



Global
Cybersecurity
Forum

ORGANIZED BY



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

GLOBAL CYBERSECURITY FORUM

2023 EDITION

GLOBAL CYBERSECURITY FORUM

2023 EDITION



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

The GCF Rule

The GCF is a platform that focuses on multistakeholder collaboration and action in Cyberspace, aiming to unite global efforts, address systemic challenges, and unlock opportunities. We aspire to be inclusive of the entire global community as we explore and collaborate on topics of critical shared concern, and delve into the intersections of technology, geopolitics, economics, and human behavior that characterize the uniquely complex Cyber domain. Through multistakeholder dialogue, we expect our attendees and speakers to identify practical, productive pathways of collaborative action in order to work toward tangible outcomes. We are also committed to supporting our participants in building networks and enduring relationships for continued collaboration long after the Annual Event's conclusion.

Thus, the GCF Rule is: Embrace diverse perspectives, engage in disruptively innovative thinking, advance substantive action, and follow through.

CONTENT

SECTION ONE

01

ABOUT
GCF

▶ 012



SECTION TWO

02

2023
EDITION

▶ 018



SECTION THREE

03

PROCEEDINGS

▶ 036



SECTION FOUR

04

KEY TAKEAWAYS

▶ 096



SECTION FIVE

05

OUTREACH AND
COLLABORATION

▶ 106



1



ABOUT GCF



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 that aims 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 strategic, socioeconomic, and geo-political issues of which Cybersecurity is a part of. ■



ABOUT GCF INSTITUTE

GCF Institute is a global non-profit organization committed to enhancing Cyberspace security and resilience. Through collaborative efforts, purposeful dialogue, and impactful initiatives, the institute unites global endeavors, champions actions to advance Cybersecurity, and fosters positive socio-economic impact.

GCF Institute aims to catalyze social impact, foster a thriving Cybersecurity ecosystem, push the boundaries of knowledge, advance collaboration and collective dialogue, and strives to become a leading world-class institute.

This involves pioneering social impact initiatives such as “Child Protection in Cyberspace” and “Women Empowerment in Cybersecurity”. It also implies nurturing global Cybersecurity human capital, accelerating sector growth through various support initiatives, strengthening thought leadership and knowledge sharing in Cybersecurity, and ensuring excellence to become a reference organization globally.

The institute operates as an independent non-profit global organization, governed by a global Board of Trustees to guide the institute direction and a Chief Executive Officer overseeing the institute’s operational efforts.

The institute acts as a collaborative hub, offering a space where global Cybersecurity stakeholders come together to collaborate and enact positive change. By leveraging intellectual power and promoting multilateral collaboration, GCF Institute strives to drive significant improvements in the Cybersecurity landscape for the benefit of people of all backgrounds and nations.

GCF Institute aims to strengthen global Cyberspace security and resilience through collaborative priorities, purpose-driven dialogue, and impactful initiatives

2



2023 EDITION



2023 EDITION CHARTING SHARED PRIORITIES IN CYBERSPACE

 01 - 02
November



164
Speakers



120+
Countries



35
Sessions

CHARTING SHARED PRIORITIES IN CYBERSPACE

The forum has charted shared priorities across five thought-provoking sub-themes:



Cyberspace Amidst Polycrisis

Advancing action for Cyber stability and progressing multilateral Cybersecurity in a global environment of overlapping crises and institutional challenges.



Cyber Growth Unlocked

Stimulating markets, shaping incentives, and building global public Cyber goods into how Cyber economics can be steered, driving growth in the Cybersecurity sector to meet current and future challenges and needs.



Across Cyber Divides

Building a human-centered and inclusive Cyberspace, asking how we can bridge social and developmental divides across stakeholders and within organizations and institutions.



Inside Cyber Minds

Exploring behavioral levers and motivations in Cyberspace maps, the behavioral and psychological aspects of Cybersecurity and Cybercrime, and illuminating the impacts of behavior and decision-making in Cyberspace.



Emerging Cyber Horizons

Maximizing the benefits of paradigm-shifting technologies, considering the future of emerging technologies and their Cybersecurity dimensions, and how we can harness their accelerative properties.

OPENING SPEECH BY

HIS ROYAL HIGHNESS PRINCE FAISAL BIN BANDAR BIN ABDULAZIZ, GOVERNOR OF RIYADH

Distinguished participants and guests,

We warmly welcome you to the Kingdom of Saudi Arabia, and on behalf of the Custodian of the Two Holy Mosques King Salman bin Abdulaziz Al Saud, I am honored to open the 2023 edition of the Global Cybersecurity Forum.

Esteemed guests,

This year's edition of the forum comes under the theme of "Charting Shared Priorities in Cyberspace". Our world today is experiencing rapid developments in the field of Cybersecurity, and these developments have made it imperative to enhance cooperation and double our joint efforts in dealing with them and benefiting from the opportunities they bring, to achieve the well-being and prosperity of humanity around the world.

We are confident that the presence of esteemed experts, decision-makers, and specialists from around the world will maximize the outcomes of the forum and provide a summary of international experiences relevant to vital and strategic topics in the field of Cybersecurity. The aim is to reach a safe and trusted Cyberspace that encourages progress and innovation and enables growth and prosperity for all peoples of the world.

Distinguished guests, I thank you for your presence, and I wish everyone success at this forum.

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



OPENING SPEECH BY

H.E. MAJED BIN MOHAMMED AL-MAZYED, GOVERNOR OF THE NATIONAL CYBERSECURITY AUTHORITY (NCA), SAUDI ARABIA

Your Royal Highness,
Your Excellencies,
Ladies and Gentlemen,

I am pleased to welcome you to Riyadh for the 2023 Global Cybersecurity Forum.

GCF is a space where we transcend physical and conceptual borders to come together as a community, share ideas, and drive forward progress in the crucial domain of Cyberspace.

At GCF 2022, we welcomed over 9,000 participants from 117 countries. Together, we took great strides in fostering engagement among diverse stakeholders and advancing our collective knowledge of the challenges and opportunities of Cyberspace.

Since then, the GCF Institute was established by Royal Decree earlier this year as an independent global nonprofit organization, and will act as a global platform committed to strengthening Cyber resilience through shared priorities, purposeful dialogue, and impactful initiatives.

Today, we come together to collaborate on our common interests under the theme of “Charting Shared Priorities in Cyberspace”. We will build upon last year’s deep exploration into the most pressing Cyberspace issues and lay the groundwork for collaborative action which will transform our goals into tangible results for the future.

We are committed to bridging social and developmental divides, making sure no one is left behind, and unleashing the potential of Cyberspace to ensure that its opportunities are accessible to people all over the world, including our most underserved communities.

We look forward to engaging with all of you as, together, we plan this next phase of the GCF journey.

I thank each of you for your commitment to enabling GCF’s mission to enhance Cyber resilience on a global scale. Through our collective efforts, we are shaping the future of Cyberspace to ensure it is an enabler of both our security and our prosperity.

Thank you.

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





GCF 2023 PROGRAM FORMAT

GCF 2023: A new format to deliver on the objectives

The Global Cybersecurity Forum is a platform dedicated to achieving tangible results and discovering solutions for Cyber challenges. The 2023 edition has been specifically designed to facilitate discussions and address shared issues among stakeholders. To accomplish this goal, the forum consists of two main tracks:

- ▶ **An Open Forum**, to deliver forward-leaning Cybersecurity knowledge in an accessible manner for all attendees, providing new perspectives and multidisciplinary lenses on a wide range of topics across the Cybersecurity and related fields.
- ▶ **A Participatory Track**, to facilitate engaging and dialogue-driven discussions, deliver valuable insights, and drive actionable progress on shared priorities in Cyberspace in closed door sessions. This year, the participatory track consisted of policy briefs, global insight sessions, knowledge community meetings, a Cyber simulation, a CxO meeting, and a high-level multi-stakeholder roundtable. ■

Global Cybersecurity Forum 2023 Program Format

Open Forum

- ▶ Open to all forum participants, the open forum program discusses the most pressing challenges, opportunities and priorities in Cyberspace across the sub-themes. It provides insights for industry leaders, decision makers and relevant stakeholders.

Plenary

- ▶ The opening session of the day's events with a panel discussion on a key topic in Cybersecurity to gather perspectives and identify collaborative actions.

Panel

- ▶ An engaging conversation with diverse leaders and experts on a specific topic of Cybersecurity to understand the challenges and potential pathways.

Fireside Chat

- ▶ One-on-one discussion with a Cybersecurity leader to gather perspectives, and insights on a specific domain of Cyberspace.

Participatory Track

- ▶ Invite-Only Program that gathers relevant stakeholders, and has an interactive nature to drive discussions, chart shared priorities, and result in collective actions in Cyberspace.

High-Level Roundtable

- ▶ Invite-Only High-Level Multi-Stakeholder Roundtable, in which government representatives, industry leaders, and IOs/NGOs representatives discuss Cybersecurity challenges each stakeholder group is facing and interventions that other groups can provide to support them in addressing these challenges.

CxO Meeting

- ▶ Invite-Only session that brings together C-suite representatives of globally reputed Cybersecurity companies in order to discuss challenges and emerging trends in Cybersecurity, its implications for private sector entities, and productive pathways for collaborative actions.

Deep Dives

- ▶ Invite-Only session that focuses on a key emerging topic of relevance in Cyberspace and shapes potential actions and collaboration mechanisms.

Knowledge Communities Meeting

- ▶ Invite-Only session bringing together a globally diverse group of entities with shared interests in the Cybersecurity domain, to discuss collaborative and collective actions.



GLOBAL CYBERSECURITY FORUM 2023 PROGRAM

OPEN FORUM

November 1, 2023 (Day 1 - Morning)

09:30 - 10:00 | **Opening Ceremony**

10:00 - 10:45 | **The Evolving Dynamics of Cyberspace**
Assessing the Landscape of Changing Strategic Priorities in Cyberspace



Plenary

10:45 - 11:00 | **Coffee Break** ☕

11:00 - 11:25 | **Securing Tomorrow**
Building Resilience Through Education



Fireside Chat

11:25 - 12:10 | **Supply Chain Fortification**
Safeguarding the Cyber Resilience of the Global Supply Chain



Panel Discussion

12:10 - 12:55 | **Catalyzing Cyber**
Stimulating Cybersecurity Market through Ecosystem Development



Panel Discussion

13:00 - 14:00 | **Lunch Break** 🍴

GLOBAL CYBERSECURITY FORUM 2023 PROGRAM

OPEN FORUM

November 1, 2023 (Day 1 - Afternoon)

14:00 - 14:35 | **Widening Lens**
A New Narrative for Media Coverage of Cyberspace



Panel Discussion

14:35 - 14:55 | **Smoke & Mirrors**
Social Engineering and Sophisticated Phishing



Fireside Chat

14:55 - 15:30 | **Cybercrime and Law Enforcement**
Conceiving Jurisdiction in a Borderless Space



Panel Discussion

15:30 - 15:55 | **Tech Transformed Cybersecurity**
AI's Role in Securing the Future



Panel Discussion

15:55 - 16:05 | **Coffee Break** ☕

16:05 - 16:30 | **Ready for Goodbyes?**
Critical System Obsolescence



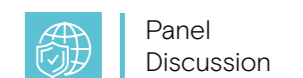
Panel Discussion

16:30 - 17:05 | **Hello from the CyberVerse**
Maximizing the Benefits of Future Technologies



Panel Discussion

17:05 - 17:30 | **The State of Cyber Diplomacy**
Momentum, Inertia, or Something Else Altogether?



