year's GCF convened key stakeholders globally to initiate such discussions in order to create real change."

Dr Yuhyun Park, CEO, The DQ Institute



Unifying all sectors for child protection

WeProtect Global Alliance is an independent organisation bringing together governments, private sector, civil society and international organisations to develop policies and solutions to protect children from exploitation and abuse online.

As Knowledge Partners, the group aimed to raise awareness of the dangers facing children with the growing use of technology. During their session, 'AI for Child Protection', leaders from both the public and private sectors, including the United Nations and Bracket Capital, came together to discuss how AI can be harnessed as a key technology to protect children through the increased implementation of AI that automate and monitor a variety of online activity, including identifying threats. ■

"The Global Cybersecurity Forum in Riyadh was a unique occasion to meet global leaders working to make the online world a safer place for everyone, including children. At WeProtect Global Alliance, we were pleased to be invited to the forum as knowledge partners, to highlight how the fight against child sexual exploitation and abuse online should be a top priority on the global agenda. We would like to thank the National Cybersecurity Authority for organising such an impactful event and offering us the opportunity to be a part of it."

Iain Drennan, Executive Director at WeProtect Global Alliance



Bringing post quantum cryptography to the masses

The Electronics and Telecommunications Research Institute (ETRI) is a Korean government-funded institute focused on the development and distribution of industrial core technologies in ICT.

ETRI shared its expertise on the world of quantum cryptography, during its session, 'Post Quantum Cryptography', which dealt with several cryptographic engineering techniques. The panelists shared their perspectives on implementation issues and how to bridge the gap between theory and practice in the real world. ■

"The Global Cybersecurity Forum was a very impressive experience for the sector. The scale of the event and calibre of experts that were brought together from all over the world was unparalleled. It was a meaningful event which allowed us to discuss the future of Post-Quantum Cryptography with Queen's University Belfast, Secure-IC from France, and UCCS from US, which have maintained international cooperative relations with ETRI for over 10 years. We see the GCF as a driving force to promote the development of cybersecurity technology around the world."

Dr. Ik-kyun Kim, Assistant Vice President of ETRI



Raising cyber awareness to create resilient societies

The United Nations Institute for Training and Research (UNITAR) provides innovative learning solutions to individuals, organizations and institutions to enhance global decision-making. UNITAR believes that in the increasingly digitalized world of today, it is essential for institutions, governments, and companies to protect Cyberspace.

Focused on creating tools to help entities create their own change, UNITAR's session, 'Whole of Society Cyber Awareness', revolved around cultivating a culture of cyber awareness with the audience and impressing the importance of cyber awareness amongst all citizens in creating more resilient societies. ■



Governance in technology today

The Observer Research Foundation (ORF) is dedicated to building both political and policy consensus focused on India and its interaction with the world.

ORF's panel discussion, 'Geo-technological Competition and Conflict', saw futurists, technologists, and policymakers share perspectives on the future of global technology and its governance in the current geo-political climate. The discussion focused on how the rise of global competition needed a local response to correctly monitor and control national activity, in order to guarantee global cybersecurity can prosper. ■

"At a time when we are witnessing the increasing weaponization of the very architecture of interdependence enabled by ICT technologies, the Global Cyber Security Forum gathered some of the best minds to cogitate upon the growing unease nations, societies and individuals face."

Sunjoy Joshi Chairman, ORF



Creating a shield for modern warfare

The Middle East Institute (MEI) is an independent, non-partisan, non-for-profit, educational organization focused on advancing education, and culture awareness for over 75 years.

MEI supported GCF 2022 by powering a key discussion titled 'Pathways to Regional Cyber De-escalation' which focused on how the cyber world is now opening the door to a new modern warfare. The panel highlighted the need for knowledge sharing and collaboration as a way to bridge the gap between nations with great technological power. The session also revealed that the Middle East is forging a path for capacity building and technical skills transfer of its people, which is helping the region lead the way to creating cyber secure nations. ■

MEI@75
Peace. Prosperity. Partnership

"From tech decoupling and the rise of the rest to advocating for safe, equitable Cyberspace and increasing cyber cooperation with India, middle powers such as Saudi Arabia are expected to take on a more active role in setting the global agenda for tech and cyber. Saudi Arabia, has proven itself well equipped to take on this role and advance the tech and cyber agenda."

Mohammed Soliman, Director, Strategic Technologies and Cyber Security Program, Middle East Institute



Focused on the future

Kearney, a leading global management consultancy has been a trusted advisor to the world's foremost organizations.

Kearney focused its sessions on the future landscape of Cyberspace. The deeply uncertain future of the global cyber order requires systematic consideration of a full range of potential future scenarios, or alternative futures.

Kearney led a two-part panel discussion looking at three potential scenarios, in both the medium and long term, for the future of Cyberspace. The sessions titled, 'Divergent Futures', offered insights from academia and government representatives on the implications each scenario could have on current policy and what adaptations might be required in the future to best prepare for the uncertainty. ■

KEARNEY

"It was a great privilege to be a knowledge partner of the Global Cybersecurity Forum – particularly at this critical and fragile moment in history. Cybersecurity represents a critical frontier in the evolution of the international operating environment. We must make multilateral progress in stabilizing it for the long-term. Indeed, we must rethink the global cyber order. This year's GCF made that possible. It was remarkable in terms of the quality of the discussions that it enabled. We very much look forward to next year's event."