Panel Discussion

GLOBAL CYBERSECURITY FORUM 2023 PROGRAM

OPEN FORUM

November 2, 2023 (Day 2 - Morning)

- 09:45 - 10:10** | **Sustainability at Risk**
Drawing Insights from Climate Talks to Elevate Cybersecurity



Plenary,
Fireside Chat
- 10:10 - 10:45** | **Omnipresent Smart Wireless**
Deploying Future Networks at Scale



Panel
Discussion
- 10:45 - 11:15** | **Safe Surfing**
Understanding Child Online Activity



Panel
Discussion
- 11:15 - 11:30** | **Coffee Break** ☕
- 11:30 - 12:05** | **Cyber Costs Reframed**
The Human Costs of Cyber Insecurity



Panel
Discussion
- 12:05 - 12:45** | **Cognitive Vulnerabilities**
Why Humans Fall for Cyber Attacks




Panel
Discussion
- 12:45 - 14:00** | **Lunch Break** 🍴

GLOBAL CYBERSECURITY FORUM 2023 PROGRAM


OPEN FORUM

November 2, 2023 (Day 2 - Afternoon)


- 14:00 - 14:30** | **Behavior Unmasked**
The Effects of Anonymity on Online Activity




Fireside
Chat
- 14:30 - 15:00** | **Cyberspace Needs You**
Attracting Women to Cybersecurity Careers




Panel
Discussion
- 15:00 - 15:15** | **Coffee Break** ☕
- 15:15 - 15:45** | **It's Over for Turnover**
Retaining Talent in Cyberspace



Panel
Discussion
- 15:45 - 16:20** | **Shaping Investment**
Spurring Investment in Cyber Sector Start-Ups



Panel
Discussion
- 16:20 - 16:55** | **Emerging Shadows**
Unmasking Cyber Threats of Generative AI



Panel
Discussion
- 16:55 - 17:10** | **Closing**

GLOBAL CYBERSECURITY FORUM 2023 PROGRAM

PARTICIPATORY TRACK

November 1, 2023 (Day 1)

- | | |
|---------------|--|
| 11:30 - 12:00 | Global Insight Session:
Evolving Threat Landscape for Children in Cyberspace, Implication and Potential Avenues for Collaboration. |
| 12:00 - 13:00 | Knowledge Community Meeting:
Securing Industrial Systems for Global Energy Supply. |
| 14:00 - 15:00 | CxO Meeting:
C-suite Meeting, Invite Only Session, to Discuss Challenges, Implications, and Collaborative Pathways of Action in Cybersecurity. |
| 14:30 - 15:00 | Deep Dive Session:
Cyber Psychology for Active Cyber Defense. |
| 15:30 - 16:30 | Knowledge Community Meeting:
Securing the Future of Urban Living. |
| 16:00 - 16:30 | Deep Dive Session:
Closing the Talent Gap: Frameworks for Capacity Building. |

GLOBAL CYBERSECURITY FORUM 2023 PROGRAM

PARTICIPATORY TRACK

November 2, 2023 (Day 2)

- | | |
|---------------|--|
| 09:00 - 09:30 | Breakfast:
Women in Cyber. |
| 10:20 - 11:00 | Cyber Simulation:
Live Interactive and Immersive Experience Engaging Multi-stakeholders with High Degree of Practical Knowledge Transfer and Engagement. |
| 11:00 - 12:00 | Knowledge Community Meeting:
Safeguarding the Future Networks & Emerging Technologies. |
| 12:00 - 12:30 | Policy Brief:
Child Protection in Cyberspace. |
| 12:15 - 13:15 | Knowledge Community Meeting:
Future of Cybersecurity. |
| 14:00 - 15:30 | High-Level Multi-Stakeholder Roundtable
From Shared Challenges to Collective Action. Invite Only Session with Public, Private, and IO Leaders on Cyber Challenges and Potential Actions. |
| 14:30 - 15:00 | Deep Dive Session:
Security in the Metaverse. |

3

PROCEEDINGS





OPEN FORUM



Cyberspace Amidst Polycrisis **OPEN FORUM**

Plenary Session

The Evolving Dynamics of Cyberspace

| Assessing the Landscape of Changing Strategic Priorities in Cyberspace

- ▶ **H.E. Kersti Kaljulaid** Former President, Estonia
- ▶ **H.E. Jose Manuel Barroso** Former President, European Commission and Former Prime Minister, Portugal
- ▶ **H.E. Shyam Saran** Former Foreign Secretary, India
- ▶ **John Defterios (Moderator)** Former CNN, Emerging Markets Editor and Anchor

The two-day annual event began with a captivating session that set context for the following two days of substantive dialogue, as speakers from around the globe led the GCF community in charting shared priorities. The world leaders sitting on the panel of the plenary session “The Evolving Dynamics of Cyberspace” each offered incisive views on the unique challenges and opportunities posed in Cyberspace, based on their own experiences leading nations in negotiation and effort to make progress on challenging yet crucial topics. The panelists emphasized that the unique challenges and opportunities of Cyberspace necessitate consideration of novel approaches to

“These are Cyber Challenges, which no country, no matter how powerful it is, can hope to resolve by its own. You need collaboration.”

H.E. Shyam Saran

“I believe we need places like this that can offer a platform for cooperation, and I hope that can be developed so this global conversation, and hopefully some action can take place.”

H.E. Jose Manuel Barros



enhance its security and stability, and highlighted a wide range of examples from which inspiration can be drawn to drive forward collaborative action.

Panelists agreed that the current global Cybersecurity landscape is increasingly fragmented amid a global environment of escalating geopolitical tensions and rapidly evolving emerging technologies. This fragmentation is compounded by Cyber capability disparities between countries, with clear need demonstrated by many in the global south, and a lack of diversity in the global workforce. Together, these factors have slowed progress in Cyberspace. Panelists emphasized that progress often calls for trade-offs between scale and speed. President Barroso gave the example of the European Union’s General Data

Protection Regulation (GDPR)—first proposed in 2006-07 but only entering into force in 2016—as an illustration of the great value of collaborative action, but also of the oftentimes slow movement it requires. In light of the urgency of the challenges presented by Cyberspace, speakers suggested kick-starting progress by forming coalitions of actors with shared priorities wherever possible.

In conclusion, panelists asserted that Cybersecurity is and must be recognized as a collective, high-priority issue—and the shared responsibility of all nations. One key pathway of progress highlighted by the speakers can be found in the development of global collaborative mechanisms to foster multi-stakeholder collaboration—including such fora as the GCF. ■

89%

of electricity, oil & gas, and manufacturing firms supporting critical infrastructure experienced Cyber attacks in 2022. Consequently, the oil and gas sector increased its spending on cybersecurity (Source: Trend Micro)

“And here I see the great role for countries like Saudi Arabia, to cooperate and call also for industry to define the set of standards together with governments.”

H.E. Kersti Kaljulaid

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Inside Cyber Minds OPEN FORUM

Fireside Chat

Securing Tomorrow

| Building Resilience Through Education

- ▶ **H.E. Yousef Al-Benyan** Minister of Education, KSA
- ▶ **Nisha Pilai (Moderator)** International Moderator, Former BBC Presenter

In “Securing Tomorrow,” H.E. Yousef Al-Benyan asserted that the continuous expansion and evolution of the technological landscape demands a new paradigm in education. It is critical, he stressed, for the global community to lay the groundwork for a resilient future by nurturing Cybersecurity literacy and growing the global Cyber skillset—starting with our youngest generation.

Al-Benyan highlighted the central importance of values in Cyber education—and their role in shaping curricula that align with national and societal norms and expectations. As emerging technologies—and AI in particular—change the ways our classrooms look and operate, it is critical that we teach our children to engage with these powerful new tools in safe and respectful ways. Global awareness raising and capacity development campaigns are of central importance in this regard. Al-Benyan also noted two critical features of the ways in which young people engage in Cyberspace—they both lack awareness of threats and demonstrate a limited sense of caution. In light of these behaviors, he emphasized that we must make young populations aware of the risks that can be faced on an individual and systemic level.



Looking forward, Al-Benyan noted that governments must take a whole-of-ecosystem approach to Cybersecurity education. This should include partnering with the private sector for awareness raising, developing the knowledge and capabilities of teachers, and implementing safe and secure AI standards for the classroom—with a particular focus on ethics and values. ■

50%
of ransomware attacks succeed due to bad user education and practices (Source: Lumifi Cyber)



To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Cyberspace Amidst Polycrisis OPEN FORUM

Panel Discussion

Supply Chain Fortification

| Safeguarding the Cyber Resilience of the Global Supply Chain

- ▶ **Amin H. Nasser** CEO, Aramco
- ▶ **Dr. Saad Saleh Alaboodi** CEO, SITE
- ▶ **Michael Ruiz** Vice President, Honeywell
- ▶ **Christophe Blassiau** Senior Vice President, Schneider Electric
- ▶ **Ryan Chilcote (Moderator)** International Moderator, Former Bloomberg, CNN, CBS, PBS, and Fox News

In his opening remarks, Amin Nasser set the tenor for a wide-ranging conversation on the critical importance of Cyber resilience in global supply chains. He emphasized that building resilience across the value chain is critical—as one weak link can cause a large-scale disruption with significant impact across the world. To illustrate the role of private sector actors in resilience, he provided the example of Aramco—which regularly runs checks on the Cybersecurity capabilities of its vendors and suppliers. While the pace of digitalization and technological change is sometimes alarming, emerging technologies must, he emphasized, be leveraged to enhance efficiencies.

Nasser noted the various efforts Aramco is undertaking to ensure a secure Cyberspace. Such efforts include the formal establishment of an Operational Technology Cybersecurity Center of Excellence (OTC COE), a partnership with Georgia Tech for a Master of Science Cybersecurity program with cutting-edge curriculum, and contributions as a founding member of the World Economic Forum (WEF) Center for Cybersecurity. These efforts are illustrations of already ongoing multi-stakeholder collaboration, though more is required specifically to develop standards and more effective governance of current and emerging technologies—and ultimately, to uphold our collective Cyber commitments.

600%
increase in supply chain attacks in 2022 from 2021 (Source: CSO)



Panelists in the “Supply Chain Fortification” session echoed and built upon Amin Nasser’s remarks, emphasizing that supply chain vulnerabilities can cascade into far-reaching disruptions, posing significant Cybersecurity risks that may not only disrupt an organization’s operations, but further cascade into negative impacts on entire economies and long-term advances in innovation.

Clearly, Cyber-attacks are not siloed by sector, though Cybersecurity approaches largely have been. In reality, all sectors are only becoming increasingly integrated, as energy, healthcare, and others rely upon connective critical infrastructures to function. In particular, the convergence of Operational Technology (OT) and Information Technology (IT) represents a significant challenge, as OT Cybersecurity lags to that of IT Cybersecurity substantially. With OT systems being a critical feature of many of the worlds vital systems, including notably energy and industry, it is critical to develop Cybersecurity solutions that work across all systems as they increasingly integrate. While

emerging technologies introduce new challenges and vulnerabilities in many ways, they also present new opportunities to advance supply chain efficiencies and security.

Ultimately, panelists asserted that some degree of autonomy should be respected by all stakeholders, yet each of us plays a role: policymakers to catalyze international collaboration, industry players to ensure the security of economic assets, and large tech players to inject Cybersecurity in all products and services. Still, panelists emphasized that governments must be interconnected globally and must encourage multi-stakeholder forums and frameworks to harmonize standards and build a common lexicon. ■

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:

Cyber Growth Unlocked **OPEN FORUM**

Panel Discussion

Catalyzing Cyber

| Stimulating Cybersecurity Market through Ecosystem Development

- ▶ **H.E Eng. Abdulrahman Ali Al-Malki** President, National Cyber Security Agency, Qatar
- ▶ **Felix A. Barrio Juarez** Director General, INCIBE, Spain
- ▶ **Dr. Megat Zuhairy bin Megat** CEO, National Cybersecurity Agency, Malaysia
- ▶ **Eng. Walid Abukhaled** CEO, SAMI, KSA
- ▶ **John Deferios (Moderator)** Former CNN, Emerging Markets Editor and Anchor

The panelists in the “Catalyzing Cyber” session introduced discussion of the critical imperative for Cybersecurity ecosystem development in order to grow the Cybersecurity market. Increased R&D and demand pull from various sectors can shape broader Cybersecurity market growth, yet there are also clear opportunities for intervention by government actors to spur and shape innovation. Speakers highlighted key opportunities to harmonize Cybersecurity standards and regulations and noted the benefits of strategic planning for national Cybersecurity ecosystem development, inclusive of effective governance, legislative enforcement, capacity building, and global collaboration.

Panelists stressed the direct relationship between safety, Cybersecurity, and prosperity of all nations. The importance of both education and direct investments in digital transformations to strengthen national ecosystems cannot be overstated. Panelists also noted the challenges posed by standardization, which on one hand can improve efficiency but on the other hand can act as a restraint to innovation.



Looking forward, panelists agreed upon the critical importance of threat and information sharing both regionally and globally—including through specialized command and control centers. They also emphasized the need for enhanced spending on capacity building, in particular supporting small and medium enterprises in innovation and capability development. ■

9 fold increased investments in Cybersecurity companies since 2011 (Source: Crunchbase)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Across Cyber Divides

OPEN FORUM

Panel Discussion

Widening Lens

| A New Narrative for Media Coverage for Cyberspace

- ▶ **John Defterios** Former CNN, Emerging Markets Editor & Anchor
- ▶ **Massimo Marioni** Europe Editor, Fortune
- ▶ **Margery Kraus** Founder and Executive Chairman, APCO Worldwide
- ▶ **Faisal J. Abbas** Editor-in-Chief, Arab News
- ▶ **Rebecca McLaughlin-Eastham** International TV Anchor, MC & Media Trainer
- ▶ **Will Ripley (Moderator)** Senior International Correspondent, CNN

The “Widening Lens” panel focused on the increasingly urgent need for a new media narrative that showcases the diverse aspects of Cyberspace—beyond Cyber threats and vulnerabilities. Panelists highlighted the ways in which the media can bring forward a more balanced and informed perspective on Cyberspace through responsible and constructive coverage.

The media plays a critical role in educating and training the general public with respect to Cyberspace. The importance of this role is particularly clear with respect to online social platforms; for example, up to 80% of Arab youth receive their news directly from social media and 70% of social media users are likely to repost fake news. In this context, stated panelists, journalists have a duty to inform society of Cybersecurity developments in a comprehensive manner, increasing general literacy by featuring coverage of both the challenges and emerging opportunities in Cyberspace, rather than only dedicating significant airtime or resources to major Cyber-attacks.

Looking forward, panelists agreed that media must take corrective steps to enhance their coverage of top Cyber issues, including through enhanced fact checking and verification of reports, more active involvement of



top experts, avoidance of sensationalism regarding Cyberspace, and a comprehensive re-balancing of their coverage in ways that highlight both challenges and opportunities. ■

94% of Gen Z use social media, spending an average time of nearly 3 hours per day (Source: Business DIT)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Inside Cyber Minds OPEN FORUM

Fireside Chat

Smoke & Mirrors

| Social Engineering and Sophisticated Phishing

- ▶ **Joy Chik** President, Identity and Network Access, Microsoft
- ▶ **Lucy Hedges (Moderator)** Technology Journalist & TV Presenter

The fireside chat “Smoke & Mirrors” with Joy Chik focused on the implications resulting from social engineering and phishing, and their rapidly increasing development and sophistication of phishing. Ms. Chik shed new light on how emerging technologies are accelerating the innovation curve of modern social engineering and escalating threats to digital society. She also provided an overview of the technologies we can deploy and the behaviors we can cultivate to create a safer online experience for all.

There has been an exponential increase in the scope and scale of phishing attacks, cited Ms. Chik. In 2021, almost 600 passwords were attacked every second, which increased to almost 1,000 in 2022 and to 4,000+ thus far in 2023. Cybercriminals are developing and deploying increasingly innovative phishing methods to break through Cybersecurity defenses, including through SIM tapping to steal authentication and the creation of fake websites. Ms. Chik also emphasized that Generative AI (GenAI) is making it ever-more possible for Cybercriminals to tailor emails in extremely sophisticated ways to make them more compelling, reducing the ability of users to filter and detect phishing emails.



In conclusion, Ms. Chik asserted that customer protection in the environment we have now entered requires end-to-end design, for example through introducing multi-factor authentication at all steps in the user journey—a practice that is proven to reduce the certainty of attacks by 99.9%. She also emphasized that GenAI should be proactively leveraged in Cyber defense, for example in automating detection to support security professionals. Looking forward, Ms. Chik emphasized that we must devise more effective ways to verify users—such as through the use of biometrics—without compromising on the user experience, in order to develop a credible and phishing-free world. ■

91% of all Cyber-attacks begin with a phishing email to an unexpected victim (Source: Deloitte)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Cyberspace Amidst Polycrisis

OPEN FORUM

Panel Discussion

Cybercrime and Law Enforcement

| Conceiving Jurisdiction in a Borderless Space

- ▶ **Dr. Albert Antwi-Boasiako** Director General, Cybersecurity Authority, Ghana
- ▶ **Shaikh Salman bin Mohammed Al Khalifa** CEO, National Center for Cybersecurity, Bahrain
- ▶ **Bernardo Pillot** Assistant Director, Cybercrime Operations, INTERPOL
- ▶ **Prof. Marco Gercke** Director, Cybercrime Research Institute

The “Cybercrime and Law Enforcement” session was centered around the importance of adapting operational strategies to address the rapidly evolving landscape of criminal tools, techniques, and the distinct legal dynamics of the domain. In a global environment that is rife with institutional challenges regarding jurisdiction, in a borderless space, panelists highlighted the instruments and agreements that are needed to ensure greater law enforcement cooperation in Cyberspace. They also noted the ways in which cooperation among law enforcement agencies in Cyberspace can serve as a starting point for broader international cooperation in the complex and ever-evolving Cyberspace.

Panelists agreed that one of the most significant challenges in the fight against Cybercrime is bringing nations together to collaborate substantively on shared challenges. While some issues such as child online protection find broad support across nations, other issues such as ransomware present challenges for greater cooperation given enduring resistance to the sharing of information. Additionally, the asymmetries of capabilities across nations pose a critical challenge and require focused attention in order to enable more effective global efforts to combat transnational Cybercrime.



Looking forward, panelists highlighted the importance of frameworks, including international conventions, as a foundational instrument to increase cooperation. In particular, they highlighted the ongoing work by the UN’s Third Committee to draft a comprehensive treaty on Cybercrime. However, they advised that progress is not only urgently required globally at the UN, but also at the regional and national levels—including through the development of new legislation and mechanisms for cooperation. ■

1%
of global GDP is lost to Cybercrime each year

(Source: Statista)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Emerging Cyber Horizons

OPEN FORUM

Panel Discussion

Tech Transformed Cybersecurity

| AI's Role in Securing the Future

- ▶ **Dr. Helmut Reisinger** CEO EMEA & LATAM, Palo Alto Networks
- ▶ **Ken Naumann** Chief Executive Officer, Netwitness
- ▶ **Sean Yang** Director of GSPO, Huawei
- ▶ **Massimo Marioni (Moderator)** Europe Editor, Fortune

The panel discussion on “Tech Transformed Cybersecurity” was centered on the indispensable role of AI in safeguarding our collective future in Cyberspace. Panelists provided a range of perspectives on how AI technologies can help identify Cybersecurity vulnerabilities and threats and resolve them with minimum human intervention. They also explored the vulnerability of AI models to data manipulation and poisoning, as well as emerging techniques for mitigating these issues.

It is well-established that the attack surface is expanding relentlessly—and this is contributing to nearly 1.5 million new attacks every year. In the first seven months of the launch of ChatGPT, Palo Alto Networks noted a 910% increase in fake ChatGPT-like websites, designed to take advantage of unwitting users. Speakers highlighted that, with the rapid increase in the deployment of AI across sectors, the speed, scale, and sophistication of attacks is almost certain to rise. However, they also noted that AI can be used for real-

time, highly automated Cybersecurity solutions to defend against these attacks.

In conclusion, panelists emphasized that Cybersecurity measures that are currently fragmented must be consolidated “from code to cloud” so as to minimize weak links. They emphasized that to harness the power of emerging technologies, all stakeholders must take concrete actions within their respective areas—policymakers should start designing comprehensive AI governance and implementing training programs for students as well as “Train the Trainer” courses, while technology vendors should review basic soft engineering practices and calibrate to AI security trends. All actors should aim for both ‘secure by design’ and ‘secure by operation’ systems to ensure a safe and secure Cyberspace in the era of emerging technologies. ■



60%

more attacks faced by metaverse companies in 2021 (Source: Tech Republic)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Emerging Cyber Horizons

OPEN FORUM

Panel Discussion

Ready for Goodbyes?

| Critical System Obsolescence

- ▶ **Ben Miller** Vice President of Threat Operation Services, Dragos, Inc.
- ▶ **Dr. Yacine Djemaiel** CEO, National Agency for Cybersecurity, Tunisia
- ▶ **Major General Manjeet Singh** Joint Secretary, National Security Council Secretariat, India
- ▶ **Joshua Kennedy** White Executive Board Member, Sirar by stc
- ▶ **Rebecca McLaughlin-Eastham (Moderator)** Former CNN, Journalist

The “Ready for Goodbyes?” panel explored the issues associated with critical system obsolescence given the clear potential for emerging technology to outpace the defense capabilities of organizations (e.g., critical national infrastructure entities) and the need to upgrade existing critical systems and capabilities. Speakers focused on the actions that must be taken by organizations to address this threat, and the power of these actions to enhance the Cyber resilience of critical infrastructure.

Panelists agreed that system obsolescence can lead to increased threats particularly to critical infrastructure, posing a major risk to the safety and security of all civilians. In particular, there is an increasing dependency between software and hardware for each component of critical systems, complicating efforts to bolster security. Speakers noted that changes in policy and regulation are most critical to protect against Cyber-attacks caused by obsolescent systems.



Looking forward, panelists emphasized the importance of developing adaptive and flexible technology systems across national ecosystems. Replacing technology systems also requires proper budgetary planning—which highlights the need for anticipatory approaches to the challenge at hand. Panelists also discussed the importance of involving all vendors and stakeholders in collaborative efforts to update and replace critical systems. ■

140% jump in high-impact Cyber attacks on critical infrastructure in 2022 from 2021 (Source: Security Intelligence)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Emerging Cyber Horizons **OPEN FORUM**

Panel Discussion
Hello from the CyberVerse

| Maximizing the Benefits of Future Technologies

- ▶ **Adam Russel** Vice President, Cloud Security, Oracle
- ▶ **Ahmed Aleisawi** Director of Cybersecurity Governance, Risk and Compliance (GRC), NEOM
- ▶ **Chante Maurio** Vice President and General Manager, Identity Management & Security, UL Solutions
- ▶ **Lucy Hedges (Moderator)** Technology Journalist and Presenter

Building on the day's discussion of how to harness the power of emerging technologies, panelists in the "Hello from the CyberVerse" session explored the potential for transformative integration of the metaverse into even more domains of everyday activities. They emphasized the criticality of understanding the implications of this transformation and taking action to address them and

lay the foundations for a stable and secure Cyberspace for future generations.

Panelists agreed that the complexity of Cyberspace is increasing in myriad ways. As ever vaster volumes of data are being generated and stored, the vulnerabilities of products and services are expanding proportionately.




Panelists indicated that perhaps the most worrying aspect of the rapid advance of emerging technologies is the regulatory unpreparedness of governments to secure these technologies. This is growing particularly urgent in light of proliferating threats such as misinformation and advanced deep fakes. The panelists further stressed the importance of striking the right regulatory balance between effective governance on the one hand and innovation on the other.

Ultimately, panelists asserted that novel problems cannot be solved with traditional solutions. The same emerging technologies that might increase Cyber-attacks should also be leveraged in security operations such as instant threat detection. At the same time, public institutions and private sector actors must collaborate to develop regulatory frameworks that can be applied consistently—as uneven adoption of controls may create new, unforeseen vulnerabilities. ■

700
 million people worldwide projected to use metaverse
 by 2030 (Source: WEF)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



 Cyberspace Amidst Polycrisis
OPEN FORUM

Panel Discussion

The State of Cyber Diplomacy

| Momentum, Inertia, or Something Else Altogether?

- ▶ **H.E. Massimo Marotti** Ambassador, International Relations, National Agency for Cybersecurity, Italy
- ▶ **Bernd Pichlmayer** Former Cyber Security Advisor to the Chancellor of Austria, Federal Chancellery
- ▶ **Jovan Kurbalija** Founding Director, DiploFoundation
- ▶ **Rudolph Lohmeyer (Moderator)** Partner, Head of the National Transformations Institute (NTI), Kearney

Panelists in the session on “The State of Cyber Diplomacy” closed the first day of the annual event by painting a picture of the evolving landscape of Cyber diplomacy, including the pace and progress of dialogue at the United Nations and other multilateral fora. Speakers discussed areas of momentum in multilateral negotiations, while also highlighting the need for sustained efforts to accelerate substantive progress toward needed international agreements on Cyberspace.