Rudolph Lohmeyer, Partner at Kearney



Female empowerment

BCG is a global consulting firm that partners with leaders in business and society to tackle their most important challenges.

As a knowledge partner BCG led sessions addressing one of the most critical challenges facing the cybersecurity sector – the growing talent gap. Sessions included, 'Mind the Gap', which brought the private and public sector together to discuss the necessary role women can play in the sector.

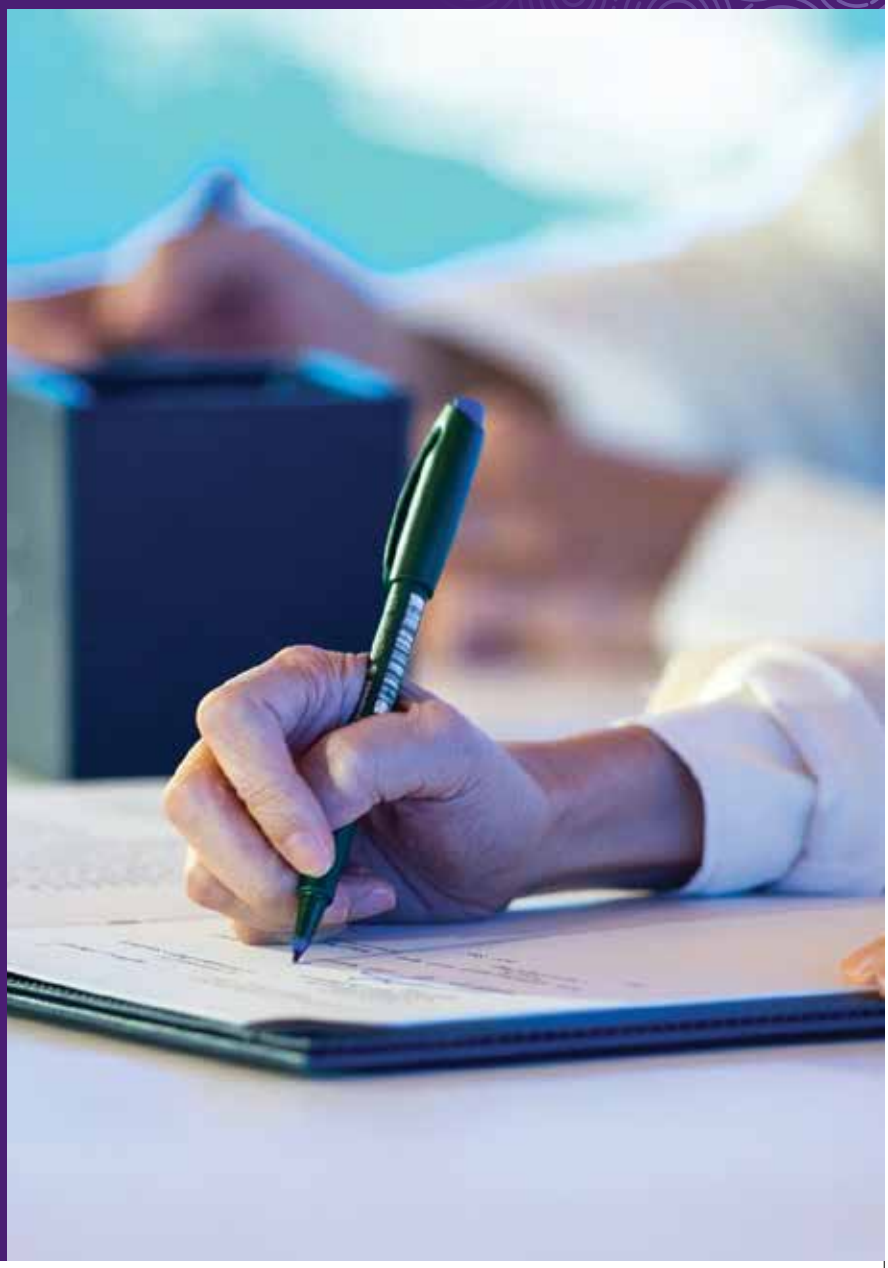
'The Future is Female', session looked at the overall benefits of increased female participation in the cyber workforce including greater skill diversity and crucially the different perspectives gender diversity brings. ■

"Cybersecurity is a fast-growing field and yet women account for only 25% of the workforce.
This presents a clear path to growth in a field where 57% of organizations report unfilled cybersecurity positions. Addressing the barriers facing women in the profession, gender pay gaps, industry-wide changes and what levers are available to drive that change, were the focus of BCG's sessions."

Shoaib Yousuf, Managing Director and Partner, BCG

Memorandum of Understanding (MoU)s

During the 2022 edition of the GCF, the Kingdom of Saudi Arabia's National Cybersecurity Authority signed Memorandum of Understanding with a cross section of entities to continue work and partnership across key areas.