Conversations were centered around three core topics: the defining characteristics of Cyber diplomacy, its current “state of play,” and promising future pathways for collaborative action. In describing Cyber diplomacy’s defining characteristics, panelists emphasized the extent to which it involves uniquely complex technical issues and requires engagement of a wide variety of stakeholders across the private sector and civil society given its cross-disciplinary nature. In discussing the current state of play in Cyber diplomacy, panelists noted

that meaningful dialogue is occurring in multilateral fora, including on Cybercrime, and that in addition, collaboration among smaller groups of closely aligned countries and other stakeholders on specific issues is becoming an important engine of progress.

Speakers noted that even amid widespread conflict, there are reasons to be optimistic—as Cyber diplomats are continuing to communicate and work toward mutually agreeable solutions to shared challenges.

Looking ahead, panelists highlighted two promising pathways for collaborative action. First, panelists noted that there are already many existing platforms, such as the UN’s First and Third Committees, in which nations can continue to make substantive progress. Second, they highlighted the increasing number of issue-specific collaborations as accelerants of progress, and the value of emerging multistakeholder platforms in creating alignment across the increasingly diverse range of actors involved in Cyber diplomacy. ■



100+ countries have signed cybersecurity-relevant cooperation agreements (Source: (ISC)²)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Fireside Chat

Sustainability At Risk

| Drawing Insights from Climate Talks to Elevate Cybersecurity

- ▶ **H.E. Adel al-Jubeir** Minister of State for Foreign Affairs, Member of the Council of Ministers, and Envoy for Climate Affairs, Saudi Arabia
- ▶ **John Defterios (Moderator)** Former CNN, Emerging Markets Editor & Anchor

In the “Sustainability at Risk” fireside chat, H.E. Adel al-Jubeir opened day two of the annual event by emphasizing the critical relationship between Cybersecurity and climate change and highlighting the opportunities for Cyber diplomacy practitioners to learn from the process and experiences of climate negotiations. His Excellency highlighted several key factors of success and roadblocks that the international community should seek to address—including increased sophistication of Cyber attacks—in a cooperative approach, avoiding unproductive competition in order to collaboratively govern a safer and more secure Cyberspace.

H.E. Adel al-Jubeir remarked that, like the challenge of climate change, no one country can tackle the challenges of Cyberspace alone. Rather, these universal challenges must be addressed through the collective effort of all nations in ways that advance shared interests. His Excellency emphasized that the Kingdom of Saudi Arabia is in a unique position by virtue of its geographic location and deep connectedness in the

100%
rise in significant nation-state incidents between 2017 and 2021 (Source: Hewlett Packard)



global economy, and that it should leverage that to help drive collective action to address shared challenges. His Excellency also noted that, with the advent of new technologies, it is imperative for governments to find a way to keep up with the latest technologies and their challenges, if not outpace them.

In concluding the session, H.E. Adel al-Jubeir asserted that both climate talks and Cybersecurity negotiations require a cooperative approach and not a competitive one—that it should not be a zero-sum game, but rather a “sum-sum game.” As such, multilateral and multi-stakeholder collaboration is of the utmost importance. The more countries that come together and bridge gaps, the better our shared odds of advancing progress in key domains and enhancing global stability. ■

“One country cannot do it alone, we have to work together, we have to share information, we have to share expertise, experience.”

H.E. Adel al-Jubeir

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



 Emerging Cyber Horizons
OPEN FORUM

Panel Discussion

Omnipresent Wireless Intelligence

| Securing Current and Future ICT Networks

- ▶ **H.E. Kyriacos Kokkinos** Former Minister for Research, Innovation and Digital Policy, Republic of Cyprus
- ▶ **Bocar A. Ba** Chief Executive Officer, SAMENA Telecommunications Council
- ▶ **H.E. Eng. Mohamed Ben Amor** Director-General, Arab ICT Organization
- ▶ **Nisha Pilai (Moderator)** International Moderator, Former BBC Presenter

The “Omnipresent Wireless Intelligence” panel discussion was centered around the immediate and future challenges of securing ICT networks in the context of next generation wireless technologies. Panelists emphasized the profound transformative power of these emerging technologies and the urgent requirement for collaborative efforts both to navigate the complexities of their deployment and to harness their capabilities for the benefit of society. They highlighted

the ways in which current and future emerging ICT technologies will revolutionize and transform our daily lives, for example by forming a universally connected ecosystem of devices.

Panelists agreed that emerging wireless technologies will shape a new Cyber environment and ecosystem, serving as infrastructure that will support global development—but also present new threats.



Specifically, 6G, which is expected to be deployed in the 2030 timeframe, requires proactive efforts from governments to develop updated standards and regulations. 6G will provide blazing internet speeds, panelists noted, and may also enable a shift from virtual reality to extended reality—resulting in seamless digital and physical world interactions—with potential implications on how individuals engage and connect with one another. Shaping that future reality is a core responsibility for regulators.

Looking to the future, speakers highlighted that deploying 6G at scale will enable a number of breakthroughs, including those related to the widening scope of Internet-of-Things (IoT) devices, and would demand increased regulatory collaboration and access to capital and investments to accelerate its deployment. They also mentioned that deploying this technology in a safe and secure manner requires collective action and collaboration between all stakeholders to ensure its equitable and effective application. ■



10 million IoT devices expected to be accommodated by 6G per square kilometer while compared to 2000 per square kilometer by 4G

(Source: CSR Wire)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Across Cyber Divides OPEN FORUM

Panel Discussion
Safe Surfing

| Understanding Child Online Activity

- ▶ **Dr. Maimoonah Alkhalil** Secretary-General, Family Affairs Council, Saudi Arabia
- ▶ **Iain Drennan** Executive Director, WeProtect Global Alliance
- ▶ **Dr. Yuhyun Park** Founder, DQ Institute
- ▶ **Rebecca McLaughlin-Eastham** International TV Anchor, MC & Media Trainer

The “Safe Surfing” panel discussion focused on the critical need to accelerate progress in ensuring child safety online. Panelists discussed recent learnings regarding children’s online activities, behaviors, and their associated psychological impacts. Speakers also discussed the importance of developing proactive, industry-wide collaboration for the protection of children in online environments.

Increasing numbers of children are spending ever-greater amounts of time online for a wide range of activities, including education and entertainment. For example, 99% of Saudi children currently use social media channels. In this context, speakers noted, the boundaries between the real world and the virtual world are blurring, making conversations on child protection in the online environment a priority. To that end, the panelists highlighted the work that Saudi Arabia has done in partnering with over 25+ stakeholders—ranging from governments to industry and civil society organizations—to design a National Child Safety Online Framework that will soon be publicly launched. In addition, with threats to children already on the rise globally including Cyberbullying and child sex abuse, panelists highlighted the need for international cooperation to curb threats and protect children’s experience online.



In concluding the discussion, panelists emphasized that technology providers have a critical role to play—given the vast reach of their products—in ensuring the prevalence of self-regulating measures with respect to moderating content and generating transparent reports. Speakers also highlighted that scaling awareness campaigns for parents and increasing education for children on responsible online behavior are crucial steps to ensure a safe Cyberspace for all. ■

72%
of children, below age 12, on social media have experienced a Cyber threat, and 48% feel unsafe
(Source: GCF)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:





OPEN FORUM

Panel Discussion

Cyber Costs Reframed

| The Human Costs of Cyber Insecurity

- ▶ **Major General (rtd.) Eng. Mohammad Abdulaziz Boarki** Chief, National Cyber Security Center (NCSC), Kuwait
- ▶ **Dan Cîmpean** Director, National Cybersecurity Directorate, Romania
- ▶ **Dr. Ahmed Abdel Hafez** Chairman of the Executive Bureau, Egyptian Supreme Cybersecurity Council
- ▶ **Ryan Chilcote (Moderator)** Master of Ceremonies, International Moderator, Former Bloomberg, CNN, CBS, PBS, and Fox News

While several sessions during the event considered the financial costs of malicious Cyber activity, panelists in the “Cyber Costs Reframed” panel emphasized the critical importance of reconceiving the costs of Cyber attacks from a more human-centric point of view. Rather than limiting our analysis of costs in strictly commercial and financial terms, they offered an approach centered around considering the impact of Cyber attacks on human welfare and well-being. Speakers highlighted the need to begin by measuring the human impact of Cyber activity in order to ensure the development of human-centered Cybersecurity policies. From this foundation, several imperatives for multilateral collaboration can be advanced, guided by the intent to reduce the human impact of malicious Cyber activity.

It is well-recognized that individuals can experience severe harm as a result of attacks to devices in proximity to everyday life, such as wearables, phones, and laptops carrying the critical, personal data of every individual. Recently, however, critical systems such as water infrastructure and healthcare systems have become increasingly targeted by ransomware attacks—with clear ability to result in indiscriminate, physical harm across populations. Nations face clear challenges in fostering the skills required to tackle these evolving threats while maintaining budget discipline.



Another critical challenge that was pointed out by the panelists is that of privacy, as nations must balance the imperatives of protecting civilians from harm and respecting individual data.

Looking forward, it is important to invest in enhanced Cyber capabilities for healthcare services and entities. It

is also important to increase awareness of and develop baseline standards for the security of critical systems. Panelists agreed that regulators must put healthcare in particular at the top of the agenda for their national Cybersecurity programs, as emerging technologies such as AI serve as an accelerant in the dissemination of new threats. ■

72% of hospitals reported longer waiting times due to Cyber-attacks, while 22% said these attacks resulted in increased death rates (Source: Verge)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Panel Discussion

Cognitive Vulnerabilities

| Why Humans Fall for Cyber Attacks

- ▶ **Gareth Maclachlan** Senior Vice President and General Manager Network and Email, Trellix
- ▶ **Philippe Vallee** Executive Vice President, Digital Identity & Security, Thales Group
- ▶ **Prof. William H. Dutton** Martin Fellow, Oxford University's Global Cyber Security Capacity Centre; Emeritus Professor, University of Southern California, University of Oxford
- ▶ **David Chow** Global Chief Technology Strategy Officer, Trend Micro
- ▶ **Lucy Hedges (Moderator)** Technology Journalist and TV Presenter

In a discussion on the impacts of behavior and decision making in Cyberspace, panelists in the "Cognitive Vulnerabilities" session highlighted the importance of human error and the relationship between human behavior and Cybercrimes to understand where and why vulnerabilities persist in user activity online. They focused on the potential benefits of increased industry collaboration to reduce Cyber vulnerabilities and create a more secure Cyberspace for users.

Panelists agreed that the most challenging aspect of Cyber defense is not technical vulnerability but rather cognitive vulnerability in all of its forms. Understanding human behavior and psychological propensities online is crucial to ensuring a safe and responsible Cyberspace. Throughout the session, speakers emphasized that online propaganda and influence campaigns are not just shaping narratives, but also beliefs—further illustrating the critical need to develop mechanisms to protect against attacks targeting cognitive vulnerabilities in general and in Cyberspace in particular.

In conclusion, panelists asserted that cultivating a



Cybersecurity mindset among all users is essential, which can be achieved through enhancing user education regarding various Cyber threats. They also highlighted that the private sector has a responsibility to design products and services with end-to-end risk management practices in order to provide the first layer of prevention of human-centric attacks. ■

53%
of adults admit that they don't know how to protect themselves from Cybercrime (Source: Norton)





OPEN FORUM

Fireside Chat

Behavior Unmasked

| The Effects of Anonymity in Online Activity

- ▶ **Prof. Mary Aiken** World leading expert in Cyberpsychology and Chair of the Cyberpsychology Department, Capitol Technology University
- ▶ **Richard Quest (Moderator)** News Anchor, CNN

In “Behavior Unmasked,” Professor Mary Aiken explored the changing complexities of anonymity online, and why understanding this evolution is essential to creating a safer and more inclusive online environment. She specifically focused on the impact of anonymity on user behavior, particularly in the case of young users. Aiken also explored potential mechanisms to prevent negative online behavior, such as toxic online disinhibition, and a range of opportunities to increase responsible digital citizenship.

Professor Aiken highlighted that as the virtual world gives users the ability to remain anonymous, many users may engage in behavior that is different from that which they would exhibit in the physical world, where anonymity is usually not a choice. She noted that children online are the most vulnerable to falling prey to negative behavior online, pointing out that 50% of 8,000 students aged 16-19 surveyed admitted to committing some form of Cybercrime. Prof. Aiken emphasized that the “attention economy”—the monetization of user attention through social media algorithms—continues its rapid ascent, creating a snowball effect on human addiction to technology.

In concluding the discussion, Professor Aiken asserted that tackling the challenge of online safety requires that all stakeholders come together to collaborate on defining regulations to handle the exploding volume,



velocity, and variety of Cybercrime. As an example of the kind of regulatory innovations needed, she highlighted that the United Kingdom has introduced the Online Child Safety Act, a broad measure to protect children in Cyberspace including tackling the multiplicity of fake profiles. Prof. Aiken also emphasized that parents having oversight of their children online—just as they do in the physical world—is the most critical measure to ensure that their human vulnerabilities are not exploited. ■

5% of monthly active users on Facebook were reported to be fake accounts during Q2, 2023 (Source: Facebook)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Across Cyber Divides

OPEN FORUM

Panel Discussion

Cyberspace Needs You

| Attracting Women to Cybersecurity Careers

- ▶ **H.E. Dr. Margarete Schrambock** Former Minister for Digital & Economic Affairs, Austria
- ▶ **Dr. Cecile Aptel** Deputy Director, United Nations Institute for Disarmament Research (UNIDIR)
- ▶ **Betania Allo** Cybersecurity Innovation and Partnerships Manager, NEOM
- ▶ **Jane Witherspoon (Moderator)** Bureau Chief Middle East, Euronews

Building on previous session themes focused on ensuring diversity in the workforce, panelists in the “Cyberspace Needs You” session discussed the critical path to making Cybersecurity a more desirable and fulfilling long-term career choice for women. In particular, they focused on the current challenges in recruiting women to Cybersecurity careers and potential incentives to draw increasing numbers of women to the sector. Speakers also highlighted the many benefits of attracting more women to Cybersecurity jobs, including creating a more inclusive Cyberspace and reducing the industry’s persistent skills shortage.

Panelists highlighted that, although diverse teams have proven to be more successful than those that are less diverse, women are still Underrepresented in Cybersecurity across the board—both on technical and also diplomatic fronts. Speakers noted that this may be exacerbated by a lack of female role models in the Cybersecurity field, especially in middle management roles. The negative consequences of gender bias and inequity in opportunities also cannot be discounted. Ultimately, panelists highlighted that even in countries with gender parity policies, Cybersecurity and technology sectors have less representation of women, and there remains much work to be done.

In concluding the session, panelists asserted that an inclusive workforce should be encouraged not only in



terms of filling positions with female candidates, but also through forming a support network for women through allyship, mentorship, and sponsorship. Mentoring and direct education, speakers argued, will increase the attractiveness of Cybersecurity as a career option for women and multiply benefits of their engagement across the sector and entire economy. ■

25% of Cybersecurity workforce is made up of women, compared to 39% of the overall workforce (Source: UNODC)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Cyber Growth Unlocked OPEN FORUM

Panel Discussion

It's Over for Turnover

| Retaining Talent in Cyberspace

- ▶ **Dr. Almerindo Graziano** Chief Executive Officer, Co-Founder, Cyber Ranges
- ▶ **Jess Garcia** Founder and Chief Executive Officer, One eSecurity
- ▶ **Oliver Vaartnou** Chief Executive Officer, Cybernetica AS
- ▶ **Filippo Cassini** Global Technical Officer and Senior Vice President, Engineering, Fortinet
- ▶ **Akshay Joshi** Head of Industry and Partnerships, World Economic Forum
- ▶ **Orhan Osmani (Moderator)** Acting Head, Cbersecurity Division (Resilience), Development Sector, ITU

The “It’s Over for Turnover” panel discussion explored the challenges of retaining top talent in Cybersecurity careers. The discussion was centered on how the field can reverse attrition trends, citing studies and real-life initiatives and programs focused on creating a better work environment for Cybersecurity professionals. Panelists also focused on potential mechanisms to help make Cybersecurity an attractive career choice and reduce the talent gap, building from the ground up.

It can be argued, as it was by the panelists, that talent attraction and retention is the most crucial workforce issue in Cybersecurity. The shortage of Cybersecurity professionals currently stands at 5.5 million, up from 3.4 million in 2022. They highlighted that this shortage results in a disproportionate burden on retention as the talent pipeline



is not promising. The most important reason for this shortage, speakers noted, is that the current workforce is aiming for careers with meaningful opportunities with an increased focus on emerging technologies—rather than simply seeking increased compensation.

tasks can free up segments of the workforce, who can then be deployed in other, more critical jobs that require the skillsets and cannot be addressed by technology alone. In addition, speakers highlighted that raising awareness of Cybersecurity as a career should start early in schools and universities. Recruitment practices should be aligned accordingly to let young professionals get sufficient time to work, explore (e.g., through internships), and pursue a career in Cybersecurity. ■

In conclusion, panelists asserted that strategic Cyber talent frameworks should be put in place to attract professionals to Cyber careers. Deploying AI in daily

70%
of organizations worldwide face a shortage of
Cybersecurity skills (Source: ISSA)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:





OPEN FORUM

Panel Discussion

Shaping Investment

| Spurring Investment in Cyber Sector Startups

- ▶ **Kenneth Pentimonti** Principal and European Manager, Paladin Capital Group
- ▶ **Peter Sund** CEO, Finnish Information Security Cluster
- ▶ **Juliette Wilcox** CMG Cyber Security Ambassador, UK
- ▶ **Shoaib Yousuf** Managing Director and Partner, BCG
- ▶ **Nisha Pilai (Moderator)** International Moderator, Former BBC Presenter

Contributing to the broader theme of exploring opportunities to accelerate economic growth, panelists in the “Shaping Investment” session focused on entrepreneurship and Cybersecurity startups. Speakers emphasized that innovative Cybersecurity solutions have never been more critical, given the increasingly sophisticated tactics that are being deployed by Cybercriminals. These innovative solutions, they highlighted, require a rich Cyber innovation ecosystem, inclusive of Cyber startups. As such, an increase in investments in Cyber start-ups is necessary to bolster our Cyber defenses and stay ahead in this evolving battleground. Speakers also focused on the various regulatory mechanisms and systems needed for encouraging wide-spread investments in the Cyber sector, particularly within Cybersecurity start-ups.

Panelists agreed that early-stage startups can play a critical role in enhancing national and global security. For national ecosystems, startups serve as an engine for innovation and economic growth. Meanwhile, for investors, these startups represent an excellent opportunity to benefit from early support. However, small companies—including Cyber startups—often lack clear business plans, pathways to customers, or plans to scale. Startups must be more proactive in defining their culture and go-to-market strategy. They



must also communicate their differentiating value proposition clearly to an expanding base of consumers and investors. For these companies then, support required is not just related to the tech solutions they develop but perhaps more importantly to the running of a business.

In concluding the discussion, panelists noted that governments can play a critical role in supporting industry innovation and entrepreneurship. One such way to accomplish this may be through grant programs to create a safe space for mentorship. Speakers also noted that emerging technologies such as AI present many opportunities for startups, and those enterprises who recognize this will be among the leaders in the future. ■

7.8 billion

is the global venture funding for the Cybersecurity industry in 2020, an all-time high (Source: Crunchbase)



To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:



Emerging Cyber Horizons

OPEN FORUM

Panel Discussion

Emerging Shadows

| Unmasking Cyber Threats of Generative AI

- ▶ **Richard Watson** Global Cybersecurity Leader, EY
- ▶ **Dr. Yazeed Alabdulkarim** Chief Scientist, Emerging Technologies, Saudi Information Technology Company (SITE)
- ▶ **Kevin Brown** COO, NCC Group
- ▶ **Dr. Victoria Baines** Independent Cybersecurity Researcher
- ▶ **Alexandra Topalian (Moderator)** International Moderator



In the concluding session of the two-day Annual Event, panelists in the “Emerging Shadows” panel highlighted the current state of progress in generative AI and the potential risks it may introduce or exacerbate in Cyberspace. Speakers focused on the mitigation mechanisms needed for managing these risks, given the increasing likelihood that generative AI will have an increasingly pervasive influence and impact in our daily lives. Panelists further highlighted that the future impact of generative AI will be a function not only of its power to fuel innovation, but of our ability to confront its challenges head-on and our willingness to take responsibility for doing so.

There are a number of emerging threats related to generative AI, including data poisoning, social engineering, and malware as a service. Panelists emphasized that these threats change daily, requiring consistently updated governance and risk management—a novel challenge for regulators and for users of AI. This challenge is compounded by a pervasive lack of qualified and interested talent in Cybersecurity, leaving incident response teams overwhelmed while attempting to tackle a widening range of emerging threats.



In concluding the discussion, panelists emphasized that regulations are critical for the protection of all users. Speakers highlighted that Cybersecurity companies must establish a clear strategy to address the attack surface in a proactive manner. Yet, while there must be controls in place, regulation must not stifle innovation or hamper the development of positive use cases. ■

85%

of Cyber professionals attribute increase in Cyber-attacks to bad actors using GenAI (Source: Security Magazine)

To listen to the full session recording, including direct quotes by the panelists, please refer to the QR Code:





HIGH-LEVEL MULTI-STAKEHOLDER ROUNDTABLE



High-Level Multi-Stakeholder Roundtable:

From shared challenges to collective solutions

The GCF 2023 convened a group of government representatives, industry leaders, and IO representatives in a high-level meeting to discuss Cybersecurity challenges that each stakeholder group is facing and identify ways in which they can work together to address those challenges. This structured and moderated conversation touched upon a set of key Cybersecurity issues, discussing the most critical aspects of this challenge and the most promising potential areas of international and/or multi-stakeholder collaboration. This year, the Multi-stakeholder Roundtable focused on the following three critical issues:

► **Managing the escalating cost of Cybersecurity:**

Intensifying competition and accelerating technological advance have driven a rapid escalation of the cost of Cybersecurity for countries, organizations and individuals. All stakeholders face growing pressure to invest in ever more sophisticated capabilities – defensive and for some offensive – to ensure their Cybersecurity. The steady rise in costs is apparent across sectors and stakeholder groups. For example, end-user spending for the information security and risk management market is expected to rise 11% each year, reaching \$267.3 billion by 2026. During the Roundtable discussion, participants focused on several potential pathways of collaborative action to minimize these costs and maximize Cybersecurity spending efficiency for the future. First, participants noted the importance of having a national centralized budget for Cybersecurity. A centralized budget with dedicated licensed service providers increases the efficiency of Cybersecurity solution delivery. Second, participants noted that, particularly for Least Developed Countries (LDCs), resources for Cybersecurity are scarce, leading to competition between organizations seeking to gain access to finances. One solution presented was to set a national minimum Cybersecurity spending baseline, where a certain percentage of information technology (IT) budgets must be invested in Cybersecurity. Third, participants highlighted the potential for shared platforms to collaborate on end-to-end solutions in order to increase spending efficiencies.



► **Proactively mitigating the human impact of ransomware (HIR) in CNI sectors:**

The Roundtable discussion then turned to the urgent issue of the human impact of ransomware. Ransomware attacks on citizen-facing Critical National Infrastructure (CNI) such as hospitals and water systems risk compromising essential services to individuals and in some cases even threaten human life. As reported by Trend Micro, 89% of electricity, oil & gas, and manufacturing firms supporting critical infrastructure experienced Cyber-attacks in 2022. Participants focused on opportunities to increase the speed of information sharing through public-private partnerships and centralized platforms for threat hunting, enabling more effective recovery and response mechanisms. Open-source monitoring tools, for example, present a unique opportunity to identify and combat attacks.

► **Strengthening systemic Cybersecurity globally through capacity building:**

Despite substantial progress, uneven distribution of

capabilities and skills gaps remain. Globally, there is a documented 5.5-million-person shortage of Cyber talent, ensuring that no nation can meet its full need. Participants focused on the importance of increasing regional cooperation, such as through conventions of ministerial councils and committees. The issues of capacity building are particularly critical in the Operational Technology (OT) environment, which is characterized by local, regional, and global concerns—particularly due to the fact that OT systems emerged as primarily industry and sector-focused and have remained isolated for decades. Finally, participants raised opportunities to create force multipliers in capacity building by employing AI and advanced analytics. In concluding the session, participants suggested to institutionalize the Multi-stakeholder Roundtable as a recurring platform within the GCF's Annual Event. They noted that this platform could serve as one way in which stakeholders can advance collective action long after the conclusion of the Annual Event. ■





CxO MEETING



CxO Meeting:

C-suite meeting, invite only session, to discuss challenges, implications, and collaborative pathways of action in Cybersecurity

The GCF 2023 hosted a CxO Meeting, the first of its kind, offering a platform for global Cybersecurity leaders to interact and collaborate, advancing GCF's strategic goal of collective action. The CxO meeting brought together C-suite representatives of globally reputed Cybersecurity companies in order to discuss challenges and emerging trends in Cybersecurity, its implications for private sector entities, and productive pathways for collaborative action.