(MoU)s



unicef

The United Nations Children's Fund (UNICEF)

Multilateral

UNICEF is the agency of the United Nations responsible for providing humanitarian and developmental aid to children worldwide.

Scope:
Cooperation in child protection in Cyberspace both regionally and globally.

The MoU aims to establish a collaborative framework between both parties to enhance cooperation for child protection in Cyberspace.

(MoU)s



The International Telecommunication Union

Multilateral

ITU is the United Nations specialized agency for information and communication technologies.

Scope:
The MoU aims to enhance cybersecurity in the IT sector, encourage cooperation among all relevant stakeholders, and bridge the gap in cybersecurity among countries, in addition to cooperation on the development of Cybersecurity capacity and women's role within the sector.

(MoU)s



DQ Institute
Global Standards for Digital Intelligence

DQ Institute
Think Tank

The DQ Institute is an international think tank dedicated to setting global standards for digital intelligence to ensure safety, empowerment, and well-being for all.

Scope:
The objective of this MoU is to enhance cooperation across common aims for the benefit of children and their families, and to discuss and define programs, activities, and projects, in addition to cooperation in international child online safety.

(MoU)s



BCG HENDERSON INSTITUTE

BCG Henderson Institute

Private Sector

BCG Henderson Institute, is a think tank dedicated to exploring and developing valuable new insights from business, technology, economics, and science by embracing the powerful technology of ideas.

Scope:
Cooperation to advance the knowledge and skills of cybersecurity, combining ambitions to develop world-leading cybersecurity research.

The objective of this MoU is to enhance cooperation between the parties for the advancement knowledge in the field of cybersecurity, through developing world-leading research and information exchange.

(MoU)s



WeProtect
Global Alliance

WeProtect Global Alliance is an independent organisation bringing together governments, private sector, civil society and international organisations to develop policies and solutions to protect children from exploitation and abuse online.

Scope:
The objective of this MoU is to enhance cooperation across common aims for the benefit of children and their families, and to discuss and define programs, activities, and projects related to protecting children in Cyberspace.

(MoU)s



SABIC
Private Sector

Saudi Basic Industries Corporation, known as SABIC, is a Saudi chemical manufacturing company.

Scope:
Cooperation in the field of cybersecurity to develop and launch national awareness campaigns in Saudi Arabia.

The MoU aims to enhance cooperation to develop and launch national cybersecurity awareness-raising campaigns in Saudi Arabia, for the benefit of both the general public and specific, targeted segments of society.



Al-Amaaria Gala Dinner

The GCF was delighted to welcome guests to enjoy the Kingdom's hospitality and rich heritage at Al-Amaaria, a village of luxury resorts, farms, freshwater and several tourist attractions and historical landmarks, such as the Cleft and the Valley of Wonders.

Scan the QR code to watch an exclusive video of the event











B2B Meetings

The dedicated Business Lounge at the GCF provided networking opportunities to meet and interact with influential individuals and decision makes across the public and private sector, building personal relationships that extend beyond formal interaction. ■




BUSINESS LOUNGE
Global
Cybersecurity
Forum











KNOWLEDGE HUB

Rethinking Cyber Podcast

As a digital extension of the Forum and its commitment to providing a space for dialogue, the GCF launched the Rethinking Cyber podcast, a weekly series revolutionizing the way we think about Cyberspace. For its inaugural season, the podcast brought together a selection of GCF speakers for thought-provoking and accessible conversations on the issues shaping Cyberspace today.

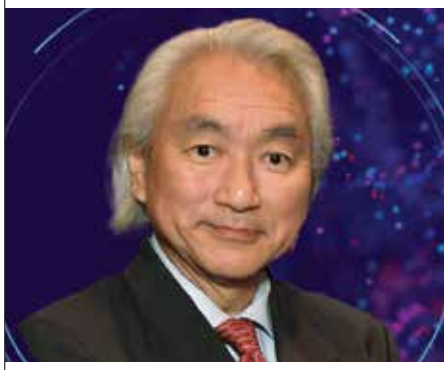
The series covered an array of topics ranging from protecting children in Cyberspace and the importance of addressing the critical talent gap in the cybersecurity workforce, to the alarming increase of cybercrime and the fascinating future of quantum computing. Beyond just technical and sector issues, season one of the Rethinking Cyber podcast also aimed to bring the issues of Cyberspace and cybersecurity to a wider audience. ■



Catch all our episodes on Spotify & Apple Music



Rethinking Cyber Podcast



Imagining a Post-Quantum Future

Dr. Michio Kaku, world-renowned author, scientist and futurist, examines the seismic impact quantum computing will have on our lives and on industry. He explains the concept of quantum computing, explores what a quantum future will look like, and explains the link between quantum physics and the multiverse. ■



Navigating Cyberspace; How Businesses Can Survive and Thrive

Will businesses ever be ahead of the curve, or forever playing catch-up as the tech revolution accelerates? Alex Liu, Managing Partner and Chairman of the Board at Kearney, sheds light on why cybersecurity is at the top of global CEO's agendas, the most pressing cybersecurity challenges businesses face, and how to transform these challenges into opportunities. ■