This structured and moderated conversation touched upon a set of key Cybersecurity issues to discuss the most persistent challenges and identify productive pathways for collaboration.

The issues discussed are:

- ▶ Advancing AI & Cybersecurity Harmoniously
- ▶ Maximizing Cybersecurity Spending Efficiency
- ▶ Bridging Cloud and IT/OT Cybersecurity Measures
- ▶ Understanding the Interplay Between Cybersecurity and Non-Cybersecurity Regulations
- ▶ Promoting Green Technology

The Key takeaways from the CxO meeting are:

1. Initiate collaborative research:

Understand how to limit AI's utility in Cybercrime and its offensive powers; and how to mitigate the security risks in its deployment and hidden influences.

2. Collaborate with government institutions:

Introduce better legislation to limit budgets from fueling Cybercrime; introduce insurance policies for Cyber damages; and ensure compliance and harmony with regulations.

3. Form industry partnership:

Work together to standardize Cybersecurity metrics and technical classifications; spread public awareness on newest industry perspectives; and collaborate on efforts to minimize carbon footprint and ensure sustainability.

4. Develop adaptable Cybersecurity strategy:

Ensure standards in supply chain management; define and pursue digital sovereignty; holistically consider the Cybersecurity industry by including smaller players; and adopt lightweight green- enabling technologies.

5. Maximize synergies and efficiency:

Efficiently deploy available assets and capabilities by ensuring optimal team and skill makeup; leverage AI to tackle talent shortages through upskilling and reskilling; and automate security processes to cut down required human capital.





DEEP DIVE SESSIONS



Breakfast: Women in Cyber

- ▶ **H.E. Dr. Hala Bint Mazyad Altuwajri** President, Human Rights Commission, Saudi Arabia
- ▶ **H.E. Kersti Kaljulaid** Former President, The Republic of Estonia
- ▶ **Doreen Bogdan-Martin** Secretary-General, International Telecommunication Union (ITU)
- ▶ **Margery Kraus** Founder and Executive Chairman, APCO Worldwide
- ▶ **Joy Chik** President, Identity and Network Access, Microsoft

The GCF 2023 hosted a networking breakfast on Day 2, prior to the start of the day's sessions. The "Women in Cyber" networking breakfast brought together a community of women and aimed to advance dialogue in order to foster professional development.

This event intended to form a community of accomplished and aspiring women in Cybersecurity and male allies to facilitate knowledge sharing and meaningful networking, seeking to promote sponsorship for women and catalyze change to pave the way for a more inclusive and impactful future, particularly in Cybersecurity.

The "Women in Cyber" session featured an informal panel discussion over a light breakfast. The panel was

followed by a networking session allowing attendees to engage in conversations and foster enduring relationships. Discussion was centered around topics of shared interest and concern for women in Cyber, including barriers for women in the Cyber domain, avenues for talent development, and the role of mentorship.

The "Women in Cyber" session helped the inception of a robust global network of women professionals and allies that will nurture enduring collaborations and knowledge exchange, generate thought-provoking insights on challenges faced by women in the workforce opportunities to cultivate an inclusive supportive environment, and identify productive pathways to hone holistic development and sustained growth of women professionals.



Policy Brief: Child Protection in Cyberspace

Today, where the virtual world intertwines seamlessly with our everyday lives, child online protection has emerged as a critical area of concern. With the proliferation of internet-connected devices, children’s digital footprints have expanded far beyond computer screens and deep into Cyberspace. This brings forth a pressing need to more effectively understand their online activities, behaviors, and patterns in order to ensure their safety, well-being, and positive development.

In this session, Dr. Yuhyun Park presented the 2023 Child Online Safety Index (COSI), a national-level metric designed to assist countries in effectively monitoring the status of children’s online safety. The Index has found that, once again, a high percentage -nearly 70% - of children and adolescents aged 8-18 worldwide have experienced at least one Cyber risk in the past year. This alarming statistic has remained virtually unchanged since the Index began in 2018, a situation DQ Institute has dubbed a “persistent Cyber pandemic.”

The COSI draws on data collected from a sample of 351,376 children spanning from 2017 to the present day. In this latest edition, the Index introduces a four-point rating scale enabling policymakers and industry leaders to precisely identify strengths and areas for improvement in their child online safety initiatives and measures.

Dr. Yuhyun Park, the founder of the DQ Institute and HumanX, is a world-leading expert in digital skills, ethics, and sustainability. She created the Child Online Safety Index, the world’s first metric tracker to help nations better understand their children’s online safety status. She also led the #DQEveryChild initiative, a digital citizenship movement that has empowered children, families, and teachers in more than 80 countries to date. ■



Cyber Simulation

GCF 2023 featured an interactive Cyber Incident Simulation, led by Dr. Marco Gercke and the Cybercrime Research Institute.

The session comprised a live Cyber-attack simulation, wherein participants voted in a poll to determine immediate actions and incident responses from the perspective of an incident response team. The simulation was then followed by a debrief, where participants further explored recovery plans and crisis-handling mechanisms. The aim of the simulation is to train decision makers and other relevant stakeholders in Cyber incident management and showcase how split-second decisions can influence outcomes in the case of a Cyber-attack.

The simulation was led by Prof. Dr. Marco Gercke. Dr Gercke is a renowned Cybersecurity specialist, scientist, and advisor. He is considered a leading expert on the opportunities and risks of digitalization.

The simulations were for several years part of the agenda of the Munich Security Conference and developed for UN Conferences as well as the World Economic Forum.



Global Insight Session: Evolving Threat Landscape for Children in Cyberspace: Implication and Potential Avenues for Collaboration

Despite the innumerable benefits that the Cyberspace offers, it also allows predators and online trolls to cause harm and hide behind screens – often without facing consequences. The impressionable young minds of children make them especially at risk. Young people continue to face a thinning bridge between the online and physical worlds – one that is not yet spoken about enough in policymaking.

This Global Insight Session led by Iain Drennan explored the evolving threat landscape for children in Cyberspace. It highlighted The Global Threat Assessment, the flagship policy document that assesses the scale and scope of child sexual exploitation and abuse online, in order to transform the response.

Since 2018, our Global Threat Assessments have evidenced and analysed the sustained rise in child exploitation and abuse online, fuelled by the increasing scale, complexity, and diversity of harm. The 2023 report concludes that a shift towards prevention, including public health safety and safety-by-design approaches, offers the only viable route to curb the sustained escalation of child sexual abuse online.

Iain Drennan has been the Executive Director of WeProtect Global Alliance since 2020. Drennan has led the work of WeProtect Global Alliance since 2017, first as International Lead at the Exploitation and Abuse Tackling Unit within the UK's Home Office and then as Executive Director.



Deep Dive Session: Cyber Psychology for Active Cyber Defense

The consequences of Cyber-attacks have become more severe as the capabilities of attackers become more sophisticated, causing disruption to enterprise operations, threatening customer relations due to data breaches, diminishing revenue, and devaluing trade names. Therefore, Professor Aiken argued that successful Cyber defense can no longer be sustained with passive defensive tactics, innovative options must be explored in order to execute active Cyber defense. Building on the recent IARPA project titled Reimagining Security with Cyberpsychology-Informed Defenses (ReSCIND), Cyberpsychologist Professor Mary Aiken discussed her latest research which argues for an industry-wide paradigm shift from passive to active forms of defense against Cyber attacks by effectively 'hacking back'.

Corporate self-help in Cyberspace is a contentious issue as private sector entities can defend their networks but are not permitted to retaliate beyond the perimeter of their own networks. However, in today's global Cybercriminal enterprise, human vulnerabilities can be targeted and exploited to disrupt Cyber-attacks. The aim is to achieve effective disruptive defensive operations without breaching the legal threshold of Cyber offensive operations. Professor Aiken also highlighted how human Cyber attackers have a wide range of psychological vulnerabilities and therefore, hypothetically, these could be identified and targeted in terms of Cyberpsychologically 'hacking back'.



Deep Dive Session: Closing the Talent Gap: Frameworks for Capacity Building

Cybersecurity centrality has been growing to ensure global security and economic growth, which has led many governments and international organizations to focus on building the capacity of nations to withstand threats to the public and its digital resources.

This session, led by Professor William H. Dutton and moderated by Alexandra Topalian, explored the importance of capacity building and how nations can most effectively build their national Cybersecurity capacity. It also highlighted the status of capacity-building across nations, the impacts of capacity-building, and the factors that are shaping national advances in capacity-building.

Prof. William H. Dutton is a Martin Fellow at Oxford University's Global Cyber Security Capacity Centre and founding director of the Oxford Internet Institute (OII). Dutton is an Emeritus Professor at the University of Southern California (USC), where he was a Fulbright Scholar to Britain, was elected President of the University's Faculty Senate, and taught until 2002 when he became the first Professor of Internet Studies at the University of Oxford.



Deep Dive Session: Security in the Metaverse

The global Cybersecurity community has been aware of Cyber-physical crossover threats for many years. Today, there is a new Cyber-physical frontier: as larger numbers of individuals are physically connected to the Internet through live environments such as the metaverse, the distinction between online and offline security is increasingly blurred. This invite-only briefing considered two challenges in emerging technology with the potential to change the work of Cybersecurity specialists.

The first is safety and security in the Metaverse. Millions of us already interact in immersive virtual worlds. As rapid developments in Virtual Reality, Augmented Reality, and Mixed Reality promise an ever-greater sense of presence and embodiment, our emotional and physical experience of online environments will be heightened. In this challenge, participants considered the implications for the Cybersecurity community, in particular how external hardware powered by haptic technology could challenge traditional divisions between online and offline crimes.

The second challenge is the Medical Internet of Things (IoT). While the security considerations of wireless implantable medical hardware for the treatment of conditions such as heart disease and diabetes are not new, the extent to which these now rely on patients' mobile Internet connections prompts new questions for Cybersecurity specialists. Who is responsible for security at different points in the value chain: the manufacturer, the healthcare provider, or the patient? Participants also looked at recent developments in Brain Computer Interfaces, some of which promise to combine features of Neurotechnology, Artificial Intelligence, and the Metaverse.

The briefing conducted by renowned Cybersecurity professor and expert Dr. Victoria Baines. Dr Victoria Baines FBCS is a leading figure in the field of online trust, safety, and Cybersecurity. She frequently contributes to major broadcast media outlets on digital ethics, Cybercrime, and the misuse of emerging technologies, including Extended Reality and Artificial Intelligence. Her areas of research include electronic surveillance, Cybercrime futures, and the politics of security. ■





KNOWLEDGE COMMUNITY MEETINGS



GCF Knowledge Communities

GCF Knowledge Communities are multistakeholder thought leadership and action-oriented groups, comprising a globally diverse group of entities with shared interests and concerns related to a given domain in Cybersecurity. These communities complement the annual GCF event, serving as semi-permanent venues for collaboration and collective action, with the aim to benefit all participating community members and the overall Cybersecurity landscape.



GCF Knowledge Communities create impact through:

► **Varied Outlooks:**

The communities bring together practitioners with diverse national and sectoral perspectives in order to pool their assessments of the topics.

All stakeholders, inclusive of private, public, and NGO actors can be members of knowledge communities, with each entity deriving distinct benefits tailored to their specific needs.

► **Unbiased Findings:**

The community will convene a mix of practitioners from around the world to generate maximally unbiased findings.

► **Valuable Knowledge Assets:**

The community will develop high-value insight-driven assets, including reports, videos, and interactive exercises.

KNOWLEDGE COMMUNITY

Securing Industrial Systems for Global Energy Supply

Lead by Aramco



In an era defined by interconnected economies and technological interdependence, securing the industrial systems for global energy supply has assumed unparalleled importance. As industrial systems play an increasingly vital role in connecting cross-border environments, vulnerabilities in any link can cascade into far-reaching disruptions, posing significant Cybersecurity risks that impacts economies and extended supply chains. The knowledge community "Securing Industrial Systems for Global Energy Supply" is committed to strengthening the resilience and Cybersecurity of the global energy environment, bringing together a diverse array of expertise from multiple stakeholder groups.

The community welcomes energy companies, technology providers, Cybersecurity research organizations, infrastructure operators, industrial manufacturers, academia, and all stakeholders with a vested interest in the security and reliability of the energy industrial systems.

Join the community and contribute to fortifying the world's energy lifelines and ensuring a resilient and secure energy future for all. ■

KNOWLEDGE COMMUNITY MEETING:

Securing Industrial Systems for Global Energy Supply

With an aim to fortify the world's energy lifelines, this community brings together 14 international stakeholders to collaborate and work towards ensuring a resilient and secure energy future for all. During this meeting, the community has discussed key challenges, opportunities, and priorities. They then defined the key priorities for the upcoming year. The ideation session helped shape a community action plan and the way forward.

Moving forward, community activities will include:

Defining shared goals: Developing a joint vision, mission statement, and shared success metrics to ensure all stakeholders' efforts are directed towards a common goal.

Developing programs and initiatives: Supporting existing initiatives in their domain of interest, or building additional efforts such as publishing whitepapers and conducting advocacy.

Holding collaboration sessions: Participating in regular sessions to advance collaboration on specific community initiatives, ensure consistent and continuous dialogue, and unify community efforts. ■



Future of Cybersecurity

Lead by SITE



In a rapidly evolving technology landscape, nearly every aspect of human life is undergoing a profound technological transformation—in which Cybersecurity represents a critical imperative. It is therefore crucial to lay the foundations of a stable and secure future of Cybersecurity to ensure the well-being of the future of humanity. “Future of Cybersecurity” is a knowledge community committed to exploring the potential opportunities and threats presented by the ever-evolving Cyberspace and developing mechanisms to maximize the benefits and address the risks looming on the horizon by bringing together a diverse array of expertise from various stakeholder groups.

The community welcomes leading technology companies, global Cybersecurity organizations, Cybersecurity research centers, reputable think tanks, academic institutions, and other stakeholders with a vested interest in exploring and acting upon the future of Cybersecurity.

Join the community to explore the future of Cybersecurity and participate in safeguarding the Cyber realm and protecting the future of our connected world. ■

Future of Cybersecurity

Bringing together diverse expertise and foresight capabilities, this community will help cope with the transformations induced by emerging technologies to enable a sustainable Cyber resilience. During this meeting, the community has discussed key challenges, opportunities, and priorities. They then defined the key priorities for the upcoming year. The ideation session helped shape a community action plan and the way forward.

Moving forward, community activities will include:

Defining shared goals: Developing a joint vision, mission statement, and shared success metrics to ensure all stakeholders’ efforts are directed towards a common goal.

Developing programs and initiatives: Supporting existing initiatives in their domain of interest, or building additional efforts such as publishing whitepapers and conducting advocacy.

Holding collaboration sessions: Participating in regular sessions to advance collaboration on the specific community initiative, ensure consistent and continuous dialogue, and unify community efforts. ■



KNOWLEDGE COMMUNITY

Safeguarding the Future Networks & Emerging Technologies

Lead by stc



In an increasingly interconnected world, the evolution of next generation ICT technologies such as 6G wireless technology has emerged as a powerful catalyst. The profound implications and transformative power of this next wave of ICT technologies demand immediate attention – both to navigate its complexities, safeguard its deployment, and to harness its capabilities for the benefit of society. The knowledge community “Safeguarding the Future Networks & Emerging Technologies” is committed to promoting and safeguarding the current and future day’s ICT networks bringing together a diverse array of expertise from multiple stakeholder groups.

The community welcomes ICT providers, telecom companies, telecom industry players, Cybersecurity research organizations, infrastructure operators, reputable think tanks, academia, and all stakeholders with a vested interest in the security of the ICT networks.

Join the community to safeguard the future of ICT networks, the backbone of our digitally connected world. ■

KNOWLEDGE COMMUNITY MEETING:

Safeguarding the Future Networks & Emerging Technologies

ICT networks are the backbone of our digitally connected world. This community is dedicated to promoting and safeguarding these networks and harnessing their capabilities for the benefit of society. During this meeting, the community discussed key challenges, opportunities, and priorities. They then defined the key priorities for the upcoming year. The ideation session helped shape a community action plan and the way forward.

Moving forward, community activities will include:

Defining shared goals: Developing a joint vision, mission statement, and shared success metrics to ensure all stakeholders’ efforts are directed towards a common goal.

Developing programs and initiatives: Supporting existing initiatives in their domain of interest, or building additional efforts such as publishing whitepapers and conducting advocacy.

Holding collaboration sessions: Participating in regular sessions to advance collaboration on specific community initiatives, ensure consistent and continuous dialogue, and unify community efforts. ■



KNOWLEDGE COMMUNITY

Securing the Future of Urban Living

Lead by NEOM



As nations embark on the exciting journey of shaping the cities and infrastructures of tomorrow, Cybersecurity remains a paramount concern. The grand visions of giga-projects and smart cities bring with them immense opportunities, but also beckon the attention of Cyber adversaries. With vast volumes of data in play and cutting-edge technologies deployed, our urban landscapes become prime targets for malicious actors. The task of securing our urban future, however, goes beyond the realm of governments. It requires a collaborative, multi-stakeholder strategy, ensuring that the diverse voices and interests from across the globe are not only acknowledged but actively engaged in shaping the path forward, taking action, and fortifying these cities, thus ensuring a safe, secure, and sustainable future for all. This mission is the driving force behind the knowledge community known as ‘Securing the Future of Urban Living’. We are dedicated to exploring and seizing opportunities to construct a more resilient, sustainable, and equitable urban future. Our strength lies in the diversity of expertise we bring together from multiple stakeholder groups.

The community welcomes smart city agencies, global Cybersecurity research organizations, large technology companies, reputable think tanks, academia, and all those with a vested interest in building a secure future.

Join the community to collaborate and advocate for potential solutions to protect future cities and their residents. ■

KNOWLEDGE COMMUNITY MEETING:

Securing the Future of Urban Living

With smart city visions turning into reality, this dedicated community composed of 9 international stakeholders is exploring opportunities to construct a more resilient, sustainable, and equitable urban future. During this meeting, the community has discussed key challenges, opportunities, and priorities. They then defined the key priorities for the upcoming year. An ideation session helped shaping the community action plan and the way forward.

Moving forward, community activities will include:

Defining shared goals: Developing a joint vision, mission statement, and shared success metrics to ensure all stakeholders’ efforts are directed towards a common goal.

Developing programs and initiatives: Supporting existing initiatives in their domain of interest, or building additional efforts such as publishing whitepapers and conducting advocacy.

Holding collaboration sessions: Participating in regular sessions to advance collaboration on specific community initiatives, ensure consistent and continuous dialogue, and unify community efforts. ■



4



KEY TAKEAWAYS

KEY TAKEAWAYS

The Annual Event's 2023 theme, "**Charting Shared Priorities in Cyberspace**" enabled deep exploration into the most pressing and pertinent Cyberspace issues of the day and pushed knowledge boundaries through expert panelist insights. In addition to the insights generated by each session, summarized in the previous pages, the discussion at this year's Annual Event yielded five critical, cross-cutting priorities. As an action-oriented platform that is empowered by its community and partners, the GCF will act through initiatives, knowledge creation, and projects to deliver on the five priorities identified.

PRIORITY#1

ADVANCING THE CYBER RESILIENCE OF KEY SECTORS

Critical systems across key sectors are becoming ever-more deeply intertwined with Cyberspace, particularly as Information Technology (IT) and Operational Technology (OT) systems converge. In the energy sector, for example, investment in digital electricity infrastructure and software has grown by over 20% annually since 2014. This deepening integration presents a host of opportunities to increase the speed and efficiency of operations. It also, however, introduces new risks and clear challenges by amplifying the potential scale of destruction, should vulnerabilities be exploited.

Across sessions, speakers highlighted the potential implications of this deepening integration in key sectors—including energy, healthcare, telecommunications, and finance. There exists today significantly more systemic risk than ever before. It became clear in discussions across the two-day annual event that enhancing Cyber resilience is of particular importance within human-facing infrastructure systems and sectors as they have the greatest potential impact on individual lives and societal well-being. There was a clear consensus on the need to advance the resilience of these critical systems by bringing together all actors from government, private sector, academia, and NGOs.

During the 2023 annual event, the GCF institute launched a number of efforts that will support this priority area of action moving forward:

► **Operational Technology Cybersecurity Center of Excellence (OTC COE):**

The OTC COE is a global, multi-stakeholder platform established in collaboration with 5 founding private sector members. The Center intends to advance the maturity of global OT Cybersecurity, including through capability development, standards and policy advocacy, and thought leadership generation.

► **Securing the Global Energy Supply Chain Knowledge Community:**

This knowledge community, led by Aramco, is committed to strengthening the resilience and Cybersecurity of global energy infrastructure and ensuring a secure energy future for all.

► **Safeguarding Future Networks & Emerging Technologies Knowledge Community:**

This knowledge community, led by stc, is committed to promoting and safeguarding current and future ICT networks and safeguard the backbone of our digitally connected world.

PRIORITY#2

SAFEGUARDING CYBERSPACE IN THE ERA OF EMERGING TECHNOLOGIES

Advancements in AI, particularly in Large Language Models (LLMs), the metaverse, quantum computing, and autonomous systems—among other emerging technologies—all signal exciting and even revolutionary advances in the human experience. Given the high degree of adoption, these technologies are expected to enhance and, in many cases, fundamentally alter our current systems of human activity, including education, commerce, and employment. However, these technologies present a new set of threats for all users. The extremely rapid evolution of these technologies, their pervasiveness across all domains of human life, and the fact that they are subject to limited or weak regulation—all represent sources of uncertainty and risk.

Across sessions, speakers remarked time and time again on the sheer speed of the evolution of these technologies and the implications of that rapid pace of change on ecosystem-wide security. This rapid evolution poses a dual challenge, presenting both opportunities and necessities. On the one hand, there's a clear opportunity to use these technologies to strengthen security capabilities. Innovations in AI, the metaverse, and autonomous systems offer solutions to enhance security across many sectors. On the other hand, there's an urgent need for new and innovative

ways to regulate these advancements. As these technologies reshape key domains of human activity, the regulations must adapt just as quickly if not faster. As all actors seek to more effectively deploy emerging technologies, balancing the potential benefits of these technologies with the establishment of effective regulatory measures is a crucial task in navigating this transformative era of technological progress.

During the 2023 Annual Event, the GCF Institute launched a number of efforts that will support this priority area of action moving forward:

► **Future of Cybersecurity Knowledge Community:**

This knowledge community, led by founding member SITE, is committed to exploring the potential opportunities and threats presented by emerging technologies and developing mechanisms to maximize their benefits.

PRIORITY#3

EMPOWERING A SAFE, SUSTAINABLE, AND INCLUSIVE CYBERSPACE

The technological landscape is expanding and changing at an unprecedented rate, connecting nations, communities, and users ever more deeply through interactions taking new forms across both virtual and physical worlds. It is estimated that each person will own up to 15 connected devices by 2030. While this increasing digital connectivity offers an improved quality of life for many users, the myriad technologies we use daily are in many ways blind to user characteristics, including the vulnerabilities that may be correlated with socioeconomic status, age, or even gender. This reality, as each individual connects to Cyberspace in more numerous and increasingly diverse ways, may render some populations and societies more vulnerable than others to the abuses that may occur in the Cyber domain.

Across sessions, speakers highlighted opportunities to better protect vulnerable populations and empower all people to productively engage in Cyberspace. In particular, as children spend an increasing amount of time online and on social media, there is a heightened risk of Cyber threats posing serious consequences. Increased incidences of Cyber bullying and extortion crimes have a significant impact on younger generations. It became clear in discussions across the two-day annual event that increased connectedness

will also have broader societal implications, given the increasingly digitalized nature of the spaces in which we live and work. Smart cities, for example, are attractive targets for malicious Cyber actors particularly because of the data being collected, transmitted, stored, and processed. Consideration of these impacts and others throughout the event led to a broad consensus among participants on the importance of fostering a human-centered Cyberspace, in which vulnerable populations are explicitly considered and protected in design processes.