Empowering Women in Cybersecurity

What are the barriers to women's empowerment in cybersecurity and how can we address them? Leila Hoteit, Managing Director and Senior Partner at BCG, discusses the imperative of including more women in the field, the obstacles they face, and how to overcome these challenges. ■



Safety Tech: Exploring a New Global Sector

Dr. Mary Aiken, a world-leading expert in cyberpsychology, joined us live at the 2022 Edition of the Global Cybersecurity Forum for a captivating discussion. As one of the acknowledged founders of a new global sector, 'Safety Tech', Dr. Aiken covers everything from the potential of this new sector, the psychology of cybercriminals and encouraging women to enter the field of cyberpsychology. ■



A Safe (Cyber)space for Children

Children accessing the internet is now a societal norm and this access is happening at ever younger ages. The benefits can be vast, but evolving cyber risks mean that protecting children online can be daunting and complex. Iain Drennan, Executive Director of the largest international network focused on ending child sexual abuse and exploitation online, the WeProtect Global Alliance, explains the growing risks and the need for collaboration across borders and across industries to ensure children's safety. ■



Rethinking Global Policing Models to Tackle Cybercrime

Interpol's first global crime trends report, launched at its 2022 General Assembly, ranked cybercrime as one of the top five growing global threats. Interpol's Director of Cybercrime, Craig JONES, discusses the increasing challenges relating to policing cybercrime, how cyber criminals are evolving their business model in Cyberspace and efforts to drive global collaboration between law enforcement agencies – and the private sector - to avert cyber-attacks and catch cybercriminals. ■



Demystifying Cryptography

How can existing technologies be leveraged to tackle the most pressing cyber challenges? Dr. Craig Wright, Chief Scientist at nChain, demystifies Distributed Ledger Technology, addresses misconceptions around crypto, and shares what inspired his career journey. ■

Catch all our episodes on Spotify & Apple Music



GCF and BCG co-authored and published two thought leadership reports, addressing pertinent issues in Cyberspace.

The first report released on 7 September 2022, 'Empowering Women to Work in Cybersecurity is a Win Win', focused on increasing women's participation in the cybersecurity sector to address the widening talent gap.

Empowering Women in Cybersecurity

Currently 57% of organizations have reported unfilled cybersecurity positions, while 75% of today's cybersecurity workers are men.

The Empowering Women to Work in Cybersecurity is a Win-Win report, focused on key actions that are needed to meet the growing gender divide in the cybersecurity workforce.

The study examined female undergraduate students studying Science, Technology, Engineering, and Mathematics (STEM) across six regions and 26 countries. The report shed light on the potential challenges facing women entering STEM studies, as well as women's long-term career prospects in cybersecurity.

The survey found an overall appetite for women to enter the field of cybersecurity at what is a crucial time for the sector. The role of early education was identified as crucial to empowering girls to pursue relevant education options and to breakdown stereotypes and other gender barriers. ■

Read the full report here

Addressing critical issues in Cyberspace with evidence



The second report released on 23 September, 'Why Children are Unsafe in Cyberspace' addressed the increasing risks to children as their interface with Cyberspace grows and the ways in which this activity can be collectively managed to keep them safe.

Protecting Children in Cyberspace

The 'Why Children Are Unsafe in Cyberspace' report focused on raising awareness of the critical issues facing the protection of children in Cyberspace, at a time when over 90% of children aged eight and above are active on the internet.

The report surveyed over 40,000 parents and children, across 24 countries in six regions, with results overwhelmingly showing that the protection of today's youth in cyberspace is falling short, impacting children globally and requiring urgent collective action. ■

Scan to read the full report here

Global Cybersecurity Forum 2022 Edition

DAY ONE: WEDNESDAY, 9 NOVEMBER 2022

09:55 Rethinking the Global Cyber Order, Why? (Room G)
Disruption Frontier, Geo-cyber Evolution and No One Left Behind.

Michio Kaku Professor of Theoretical Physics, City University of New York	**Shyam Saran** Former Foreign Secretary, India	**Mary Aiken** Professor of Cyberpsychology and Chair of the Department of Cyberpsychology, Capitol Technology University	*Moderator*: **John Defterios** Former CNN Emerging Markets Editor & Professor of Business, NYU Abu Dhabi

10:40 – 11:25 Keeping the Lights On (Room G)

10:40 – 10:50
Introductory Remarks

10:50 – 11:25
Panel: Safeguarding Cybersecurity Resilience Across the Energy Supply Chain

Amin Nasser CEO, Aramco	**Saad Alaboodi** CEO, SITE, Saudi Arabia	**Robert Putnam** Global Manager for Cybersecurity Products and Services, ABB	**Jeremy Jurgens** Managing Director, World Economic Forum	**Christophe BLASSIAU** SVP, Cybersecurity & Global CISO, Schneider Electric	*Moderator*: **Sasha Qadri** Journalist

10:40 – 11:15 A Cyber War Deterred? (Room C)
Assessing the Effectiveness of Deterrence as a Means for Countering Cyber Conflict.

Dr. Khalid Biyari Assistant, Minister of Defense for Executive Affairs, Ministry of Defense, Saudi Arabia	**Rajesh Pant** National Cyber Security Coordinator, National Security Council Secretariat, Government of India	**Robin Geiss** Director, United Nations Institute for Disarmament Research (UNIDIR)	*Moderator:* **Rebecca McLaughlin-Eastham** TV Anchor & MD, RME Media

11:25 - 12:00 The Rising Tide (Room G)
Quantifying the Shared Cost of Global Cyber Insecurity.

Alex Liu Managing Partner and Chairman, Kearney	**Olayan Alwetaid** Group CEO, STC Group	**Abdulrahman S. Al-Fageeh** Acting CEO, Saudi Basic Industrial Corporation (SABIC)	**Isa Ali Ibrahim** Minister of Communications and Digital Economy, The Federal Republic of Nigeria	**Khaled Al-Dhaher** Vice Governor for Supervision and Technology, Saudi Central Bank (SAMA)	*Moderator*: **Ramia Farrage** Senior Presenter and Producer, Forbes Middle East

11:25 - 12:00 Ensuring Resilience and Interoperability While Integrating Diversity (Room C)
Understanding the Implications of a Fractured Internet.

Ursula Owusu-Ekuful Minister for Communications and Digitalisation, Republic of Ghana	**Göran Marby** President and CEO, ICANN	*Moderator*: **John Defterios** Former CNN Emerging Markets Editor & Professor of Business, NYU Abu Dhabi

Global Cybersecurity Forum 2022 Edition

DAY ONE: WEDNESDAY, 9 NOVEMBER 2022

12:00 - 12:35 No Nation Left Behind (Room G)
Why and How Nations Should Accelerate Cybersecurity Development.

Doreen Bogdan-Martin Secretary-General, International Telecommunication Union	**Eng. Abdullah A. Alswaha** Minister of Communications & Information Technology, Saudi Arabia	**Khumbudzo Ntshavheni** Minister of Communications and Digital Technologies, South Africa	*Moderator*: **Rebecca McLaughlin-Eastham** TV Anchor & MD, RME Media

12:00 - 12:35 Incentive Reinvention (Room C)
Reducing Economic Incentives Driving Cybercrime.

Craig JONES Cybercrime Director, INTERPOL	**Elvira Tejada De La Fuente** Chamber Prosecutor of the Supreme Court, Head of the Cybercrime Unit, State Attorney General's Office, Spain	**Marco Gercke** Director, Cybercrime Research Institute	*Moderator*: **Rawan Radwan** Deputy Section Head, Arab News

12:35 - 13:05 Securing the Energy's Supply Chain (Room G)
An Imperative at The National and International Levels.

H.R.H Prince Abdulaziz Bin Salman Al-Saud Minister of Energy, Saudi Arabia	*Moderator*: **Rima Maktabi** London Bureau Chief, Al Arabiya News Channel

14:00 - 14:25 Distributed Ledger Technology - Opportunity or Obstacle? (Room G)
How Governments Can Harness DLT for Transparent, Safe, & Citizen-Centric Systems.

Dr. Craig Wright Founder and Chief Scientist, nChain	*Moderator*: **Ramia Farrage** Senior Presenter and Producer, Forbes Middle East

14:00 - 14:40 Safe Children in Cyberspace (Room C)
Keeping Children's Best Interests Paramount.

Prof. Amanda Third Co-Director, Young and Resilient Research Centre, Western Sydney University	**Sanjay Wijesekera** Director, Programme Group UNICEF	**Natasha Jackson** Head of Public Policy & Consumer Affairs, GSMA	**Dr. Albert Antwi-Boasiako** Ag. Director-General, Cyber Security Authority, Republic of Ghana	*Moderator*: **Afrooz Kaviani Johnson** Child Protection Specialist, UNICEF, New York

14:25 - 14:50 Cooperation as an Imperative to Tackle Cyber Crime (Room G)
Conceiving Proactive and Effective Frameworks for International Cooperation Against Cyber Crime in a Borderless Space.

Major General Dr. Ahmed Naser Al-Raisi President, INTERPOL	*Moderator*: **Rima Maktabi** London Bureau Chief, Al Arabiya News Channel

Global Cybersecurity Forum 2022 Edition

DAY ONE: WEDNESDAY, 9 NOVEMBER 2022

14:50 - 15:25 The Cybersecurity Market (Room G)
Analyzing the Sustainability of Growth in the Global Cybersecurity Market.

Eugene Kaspersky CEO, Kaspersky	**Fahad Al-Jutaily** CEO, sirar by STC	**Sheikh Salman bin Mohammed Al Khalifa** CEO, The National Center for Cybersecurity, Bahrain	*Moderator*: **Rawan Radwan** Deputy Section Head, Arab News

14:50 - 15:25 The Topography of Cyber Threats (Room C)
A Glimpse Into the Evolving Landscape of Cyber Threats.

Pierre-Yves Jolivet Vice President, Cyber Defence Solution Business Line, Thales	**Helmut Reisinger** CEO EMEA & LATAM, **Palo Alto Networks**	**Chris Gibson** Executive Director, Forum of Incident Response & Security Teams	**Nezar AlOmar** Cyber Technologies & Operations Deputy Governor, National Cybersecurity Authority, Saudi Arabia	**David Kanamugire** Chief Executive Officer, National Cyber Security Authority (NCSA), Rwanda	*Moderator*: **Chris Fox** Technology Presenter, BBC

15:25 - 15:35 Cybersecurity for Critical National Infrastructure (Room G)
Protecting the Future Smart Cities.

Eng. Nadhmi Alnasr
CEO, NEOM

15:25 - 16:00 Promoting Internet Security Best Practices (Room C)
Sharing and Learning from Successful Experiences.

Hanna M. Kreitem Senior Advisor, Internet Society	**John Crain** SVP, Chief Technology Officer, ICANN	**Dr. Chafic Chaya** Regional Manager Public Policy and Government Affairs - Middle East Region, RIPE NCC	*Moderator*: **Baher Esmat** Regional Vice President for Stakeholder Engagement in the Middle East, and Managing Director for the Middle East and Africa (MEA) Regional Office, ICANN

15:35 - 16:00 Divergent Futures (1/2) (Room G)
A Scenario-based Session Examining the Future of the Cybersecurity Landscape.

Gwenda Fong Assistant Chief Executive, Strategic Planning & Digital Readiness, Infocomm Media Development Authority (IMDA), Singapore	**Pano Yannakogeorgos** Clinical Associate Professor and Program Director, New York University, Center for Global Affairs	*Moderator*: **Rudolph Lohmeyer** Partner, Kearney

Global Cybersecurity Forum 2022 Edition

DAY ONE: WEDNESDAY, 9 NOVEMBER 2022

16:15 - 16:40 Divergent Futures (2/2) (Room G)
A Scenario-based Session Examining the Future of the Cybersecurity Landscape.

Gwenda Fong Assistant Chief Executive, Strategic Planning & Digital Readiness, Infocomm Media Development Authority (IMDA), Singapore	**Pano Yannakogeorgos** Clinical Associate Professor and Program Director, New York University, Center for Global Affairs	*Moderator*: **Rudolph Lohmeyer** Partner, Kearney

16:15 - 16:50 The Future is Female (Room C)
Unique Benefits of Gender Diversity in the Cybersecurity Workforce.

Monique Morrow Sr. Distinguished Architect, Emerging Technologies, Syniverse	**Nathalie Rivat** VP System Engineering, Fortinet	**Shoaib Yousuf** Managing Director and Partner, Boston Consulting Group	*Moderator*: **Rebecca McLaughlin-Eastham** TV Anchor & MD, RME Media

16:50 - 17:25 Move Fast and Break Things? (Room G)
How VCs and Tech Accelerators are Driving Cyber Advancement.

Oliver Tavakoli Global CTO, Vectra AI	**Peter Sund** CEO, Finnish Information Security Cluster	**Seena Amidi** Managing Director of EMEA and Board Member, Plug and Play	*Moderator*: **Basmah M. Aljedia** Cybersecurity Industry & Local Content Development General Manager, National Cybersecurity Authority

16:50 - 17:25 The Race for Quantum Supremacy (Room C)
As States and Private Sector Players all Race Toward Supremacy, What are the Implications for Cybersecurity?

Visa Vallivaara Senior Scientist, VTT Research Centre of Finland	**Charles Lim** Global Head of Quantum Communications and Cryptography, JPMorgan Chase & Co	**Simon Sinisha Patkovic** VP Quantum Safe Solutions, IDQuantique	**Bilel Jamoussi** Chief of the Study Groups Department, ITU Standardization Bureau (TSB)	*Moderator*: **Chris Fox** Technology Presenter, BBC

17:25 - 18:00 Fierce Competition (Room G)
The Battle Over Cyber Talent and the Driving Forces of Talent Concentration.

Flavio Aggio Chief Information Security Officer (CISO), World Health Organization (WHO)	**Adrian Victor** General Director, National Institute for Research and Development in Informatics - ICI, Bucharest	**George Patsis** CEO, Obrela Security Industries	*Moderator*: **Sasha Qadri** Journalist

17:25 - 18:00 Geo-technological Competition and Conflict (Room C)
The Coming Battles in Technology, Internet Infrastructure, and Global Governance.

Dr. Beyza Unal Head of Science, Technology and International Security Unit, UN Office for Disarmament Affairs (UNODA), New York	**Sunjoy Joshi** Chairman and Chief Executive, The Observer Research Foundation (ORF), New Delhi	*Moderator*: **Ramia Farrage** Senior Presenter and Producer, Forbes Middle East

Global Cybersecurity Forum 2022 Edition

DAY TWO: THURSDAY, 10 NOVEMBER 2022

09:10 - 09:50 Rethinking the Global Cyber Order, Why? (Room G)
Cyber Economics and Future of Cyber Work.

Ian Goldin Professor of Globalisation and Development, University of Oxford	**Andreas Ekstrom** Award Winning Journalist Author and, Digital Futurist	*Moderator*: **John Defterios** Former CNN Emerging Markets Editor & Professor of Business, NYU Abu Dhabi

09:50 - 10:25 Pervasive and Insecure (Room C)
Illuminating the Threat of Supply Chain and Third-Party Attacks.

Mary O'Brien General Manager, IBM Security	**Ben Miller** Vice President of Services, Dragos Inc.	**Victoria Coates** Senior Fellow for International Relations and National Security, The Heritage Foundation	**Lothar Renner** Managing Director, Cisco Security, EMEA	**Dr. Albert Antwi-Boasiako** Ag. Director-General, Cyber Security Authority, Republic of Ghana	*Moderator*: **Sasha Qadri** Journalist and *Moderator*

09:50 - 10:25 Shaping Markets (Room G)
Proactive Public–Private Approaches to Shaping Markets and Driving Cyber Innovation.

Dr. Mohamed Al Kuwaiti Head of Cyber Security, United Arab Emirates Government	**Paul Griswold** Chief Product Officer, Cybersecurity, Honeywell	**Francois Candelon** Managing Director and Senior Partner, BCG Henderson Institute	**Fabien Rech** Senior Vice President EMEA, Trellix	*Moderator*: **Rebecca McLaughlin-Eastham** TV Anchor & MD, RME Media

10:25 - 11:00 Cybersecurity at the Heart of the Next-Gen Telco (Room G)
Best Practices to Ensure Telco Resilience in Cyberspace.

Bocar Alpha BA. CEO & Board Member, SAMENA Telecommunications Council FZ LLC	**Jabiri Kuwe Bakari** Director General, Tanzania Communications Regulatory Authority	**Konstantinos Masselos** President, Hellenic Telecommunications & Post Commission (EETT)	*Moderator*: **Chris Fox** Technology Presenter, BBC

10:25 - 11:00 AI for Child Protection (Room C)
The Importance of Multi Stakeholder Collaboration.

Irakli Beridze Head, Centre for Artificial Intelligence and Robotics, UNICRI, United Nations	**Yalda Aoukar** Co-Founder and Managing Partner, Bracket Capital	**Lt. Col. Dana Humaid** Director General, International Affairs Bureau, Ministry of Interior, United Arab Emirates	**Laura Taddei** Director of Business Affairs, BenevolentAI	*Moderator*: **Iain Drennan** Executive Director, WeProtect Global Alliance

Global Cybersecurity Forum 2022 Edition

DAY TWO: THURSDAY, 10 NOVEMBER 2022

11:15 - 11:50 Mind the Gap (Room C)
Identifying and Responding to the Challenges for Women in Cybersecurity.

Juliette Wilcox UK Cyber Security Ambassador, His Majesty's Government (UK Government)	**Olga Botero** Co-Founder and Chair, Seccuri Inc	**AnaMaria Meshkurti** WEF Global Shaper, Fongit	*Moderator*: **Stefan Deutscher** Partner & Associate Director, BCG

11:15 - 11:50 Shaping the Global Cybersecurity Agenda (Room G)
A Global Framework for Dialogue and International Cooperation.

Marco Obiso Chier a.i. Digital Networks and Society Department, International Telecommunication Union	**Vanessa Copetti Cravo** Telecommunication Regulation Expert Cybersecurity Technical, ANATEL	**Howard Taylor** Executive Director, Global Partnership to End Violence Against Children	*Moderator*: **Andrea Rigoni** Senior Partner - EU Digital Policy Director, Deloitte Risk Advisory

11:50 - 12:25 FinTech - Catalysts for Transformation (Room C)
Realizing National Transformation Through Responsible Fintech.

Issam Abousleiman Regional GCC Director, World Bank	**Martin Boer** Senior Director, Regulatory Affairs, Institute of International Finance (IIF), Washington	*Moderator*: **Sasha Qadri** Journalist

11:50 - 12:10 Hacking the Mind of a Cybercriminal (Room G)
Examining the Motivation and Psychology of Cybercriminals.

Mary Aiken Professor of Cyberpsychology and Chair of the Department of Cyberpsychology, Capitol Technology University	*Moderator*: **Marco Gercke** Director, Cybercrime Research Institute

12:10 - 12:30 Trust in Emergent Technologies (Room G)
Trust in Emergent Technologies

Amandeep Singh Gill UN Secretary - General Envoy on Technology, United Nations	*Moderator*: **Rudolph Lohmeyer** Partner, Kearney

Global Cybersecurity Forum 2022 Edition

DAY TWO: THURSDAY, 10 NOVEMBER 2022

12:25 - 13:00 Post Quantum Cryptography (Room C)
Harnessing Cryptographic Engineering to Maximize Device Security.

Sang-Yoon Chang Associate Professor, University of Colorado Colorado Springs	**Sylvain Guilley** General Manager and CTO, Secure-IC	**Kim Ik Kyun** Assistant Vice President, Cyber Security Research Division, Electronics and Telecommunications Research Institute (ETRI), Korea	**Dr. Godfrey Gaston** Cybersecurity Innovation Consultant	*Moderator*: **Sasha Qadri** Journalist and *Moderator*

12:30 - 13:00 The Security of Algorithms (Room G)
Understanding the challenges and opportunities of AI.

Piotr Ciepiela Partner, Global Cyber Architecture, Engineering & Emerging Technologies Leader, EY	**Preetam Maloor** Head, Emerging Technologies Division, ITU/ UN	**Kashif Kifayat** Chairman /Director NCCS, National Centre for Cyber Security	*Moderator*: **Chris Fox** Technology Presenter, BBC

14:00 - 14:35 'Whole of Society' Cyber Awareness (Room C)
Cultivating a Culture of Cyber Awareness and Cyber Hygiene.

Alexander Mejia Director, Division for People and Social Inclusion, UNITAR	**Nadezhda Neynsky** Former Foreign Minister of Bulgaria, Former Ambassador to Turkey, Member of 2022 Cohort of Advanced Leadership Initiative (ALI), Harvard	**Esa Alsumiri** Member, Saudi Shura Council	*Moderator*: **Rebecca McLaughlin-Eastham** TV Anchor & MD, RME Media

14:00 - 14:35 Metrics for Success (Room G)
Co-creating a Global Measurement for the Child Online Safety Index.

Dr. Yuhyun Park Founder, DQ Institute	**Sri Chandrasekaran** Sr. Director, IEEE Standards Association	**Mark Zelman** Consultant, World Bank	*Moderator*: **Chris Fox** Technology Presenter, BBC

14:35 - 15:10 Securing Development (Room C)
How to Accelerate a Trusted and Secured Global Development.

John Omo Secretary General, African Telecommunications Union (ATU)	**Masanori Kondo** Secretary General, Asia-Pacific Telecommunity	**Rodney Taylor** Secretary-General, Caribbean Telecommunications Union	**Mohamed Ben Amor** Secretary General, Arab ICT Organization	*Moderator*: **Sasha Qadri** Journalist

Global Cybersecurity Forum 2022 Edition

DAY TWO: THURSDAY, 10 NOVEMBER 2022

14:35 - 15:10 Co-Creating the Future of Cyber (Room G)
How Regulators and Tech Companies Can Create Optimized Regulatory Environments.

Purvi Kay Head of Cyber Security Governance, Risk and Compliance, BAE Systems PLC	**Kevin Emery** Global Director of Cybersecurity, UL Solutions	**Hazim Almuhimedi** Risk & Compliance Deputy Governor, National Cybersecurity Authority, Saudi Arabia	*Moderator*: **Ramia Farrage** Senior Presenter and Producer, Forbes Middle East

15:25 - 16:00 Unleashing the Potential of the Cloud (Room G)
Stakeholders' Engagement for Adaptive Solutions to Secure the Cloud.

Mark Ryland Director of the Office of the Chief Information Security Officer, Amazon Web Services	**Abbas Kudrati** APAC Chief Cybersecurity Advisor, Microsoft	**Suliman Alsamhan** Chief Executive Advisor, SITE, Saudi Arabia	*Moderator*: **Rawan Radwan** Deputy Section Head, Arab News

15:25 - 16:00 Pathways to Regional Cyber De-escalation (Room C)
Protecting the Middle East from Future Threats.

Mohammed Soliman Manager, McLarty Associates	**Steph Shample** Non-Resident Scholar, Middle East Institute	**Bassant Hassib** Assistant Professor of Political Science, The British University in Egypt	*Moderator*: **Rebecca McLaughlin-Eastham** TV Anchor & MD, RME Media

16:00 - 16:35 Intelligence in Real Time (Room G)
How Technology and Partnerships Can Revolutionize Information Sharing.

Adrian Colbrook Strategic Growth Director, BAE Systems Digital Intelligence	**Oliver Väärtnõu** CEO, Cybernetica	**Christopher Ahlberg** CEO/Co-founder, Recorded Future Inc.	**Dr. Bushra AlAhmadi** Engineering Consultant, SITE, Saudi Arabia	*Moderator*: **Sasha Qadri** Journalist and *Moderator*

16:00 - 16:35 The Cyber Corps (Room C)
Public-Private Partnerships that Build Elite Cadres of Cyber Professionals.

Almerindo Graziano CEO, Cyber Ranges	**Andrés Jesús Ruiz** Senior Policy Advisor, Cybersecurity Unit, National Security Department, Cabinet of the Prime Minister, Spain	**Aapo Cederberg** Founder and CEO, Cyperwatch Finland	**Joe Sarno** Senior Vice President for International Sales APJ & Emerging, Fortinet Inc	*Moderator*: **Chris Fox** Technology Presenter, BBC

16:35 - 16:45 Closing Ceremony (Room G)

Ramia Farrage
Senior Presenter and Producer, Forbes Middle East



The next chapter

The 2022 edition of the Global Cybersecurity Forum provided an unprecedented opportunity to Rethink the Global Cyber Order. Discussions across the Forum crystalized that the global cyber order is still in the early stages of accelerated transformation. To not just prepare for the emerging future of the cyber order, but to shape it in ways that are aligned with our shared interests and values, requires new perspectives and collaboration between countries, the public and private sector and civil society.

It is the intention of the Global Cybersecurity Forum to continue to evolve in the years ahead into an action and initiative oriented global platform, that integrates the global cybersecurity community and helps shape the future of Cyberspace.

We look forward to seeing you at the next edition. ■



www.globalcybersecurityforum.com