During the 2023 Annual Event, the GCF Institute launched a number of efforts that will support this priority area of action moving forward:

► **Child Protection in Cyberspace Initiative:**

The GCF Institute has advanced discussions with multiple international partners to start global projects on child protection in Cyberspace. This global initiative aims to take targeted action to enhance the safety of Cyberspace for children.

► **Future of Urban Living Knowledge Community:**

This knowledge community led by Neom is committed to exploring potential opportunities to build a more resilient, sustainable, and equitable urban future for all.

PRIORITY#4

HARNESSING CYBERSPACE AS AN ENGINE FOR GROWTH

Cybersecurity is one of the fastest growing industries in the world, with investment in Cybersecurity companies having increased more than ninefold since 2011. Prospects of growth for the future continue to look promising: the Cybersecurity market is expected to grow to \$538 billion by 2030, up from \$202 billion today. The Cybersecurity sector therefore represents an enormous opportunity as an engine for economic growth. Yet, as innovators, investors, and national governments seek to unlock the economic potential of a thriving Cybersecurity ecosystem, they must contend with the challenges inherent in the sector.

Throughout the event, experts and policy practitioners highlighted the myriad factors that have limited the growth of the global Cybersecurity ecosystem and market. The global talent shortage in the field, for example, is a clear obstacle for companies large and small. Yet, there is no shortage of innovation. Rather, in many instances—particularly for small companies such as Cyber startups—it is the business side of a Cyber company that needs support to be propelled. While technological innovation is the foundation of a Cyber company, a clear unique value proposition complemented by business and customer acquisition models is crucial to survive in a highly competitive marketplace. It became clear in discussions across

the two-day annual event that unlocking the full economic potential of the Cybersecurity sector requires governments to play a more active role in supporting Cyber startups, including supporting through innovation hubs or accelerators, and other ecosystem-wide measures. There was broad consensus that sustained market growth can only be realized through greater interaction between government and innovators, with the provision of support from across the Cyber community.

During the 2023 Annual Event, the GCF Institute launched a number of efforts that will support this priority area of action moving forward:

► **Women Empowerment in Cybersecurity:**

The Institute has advanced discussion with international partners to start global projects on women empowerment in Cyberspace. This global initiative aims to empower women in Cyberspace and increase the number of women in the Cybersecurity workforce.

► **Substantive cooperation:**

The Institute issued a broader call for stakeholders to institutionalize cooperation with the objective of fostering entrepreneurship and support with investment and other incubator support.

PRIORITY #5 DISINCENTIVIZING CYBERCRIME

In an ever-more pervasively interconnected world, Cybercrime represents an increasingly costly threat—in financial, operational, and reputational terms. An ever-evolving challenge, Cybercrime is projected to cost governments and organizations \$10.5 trillion by 2025, up from \$8 trillion in 2023. The escalating scale and costs of Cybercrime and its increasingly disruptive impacts make apparent the clear imperative to gain a comprehensive understanding of the behavior and motivations of Cybercriminals. This understanding is pivotal in developing targeted strategies to prevent and combat Cybercrime—an inherently transnational challenge requiring cooperation among a wide array of actors.

Across discussions, participants offered new perspectives on the evolving threat of Cybercrime and presented alternative lenses for understanding criminal actors. While traditionally understood to be largely financially motivated, experts across the fields of Cybersecurity, law enforcement, and psychology highlighted that the motivations of Cybercriminals may be shifting. With the rising sophistication of Cybercrime, it is imperative to develop a greater understanding of the incentives and motivations that shape criminal behavior, in order to develop targeted strategies and robust defenses. Across the two-day annual event, the contribution

of a wide diversity of perspectives made clear the imperative for an explicitly inter-disciplinary approach to countering Cybercrime—integrating the technical, behavioral, and psychological expertise necessary to effectively understand the behavior of Cyber criminals. Thus, a priority emerged to not only counter Cybercrime, but tackle the motivations and structural incentives that give rise to it—thereby disincentivizing Cybercrime.

During the 2023 annual event, the GCF Institute launched a number of efforts that will support this priority area of action moving forward:

► **Global Collaboration:**

The GCF Institute is engaging with international organizations and other key stakeholders on multi-stakeholder initiatives and programs to initiate projects on disincentivizing Cybercrime.

5



OUTREACH AND COLLABORATION

GCF Media

LIVE STREAM

Live streams were provided for all events in the main forum on our YouTube Channel: Global Cybersecurity Forum [@GCFRIYADH](#)

MEDIA LIBRARY

Videos and Photos of sessions, discussions, interviews, and other highlights are available in the media hub section of our website.



GCF LIVE STUDIO

A world-class, multi-camera, field broadcast Studio that connected and provided interviews to any global news network in real time, enabling participants to speak to any journalist, anywhere, anytime, right from the Global Cybersecurity Forum.

SOCIAL MEDIA ACTIVITIES

Extensive and real-time coverage of the GCF discussions, sessions, and highlights were provided on our social media channels:

-  [@GCFRIYADH](#)
-  [@GCFRIYADH](#)
-  [@GCFRIYADH](#)
-  [@GCFRIYADH](#)
-  [@GCFRIYADH](#)



Communications Impact

GCF DIGITAL CHANNELS

OUT OF HOME ADVERTISING

GCF LIVE STUDIO

DIGITAL TOTAL IMPRESSIONS

LIVESTREAM VIEWS



230m+



1.6m+

TRADITIONAL MEDIA MENTIONS



650+



INTERNATIONAL INTERVIEWS

50+



MOMENT OF GENIUS



"Award-winning journalists identified key newsmaking moments from across our incredible selection of panels at the Global Cybersecurity Forum in real time. Then, distributed them to more than 200 tier-one global news sites within two hours or less."

TOTAL IMPRESSIONS

3.6m+

HOURS VIEWED

8k+



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 first season 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 sectoral issues, season one of the Rethinking Cyber podcast also aimed to bring the issues of Cyberspace and Cybersecurity to a wider audience. Join us for the first episodes of the second season.



Catch all our episodes on
Spotify & Apple Music

LISTEN ON  Spotify

Listen on  Music



Rethinking Cyber Podcast - Season#1



Imagining a Post-Quantum Future

Dr. Michio Kaku,
Professor of Theoretical Physics,
City University of New York



A safe (Cyber)space for children

Iain Drennan
Executive Director,
WeProtect Global Alliance



Navigating Cyberspace; How Businesses Can Survive and Thrive

Alex Liu
Managing Partner and Chairman,
Kearney



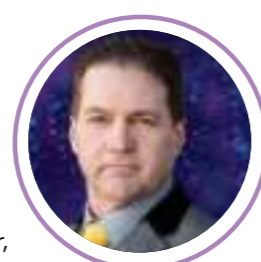
Rethinking global policing models to tackle Cybercrime

Craig Jones
Cybercrime Director,
Interpol



Empowering Women in Cybersecurity

Leila Hoteit
Managing Director and Senior Partner,
BCG



Demystifying Cryptography

Dr. Craig Wright
Founder and Chief Scientist,
nChain



Safety Tech: Exploring a New Global Sector

Prof. Mary Aiken
Professor of Cyberpsychology and Chair,
Department of Cyberpsychology, Capitol
Technology University

Rethinking Cyber Podcast - Season#2



Rethinking Industrial Cybersecurity: What Are We Missing?

As our world evolves against the backdrop of ongoing polycrisis and technological advancement, are we doing enough to secure industrial infrastructure? Robert Lee, CEO and Co-founder, Dragos, shares his insights on the urgent need for better collaboration, information sharing, and improved defenses in industrial automation environments to advance collective action for Cyber stability. He emphasizes the social aspects of technologies and placing human safety and wellbeing at the core of Cybersecurity strategies.



In the Newsroom and Beyond: Why should Cybersecurity be a Top Five Priority?

Is the importance of Cybersecurity reflected in the news agenda? John Defterios, former CNN anchor and Senior Strategic Advisor at APCO Worldwide, joins us to explore the interconnected topics shaping the global Cyber agenda and how it is represented in the media. He answers why there is a tendency for Cybersecurity to take a backseat to other issues such as geopolitics and energy security, and why it is crucial to ensure that the Global South is not left behind in discussions about Cyberspace. Brought to you by the Global Cybersecurity Forum, the Rethinking Cyber podcast is here to share insights from the world's leading minds as we navigate our Cyber future.



Empowering Women in Tech: A Cybersecurity Perspective

Join Her Excellency Kersti Kaljulaid, Former President of Estonia, as she explores the crucial role of women in Cyberspace. In this episode, H.E. Kaljulaid advocates for gender equality and inclusivity in the tech sector, shedding light on Estonia's unique Cybersecurity stance. Discussing global collaboration between public and private sectors, she addresses challenges and opportunities presented by next-gen technologies and underscores the role transparency plays in fostering Cyber resilience. Tune in for a thought-provoking discussion on Cybersecurity, representative leadership, and Estonia's commitment to shaping the international Cybersecurity landscape.



Capacity Building in Cyberspace: A Global Imperative

How do nations navigate the evolving landscape of Cyberspace and bolster their defenses against digital threats? Join Cybersecurity expert Professor William H. Dutton as he addresses this pivotal question and unveils strategies for building Cybersecurity capacity. From the early days of computer security, to the challenges of our interconnected world, Professor Dutton shares insights on the complexities of assessing a nation's Cybersecurity maturity. Explore surprising findings, the impact of economic development, and key skills essential for individual and organizational resilience.



Catch all our episodes on
Spotify & Apple Music

B2B Meetings

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



Albukairi Gala Dinner

The GCF was delighted to welcome guests to enjoy the Kingdom's hospitality and rich heritage at Albukairi





GLOBAL CYBERSECURITY FORUM PARTNERS

Founding Partners



Strategic Partners



Digital Enabler



Conclusion

This book summarizes the key outcomes and priorities from the 2023 Global Cybersecurity Forum (GCF). GCF 2023 underscored the pressing need for an international platform to address Cyberspace issues comprehensively, spanning geopolitical, economic, developmental, and behavioral dimensions. The forum emphasized its continued commitment to supporting vulnerable communities globally and tracking trends in emerging technologies.

Informed by the outcomes of previous editions, the theme and sub-themes for GCF 2023 stressed the importance of uniting the international Cyber community to set shared, strategic priorities for the development of the global Cybersecurity sector. Participants at GCF 2023, including thought leaders, decisionmakers and international experts recognized the potential for economic and social development globally by harnessing opportunities in Cyberspace for the benefit of human well-being and prosperity.

We attribute the Global Cybersecurity Forum's growth and achievements to the support of both our local and international partners, who share our mission to create a platform that addresses shared concerns and maximizes opportunities in Cyberspace.

While the outcomes and priorities identified at GCF 2023 aim to maximize strategic collaboration on vital Cyberspace issues, the GCF Institute will facilitate ongoing dialogue between our various partners and support relevant projects in the months ahead. The GCF Institute aims to consolidate international partnerships and cooperation within the global Cybersecurity ecosystem and leverage the opportunities that abound in the Cybersecurity sector to stimulate development, growth, and prosperity.

In collaboration with our partners from all over the world, the Global Cybersecurity Forum remains committed to its role as an international platform on Cyberspace issues, grounded in three strategic pillars:

► **Forum for strategic discussions on Cybersecurity:** Addressing Cybersecurity issues that affect individuals, communities, and nations globally. Focusing on the priorities of the public sector, private entities, think tanks, research centers, and NGOs worldwide.

► **Platform for international collaboration:** Uniting the international community to bring positive change in the sector. This involves fostering dialogue between leaders and decisionmakers from governmental and non-governmental entities, the private sector, thinktanks, and research centers, promoting international cooperation for a safer and more stable Cyberspace.

► **Hub for building long-term partnerships:** Extending beyond the Annual Event, the forum serves as fertile ground for building enduring partnerships. Topics discussed during the forum continue to resonate among stakeholders globally, fostering ongoing discussions and the exchange of views even after the event concludes.

In conclusion, we extend our thanks and appreciation to our partners worldwide, who have been integral to the Global Cybersecurity Forum's journey and achievements, contributing to its position as a leading international platform for dialogue and action in Cyberspace. We look forward to building on these accomplishments to advance global development and prosperity for all.



Global
Cybersecurity
Forum

ORGANIZED BY



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority