GCF ANNUAL MEETING 2025

SCALING COHESIVE ADVANCEMENT IN CYBERSPACE

GLOBAL CYBERSECURITY FORUM

ANNUAL MEETING
1-2 OCTOBER 2025

Under the patronage of the
Custodian of the Two Holy Mosques
King Salman bin Abdulaziz Al-Saud

His Royal Highness
Prince Mohammed bin Salman
bin Abdulaziz Al-Saud
Crown Prince and Prime Minister

TABLE OF CONTENTS

01

INTRODUCTION

INTRODUCTION

The Global Cybersecurity Forum (GCF) was established by Royal Order as a global non-profit platform dedicated to supporting and unifying international efforts toward a safe and trusted cyberspace for all. GCF focuses on strengthening collaboration, fostering constructive dialogue, identifying shared priorities, and launching impactful initiatives that advance cybersecurity at the international level. By working with diverse international partners across multiple sectors and integrating its efforts with global initiatives, GCF aims to deepen dialogue and cooperation, reinforce social impact, promote economic development, and expand knowledge in this vital and promising sector.

The Global Cybersecurity Forum Annual Meeting represents one of the key initiatives of GCF. Its fifth edition, held in Riyadh on October 1–2, 2025, welcomed a wide audience of experts, decision-makers, and leaders from over 130 countries and various sectors. The event provided a platform to address critical topics in cyberspace and identify shared pathways to strengthen international cooperation in setting cybersecurity priorities.

Under the theme "Scaling Cohesive Advancement in Cyberspace," the 2025 edition translated strategic dialogues and collaborative efforts into tangible outcomes through initiatives, partnerships, and programs designed to address pressing challenges across key cybersecurity domains.

On the capacity-building front, the 2025 Annual Meeting witnessed the announcement of the Global Initiative for Capacity Building in Cyberspace, a strategic partnership between the Kingdom of Saudi Arabia and the United Nations. The initiative was launched in response to pressing global cybersecurity challenges, particularly in areas of highest need, such as the global shortage of cybersecurity professionals, estimated at 2.8 million according to the Cybersecurity Workforce Report 2024: Addressing Workforce and Skills Gaps, published by GCF.

Discussions during the Annual Meeting also reinforced the real-world impact of GCF initiatives, including the two global initiatives launched by His Royal Highness the Crown Prince and Prime Minister – may God protect him – namely: the Child Protection in Cyberspace (CPC) initiative and the Women Empowerment in Cybersecurity (WEC) initiative. The Annual Meeting 2025 stimulated action across multiple programs aimed at strengthening child online safety and addressing the cybersecurity workforce skills gap through efforts to upskill and empower more women, who currently make up only 24% of professionals in the sector.

This report documents the fifth edition of the GCF Annual Meting as a new phase of high-level collaboration and a steadfast commitment among GCF's partners to maximize impact through collective action. GCF continues to build toward a future Cyberspace that is safer, more trusted, and inclusive, contributing to sustainable development and prosperity for communities around the world.

02

GCF ANNUAL MEETING 2025: SCALING COHESIVE ADVANCEMENT IN CYBERSPACE

OPENING ADDRESS

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

Distinguished participants and guests,

Peace, mercy, and blessings of God be upon you.

We welcome you today to the Kingdom of Saudi Arabia, and on behalf of the Custodian of the Two Holy Mosques, King Salman – may God protect him – I am pleased to announce the commencement of the fifth edition of the Global Cybersecurity Forum in Riyadh.

Distinguished attendees, last year's edition was honored by a comprehensive and insightful address from His Royal Highness Prince Mohammed bin Salman bin Abdulaziz Al-Saud, Crown Prince and Prime Minister, in which he emphasized – may God protect him – the close connection between Cyberspace and the growth of economies, the prosperity of societies, the security of individuals, and the stability of nations, and its nature, which transcends borders. This underscores the growing importance of unifying and aligning international efforts to seize opportunities and address challenges in Cyberspace through investment in human capital.

Therefore, this year's forum, themed "Scaling Cohesive Advancement in Cyberspace," reaffirms these principles and builds upon the significant achievements of previous forums in unifying international efforts and maximizing collaboration. We are confident that the distinguished presence of leaders, decision-makers, and experts from around the world will, God willing, enhance the forum's outcomes and provide valuable global insights, contributing to a secure and reliable Cyberspace that enables growth and prosperity for people around the world.

Dear guests, thank you for your attendance. I pray for everyone's success in the forum. Peace, mercy, and blessings of God be upon you.

OPENING REMARKS

HIS EXCELLENCY MAJED BIN MOHAMMED AL-MAZYED, GOVERNOR OF THE NATIONAL CYBERSECURITY AUTHORITY, SAUDI ARABIA, ACTING ON BEHALF OF THE BOARD OF TRUSTEES, GLOBAL CYBERSECURITY FORUM

Your Royal Highness, Your Excellencies, Distinguished Guests:

It is my honor to welcome you to the Global Cybersecurity Forum Annual Meeting 2025.

Building on the progress of previous editions and the year-round collaboration of the GCF community, this year's Annual Meeting advances our collective momentum under the theme of "Scaling Cohesive Advancement in Cyberspace."

This theme underscores a new phase of deepened collaboration, and our intent to exponentially expand the transformative impact that GCF has already achieved across its growing range of activities.

The global economy depends on Cyberspace, yet our collective understanding of the economic dimension of cybersecurity remains limited. The Centre for Cyber Economics – launched in partnership with the World Economic Forum – will equip decision-makers and sector leaders with evidence-based research and strategies to unlock the full economic value of cybersecurity. In this year of unprecedented complexity and an increasingly volatile threat landscape, we are working to gain deep insight into the mechanisms underlying cybercrime through collective research and purposeful dialogue. In parallel, global stakeholders continue to collaborate through the Operational Technology Cybersecurity Center of Excellence to strengthen the vitally important resilience of OT supply chains.

This continuous progress is driven by the unwavering commitment of our partners, who remain the true catalysts of these vital activities. I would also like to thank our Strategic Partners, Annual Meeting Partners, and our ever-expanding community of Knowledge Contributors who help sustain this momentum as we scale the scope and impact of our joint efforts.

At last year's Annual Meeting, His Royal Highness Prince Mohammed bin Salman bin Abdulaziz Al-Saud, Crown Prince and Prime Minister of Saudi Arabia, stated that: "The Kingdom of Saudi Arabia has always been a force for good for the benefit of humanity and human prosperity around the world."

In this spirit, I am pleased to announce that the Kingdom is launching a Global Initiative for Capacity Building in Cyberspace in partnership with the United Nations. By harnessing the expertise of a wide range of international stakeholders, this initiative will deliver accelerated capacity development at scale in areas of greatest need - from training and education to research and policy development. I take this opportunity to thank His Excellency United Nations Secretary-General António Guterres for his commitment to this important topic and to our partners, UN agencies, and organizations for their continued support and collaboration.

Together, we are not only responding to evolving cyber threats – we are shaping a more secure and inclusive Cyberspace, and with it a more peaceful and prosperous future for all humanity. I wish you all a productive two days of purposeful dialogue, collaborative action, and transformative partnership.

Thank you.

VIDEO ADDRESS

HIS EXCELLENCY ANTÓNIO GUTERRES, SECRETARY-GENERAL OF THE UNITED NATIONS

Excellencies, Dear Friends,

I send my warm greetings to this Global Cybersecurity Forum in Riyadh.

In our interconnected world, Cyberspace is essential for innovation and opportunity. At the same time, vulnerabilities can undermine trust, disrupt societies, and threaten peace.

We must act together to ensure Cyberspace serves the common good by investing in people, building skills, and fostering inclusion.

As digitization accelerates, we must forge global partnerships rooted in solidarity and shared responsibility, leaving no country or community behind.

The United Nations remains committed to advancing a vision of Cyberspace that is open, secure, and anchored in international law. To achieve this vision, we are working to ensure all countries have the capacity to maximize digital opportunities while minimizing risks.

I want to recognize the Kingdom of Saudi Arabia's initiative on capacity building and this forum's focus on issues like child protection and women's empowerment.

Let us work together to build trust, establish common rules, and protect human rights for a more secure digital future for all.

Thank you.

GCF ANNUAL MEETING 2025

Scaling Cohesive Advancement in Cyberspace

1st - 2nd October 2025 The Ritz-Carlton, Riyadh, Saudi Arabia

The GCF Annual Meeting is an action-oriented event that convenes thought leaders, decision makers, and experts from around the world to advance multistakeholder collaboration and action on the challenges and opportunities Cyberspace presents globally.

This year's Annual Meeting builds on the momentum of previous editions, driving forward a strategic and action-oriented dialogue. The GCF 2023 theme of "Charting Shared Priorities in Cyberspace" represented an ideal progression in order to build upon the foundation set by the 2022 theme of "Rethinking the Global Cyber Order." The 2024 edition continued the narrative movement toward driving substantive action under the theme "Advancing Collective Action in Cyberspace." This year, we aim to scale these cohesive advancements—broadening their scope, strengthening their impact, and fostering deeper collaboration to build a safer and more resilient future for all.

Building on the momentum of previous editions, the event shifted the focus from driving substantive action under the 2024 theme 'Advancing Collective Action in Cyberspace,' to scaling the cohesive advancements accomplished by the GCF community, with a focus on elevating the scope, capacity and impact of the efforts to ensure a safer, more resilient Cyberspace for all.

PARTNERS

GCF FOUNDING PARTNERS

GCF STRATEGIC PARTNERS

GCF ANNUAL MEETING PARTNERS 2025

GCF ANNUAL MEETING MEDIA PARTNERS

GCF KNOWLEDGE CONTRIBUTORS

GCF ANNUAL MEETING 2025

Scaling Cohesive Advancement in Cyberspace

SUB-THEMES

The GCF Annual Meeting 2025 was structured around five key sub-themes, encompassing the geopolitical, economic, social, behavioral, and technical dimensions of Cyberspace:

Beyond the Inflection Point

Fostering alignment in a rapidly evolving and divided global landscape

Cyber Economics Redefined

Advancing cyber economic cohesion and fostering scalable growth toward shared prosperity

Strengthening Cyber Inclusion

Strengthening collective action for a human-centered inclusive Cyberspace

Behavioral Lens in Cyberspace

Leveraging behavioral insights to influence actions, counter manipulations, and foster safe cyber environments

Opportunities at the Cyber Horizon

Harnessing technological advancements to tackle fast-evolving challenges in Cyberspace

PROGRAM FORMAT

The GCF Annual Meeting brings together global stakeholders to strengthen collaboration and advance shared priorities.

To achieve this, the Annual Meeting is structured around two main program tracks:

OPEN FORUM

The Open Forum facilitates dialogue and knowledge-sharing in an accessible manner, welcoming all Annual Meeting participants, with the aim of providing diverse perspectives and multidisciplinary lenses across key cybersecurity issues.

- **Plenary Session**
- **Panel Discussions**
- **Fireside Chats**

PARTICIPATORY TRACK

Held in a range of formats, the expanded program of Participatory Track sessions at this year's Annual Meeting enabled interactive, action-oriented discussions on a variety of topics across diverse stakeholder groups.

- **Roundtables**
- **Knowledge Community Meetings**
- **Panel Discussions**
- **Fireside Chats**
- **Community Meetings**
- **Hosted Events**

KEY FIGURES

Action-Oriented Program

130 Countries represented

143 International speakers

28 Open Forum sessions

54 Participatory Track sessions

8 Roundtables

36 Interactive sessions

10 Community meetings

5 Centre for Cyber Economics meetings

Impact Network meeting

OT Cybersecurity Center of Excellence meeting

3 Knowledge Community meetings

3 Hosted events

EU-GCC Cyber Diplomacy 1.5 Dialogue

Arab CxO

World Economic Forum (WEF) meeting

Global Engagement

450M Total media reach

6.5M Video views on GCF channels

134 Tier 1 media interviews from the GCF Live Studio

GCF ANNUAL MEETING PROGRAM

OPEN FORUM - OCTOBER 1ST, 2025 (DAY 1) ROOM G

10:00 **Opening Ceremony**

10:20 **Against the Odds:** Gaining Consensus Amid Complexity

John Defterios (Moderator)
Former CNN Emerging Markets Editor and Anchor

Kolinda Grabar-Kitarović
President of Croatia (2015 – 2020)

Macky Sall
President of Senegal (2012 – 2024)

Chris Inglis
National Cyber Director, United States (2021 – 2023)

10:50 **The Economic Dimension of Cyberspace**

Dr. Saad Alaboodi
Chief Executive Officer, Saudi Information Technology Company (SITE)

11:00 **Cybersecurity as an Economic Imperative:** Driving Growth in the Global Economy

Nisha Pillai (Moderator)
International Moderator and Journalist

Florian Schütz
Director, Federal Office for Cyber Security, Switzerland

Heidi Crebo-Rediker
Senior Fellow for Geoeconomics, Council on Foreign Relations

Akshay Joshi
Head of Centre for Cybersecurity, World Economic Forum

Dr. Stéphane Straub
Chief Economist for Infrastructure, World Bank

Sub-Themes
Beyond the Inflection Point | Cyber Economics Redefined | Strengthening Cyber Inclusion | Behavioral Lens in Cyberspace | Opportunities at the Cyber Horizon

11:30 **Shaping Resilience:** Investing in Women as a Global Economic Imperative

Rebecca McLaughlin-Eastham (Moderator)
Independent TV Anchor and CEO, RME Media

H.E. Dr. Hala Bint Mazyad Altuwaijri
President, Human Rights Commission of Saudi Arabia

Jim O'Connor
Chairman and CEO, United States Telecommunications Training Institute (USTTI)

Sarah E. Hendriks
Deputy Executive Director, UN Women

12:00 **Collaboration for Growth:** Building a Thriving and Innovative Security and Defense Ecosystem

Lara Habib (Moderator)
Senior Business News Presenter Al Arabiya

Shaikh Salman bin Mohammed Al Khalifa
Chief Executive Officer, National Cyber Security Center Kingdom of Bahrain

General (Rtd) Jean-Paul Paloméros
Supreme Allied Commander Transformation, NATO (2012-2015)

Dan Cîmpean
Director
National Cyber Security Directorate, Romania

12:30 **Powering Tomorrow:** The Economic Imperative for Securing the Global Energy Supply Chain

John Defterios (Moderator)
Former CNN, Emerging Markets Editor & Anchor

Ahmad Al-Khowaiter
Executive Vice President Aramco

12:50 **AI for Security and Security for AI:** Ensuring Resilience and Building Trust

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

Dr. Bilel Jamoussi
Deputy Director, Telecommunication Standardization Bureau, ITU

Rob Duhart
Chief Security Officer, Oracle

Bob Willen
Global Managing Partner and Chairman, Kearney

Sub-Themes
Beyond the Inflection Point | Cyber Economics Redefined | Strengthening Cyber Inclusion | Behavioral Lens in Cyberspace | Opportunities at the Cyber Horizon

13:20 **The Q-Cyber Frontier:** Harnessing Quantum Innovation for Cyber Resilience

Ryan Chilcote (Moderator)
International Broadcaster and Journalist

Jinyoung Oh
Vice President
Korea Internet & Security Agency (KISA)

Mark Hughes
Global Managing Partner, Consulting Cybersecurity Services, IBM

David Panhans
Managing Director & Senior Partner, BCG

Arnaud Taddei
Chair of Study Group 17, Standardization Sector, ITU

13:50 **Defending the Grid:** Uniting Forces to Protect Critical Infrastructure

Lara Habib (Moderator)
Senior Business News Presenter Al Arabiya

Miguel Ángel Cañada
Head of Cabinet and National Coordination Center (NCC-ES), Spanish National Cybersecurity Institute (INCIBE), Spain

Rohit Unnikrishnan
Senior Vice President of Product Management, Trellix

Hosam A. Alsuliman
Policies & Regulations Deputy Governor, National Cybersecurity Authority, Saudi Arabia

14:20 **Reinforcing the Links:** Securing Global Energy Supply Chains

Nisha Pillai (Moderator)
International Moderator and Journalist

Robert M. Lee
CEO AND CO-Founder, Dragos, INC.

Saeed AlSaeed
Chief Executive Officer, Cyberani

Chase Carpenter
Chief Security Officer, Honeywell

Sub-Themes
Beyond the Inflection Point
Cyber Economics Redefined
Strengthening Cyber Inclusion
Behavioral Lens in Cyberspace
Opportunities at the Cyber Horizon

14:50 **The Hidden Web:** Inside the Tactics of Link-Based Crime Networks

Sarah Al-Khaldi (Moderator)
Business News Anchor, Channel NewsAsia

Dr. Neal Jetton
Director Cybercrime, INTERPOL

Prof. Marco Gercke
Director, Cybercrime Research Institute

Eric Skinner
VP Market Strategy, Trendmicro

Christopher Porter
Head of International Security Cooperation, Google Cloud

15:20 **Securing Prosperity:** AI Preparedness in a Connected World

Ryan Chilcote (Moderator)
International Broadcaster and Journalist

Doreen Bogdan-Martin
Secretary-General, International Telecommunication Union (ITU)

15:40 **From Gaps to Gains:** Scaling Global Cyber Capability Development Through Collective Action al Infrastructure

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

Chris Gibson
CEO/Executive Director, Forum of Incident Response & Security Teams (FIRST)

Prof. William H. Dutton
Oxford Martin Fellow, Global Cyber Security Capacity Centre, University of Oxford

Ahmed Almalki
CISO, SABIC

Sub-Themes
Beyond the Inflection Point
Cyber Economics Redefined
Strengthening Cyber Inclusion
Behavioral Lens in Cyberspace
Opportunities at the Cyber Horizon

OPEN FORUM - OCTOBER 2ND, 2025 (DAY 2) ROOM G

9:30 **Converging Crisis :** The Future of Cyberspace in Complex Global Dynamics

John Defterios (Moderator)
Former Emerging Markets Editor and Anchor, CNN

Jürgen Stock
Secretary General, INTERPOL (2014 – 2024)

Dr. Robin Geiss
Director, United Nations Institute for Disarmament Research (UNIDIR)

H.E. José Manuel Barroso
President of the European Commission (2004 – 2014)

Robert Hannigan
Director, GCHQ, United Kingdom (2014 – 2017)

10:05 **Trust in Action:** Reimagining Citizen Services in a Cyber-First World

Riz Khan (Moderator)
International Journalist and TV host Al Arabiya English

H.H. Prince Dr. Bandar bin Abdullah bin Mishari
Assistant Minister of Interior for Technology Affairs, Saudi Arabia

Ir. Dr. Megat Zuhairy bin Megat Tajuddin
Chief Executive, National Cyber Security Agency (NACSA), Malaysia

H.E Shaza Fatima Khawaja
Minister of State, Ministry of Information Technology and Telecommunication, Pakistan

10:30 **CyberSafe Futures:** Scaling Inclusion & Protection for Every Child

Rebecca McLaughlin-Eastham (Moderator)
Independent TV Anchor and CEO, RME Media

H.E. Dr. Maimoonah AlKhalil
Secretary General, Family Affairs Council, Saudi Arabia

H.E. Sofiene Hemissi
Minister of Communication Technologies, Tunisia

Dr. Iain Drennan
Executive Director, WeProtect Global Alliance

Sheema Sen Gupta
Global Director of Child Protection, UNICEF

Sub-Themes
Beyond the Inflection Point · Cyber Economics Redefined · Strengthening Cyber Inclusion · Behavioral Lens in Cyberspace · Opportunities at the Cyber Horizon

11:00 **The Cyber Frontier:** Harnessing Emerging Tech for Global Security

Kaiyi Dai (Moderator)
Television News Reporter at CGTN

Eng. Yasser Alswailem
CEO, Sirar

Filippo Monticelli
Vice President, Fortinet

John Crain
SVP, Chief Technology Officer, ICANN

Mikko Karikytö
Chief Product Security Officer, Ericsson

11:30 **The Talent Imperative:** Unlocking the Power of Women in Cyber

Leila Hoteit (Moderator)
Managing Director & Senior Partner, BCG

David Hoffman
Steed Family Professor of the Practice of Cybersecurity Policy, Duke University

Silvana Koch-Mehrin
Founder and President, Women Political Leaders (WPL)

Rummana Dada
Founder, Managing Partner, Vitality Capital

Linda Gray Martin
Senior Vice President and Chief of Staff, RSA Conference

12:05 **The Cost of Cyber Insecurity:** Quantifying Financial Risks and Economic Fallout

Laura Buckwell (Moderator)
Event MC and Broadcast Journalist

Johan Gerber
Executive Vice President, Global Head of Security Solutions, Mastercard

Jacky Fox
Senior Managing Director and EMEA Security Lead, Accenture

Dr. Yiannis Pavlosoglou
Vice Governor, National Cybersecurity Authority, Greece

Brigadier General Abdellah Boutrig
Director General, General Directorate of Information Systems Security (DGSSI), Morocco

Sub-Themes
Beyond the Inflection Point · Cyber Economics Redefined · Strengthening Cyber Inclusion · Behavioral Lens in Cyberspace · Opportunities at the Cyber Horizon

12:35 **Cyber Law:** Regulating the Next Tech Revolution

Jane Witherspoon (Moderator)
Managing Editor, Euronews

Dr. Igli Tafa
General Director, National Cyber Security Authority (AKSK), Albania

Dr. Yacine Djemaiel
CEO, National Agency for Cybersecurity (TunCERT), Tunisia

13:05 **Securing Investment:** Why Cybersecurity is a Key Imperative for FDI

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

Wael Fattouh
Chief Advisory Officer, SITE

Christopher Steed
Chief Investment Officer and Managing Director, Paladin Capital Group

Bocar A. Ba.
Chief Executive Officer, SAMENA Telecommunications Council

13:35 **Strength in Reinforcements:** Capacity Building in the Global South

Alexandra Topalian (Moderator)
International Presenter & Panel Moderator

Eng. Mohamed Ben Amor
Director General, Arab ICT Organization

Craig Jones
Member of the GFCE Foundation Board

Dr. Almerindo Graziano
CEO, Cyber Ranges

Sub-Themes Beyond the Inflection Point · Cyber Economics Redefined · Strengthening Cyber Inclusion · Behavioral Lens in Cyberspace · Opportunities at the Cyber Horizon

14:05 **Next-Gen Cyber Resilience:** Turning Tech Disruption into Security Innovation

Laura Buckwell (Moderator)
Event MC and Broadcast Journalist

Dr. Marcus Fowler
CEO, Dark Trace

Ultan Mulligan
Chief Standardization Officer, European Telecommunications Standards Institute (ETSI)

14:35 **The Psychology of Cyber Trust:** Leadership Strategies for Building Resilient Societies

Riz Khan (Moderator)
International Journalist and TV host Al Arabiya English

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

Odhran McCarthy
Programme Officer, United Nations Interregional Crime and Justice Research Institute (UNICRI)

15:05 **Funding the Future of Cyber:** Public-Private Investment Models for Scalable Growth

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

Norman Sadeh
Professor of Computer Science, Software and Societal Systems Department, Carnegie Mellon University (CMU)

Margarete Schramböck
Minister of Digital and Economic Affairs, Austria (2020 – 2022) Board Member, Aramco Digital

15:45 **Closing Ceremony**

Sub-Themes Beyond the Inflection Point · Cyber Economics Redefined · Strengthening Cyber Inclusion · Behavioral Lens in Cyberspace · Opportunities at the Cyber Horizon

PARTICIPATORY TRACK - OCTOBER 1ST, 2025 (DAY 1)

9:00 **Track 1.5 EU-GCC Cyber Dialogue -** Opening — ROOM F

11:00 **The Digital Emblem:** Protecting Critical Infrastructure in Cyberspace — ROOM C1

Rob van Dale
Moderator

Laurent Gisel
Head of the Arms and Conduct of Hostilities Unit, ICRC

11:00 **Cybersecurity Workforce Development** — ROOM C2

11:00 **Harms to Children from Online Gaming:** Understanding the Evidence and Exploring Solutions — ROOM C3

Srivatsan Raj
Senior Research Analyst, WeProtect Global Alliance

Dr. Iain Drennan
Executive Director, WeProtect Global Alliance

11:00 **Safeguarding Cyber Trust:** Dismantling Organized Criminals' Exploitation of the Internet — ROOM C4

11:40 **Houston, We Have a Problem:** Securing Space Assets — ROOM C1

Alexandra Topalian
Moderator

Mohammed Aljameele
Sanford School of Public Policy

James Pavur, PhD
Director - Cysec Labs, CysecSA

11:40 **CXO Roundtable** — ROOM F

12:00 **Sovereign Shield:** A Real World Simulation for Government Leaders — ROOM C2

12:00 **Bridging the Gender Gap in Cybersecurity:** Addressing Barriers and Expanding Workforce Participation — ROOM C3

Jay Bhatnagar
Moderator

Prof. David Hoffman
Steed Family Professor of the Practice of Cybersecurity Policy, Duke University

By Invite Only

12:00 **Gaming for Safety:** Protecting Children from Cyber Risks — ROOM C4

12:10 **The AI Advantage:** Transforming Cyber Defense at Scale — ROOM C1

Alberto Pardo
Moderator

Rohit Unnikrishnan
VP - Product Management, Network & Email Security Business, Trellix

12:40 **The UN Convention Against Cybercrime** — ROOM C3

Sanidhya Jain
Moderator

Nguyen Dinh Do Thi
Deputy Chief of Information Security Division under the Department of Cybersecurity and High-Tech Crime Prevention Ministry of Public Security, Vietnam

Mustafa Ünal Erten
Chief of the Regional Center for Combating Cybercrime, UNODC

12:50 **The AI Security Challenge:** Building a Resilient Infrastructure for Tomorrow's Threats — ROOM C1

Rob van Dale
Moderator

Lothar Renner
Managing Director of Security Sales and Engineering, Cisco

13:10 **Securing the Future Skies -** Knowledge Community Meeting — ROOM C4

13:15 **Quantifying the Economic Impact of Cyber incidents** — ROOM C2

13:20 **Cyber Immunity:** Strengthening Cyber Resilience for Global Health Systems — ROOM C1

Alexandra Topalian
Moderator

Prof. Richard Staynings
Professor of Cybersecurity, University of Denver

Prof. Attila J. Hertelendy
Assistant Professor, Department of Information Systems and Business Analytics, Florida International University

13:20 **CyberSafe Futures:** Parenting to Protect our Children in a Digital Age — ROOM C3

Dr. Afrooz Kaviani Johnson
Child Protection Specialist, UNICEF

13:30 **High-Level Roundtable on Women Empowerment in Cybersecurity** — ROOM F

13:45 **Track 1.5 EU-GCC Cyber Dialogue** — ROOM C4

13:50 **AI Driven Cyberattacks and Defenses** — ROOM C1

Ramia Farrage
Moderator

Fahad AlSamari
General Manager of Managed Detection and Response (MDR), Sirar by stc

13:50 **Cyber Frontiers:** Deepening Public–Private Collaboration for a More Resilient Future — ROOM C3

Alberto Pardo
Moderator

Britta Glade
Senior Vice President for Content & Communities, RSA Conference

14:00 **Measuring Cyber Resilience:** From Insight to Action — ROOM C2

14:20 **Cybersecurity at Scale:** Building Resilience for a Hyperconnected World — ROOM C1

Ryan Chilcote
Moderator

Alain Sanchez
EMEA CISO, Fortinet

14:25 **From Armor to Algorithms:** Protecting the Modern Defense Ecosystem Resilience — ROOM C3

Alexandra Topalian
Moderator

Oliver Waghorn
Business Development and Strategy Director, BAE Systems

Rahul Anand
Partner, Kearney

Usman Choudhary
General Manager, VIPRE Security Group

15:00 **The Cyber Risk Equation:** Enabling Security and Readiness Through Cyber Risk Assessment — ROOM C3

Elias Aad
Moderator

Charlie Sammut
Deputy Director Assessment, NCSC UK

Saâd Elkhadiri
Director General, Directorate of Information Systems Security (DGSSI), Morocco

15:15 **Centre for Cyber Economics -** Executive Committee Meeting — ROOM C4

15:30 **The Next Frontier of Cyber Risk:** Integrating Technology, Policy and Resilience — ROOM C3

Matteo Coppola
Moderator

Frank Van Caenegem
VP for Cybersecurity and CISO - EMEA, Schneider Electric

Prof. Norman Sadeh
Professor in the School of Computer Science, Carnegie Mellon University (CMU)

15:45 **The Future of Cyber Diplomacy:** Key Forces of Change and Strategic Outlook — ROOM C2

16:00 **Securing Tomorrow's Power:** An Energy Leadership Dialogue — ROOM C4

16:10 **The Evolving Dynamics of OT Cybersecurity** — ROOM C1

Dr. Saad Alaboodi
Chief Executive Officer, Saudi Information Technology Company (SITE)

Rob Lee
Chief Executive Officer, Dragos

16:30 **Track 1.5 EU-GCC Cyber Dialogue** — ROOM C4

17:00 **Arab CxO** — ROOM F

By Invite Only

PARTICIPATORY TRACK - OCTOBER 2ND, 2025 (DAY 2)

9:00 **Women in Cyber Breakfast** ROOM C

9:30 **Track 1.5 EU-GCC Cyber Dialogue** ROOM C4

10:00 **Closing the Gap:** Approaches Towards Cyber Equity - Community Meeting ROOM C2

10:15 **Quantum Safe:** Accelerating the Enterprise Roadmap for Resilience in the Quantum Era ROOM C1

Laura Buckwell
Moderator

Michael Osborne
CTO for Quantum Safe, IBM

10:15 **Governing Cyberspace:** Understanding the Applicability of International Law ROOM C3

Mauricio Zuazua
Moderator

Andraz Kastelic
Security and Technology Programme, United Nations Institute for Disarmament Research (UNIDIR)

10:55 **From Cloud to Edge:** Building a Borderless Security Future ROOM C1

Nisha Pillai
Moderator

Haider Pasha
Chief Security Officer EMEA, Palo Alto Networks

11:00 **Safeguarding Future Networks & Emerging Tech Knowledge Community Meeting** ROOM C4

11:00 **National Cyber Leadership High-Level Roundtable** ROOM F

11:15 **Impact Network Protection of Critical Infrastructure** ROOM C2

11:15 **Cybersecurity Economics for Emerging Markets** ROOM C3

Jan Grasshoff
Moderator

Dr. Estefania Vergara Cobos
Economist, World Bank

By Invite Only

11:35 **CyberSafe Futures:** The Evolving Role of Child Helplines to Protect Children in Cyberspace ROOM C1

Dr. Afrooz Kaviani Johnson
Moderator

Helen Mason
Executive Director, Child Helpline International

Michael Marwa
Director, The Tanzanian National Child Helpline

12:00 **Securing Prosperity:** Building Trustworthy AI Innovations ROOM C3

Rob van Dale
Moderator

Srinivas Tummalapenta
CTO, Security Services, IBM

Anand Kashyap
CEO, Fortanix

12:05 **Power Up:** Empowering Cyber Women Leaders ROOM C1

Jim O'Connor
Moderator

Judith Ann Sarjeant
Senior Manager - Cloud Security, CIBC Caribbean

Yemurai Rabvukwa
WAF and DDOS Analyst, Cyber Careers Content Creator

Vesna Gabric Kesina
Senior Legal Advisor, Croatian Regulatory Authority for Network Industries (HAKOM)

Frida Inchoga
Senior Manager, Digital Commerce and Industrial Policy, Tony Blair Institute for Global Change

12:30 **The Quantum Leap:** Navigating the Future of Computing ROOM C2

12:30 **OTC COE Members Meeting** ROOM F

12:40 **The Convergence Effect:** The Future of Cyber Threats in an Age of Emerging Tech ROOM C1

Nisha Pillai
Moderator

George Patsis
CEO, Obrela

Rashed Alharbi
VP, Cybersecurity Products, SITE

Prof. Nicolas Christin
Faculty member, CyLab Professor, Carnegie Mellon University

12:45 **Rebalancing Cybersecurity at Hyper Scale:** Cybersecurity Standardization, the Hidden Growing Force — ROOM C3

Lukas de Sonnaville
Moderator

Arnaud Taddei
Chair, Study Group 17, Telecommunication Standardization Sector, ITU

12:45 **Safer Play:** Evidence-Based Solutions for Protecting Children from Online Gaming Harms — ROOM C4

13:15 **The Future of OT Cybersecurity:** Building Resilience for the Industries and Infrastructures — ROOM C1

Radu Balanescu
Moderator

Abdullah Aljallal
Sr. Commercial Director, Cyberani

13:15 **The Macroeconomic Impact of Cybersecurity -** Community Meeting — ROOM C2

13:15 **The Future Formula:** Women Shaping Tomorrow's Tech Frontier — ROOM C3

Salma Al-Rashid
Moderator

Carmen Marsh
President and CEO, United Cybersecurity Alliance and Global Council for Responsible AI

Silvana Koch-Mehrin
Founder and President, Women Political Leaders (WPL)

14:00 **Clicks, and Links, and URLs—Oh My! How Organized Crime Exploits the Web** — ROOM C3

Ottavia Galuzzi
Associate Expert, United Nations Interregional Crime and Justice Research Institute (UNICRI)

Odhran McCarthy
Liaison Officer, United Nations Interregional Crime and Justice Research Institute (UNICRI)

Janey Young
Consultant, United Nations Interregional Crime and Justice Research Institute (UNICRI)

14:00 **Future of Cybersecurity -** Knowledge Community Meeting — ROOM C4

14:15 **From Data to Action:** Launching the Child Protection in Cyberspace Index — ROOM C1

Nisha Pillai
Moderator

Dr. Yuhyun Park
Founder and CEO, DQ Institute

14:30 **Enterprise Compass:** Cyber Resilience and Preparedness Simulation for Business Leaders — ROOM C2

14:30 **The Cyber Effect:** Understanding Technology's Impact on Human Behavior — ROOM C3

Alexandra Topalian
Moderator

Nirali Bhatia
Cyber Psychologist & Psychotherapist. Founder Director, Nirali Bhatia Cyber Wellness Foundation

Sonali Patankar
Founder & CEO, Responsible Netism

14:30 **High Level Multi-Stakeholder Roundtable on Capacity Building** — ROOM F

15:15 **Advancing Responsible State Behavior in Cyberspace** — ROOM C3

Virginia Browning
Programme Management Officer, UN Office for Disarmament Affairs

15:45 **Track 1.5 EU-GCC Cyber Dialogue -** Closing Meeting — ROOM F

By Invite Only

OPEN FORUM

Plenary Session | **Beyond the Inflection Point**

OPEN FORUM

AGAINST THE ODDS

Gaining Consensus Amid Complexity

- **H.E. Kolinda Grabar-Kitarović,** President of Croatia (2015 – 2020)
- **H.E. Macky Sall,** President of Senegal (2012 – 2024)
- **Hon. Chris Inglis,** National Cyber Director, United States (2021 – 2023)
- **John Defterios (Moderator),** Former CNN Emerging Markets Editor & Anchor

The first open forum session of the GCF Annual meeting 2025 examined how international collaboration can endure in an era of intensifying geopolitical competition, technological advancements, growing economic and developmental uncertainty. Participants agreed that the cyber domain has become both the frontline and the primary testing ground for global cooperation: while threats multiply at unprecedented scale, shared interests in security, stability, and innovation continue to provide a solid foundation for collective action.

Discussions emphasized that durable progress would depend less on grand declarations and more on building trust through practical measures. These include joint cyber exercises, information sharing, and coordinated incident-response mechanisms that strengthen international cooperation. It was underscored that trust should be earned through tangible successes, agreements signed, improvements in cyber resilience achieved through collaboration.

The conversation further highlighted the growing growing disparities in cyber capabilities and resources. A persistent spending gap was described as both a moral and strategic vulnerability. Without targeted investment and accessible training, large segments of the global population remain exposed, with implications for global cybersecurity.

Participants observed that effective cooperation also requires re-imagining multilateralism. Instead of relying on rigid or ineffective treaties, a more agile model of "coalitions of capability" was proposed, referring to flexible partnerships that unite governments, private industry, academia, and civil society around shared objectives such as the protecting children online, safeguarding critical infrastructure, and governing emerging technologies.

The session concluded that cyber diplomacy should evolve toward practical, practical, outcome-driven results. The ultimate benchmark of success is not consensus for its own sake but tangible improvements improvement in cyber trust, resilience, and inclusiveness. Cohesion was framed not as uniformity but as the collective capacity to act decisively despite differing interests.

30$ per capita

Cybersecurity spending gap – around $30 per capita in advanced economies compared with less than $1 in many developing states in 2023

(Source: World Bank)

Scan the QR code to watch this session

SCAN HERE

Introductory Remarks | **Cyber Economics Redefined**

OPEN FORUM

THE ECONOMIC DIMENSION OF CYBERSPACE

- **Dr. Saad Alaboodi,** Chief Executive Officer, Saudi Information Technology Company (SITE)

This introductory keynote addressed the urgent need to redefine cybersecurity through an economic lens, positioning cyber resilience as a principal driver of growth, productivity, and global competitiveness. It was noted that the modern economy is now inseparable from Cyberspace: every transaction, supply chain, and innovation depends on secure cyber infrastructure. Yet, investment patterns continue to reflect a narrow view of cybersecurity as a cost rather than as a means to safeguard value.

Dr. Alaboodi stressed that this perception should change. According to Gartner, global spending on information and communications technology (ICT) is expected to reach USD 5.6 trillion in 2025, yet only 4% of this (approximately USD 213 billion) is allocated to cybersecurity. This imbalance represents a systemic protection deficit that already translates into global losses exceeding USD 10 trillion annually (eSentire). He also highlighted that bridging this gap is an economic imperative, as cyber incidents now ripple across markets, disrupt supply chains, and erode investor confidence.

$5.6T Global ICT investment is projected at $5.6 trillion in 2025, yet only $213 billion (≈ 4%) will be devoted to cybersecurity, illustrating the global protection gap

(Source: Gartner)

Dr. Alaboodi also discussed how artificial intelligence is redefining the economics of risk. As a productivity catalyst, AI multiplies efficiencies across industries, yet it simultaneously accelerates the sophistication and frequency of attacks. The introductory remarks underscored that quantifying cybersecurity's economic contribution should become central to policymaking. Measuring not only direct spending but also the avoided cost of disruption would enable governments and enterprises to recognize cybersecurity as a strategic investment yielding macro-economic returns.

The establishment of the Centre for Cyber Economics (CCE), a partnership between GCF and the World Economic Forum (WEF), was cited as a crucial step. CCE will develop models to evaluate how security expenditure influences GDP growth, innovation cycles, and employment, providing data-driven guidance for fiscal and industrial planning.

In conclusion, cybersecurity is no longer peripheral; it is infrastructure, a precondition for trust, trade, and sustainable development. Redefining cyber economics is therefore a roadmap for inclusive and secure prosperity.

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Cyber Economics Redefined**

OPEN FORUM

CYBERSECURITY AS AN ECONOMIC IMPERATIVE

Driving Growth in the Global Economy

- **Florian Schütz,** Director, Federal Office for Cyber Security, Switzerland
- **Heidi Crebo-Rediker,** Senior Fellow for Geoeconomics, Council on Foreign Relations
- **Dr. Stéphane Straub,** Chief Economist for Infrastructure, World Bank
- **Akshay Joshi,** Head of Centre for Cybersecurity, World Economic Forum
- **Nisha Pillai (Moderator),** International Moderator and Journalist

The discussion examined how cybersecurity readiness functions as a macroeconomic determinant, shaping growth trajectories, productivity, investment confidence, and financial stability. Participants agreed that resilience is best understood as a public good, since market incentives alone do not yield optimal levels of protection across interconnected supply chains and critical infrastructure. It was emphasized that underinvestment in cyber capabilities suppresses development in cyber-dependent sectors, with utilities, manufacturing, logistics, and extractive industries cited as particularly sensitive to weak preparedness.

A central theme was the need to move beyond treating cybersecurity as a narrow technical cost. The exchange highlighted the case for integrating cyber risk into national economic planning, fiscal policy, and disaster preparedness frameworks, with avoided loss recognized as measurable economic gain. Financial system exposure received particular attention, with the transmission of cyber shocks through payments, credit, and market plumbing identified as a channel that can amplify localized events into systemic risk. However, participants noted that cumulative, lower-visibility incidents erode small and medium-sized enterprise continuity, producing economy-wide drag that rarely appears in headline statistics.

The conversation underscored that public policy should blend proportionate regulation with practical collaboration. Examples discussed included sector hubs that share data, exercise together, and integrate industry into government crisis processes, improving transparency on risk and aligning actions before incidents escalate. At the same time, incentives should be clarified so that public and private actors can co-invest in resilience with predictable returns, rather than relying on ad hoc interventions after severe disruptions.

Artificial intelligence was framed as both a productivity catalyst and a risk accelerant. Participants stressed that a macroeconomic framework for cybersecurity should capture two sides of the ledger, the value created by secure digital adoption and the value preserved by preventing disruptions. The session concluded that reframing cybersecurity as a core pillar of prosperity, alongside infrastructure and education, is essential to unlock growth, jobs, and innovation while containing systemic risk.

1.5% Improving national cybersecurity preparedness from the lowest quintile to the highest quartile can increase GDP per capita by about 1.5%

(Source: World Bank)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Cyber Economics Redefined**

OPEN FORUM

SHAPING RESILIENCE

Investing in Women as a Global Economic Imperative

- **H.E. Dr. Hala Bint Mazyad Altuwaijri,** President, Human Rights Commission of Saudi Arabia
- **Sarah E. Hendriks,** Deputy Executive Director, UN Women
- **Jim O'Connor,** Chairman and CEO, United States Telecommunications Training Institute (USTTI)
- **Rebecca McLaughlin-Eastham (Moderator),** Independent TV Anchor and CEO, RME Media

The session examined the strategic and economic importance of women's participation in cybersecurity, positioning inclusion as a cornerstone of national resilience and sustainable growth. Participants agreed that increasing women's leadership and workforce representation strengthens innovation, alleviates talent shortages, and enhances the agility of organizations navigating complex and evolving threats.

Inclusion, it was emphasized, should be treated not as a symbolic gesture but as a core economic priority. Expanding women's share of the cybersecurity workforce improves risk detection, policy diversity, and institutional resilience. Although women only currently occupy about a quarter of roles in the sector, steady progress was noted, supported by targeted education pathways, coordinated recruitment and retention strategies, and structured mentorship programs.

Equitable policy frameworks were identified as essential to sustaining these gains. Governments were urged to set measurable national objectives for women's empowerment, prohibit discriminatory practices, and establish mechanisms that hold leadership accountable for diversity outcomes. Participants noted that recruitment remains a persistent weak link, often constrained by implicit bias. Human-resource reforms promoting transparency, equal pay, and safe workplace cultures were presented as indispensable for retention and advancement.

Training and capability building were highlighted as the foundation for durable change. Initiatives that connect academic study with industry practice, particularly those supporting women in emerging economies, were cited as powerful accelerators of inclusion. Effective collaboration among governments, academia, and the private sector was viewed as vital to ensuring equitable access to opportunity.

The discussion concluded that investing in women in cybersecurity is both a social and economic imperative. Countries that cultivate women's cyber skills demonstrate greater competitiveness, higher productivity, and stronger innovation capacity. Empowering women in this domain was described as an investment in collective resilience, with global cooperation essential to sustain the momentum and close remaining equity gaps.

24% Women now represent approximately 24% of the global cybersecurity workforce, up from 10% in 2012, illustrating measurable yet modest progress toward parity

(Source: GCF)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Opportunities at the Cyber Horizon**

OPEN FORUM

COLLABORATION FOR GROWTH

Building a Thriving and Innovative Security and Defense Ecosystem

- **Shaikh Salman bin Mohammed Al Khalifa,** Chief Executive Officer, National Cybersecurity Center, Kingdom of Bahrain
- **Dan Cîmpean,** Director, National Cyber Security Directorate, Romania
- **General (Rtd.) Jean-Paul Paloméros,** Supreme Allied Commander Transformation, NATO (2012–2015)
- **Lara Habib (Moderator),** Senior Business News Presenter, Al Arabiya

The session explored how collaboration across governments, industries, and defense alliances can accelerate innovation and resilience within the global cybersecurity and defense ecosystem. The discussion emphasized that modern security threats no longer exist within physical borders. With attacks now originating from code, algorithms, and artificial intelligence, collective action has become the defining condition of defense readiness.

Cyber threats today transcend borders and sectors, creating shared vulnerabilities that demand unified responses. Panelists agreed that modern defense readiness relies as much on partnerships as on technology, with cross-border collaboration, information sharing, and joint training exercises emerging as key levers of resilience. Examples cited included GCC regional coordination mechanisms and NATO-inspired models that have accelerated maturity among national cybersecurity authorities. Participants stressed that in an interconnected threat landscape, an attack on one actor can rapidly cascade across systems and economies, underscoring the need for common defense frameworks and trusted operational networks.

The conversation also underscored that cyber defense has become inseparable from technological innovation. Artificial intelligence was identified as both a force and vulnerability multiplier. Panelists cautioned that while AI enhances analytical capacity and operational efficiency, it also lowers the cost and increases the frequency of cyberattacks. This dual reality requires global cooperation to establish ethical and technical guardrails while promoting innovation.

Long-term resilience, the panel concluded, will depend on continuous investment in joint simulations, advanced research, and workforce development. Integrating public and private sectors into unified crisis management systems was seen as essential for aligning governance standards and enabling coordinated responses.

Ultimately, the panel emphasized that collaboration in cybersecurity and defense is not a diplomatic aspiration but a strategic necessity. Sustainable security will rely on shared trust, collective situational awareness, and a culture of innovation that allows knowledge and readiness to circulate freely across borders.

Faster The cost of launching a cyberattack continues to decline, making such operations cheaper, faster, and more accessible to non-state actors, thereby increasing global exposure to cyber threats

(Source: ClearSale)

Scan the QR code to watch this session

SCAN HERE

Fireside Chat | **Cyber Economics Redefined**

OPEN FORUM

POWERING TOMORROW

The Economic Imperative for Securing the Global Energy Supply Chain

- **Ahmad Al-Khowaiter,** Executive Vice President of Technology and Innovation, Aramco
- **John Defterios (Moderator),** Former CNN Emerging Markets Editor and Anchor

The session examined cybersecurity as an essential dimension of global energy security and economic continuity. The discussion underscored that energy systems have become a prime target for sophisticated cyberattacks, with one in ten incidents worldwide now directed at the energy sector. Participants highlighted that the stability of energy supply chains, digital transformation of production systems, and integration of artificial intelligence are reshaping the security landscape at a rapid pace.

It was emphasized that cybersecurity in the energy industry has evolved from a discrete layer of protection to an integrated operational requirement. Every aspect of energy generation, distribution, and innovation now depends on embedded cyber safeguards. The conversation illustrated that modern energy companies treat cybersecurity as a foundational element of business continuity and safety, rather than a separate compliance function.

Artificial intelligence was described as both a growth and vulnerability a source of vulnerabilities. Predictive maintenance, automated monitoring, and optimized energy flows have enhanced performance and sustainability. Yet the same technologies introduce vulnerabilities through data manipulation, compromised algorithms, and malicious code injection. The importance of securing every layer of the AI supply chain was emphasized: from data collection and model training to system deployment.

The dialogue also addressed the crucial role of public–private collaboration in maintaining resilience. The Saudi National Cybersecurity Authority's model of real-time incident reporting and coordinated response was cited as an example of how national frameworks can serve as a global reference for rapid containment and collective defense.

In conclusion, cybersecurity emerged as the defining frontier of global energy reliability. Its effectiveness now determines not only the safety of critical infrastructure but also the competitiveness of national economies. The discussion underscored that sustained investment in skilled talent, the advancement of forward-looking regulation, and the strengthening of strategic partnerships are essential to ensure that digital transformation enhances the stability and sustainability of the global energy system.

1 in 10 Approximately one in ten cyberattacks worldwide targets the energy sector, confirming the industry's position as one of the most exposed to cyber threats

(Source: GCF)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Opportunities at the Cyber Horizon**

OPEN FORUM

AI FOR SECURITY AND SECURITY FOR AI

Ensuring Resilience and Building Trust

- **Rob Duhart,** Chief Security Officer, Oracle
- **Dr. Bilel Jamoussi,** Deputy Director, Telecommunication Standardization Bureau, ITU
- **Bob Willen,** Global Managing Partner and Chairman of the Board, Kearney
- **Ramia Farrage (Moderator),** Senior Presenter and Producer, Forbes Middle East

The panel examined the interplay between artificial intelligence and cybersecurity, exploring how AI serves as both a catalyst for stronger defenses and a source of new vulnerabilities. The conversation reflected on how the rapid expansion of AI across critical sectors is transforming cybersecurity from a technical discipline into a matter of governance, accountability, and trust.

Participants agreed that the challenge of securing AI systems lies not only in protecting networks and infrastructure but also in ensuring the integrity of data, models, and algorithms. Adversarial AI was described as a rising threat capable of manipulating inputs or altering model behavior to produce misleading outcomes. Addressing these risks requires a new generation of interdisciplinary expertise that combines cybersecurity, data science, and ethical governance. Despite progress, it was observed that many organizations remain underprepared to manage these emerging challenges effectively.

The discussion highlighted that responsible AI deployment should be matched with strong governance and transparency mechanisms. International standards and proportionate regulatory frameworks were recognized as

essential tools for building trust without stifling innovation. Participants emphasized the importance of establishing shared global principles and fostering cooperation among governments, the private sector, academia, and civil society. Such collaboration is crucial to reducing bias, ensuring equitable data representation, and enabling developing economies to contribute meaningfully to global AI governance.

At the organizational level, companies were encouraged to treat AI workloads as critical infrastructure, integrating security into every stage of model design, deployment, and monitoring. Participants noted that the private sector should demonstrate leadership through voluntary transparency, cross-functional governance, and common assurance frameworks that make AI systems secure by design.

The session concluded that the future of AI resilience depends on viewing cybersecurity and AI as mutually reinforcing disciplines. Innovation and protection should evolve together, guided by shared international standards and proactive risk management to ensure that AI remains a trusted enabler of progress rather than a source of systemic vulnerability.

2% Only 2% of firms report that they are ready for AI adoption, highlighting a significant global readiness gap

(Source: World Economic Forum)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Opportunities at the Cyber Horizon**

OPEN FORUM

THE Q CYBER FRONTIER

Harnessing Quantum Innovation for Cyber Resilience

- **Mark Hughes,** Global Managing Partner, Consulting Cybersecurity Services, IBM
- **Jin Young Oh,** Vice President, Korea Internet & Security Agency (KISA)
- **Arnaud Taddei,** Chair, Study Group 17, Telecommunication Standardization Sector, ITU
- **David Panhans,** Managing Director & Senior Partner, Boston Consulting Group (BCG)
- **Ryan Chilcote (Moderator),** International Broadcaster and Journalist

The discussion addressed the implications of quantum computing for global cybersecurity, emphasizing the urgent need to prepare for an era when quantum capability will render current encryption systems obsolete. What was once a theoretical issue has evolved into an emerging commercial reality, capable of reshaping cybersecurity frameworks and redefining how data is protected, transmitted, and trusted across borders.

Panelists observed that quantum computing introduces a new class of threats that could overturn the foundations of modern cryptography. Algorithms such as Shor's, which can factorize encryption keys exponentially faster than classical computers, pose a risk to current asymmetric encryption models. This capability could enable "harvest now, decrypt later" strategies, where adversaries collect encrypted data today in anticipation of decrypting it once quantum computing reaches maturity. Experts cautioned that this scenario could become viable by 2030, reinforcing the need for early adoption of post-quantum cryptography (PQC) and a coordinated transition plan.

Preparing for the quantum era requires systematic action. Governments, enterprises, and other critical institutions should begin mapping cryptographic assets, assessing vulnerabilities, and initiating migration to quantum-resistant algorithms. The development of cryptographic bills of materials was recommended to identify encryption dependencies, while hybrid approaches combining classical and quantum-safe methods were presented as practical interim solutions. Cross-border collaboration will be essential to ensure interoperability and consistency across sectors.

Standardization was recognized as a decisive enabler of readiness. International organizations, including the International Telecommunication Union (ITU), National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO), were encouraged to align standards and accelerate the development of frameworks that facilitate global adoption. Participants acknowledged that the absence of prescriptive guidance and the complexity of legacy systems remain significant obstacles.

The discussion concluded that securing the quantum future demands collective commitment to research, standardization, and talent development. As no single nation or entity can address this challenge alone, sustained international cooperation will determine whether quantum technology becomes a force for resilience and innovation or a catalyst for systemic vulnerability in the global cyber order.

2029 Quantum-enabled decryption of today's encryption algorithms could become feasible as early as 2029–2030, underscoring the urgency of migrating to post-quantum cryptographic standards

(Source: NIST)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Beyond the Inflection Point**

OPEN FORUM

DEFENDING THE GRID

Uniting Forces to Protect Critical Infrastructure

- **Hosam A. Alsuliman,** Policies & Regulations Deputy Governor, National Cybersecurity Authority, Saudi Arabia
- **Miguel Ángel Cañada,** Head of Cabinet and National Coordination Center, Spanish National Cybersecurity Institute (INCIBE)
- **Rohit Unnikrishnan,** Senior Vice President of Product Management, Trellix
- **Lara Habib (Moderator),** Senior Business News Presenter, Al Arabiya

The panel examined how governments, regulators, and the private sector are strengthening collaboration to safeguard the world's most vital infrastructure in the face of escalating global cyberattacks. As digitalization accelerates across critical sectors, the discussion highlighted the essential systems – energy, transport, healthcare, and finance – that are facing unprecedented exposure. More than 420 million cyber-attacks were recorded within a single year in 2023, underscoring that resilience can no longer rely on technology alone but should be built on governance, coordination, and shared intelligence.

Speakers underlined that the interdependence of modern infrastructure makes isolated approaches obsolete. A single vulnerability in one sector or supplier can create cascading effects across others. Examples given included attacks on transport networks and industrial systems, where small disruptions triggered continent-wide consequences. Participants highlighted the need to integrate industrial and operational technology security with IT security to ensure comprehensive resilience.

The dialogue stressed that effective protection depends on collaboration at every level. National frameworks such as the Saudi Model, which is based on the centralization of cybersecurity governance at the national level, while allowing for the decentralization of on-premises operations, which remain the responsibility of national entities. Regional initiatives within the GCC and the Arab League were also noted for fostering intelligence sharing, joint exercises, and alignment with international partners. These partnerships strengthen collective awareness and allow rapid coordinated responses to threats. Participants warned that the use of artificial intelligence by attackers is transforming the threat landscape. Automated reconnaissance and precision targeting have lowered the barriers to entry for cybercriminals and state-sponsored actors. To counter this, governments and enterprises were urged to invest in defensive AI, continuous monitoring, and resilient recovery frameworks that minimize downtime after incidents.

The discussion concluded that the future of critical infrastructure protection will hinge on three factors: continuous investment in cyber defense in response to emerging technologies, coordinated multi-stakeholder cooperation, and a culture of readiness. Participants emphasized that no system can be entirely immune, but robust recovery mechanisms and transparent collaboration can ensure that essential services remain operational even under persistent attack.

30/sec Between January 2023 and January 2024, more than 420 million cyber-attacks targeted critical infrastructure worldwide, an average of 30 attacks per second

(Source: KnowBe4)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Beyond the Inflection Point**

OPEN FORUM

REINFORCING THE LINKS

Securing Global Energy Supply Chains

- **Robert M. Lee,** Chief Executive Officer and Co-Founder, Dragos Inc.
- **Saeed AlSaeed,** Chief Executive Officer, Cyberani
- **Chase Carpenter,** Chief Security Officer, Honeywell
- **Nisha Pillai (Moderator),** International Moderator and Journalist

The session focused on the intersection of cybersecurity, operational technology, and energy supply chains, emphasizing that the global energy sector has become one of the most targeted and interconnected domains in recent years. Participants agreed that cyber resilience should now be treated as an intrinsic part of industrial design, not a layer added after deployment. The panel explored how emerging technologies, particularly artificial intelligence and cloud-based systems, are reshaping security strategies while simultaneously introducing new vulnerabilities.

Panelists noted that attacks on operational technology (OT) have risen sharply, with a 146% increase recorded in 2024. Where industrial systems were once protected by isolation, today's energy infrastructure relies on interconnected digital networks, remote maintenance systems, and real-time data analytics. This high degree of integration has blurred the boundaries between information technology and operational technology, exposing critical systems to a vastly expanded attack surface.

Participants highlighted that collaboration between governments, technology providers, and energy producers is vital to mitigate systemic risk. The discussion underscored the importance of security "by design," ensuring that industrial systems and hardware are built with embedded safeguards and supported by continuous monitoring. The concept of defense in depth,

meaning multiple layers of security controls that delay attackers and provide time for response, was presented as an operational standard for modern energy infrastructure.

The conversation also explored how artificial intelligence is transforming both attack and defense. AI tools now enable automated reconnaissance and targeted exploitation, but they also empower defenders to detect anomalies faster and manage incident response at scale. Participants noted that organizations deploying AI should implement rigorous testing, penetration audits, and responsible governance frameworks to prevent unintended vulnerabilities.

146% Cyberattacks targeting operational technology environments increased by 146% in the first half of the year, reflecting the expanding vulnerability of interconnected energy systems

(Source: Cybervizer)

The session concluded that protecting global energy supply chains demands a holistic approach integrating secure design, regulatory alignment, and long-term partnerships. As technology evolves, the sector should strengthen resilience through standardization, proactive collaboration, and investment in human expertise. Participants cautioned that while innovation fuels growth, it should advance in tandem with trust and security, ensuring that the energy systems powering the world remain stable, reliable, and secure.

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Behavioral Lens in Cyberspace**

OPEN FORUM

THE HIDDEN WEB

Inside the Tactics of Link-Based Crime Networks

- **Dr. Neal Jettton,** Director, Cybercrime, INTERPOL
- **Christopher Porter,** Head of International Security Cooperation, Google Cloud
- **Prof. Marco Gercke,** Director, Cybercrime Research Institute
- **Eric Skinner,** Vice President, Market Strategy, Trend Micro
- **Sarah Al-Khaldi (Moderator),** Business News Anchor, Channel News Asia (CNA)

The panel explored increasingly sophisticated link-based cybercrime networks and their growing impact on global security and digital trust. Described by participants as the "highways of cybercrime," these networks enable the rapid exchange of data, illicit goods, and malicious code through interconnected servers and online platforms that are difficult to trace, disrupt, or dismantle. The discussion underscored that cybercriminals exploit the same attributes that drive globalization (i.e., borderless reach, distributed infrastructure, and rapid innovation) allowing them to operate across jurisdictions with unprecedented agility.

Law enforcement experts noted that dismantling such networks requires international cooperation, real-time intelligence sharing, and the involvement of private sector partners who possess the necessary data visibility. The collaboration between global technology firms and institutions like INTERPOL was highlighted as a model for operational success, with shared threat intelligence playing a decisive role in several cross-border investigations.

Panelists observed that artificial intelligence is amplifying both the scale and speed of cybercrime. AI enables attackers to automate coding, rotate domains, and adapt networks of malicious links and domains faster than traditional defenses can respond. Criminal groups use AI to enhance phishing campaigns, impersonate victims, and manage operations as efficiently as legitimate enterprises. To counter these threats, experts called for a shift from static defenses toward behavioral detection and zero-trust frameworks, which can identify abnormal patterns even when attackers continuously change infrastructure.

The conversation also highlighted the need for harmonized legislation and common international standards for cybercrime prosecution. While technology evolves at unprecedented speed, laws remain largely national and fragmented. Participants urged governments to close this gap through legal harmonization, information-sharing treaties, and capacity-building programs for under-resourced nations.

Looking ahead, panelists warned that agentic AI could define the next frontier of cybercrime. The rise of AI-generated malware, quantum-enabled decryption, and synthetic digital identities were identified as emerging threats that demand urgent, coordinated global action. Yet, the conversation concluded on a note of guarded optimism: with sustained innovation, agile governance, and public–private collaboration, collective resilience can still outpace even the most adaptive adversaries.

60% Over 60% of the world's population now owns a mobile phone, giving cybercriminals a near-universal channel to target victims with link-based scams and phishing attacks

(Source: Bankmycell)

Scan the QR code to watch this session

SCAN HERE

Fireside Chat | **Opportunities at the Cyber Horizon**

OPEN FORUM

SECURING PROSPERITY

AI Preparedness in a Connected World

- **Doreen Bogdan-Martin,** Secretary-General, International Telecommunication Union (ITU)
- **Ryan Chilcote (Moderator),** International Broadcaster and Journalist

This fireside chat explored how artificial intelligence can serve as a catalyst for inclusive and sustainable prosperity. The discussion emphasized that AI preparedness is not solely a technological undertaking but also a strategic priority that links innovation to development, trust, and resilience in the digital age.

Central to the conversation was the role of international standards in building interoperability and transparency in AI systems. The ITU's collaboration with ISO and IEC on multimedia authenticity and deepfake detection was presented as a tangible example of how standards can help mitigate the misuse of digital content. Similarly, the Common Alerting Protocol (CAP X1303) was highlighted as a model for how shared frameworks enable early warning systems across devices and networks. When combined with AI-driven disaster prediction tools, such standards demonstrate how technology can save lives while enhancing public trust in Cyberspace.

The conversation also examined the human dimension of AI preparedness. The ITU estimates that while AI could displace approximately 92 million jobs globally by 2030, it also has the potential to create 170 million new ones. Investments in relevant skills, education, and capacity building were identified as the cornerstone of an equitable digital transition.

The AI Skills Coalition, targeting learners from primary school to university, was cited as a flagship initiative to expand access to digital literacy and upskilling opportunities, especially in developing regions.

The discussion concluded by reaffirming that closing the global connectivity and compute gap is a prerequisite for inclusive AI: 2.6 billion people remain offline, and more than 150 countries do not have access to access to high-performance AI compute at meaningful scale. Ensuring access, affordability, and accountability in technology adoption will determine whether AI becomes a driver of inequality or a foundation for shared global prosperity.

2.6B

Globally, an estimated 2.6 billion people remain offline, and over 150 countries lack access to AI compute, representing the most significant barrier to inclusive AI adoption

(Source: ITU, SSRN)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Cyber Economics Redefined**

OPEN FORUM

FROM GAPS TO GAINS

Scaling Global Cyber Capability Development Through Collective Action

- **Chris Gibson,** Chief Executive Officer and Executive Director, Forum of Incident Response and Security Teams (FIRST)
- **Professor William H. Dutton,** Oxford Martin Fellow, Global Cybersecurity Capacity Centre, University of Oxford
- **Ahmed Almalki,** Chief Information Security Officer, SABIC
- **Ramia Farrage (Moderator),** Senior Presenter and Producer, Forbes Middle East

The panel explored how persistent disparities in global cybersecurity capability continue to heighten systemic risk and examined practical pathways to overcome these vulnerabilities. Participants emphasized that addressing these gaps requires a comprehensive approach that integrates infrastructure modernization, legal coordination, and long-term skills development.

The panel highlighted that many industrial sectors, especially petrochemicals and critical infrastructure, are constrained by legacy systems designed decades ago without cybersecurity considerations. Bridging this gap demands large-scale investment in modernization and workforce training, particularly in operational technology security and industrial internet of things (IIoT) integration.

The discussion highlighted that jurisdictional and legal fragmentation remains a major barrier to effective international response. Without harmonized frameworks, cross-border cooperation is slow, limiting timely mitigation of cyber incidents.

Developing economies were identified as disproportionately affected by limited cyber capacity and workforce shortages. The panel called for regional cooperation models that pool expertise and resources, emphasizing the role of regional partnerships, mentorship networks, and centers of excellence in transferring knowledge and strengthening institutional maturity.

Beyond technical measures, participants described resilience as a mindset requiring collective awareness and proactive leadership. Governments and enterprises were encouraged to conduct regular crisis simulations, integrate cyber resilience into governance and business continuity frameworks.

The discussion concluded that closing the global cyber capability gap requires political will, shared accountability, and sustained investment. Participants agreed that cybersecurity should be reframed as an ecosystem of trust, aligning governments, academia, and industry around a collective mission to secure progress and transform risk into opportunity.

76

A single malware attack on a global logistics company disrupted 76 ports and over seven million containers within minutes, demonstrating the economic cost of weak cyber coordination

(Source: Wired)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Beyond the Inflection Point**

OPEN FORUM

CONVERGING CRISIS

The Future of Cyberspace in Complex Global Dynamics

- **Jürgen Stock,** Secretary General (2014 – 2024), INTERPOL
- **Dr. Robin Geiss,** Director, United Nations Institute for Disarmament Research (UNIDIR)
- **Robert Hannigan,** Director, GCHQ, United Kingdom (2014 – 2017)
- **H.E. José Manuel Barroso,** President of the European Commission (2004 – 2014)
- **John Defterios (Moderator),** Former Emerging Markets Editor and Anchor, CNN

The session explored how cybersecurity has become the defining challenge of an interconnected world in which technology, geopolitics, and economics increasingly converge. Panelists noted that the boundaries between physical and cyber conflict are dissolving, with cyber operations now intertwined with global security, economic stability, and societal trust. They cautioned that fragile supply chains, the evolution of organized cybercrime, and the erosion of trust between major powers have created vulnerabilities within the ecosystem. With over 80% of major cyberattacks in recent years linked to supply chains, participants emphasized that global interdependence has amplified systemic risk across every sector of the digital economy.

The conversation highlighted how emerging technologies such as artificial intelligence, quantum computing, and automation are transforming the scale, sophistication, and speed of cyber operations. However, technological progress continues to outpace policy, legislation, and enforcement. Drawing on lessons from the Russia–Ukraine conflict, panelists described how cyber warfare has become a central feature of modern defense, merging traditional military operations with digital infrastructure. Europe's shift toward

recognizing a state of "hybrid war" has catalyzed new commitments and revealed the urgency of strengthening resilience, information sharing, and regional preparedness.

Panelists argued that despite geopolitical divides, pragmatic cooperation through regional and multilateral frameworks remains indispensable. They highlighted successful examples, including the European Union's cybersecurity liability standards and Saudi Arabia's 24/7 cross-sector cyber-monitoring model, which were praised for fostering real-time coordination between government, industry, and critical infrastructure operators. These examples illustrated that effective cyber defense extends far beyond governments, demanding engagement from small enterprises, regulators, and civil society.

The session concluded with a call for agile global architectures for data exchange, capacity building, and security-by-design integration across all systems. The discussion reaffirmed that no nation or organization can address these challenges alone. Sustained leadership, transparency, and renewed multilateralism are imperative to prevent Cyberspace from becoming the next frontier of global conflict.

54% 54% of large organizations say supply-chain interdependencies are the biggest barrier to cyber resilience

(Source: World Economic Forum)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Behavioral Lens in Cyberspace**

OPEN FORUM

TRUST IN ACTION

Reimagining Citizen Services in a Cyber-First World

- **H.H. Prince Dr. Bandar bin Abdullah bin Mishari,** Assistant Minister of Interior for Technology Affairs, Saudi Arabia
- **H.E. Shaza Fatima Khawaja,** Minister of State, Ministry of Information Technology and Telecommunication, Pakistan
- **Ir. Dr Megat Zuhairy bin Megat Tajuddin,** Chief Executive, National Cyber Security Agency (NACSA), Malaysia
- **Riz Khan (Moderator),** International Journalist and TV Host, Al Arabiya English

The session examined how governments worldwide are working to embed trust, transparency, and cybersecurity into public service delivery. The discussion emphasized that in an era where nearly every citizen interaction is moving into Cyberspace, trust has become the true currency of effective governance. Panelists highlighted that as societies transition from physical to technological systems, the ability to protect personal data, ensure inclusivity, and maintain transparency determines whether citizens will embrace or resist technological transformation.

Speakers underscored that successful models of e-government are founded on comprehensive national strategies that integrate security and innovation "by design." Examples from across regions illustrated how digital identity systems and unified service portals are enabling citizens to access government services seamlessly. National visions set ambitious targets for becoming global leaders in digital service delivery, underpinned by continuous innovation through artificial intelligence and advanced cybersecurity frameworks.

Inclusive digitalization was identified as a critical priority. Participants emphasized that technological progress should narrow societal divides. With young people forming the majority in many countries, participants stressed that awareness, safe feedback mechanisms, and transparency are essential to build participation and trust. Transparency reports, citizen engagement in policy design, and zero-trust architectures were highlighted as practical mechanisms to enhance accountability and confidence in online governance.

Speakers also recognized that legislative and regulatory frameworks form the backbone of cyber trust. New cybersecurity and data protection laws are making it mandatory for public and private entities to safeguard critical infrastructure, while emerging cybercrime legislation aims to deter and prosecute offenses more effectively.

In conclusion, the panel stressed that sustaining public trust requires not only technological excellence but also ethical governance. Trust, transparency, and inclusivity should be embedded at every stage of the technological transformation journey to ensure that technology serves as an equalizer.

9.8T The GovTech market is expected to expand to USD 1.4 trillion in 2034, creating a USD 9.8 trillion opportunity to generate public value in 2034

(Source: World Economic Forum)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Strengthening Cyber Inclusion**

OPEN FORUM

CYBERSAFE FUTURES

Scaling Inclusion & Protection for Every Child

- **H.E. Sofiene Hemissi,** Minister of Communication Technologies, Tunisia
- **Sheema Sen Gupta,** Director, Child Protection and Migration, UNICEF
- **H.E. Dr. Maimoonah AlKhalil,** Secretary General, Family Affairs Council, Saudi Arabia
- **Dr. Iain Drennan,** Executive Director, WeProtect Global Alliance
- **Rebecca McLaughlin-Eastham (Moderator),** Independent TV Anchor and CEO, RME Media

The session focused on the growing urgency of safeguarding children in an increasingly interconnected world. Panelists highlighted that 72% of children under 12 who use social media have been exposed to harmful content, cyberbullying, grooming, and data exploitation [risen to 76% in 2025, according to the new CPC Index]. The discussion underscored that protection frameworks should evolve at the same speed as technology to ensure that Cyberspace remains safe.

Speakers emphasized that safety should be designed into technology from the outset. Child protection should be embedded within cyber platforms, governance systems, and innovation policies, ensuring that children's perspectives are reflected "from the design phase onward." A unified national and international framework is essential to define shared responsibilities, align performance indicators, and build capacity among educators, parents, and front-line professionals. Saudi Arabia's National Framework for Child Online Safety (collaboration of 14 ministries and 24 institutional partners) was presented as a model of multi-sectoral coordination and accountability.

Panelists referenced the 'Five Cs' holistic framework for understanding online risks: content, contact, conduct, contract (commercial practices), and cross-cutting well-being. New threats from AI, deepfakes, and immersive gaming demand equally innovative responses.

Research supported by GCF revealed that online grooming can begin in as little as 19 seconds, while unsafe interactions can develop within 45 minutes, reinforcing the need for proactive prevention.

The conversation closed with a call for global cooperation: harmonized cyber laws, intelligence sharing, and capacity-building for front-line professionals. Panelists agreed that technology evolves faster than legislation, making international partnerships indispensable. Their collective message was clear: prevention should outweigh reaction, and "safety by design" should become the universal standard to ensure that every child's online experience is empowering, inclusive, and secure.

76% 76% of children aged 8–18 faced at least one cyber risk in 2023–2025, up from 72% during the COVID-19 pandemic

(Source: CPC Global Index)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Opportunities at the Cyber Horizon**

OPEN FORUM

THE CYBER FRONTIER

Harnessing Emerging Tech for Global Security

- **Eng. Yasser Alswailem,** CEO, Sirar by stc
- **Filippo Monticelli,** Vice President, International Emerging, Fortinet
- **Mikko Karikytö,** Vice President, Chief Product Security Officer, Ericsson
- **John Crain,** Senior Vice President & Chief Technology Officer, ICANN
- **Kaiyi Dai (Moderator),** Television News Reporter, CGTN

The session examined how emerging technologies, including artificial intelligence, quantum computing, and next-generation telecommunications, are redefining the global cybersecurity landscape. Panelists reflected on how these advancements are transforming security operations, decision-making, and real-time response capabilities. The discussion emphasized that as innovation accelerates, speed and creativity should be guided by ethics, accountability, and resilience, principles that should be embedded into the design of every technological breakthrough.

Speakers discussed how AI has revolutionized threat detection and data analysis, accelerating response times across industries. Yet the same tools are being exploited by adversaries, forcing organizations to balance automation with human judgment. Transparency, training, and human oversight were cited as critical safeguards to prevent over-reliance on algorithms. In telecommunications, the rise of 5G and the coming 6G networks represents a new frontier of complexity, requiring "security-by-design" principles and standardization across global systems. As one panelist noted, this is the first era in which technology itself can make unpredictable decisions – demanding vigilance at every stage from design to deployment.

The conversation also turned to quantum computing, where panelists warned that the window to prepare for quantum-enabled threats is narrowing. Although progress in post-quantum cryptography continues, practices such as "harvest now, decrypt later" highlight the urgency of adopting crypto-agile solutions.

Resilience emerged as a defining measure of cybersecurity maturity. The ability to recover critical services swiftly after disruption, supported by simulations and fail-safe systems, was seen as a key indicator of readiness.

Concluding the discussion, speakers called for global cooperation and inclusive capacity-building. Cyber threats are borderless and can only be countered through shared intelligence, international partnerships, and ethical technology governance.

47% Nearly 47% of organizations cite adversarial advances powered by generative AI as their primary concern

(Source: World Economic Forum)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Cyber Economics Redefined**

OPEN FORUM

THE TALENT IMPERATIVE

Unlocking the Power of Women in Cyber

- **Silvana Koch-Mehrin,** Founder & President, Women Political Leaders (WPL)
- **Prof. David Hoffman,** Steed Family Professor of the Practice of Cybersecurity Policy, Duke University
- **Linda Gray Martin,** Senior Vice President and Chief of Staff, RSA Conference
- **Rummana Dada,** Founder, Managing Partner, Vitality Capital
- **Leila Hoteit (Moderator),** Managing Director & Senior Partner, BCG

The session examined how empowering women is central to solving cybersecurity's widening talent gap and building a more resilient cyber ecosystem. Despite progress, women make up only 24% of the global cybersecurity workforce, while the sector faces a talent shortage of 2.8 million professionals, a gap that was described as both a business and national security risk.

Drawing on new research by GCF and Duke University surveying women in cybersecurity in Latin America, the discussion revealed that 70% of respondents lacked access to mentorship and 70% cited the absence of entry-level opportunities. Awareness of routes into cybersecurity careers also remains limited. Panelists agreed that structured mentorship programs, transparent career pathways, and inclusive recruitment practices that look beyond formal degree requirements are key to unlocking untapped potential.

Panelists emphasized that women's participation is not only a moral imperative but an operational advantage. Studies show that companies with more women in leadership positions deliver higher profitability and stronger governance, while diverse teams demonstrate greater innovation and risk awareness, critical in the fast-evolving cyber landscape.

The conversation also highlighted successful initiatives such as accelerators, community partnerships, and global fellowships that expand access for women in cyber. Platforms like the RSA Conference, where many of the keynote speakers are women, play a powerful role in promoting visibility and inspiring future generations of women in cybersecurity. Panelists called for broader support for female-led startups, venture funding, and innovation ecosystems to scale women's impact in technology.

Finally, the panel explored the role of AI and emerging technologies in reshaping the talent landscape. AI can democratize access to training and augment skills, but biases in algorithmic design reinforce the need for women's inclusion in AI development itself.

24% Women comprise only 24% of the current global cybersecurity workforce, compared to 36% in the broader technology industry

(Source: GCF)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Cyber Economics Redefined**

OPEN FORUM

THE COST OF CYBER INSECURITY

Quantifying Financial Risks and Economic Fallout

- **Jacky Fox,** Senior Managing Director and EMEA Security Lead, Global Lead Security Strategy Practice, Accenture
- **Dr. Yiannis Pavlosoglou,** Vice Governor, National Cybersecurity Authority, Greece
- **Johan Gerber,** Executive Vice President, Global Head of Security Solutions, Mastercard
- **Laura Buckwell (Moderator),** Event MC and Broadcast Journalist

The session delved into the escalating economic and strategic toll of cyber threats in an increasingly connected world. Panelists observed that the average cost of a data breach now exceeds USD 5 million, while the global cost of cybercrime is set to reach nearly USD 10 trillion annually. Against this backdrop, the discussion emphasized that cyber risk is a macroeconomic and geopolitical challenge, demanding a coordinated global response.

Speakers identified three dominant trends shaping the threat landscape: Weaponization of artificial intelligence; acceleration of global digitization; and erosion of multilateral cooperation

Generative AI has transformed both attack and defense capabilities, fueling competition between adversaries who automate intrusions and defenders who build "AI antibodies" to counter them. The private sector was highlighted as a cornerstone of resilience, with global companies investing billions in cybersecurity. Mastercard's USD 10.7 billion investment in digital protection was cited as an example of corporate responsibility driving systemic stability.

Panelists warned that small and medium-sized enterprises remain particularly exposed. Many lack the resources, expertise, and access to affordable security solutions needed to counter sophisticated, AI-driven threats. Scalable defense mechanisms, public–private partnerships, and awareness campaigns were recognized as critical to fortifying this vital segment of the global economy.

Panelists also addressed the widening "third-party risk" inherent in global supply chains, where a single vendor compromise can cascade across industries. Governments were urged to foster cyber resilience over compliance, emphasizing cultural awareness, agile partnerships, and risk-based regulation.

Innovation supports cautious optimism. Advances in AI-powered threat intelligence, automated defense systems, and quantum-safe cryptography are shifting organizations from reaction to prevention. Yet human judgment remains irreplaceable – the weakest link in breaches but also the ultimate safeguard when technology fails.

In conclusion, speakers agreed that the cost of cyber insecurity extends beyond financial loss to national stability and trust. Embedding collaboration and human oversight into the digital economy is now the defining challenge of the next decade.

10.5T Global cybercrime costs to grow by 15% per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015

(Source: Cybersecurity Ventures)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Opportunities at the Cyber Horizon**

OPEN FORUM

CYBER LAW

Regulating the Next Tech Revolution

- **Prof. Assoc. Dr. Igli Tafa,** General Director, National Cyber Security Authority (AKSK), Albania
- **Dr. Yacine Djemaiel,** CEO, National Agency for Cybersecurity (TunCERT), Tunisia
- **Jane Witherspoon (Moderator),** Managing Editor, Euronews

The session explored how nations can adapt their legal and regulatory frameworks to keep pace with the rapid evolution of technologies such as artificial intelligence, blockchain, quantum computing, and advanced cloud systems. Panelists emphasized that in a borderless Cyberspace, effective governance depends not only on robust legislation but also on its ability to evolve with innovation.

A key theme was the growing global emphasis on agile, principle-based regulation that integrates ethical safeguards, accountability, and technological foresight. Albania's recent leap in the Global Cybersecurity Index (from 54th to 18th place in just over a year) was cited as an example of the impact that comprehensive reform can have. Its adoption of the EU NIS2 Directive, the Cybersecurity Resilience Act, and the creation of 21 detailed bylaws were highlighted as good practices for ensuring consistency and enforceability.

Tunisia's modernization of its national cybersecurity law, first enacted in 2004, was also recognized as a model of proactive adaptation. The introduction of a certification and labeling system for connected devices and AI systems aims to ensure safe and ethical deployment of emerging technologies. Recognizing that legislation often lags behind innovation, Tunisia has also developed reference guides and technical standards to help organizations manage AI and 5G securely while broader legal reforms are underway.

Panelists stressed that cyber threats and AI misuse transcend jurisdictions, demanding stronger regional and international collaboration. Harmonized frameworks, shared threat intelligence, and coordinated incident-response mechanisms were identified as critical to a resilient and interoperable global ecosystem. Public–private partnerships and collective accountability were seen as essential for translating legal provisions into effective, real-world protection.

Looking forward, the session called for the creation of agile, principles-based cyber laws that integrate emerging technologies into governance by design. Building public awareness, embedding ethics and human oversight into AI systems, and developing inclusive strategies that empower underrepresented groups were seen as priorities for the next decade.

The panel concluded that adaptable, future-ready cyber legislation, supported by collaboration and trust, will be the defining foundation of a secure cyber future.

58%

Only 58% of UN member states have fully implemented national cybersecurity strategies that include legislative and regulatory frameworks, while 24% are still in the drafting phase

(Source: ITU)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Cyber Economics Redefined**

OPEN FORUM

SECURING INVESTMENT

Why Cybersecurity is a Key Imperative for FDI

- **Bocar A. Ba,** Chief Executive Officer, SAMENA Telecommunications Council
- **Christopher Steed,** Chief Investment Officer and Managing Director, Paladin Capital Group
- **Wael Fattouh,** Chief Advisory Officer, SITE
- **Ramia Farrage (Moderator),** Senior Presenter & Producer, Forbes Middle East

The session examined how cybersecurity has become a cornerstone of global investor confidence, shaping the flow of capital and defining long-term competitiveness. Panelists emphasized that in today's interconnected economy, cybersecurity is not a cost center but a strategic enabler: a signal of national stability, institutional maturity, and market trust.

The discussion underscored that foreign direct investment (FDI) decisions are now influenced as much by a country's cyber resilience as by traditional factors like political stability and macroeconomic policy. Technological infrastructure, once seen as purely technical, has become the backbone of modern economies, underpinning banking, logistics, healthcare, and defense systems. Markets that can demonstrate digital safety and continuity are increasingly viewed as lower-risk and more attractive investment destinations.

Speakers highlighted that telecom and technological infrastructure resilience is now inseparable from economic competitiveness. Nations and enterprises capable of maintaining continuity during disruptions are seen as reliable partners. The conversation cited models such as the Smart Africa Alliance, which harmonizes cybersecurity policies across 54 countries to reduce regulatory fragmentation and boost investor confidence.

The Kingdom of Saudi Arabia's growing cybersecurity ecosystem was presented as a case study of this new paradigm. With cyber spending projected to rise from SAR 13 billion to SAR 15 billion in a single year, the country has positioned itself as a regional hub for secure innovation. Massive investment in human capital development has further strengthened its investment appeal.

The session concluded that cybersecurity should be elevated to a leadership and boardroom priority. Investors now expect transparency, accountability, and recovery readiness from both public and private sectors. As one key takeaway, panelists agreed that cybersecurity is the enabler of trust, making it the defining foundation for sustainable economic growth in the digital era.

12.2% Global security spending is expected to increase by 12.2% in 2025, driven by rising cyber threat complexity and the adoption of advanced defensive measures

(Source: IDC Research)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Strengthening Cyber Inclusion**

OPEN FORUM

STRENGTH IN REINFORCEMENTS

Capacity Building in the Global South

- **H.E. Mohamed Ben Amor,** Director General, Arab ICT Organization
- **Dr. Almerindo Graziano,** CEO, Cyber Ranges
- **Craig Jones,** Member of the Global Forum on Cyber Expertise (GFCE) Foundation Board
- **Alexandra Topalian (Moderator),** International Presenter & Panel Moderator

The session examined how strengthening cyber capacity in least developed countries and emerging economies is critical to safeguarding the stability of the global technology ecosystem. Panelists emphasized that cybersecurity is a shared responsibility: vulnerabilities in one region can quickly cascade across borders. Building collective resilience therefore requires equitable access to resources, expertise, and partnerships that empower every nation to participate fully in global security efforts.

The discussion highlighted that many developing countries remain underprepared due to limited resources, workforce shortages, and fragmented policy frameworks. Capacity building, they agreed, should extend beyond technology acquisition to encompass human capital development and institutional strengthening. Hands-on, simulation-based training was cited as one of the most effective methods for developing technical expertise.

Panelists also stressed the importance of embedding cybersecurity into national development strategies. Initiatives such as the Global Forum on Cyber Expertise (GFCE) were noted for their role in connecting donor resources with countries' specific needs and fostering regional delivery mechanisms. However, participants underscored that sustained progress depends on predictable funding and long-term partnerships, not one-off projects.

Cross-sectoral collaboration emerged as a cornerstone of capacity development. Governments, academia, industry, and civil society should coordinate through inclusive, multi-stakeholder frameworks that encourage transparency, knowledge exchange, and shared accountability. Examples such as regional ICT councils and multi-agency cyber exercises were recognized as effective platforms for aligning national priorities and fostering cooperation across sectors.

The session concluded that by investing in people, strengthening institutional frameworks, and fostering international collaboration, the global community can create a self-reinforcing ecosystem of resilience. As panelists agreed, no nation can be secure in isolation; cybersecurity capacity in the Global South is both a regional necessity and a global imperative for cyber stability.

7.1M

The global cybersecurity workforce currently stands at 7.1 million professionals, where Africa is severely underrepresented, with fewer than 300,000 cybersecurity professionals

(Source: GCF)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Opportunities at the Cyber Horizon**

OPEN FORUM

NEXT-GEN CYBER RESILIENCE

Turning Tech Disruption into Security Innovation

- **Dr. Marcus Fowler,** CEO, Dark Trace
- **Ultan Mulligan,** Chief Services Officer, European Telecommunications Standards Institute (ETSI)
- **Laura Buckwell (Moderator),** Event MC and Broadcast Journalist

The session explored how emerging technologies (especially artificial intelligence, automation, and quantum computing) are transforming cybersecurity strategies across industries. Panelists emphasized that while artificial intelligence (AI) has become one of the most disruptive forces in the digital era, it also holds immense potential to strengthen defense mechanisms and redefine operational resilience.

The discussion opened by noting that AI is leading to more effective cyber-attacks, enabling targeted phishing, automated reconnaissance, and self-evolving malware. However, the same technology is also revolutionizing defensive capabilities, allowing organizations to more rapidly anticipate, detect, and neutralize threats. The conversation underscored that AI-augmented human teams will increasingly outperform those relying solely on manual processes, reducing alert fatigue, automating investigations, and empowering analysts to focus on higher-level decision-making.

Panelists agreed that the key to leveraging AI securely lies in transparency, explainability, and trust. Security leaders should ensure that AI systems are designed to be auditable, ethically governed, and integrated into core workflows rather than treated as black-box tools. AI's value is realized not in replacing humans, but in amplifying their analytical capacity and accelerating response times.

A significant part of the session focused on regulatory evolution and standardization, with the European Union's Cyber Resilience Act (CRA) highlighted as a landmark initiative. Coming into effect in December 2027, the CRA will require all digital products sold in Europe (including imported software and connected devices) to meet essential cybersecurity standards throughout their lifecycle. Industry-driven standards, including quantum-safe cryptography and secure AI protocols, will play a vital role in compliance and global alignment.

The session concluded that next-generation cyber resilience depends on collaboration between innovators, regulators, and end-users. By embedding security by design, fostering agile industry standards, and applying AI responsibly, technology disruption can become a driver of security innovation. As panelists affirmed, the future of cybersecurity lies not in resisting change but in transforming it into a foundation for global cyber trust.

66% 66% of organizations expect AI to have a significant impact on cybersecurity by 2025, yet only 37% of them currently have processes to evaluate the security of AI tools before deployment

(Source: World Economic Forum)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Behavioral Lens in Cyberspace**

OPEN FORUM

THE PSYCHOLOGY OF CYBER TRUST

Leadership Strategies for Building Resilient Societies

- **Prof. Mary Aiken,** Chair of the Department of Cyberpsychology, Capitol Technology University
- **Odhran McCarthy,** Programme Officer, United Nations Interregional Crime and Justice Research Institute (UNICRI)
- **Riz Khan (Moderator),** International Journalist and TV host Al Arabiya English

The session examined how human behavior, psychology, and technology intersect to shape public trust in Cyberspace. Panelists emphasized that as societies become increasingly technological, trust has become the new currency of the cyber age; yet it remains fragile in the face of manipulation, fraud, and psychological exploitation online.

Drawing on research from the Oxford Internet Institute, speakers noted that manipulation campaigns have been detected in 81 countries, with misinformation now used as a political or social strategy in 93% of them. Globally, more than USD 1 trillion was lost to scams in 2024, while surveys indicate that 90% of individuals worry about cyber fraud, and more than half have personally fallen victim. Panelists warned that these figures reflect not only economic damage but a more profound erosion of public confidence in digital ecosystems.

Panelists explained that cybercriminals increasingly exploit psychological vulnerabilities, such as authority bias, urgency, and emotional triggers, to manipulate victims. For example, an urgent message from a supposed bank official taps into "authority bias," compelling users to act without question. AI-driven scams now amplify these attacks, using behavioral profiling and generative content to make deception nearly indistinguishable from reality.

Panelists agreed that combating these threats requires empowering citizens through education, critical thinking, and behavioral awareness. Generic warnings, they argued, should be replaced by practical guidance that trains individuals to "stop, think, and check" before engaging online. Cyber awareness should be embedded in school curricula and civic education to cultivate a culture of responsibility, discernment, and digital resilience from an early age.

The session further highlighted how cybercrime has evolved into a transnational human rights issue, with victims being trafficked into scam operations. The recent United Nations Cybercrime Convention was hailed as a milestone for cross-border cooperation.

In conclusion, panelists agreed that combating cyber fraud requires blending technological defenses with psychological insight. Building cyber trust, they said, means understanding not just how systems are attacked – but how minds are manipulated. Trust, once rebuilt, becomes the foundation for a safer, more resilient technological society.

12B In 2024 people in US reported losing over USD 12 billion to fraud, with over USD 5 billion of that from investment-related scams

(Source: Consumer Sentinel Network)

Scan the QR code to watch this session

SCAN HERE

Panel Discussion | **Cyber Economics Redefined**

OPEN FORUM

FUNDING THE FUTURE OF CYBER

Public-Private Investment Models for Scalable Growth

- **Prof. Norman Sadeh,** Professor of Computer Science, Software and Societal Systems Department, Carnegie Mellon University (CMU)
- **H.E. Dr. Margarete Schramböck,** Minister of Digital and Economic Affairs, Austria (2020 – 2022), Board Member, Aramco Digital
- **Ramia Farrage (Moderator),** Senior Presenter & Producer, Forbes Middle East

The session examined how strategic investment, innovation, and cross-sector collaboration can shape a more secure cyber economy. Panelists emphasized that cybersecurity is a national and economic imperative that underpins global competitiveness, investor confidence, and long-term prosperity.

The discussion opened with a clear message: cyber threats are escalating in scale and sophistication, driven by the convergence of AI, quantum computing, and automation. These developments demand that both public and private sectors align to fund research, infrastructure, and education that build collective resilience. While Europe continues to advance through regulation and standard-setting, the Middle East – particularly Saudi Arabia – has distinguished itself by fostering agility, pilot programs, and sandboxes that accelerate innovation without compromising security.

Panelists agreed that investment in cybersecurity should move in parallel with investment in human capital. The human factor remains the weakest link in cyber defense; therefore, empowering people through training and awareness is essential. Yet training alone is not enough – AI and intelligent systems will increasingly serve as "digital sentinels," augmenting human decision-making and preventing threats in real time.

The conversation also highlighted how public–private partnerships can de-risk innovation and attract capital. Co-investment models are proving particularly effective in catalyzing research and commercialization. Examples included cash-back R&D incentives and regional innovation hubs that link universities, small and medium enterprises (SMEs), and industry leaders to create localized centers of excellence.

Panelists underscored that no nation could achieve cyber resilience in isolation. Shared standards, open collaboration, and the creation of global innovation ecosystems are vital to scaling secure growth. As cyber risk expands, the global cybersecurity market (valued at over USD 250 billion in 2025) will require exponential growth in both venture funding and regulatory alignment to sustain its momentum.

The session concluded that the future of cybersecurity funding lies in a balance between regulation and experimentation, protection and innovation. By combining visionary policy, academic research, private investment, and human-centered design, nations can transform cybersecurity from a defensive expense into a driver of global prosperity.

~10% The global cybersecurity market is projected to grow from USD 243.15 billion in 2024 to USD 267.51 billion in 2025, registering a CAGR of ~10%

(Source: Research and Markets)

Scan the QR code to watch this session

SCAN HERE

PARTICIPATORY TRACK

ROUNDTABLES

ROUNDTABLES

HIGH-LEVEL ROUNDTABLE ON WOMEN EMPOWERMENT IN CYBERSECURITY

Excluding women from cybersecurity weakens national resilience and innovation, while diverse perspectives – particularly in systems design and leadership – strengthen outcomes. Persistent barriers such as online harassment, biased recruitment, limited career translation from education to employment, and 'presence equals productivity' norms continue to hinder progress.

With fewer than 11% of national cyber strategies referencing women and less than 3% of venture funding reaching women-led startups, leadership commitment and measurable accountability are critical. Political prioritization, male allyship, and private-sector engagement can accelerate change, as seen in Saudi Arabia's Vision 2030 initiatives.

Globally, momentum is building through programs that embed inclusion in policy, education, and investment – from the G20 and UN to partnerships led by HRH and CYBOK leadership. Achieving sustainable equity requires building clear pathways from education to leadership, dismantling structural barriers, and embedding family-supportive, flexible ecosystems where 'security by design' extends to making Cyberspace safe and accessible for women.

CXO MEETINGS

CXO ROUNDTABLE

Organizations are increasingly balancing global platform models with localized architectures, with success hingeing on reliability, trust, and agility rather than uniformity. As regulatory fragmentation accelerates, harmonized and borderless trust frameworks are needed to navigate differing compliance regimes. A hybrid model combining global standards with local infrastructure, partnerships, and talent is emerging as the preferred path. Firms are urged to prioritize fit and capability over speed, embedding 'secure-by-default' and 'compliant-by-default' principles into their design processes.

Localization should be viewed as a strategic lever for capacity building and sustainable innovation, enabling knowledge transfer and repeatable, residency-compliant architectures. At the same time, the adoption of AI is reshaping defenses and reducing breach costs but heightening adversarial sophistication, underscoring the importance of contextual trust, human oversight, and cross-vendor collaboration to maintain resilience and accountability at scale.

100

ROUNDTABLES

NATIONAL CYBER LEADERSHIP HIGH-LEVEL ROUNDTABLE

The discussion highlighted that cybersecurity leadership, not just technical expertise, is the critical gap in national readiness, with the greatest shortage seen at the management and policy levels. Workforce development strategies should therefore extend beyond training specialists to cultivating leaders capable of integrating cyber resilience into national planning and governance. Universities and executive education programs are urged to embed cyber fluency into curricula, while shared service models and cross-sector rotations can help retain scarce expertise.

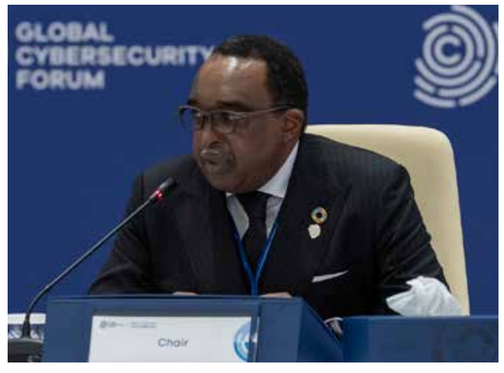
The newly launched Child Protection in Cyberspace (CPC) Index was presented as a model, providing a unified, non-ranking framework and toolkit to guide national implementation. Participants underscored the need for KPI-based frameworks linking capacity building to enforcement and real-world outcomes, and for modular collaboration mechanisms that connect national initiatives into a cohesive global readiness ecosystem — advancing cyber resilience through coordinated leadership, shared accountability, and sustained capability exchange.

ROUNDTABLES

HIGH-LEVEL MULTI-STAKEHOLDER ROUNDTABLE ON CAPACITY BUILDING

Cyber capacity building is shifting from fragmented initiatives toward coordinated, inclusive, and context-specific ecosystems that link education, workforce development, and policy implementation. Participants emphasized that national frameworks like SCYWF and CyberEDU demonstrate how early-stage cyber education, practical certification pathways, and targeted programs can institutionalize capability development. Capacity building should be locally owned yet globally connected, aligning public-private partnerships and donor funding with national strategies to avoid duplication and ensure measurable outcomes.

Sustained funding in volunteer networks, university–industry partnerships, and regional collaboration – particularly across Africa and Oceania – was recognized as essential for scalability. Inclusion was reframed as both a security and an economic enabler, integrating gender, youth, and community participation into cyber ecosystems. The dialogue also highlighted the need to balance human and technological capacity, strengthen practitioner retention, and translate awareness into applied operational competence through continuous learning and coordinated national strategies.



ROUNDTABLES

SAFEGUARDING CYBER TRUST: DISMANTLING ORGANIZED CRIMINALS' EXPLOITATION OF THE INTERNET

The session on safeguarding cyber trust examined UNICRI's findings on how organized criminal groups exploit digital trust to conduct identity theft, data breaches, and trafficking. Participants discussed how these groups increasingly rely on automation, machine learning, and AI-driven exploits to map vulnerabilities and execute large scale operations across blockchain and digital domains. The conversation emphasized that trust in digital systems should be continuously verified, not assumed, with participants calling for a zero trust mindset as the foundation of modern cybersecurity. A human and victim centered approach was highlighted as essential, prioritizing safety, rights, and resilience while empowering users to think critically about online behavior. Public awareness and digital literacy initiatives that teach citizens to recognize manipulation and deception were identified as key components of prevention.

Experts also called for stronger regulation of cryptocurrency channels used to fund cybercrime and for more coordinated global enforcement mechanisms under the UN Convention on Crime. Protecting digital trust, they agreed, depends on multi layered collaboration across governance, technology, and human capacity, combining technical innovation, information sharing, and community engagement to create transparent and accountable digital ecosystems

ROUNDTABLES

SECURING TOMORROW'S POWER: AN ENERGY LEADERSHIP DIALOGUE

The energy sector is undergoing a rapid transformation driven by digitalization, AI, automation, and the integration of IT and OT systems. While these technologies improve efficiency and sustainability, they also expand the attack surface and expose critical infrastructure to increasing cyber risks. Ransomware and supply chain compromises targeting oil, gas, and power systems highlight that energy security has become a matter of national security, requiring coordinated operational, regulatory, and policy measures.

Strengthening defenses depends on adopting Zero Trust principles, ensuring clear segmentation between IT and OT, and deploying continuous monitoring across distributed networks. AI-powered detection and digital twin simulations were cited as tools that can reduce false alerts and improve readiness by enabling faster and more accurate responses.

Policymakers were urged to define sector wide cybersecurity standards, enforce vendor accountability, and establish governance frameworks for AI applications in energy systems. Persistent talent shortages remain a challenge, underscoring the need to develop specialized OT cyber skills through targeted training and international collaboration. Ultimately, participants agreed that cybersecurity is not only a protective measure but a strategic enabler of trust, operational continuity, and sustainable energy transition.

ROUNDTABLES

GAMING FOR SAFETY: PROTECTING CHILDREN FROM CYBER RISKS

Online gaming now connects more than three billion people worldwide and has become both a major form of entertainment and a shared social environment for children. Participants emphasized that safety should be built into game design from the outset, integrating child rights, privacy, and wellbeing through a safety by design approach. The UNICEF 5Cs Framework, which examines content, contact, conduct, commercial practices, and cross cutting themes, was highlighted as a practical tool for identifying risks and guiding intervention strategies.

Speakers noted the growing threat of grooming and sextortion, particularly targeting young boys, and called for closer collaboration between gaming companies, helplines, and regulators to strengthen early detection and prevention. The Child Protection in Cyberspace (CPC) Index was introduced as a shared measurement framework to standardize safety metrics and align reporting across industries and governments.

Participants agreed that children should be active co-creators in shaping safer cyber spaces rather than passive recipients of protection, with community moderation, peer reporting, and youth led feedback tools enhancing accountability. An International Pact on Safe Gaming was proposed to define responsibilities across governments, companies, and caregivers, while discussions on AI moderation underscored the need for ethical oversight to prevent bias and misuse.

ROUNDTABLES

SAFER PLAY: EVIDENCE-BASED SOLUTIONS FOR PROTECTING CHILDREN FROM ONLINE GAMING HARMS

The session reviewed the "Evidence Review of Risks to Children in Online Gaming" report, which provides a data-driven view of online gaming risks and how they affect children in increasingly social and immersive environments. With more than three billion gamers worldwide, the discussion emphasized the importance of embedding safety and privacy into gaming through a safety by design approach.

The UNICEF 5Cs framework remains a key reference for understanding harm typologies and guiding interventions. Participants noted that misaligned incentives between policymakers and gaming companies continue to hinder progress and called for stronger cooperation through platforms such as the Fair Play Alliance. Advances in AI moderation tools have improved detection, but global adoption and governance still lag. Cross platform exploitation was identified as a growing concern, particularly where extremist content and grooming occur in games and social channels. Panelists agreed that children should be active contributors to safety policies through youth councils and co-design initiatives rather than passive beneficiaries.

The discussion concluded that sustainable child safety requires shared accountability across governments, industry, and researchers, supported by continued collaboration between UNICEF, WeProtect Global Alliance, and technology partners to strengthen the CPC Index as a global benchmark for child online safety.

INTERACTIVE SESSIONS

Fireside Chat

DEEP DIVE SESSIONS

THE DIGITAL EMBLEM

Protecting Critical Infrastructure in Cyberspace

- **Laurent Gisel,** Head of the Arms and Conduct of Hostilities Unit, ICRC
- **Rob van Dale,** Moderator

The Digital Emblem initiative extends the protective mandate of the Red Cross and Red Crescent into Cyberspace by identifying and shielding digital assets belonging to medical and humanitarian organizations. As militaries increasingly rely on digital operations, the discussion emphasized the growing vulnerability of humanitarian and medical data in conflict zones.

The emblem serves as a chain of cryptographic certificates that link protected digital assets to verified humanitarian entities, coordinated through Geneva and national societies such as the Saudi Red Crescent. Collaboration among military, technological, and humanitarian actors was seen as critical to ensure recognition and interoperability, while misuse of the emblem was clarified as a war crime under international humanitarian law. The governance model remains decentralized, granting autonomy to national societies over emblem deployment. Ongoing efforts focus on achieving global standardization through the Internet Engineering Task Force (IETF), balancing security with operational feasibility, and integrating prototypes into legal frameworks once finalized.

Briefing

SIMULATIONS

SOVEREIGN SHIELD – A REAL WORLD SIMULATION FOR GOVERNMENT LEADERS

- **Prof. Dr. Marco Gercke,** Director, Cybercrime Research Institute

The Sovereign Shield simulation placed government leaders in a high-pressure scenario mirroring a nation-state cyberattack on critical infrastructure, testing real-time decision-making, coordination, and communication. The exercise revealed that technical expertise alone is not enough; effective crisis management depends equally on leadership clarity, structured delegation, and coordinated messaging among agencies and sectors.

Communication gaps between national Computer Emergency Response Teams (CERTs), ministries, and private operators emerged as recurring weaknesses, highlighting the need for integrated protocols and regular rehearsals that reflect both technical and political realities. Participants underscored the importance of maintaining offline continuity mechanisms such as printed playbooks and analog communication systems to preserve command control during blackouts or infrastructure failures.

The session also emphasized that future crises will span jurisdictions, requiring synchronized civil-military cooperation and sustained collaboration with regional and private partners. A resilient national response depends on clearly defined leadership roles, rapid escalation protocols backed by scenario-based drills, and continuous coordination with allies to ensure preparedness across borders and sectors.

Panel Discussion

DEEP DIVE SESSIONS

HOUSTON, WE HAVE A PROBLEM

Securing Space Assets

- **Mohammed Aljameele,** Sanford School of Public Policy
- **James Pavur,** PhD, Director - Cysec Labs, CysecSA
- **Alexandra Topalian,** Moderator

The cybersecurity threats facing global space infrastructure are growing, however, many satellites still lack security-by-design architecture. Exposed communication channels such as radio links, GPS systems, and unpatched software remain major vulnerabilities, as demonstrated by real incidents like the Viasat modem attacks that underscored the operational risks of insecure satellite networks. Nonetheless, fragmented standards and the private sector's tendency toward secrecy hinder coordinated defense and resilience efforts. As the space sector expands rapidly, there is an urgent need for multilateral norms, consistent incident reporting, and resilience-by-design principles to safeguard critical assets.

The discussion also highlighted Saudi Arabia's priorities in balancing national security, economic growth, and public-private collaboration to ensure the long-term protection and sustainability of the space domain.

Fireside Chat

Trellix

DEEP DIVE SESSIONS

THE AI ADVANTAGE

Transforming Cyber Defense at Scale

- **Rohit Unnikrishnan,** VP - Product Management, Network & Email Security Business, Trellix
- **Alberto Pardo,** Moderator

Artificial intelligence is reshaping the cybersecurity landscape by simultaneously accelerating cyberattacks and defensive capabilities. Organizations are increasingly challenged to balance automation with human oversight as phishing and social engineering attacks become AI-driven, making detection and user awareness more complex. Security Operations Centers now depend on AI tools to manage alert fatigue and enhance detection accuracy, yet the growing reliance on these systems underscores the need for explainability and accountability.

The participant cautioned that opaque, black-box AI models are unsuitable for security decision-making where transparency is essential. They also highlighted that strong data governance, clear accountability frameworks, and responsible integration practices are critical to prevent AI misuse, sustain trust, and ensure that AI augments, rather than undermines effective cyber defense.

Briefing

DEEP DIVE SESSIONS

HARMS TO CHILDREN FROM ONLINE GAMING

Understanding the Evidence and Exploring Solutions

- **Srivatsan Raj,** Senior Research Analyst, WeProtect Global Alliance
- **Dr. Iain Drennan,** Executive Director, WeProtect Global Alliance

Risks children face in online gaming environments are growing, where exposure to grooming and exploitation can escalate rapidly. While global awareness of these dangers is increasing, research remains uneven and heavily focused on Western contexts, leaving significant gaps in understanding experiences across other regions and demographics.

The absence of a unified framework for measuring online harms or tracking long-term safety outcomes was identified as a key policy challenge. Current platform models often prioritize engagement and monetization over protection, resulting in fragmented and voluntary safeguards. The discussion underscored the importance of safety-by-design principles such as verified messaging, spending limits for minors, and human-in-the-loop content moderation, alongside digital literacy education for parents, teachers, and children.

Stronger regulatory alignment, transparency, and independent safety audits are needed to leverage the industry's scale to set global child protection standards in gaming.

Fireside Chat

DEEP DIVE SESSIONS

BRIDGING THE GENDER GAP IN CYBERSECURITY

Addressing Barriers and Expanding Workforce Participation

- **Prof. David Hoffman,** Steed Family Professor of the Practice of Cybersecurity Policy, Duke University
- **Jay Bhatnagar,** Moderator

Gender disparities persist in cybersecurity, particularly around pay equity, leadership representation, and career advancement. Despite growing awareness, structural barriers continue to limit women's entry and progression within the field.

Leadership instability marked by short CISO tenures and under-resourced roles is a factor that disproportionately affects women's advancement. The lack of visible role models and mentorship opportunities further compounds this gap, discouraging participation and retention. Traditional academic pathways often fail to prepare students for real-world cybersecurity challenges, calling for stronger partnerships between academia, industry, and government to build practical experience pipelines.

Achieving equity requires more than policy reform; it depends on sustained investment in mentorship, internships, and targeted training programs that provide women with the access, confidence, and networks necessary to thrive in the cybersecurity workforce.

Fireside Chat

DEEP DIVE SESSIONS

THE AI SECURITY CHALLENGE

Building a Resilient Infrastructure for Tomorrow's Threats

- **Lothar Renner,** Managing Director of Security Sales and Engineering, Cisco
- **Rob van Dale,** Moderator

The session highlighted the growing impact of AI on cybersecurity readiness, noting that 91% of organizations have experienced AI-related security incidents involving model theft, social engineering, or data poisoning. Overreliance on fragmented security tools has led to inefficiencies, with 84% of organizations reporting slower detection and recovery due to stack complexity.

As AI reshapes infrastructure demands, new requirements such as reducing network bottlenecks, managing latency, and establishing private data centers for compliance are becoming priorities. Managing "shadow AI" and unmanaged devices particularly within IoT environments was identified as a persistent vulnerability affecting supply chains. Data sovereignty is now central to security strategy, with national regulations driving the need for standardized frameworks and cross-border interoperability. Ultimately, the secure and responsible adoption of AI hinges on strong governance, controlled access, and the integration of trusted frameworks to ensure resilience across distributed cyber ecosystems.

Panel Discussion

DEEP DIVE SESSIONS

CYBER IMMUNITY

Strengthening Cyber Resilience for Global Health Systems

- **Prof. Richard Staynings,** Professor of Cybersecurity, University of Denver
- **Prof. Attila J. Hertelendy,** Assistant Professor, Department of Information Systems and Business Analytics, Florida International University
- **Alexandra Topalian,** Moderator

Healthcare remains one of the sectors most targeted by cyberattacks due to the value of its sensitive data such as personal information, research, and medical innovations to both criminal and state actors. Ransomware incidents can paralyze hospital operations for weeks, leading to financial losses, legal exposure, and risks to patient safety.

Despite the scale of the threat, underreporting and limited transparency continue to obscure the true extent of cyber incidents across the sector. Insider threats and human error account for most breaches, while traditional, one-size-fits-all training fails to build lasting resilience. Instead, role-based, continuous education supported by AI-driven alerts can significantly improve staff awareness and risk mitigation. Therefore, cybersecurity should shift from being viewed as a cost center to a strategic enabler of innovation and patient safety, with stronger collaboration among healthcare providers, technology partners, and leadership teams to close maturity gaps.

Panel Discussion

DEEP DIVE SESSIONS

THE UN CONVENTION AGAINST CYBERCRIME

- **Mustafa Ünal Erten,** Chief of the Regional Center for Combating Cybercrime, UNODC
- **Nguyen Dinh Do Thi,** Deputy Chief of Information Security Division under the Department of Cybersecurity and High-Tech Crime Prevention Ministry of Public Security, Vietnam
- **Sanidhya Jain,** Moderator

The UN Convention Against Cybercrime is a landmark achievement marking the first global treaty dedicated to combating cybercrime. Building upon the Arab, African, and Budapest conventions, the treaty establishes a unified framework through nine chapters and 68 articles, requiring member states to criminalize cyber offenses, strengthen investigative capabilities, and enhance cross-border cooperation. Crucially, it differentiates between cybersecurity focused on infrastructure protection and cybercrime, which targets individuals and organizations.

However, effective implementation will hinge on shared international standards, robust capacity-building programs, and sustained collaboration among nations. The ratification process requires at least 40 signatures within 90 days, after which a Conference of State Parties will oversee governance and execution. The Convention was widely recognized as a foundational step toward harmonizing global cyber norms and closing jurisdictional gaps in addressing cyber threats.

Briefing

DEEP DIVE SESSIONS

CYBERSAFE FUTURES

Parenting to Protect Our Children in a Digital Age

- **Dr. Afrooz Kaviani Johnson,** Child Protection Specialist, UNICEF

Effective child online protection begins with community-based engagement rather than reliance on digital campaigns alone. Parents tend to benefit most from in-person sensitization programs and interactive training that help them recognize and manage the online risks their children face. With children frequently using shared or family devices, protective measures such as supervised access, privacy settings, and open communication should be prioritized to minimize exposure.

The responsibility is shared between educators and families in shaping responsible digital habits and modeling safe online behavior. By fostering active dialogue, awareness, and shared accountability, communities can strengthen children's digital resilience and ensure that online safety becomes a sustained, collective effort grounded in both education and empathy.

Fireside Chat

DEEP DIVE SESSIONS

AI DRIVEN CYBERATTACKS AND DEFENSES

- **Fahad AlSamari,** General Manager of Managed Detection and Response (MDR), Sirar by stc
- **Ramia Farrage,** Moderator

Artificial intelligence is reshaping the dynamics between cyber offense and defense, lowering the barrier to entry for attackers while enabling more sophisticated and efficient operations. AI-generated content has made phishing and social engineering attacks increasingly difficult to distinguish from legitimate communications, and deepfake-based scams now pose growing risks to financial and executive workflows.

On the defensive side, AI is transforming Security Operations Centers by filtering noise, accelerating analysis, and improving response times. However, human oversight remains indispensable, as AI lacks the contextual understanding and ethical judgment necessary for autonomous decision-making.

Verification mechanisms and simulation-based awareness training are essential to counter AI-driven manipulation, while emerging national regulations should evolve toward global frameworks to address cross-border threats. The discussion concluded that the future of cybersecurity will increasingly unfold as an "algorithm versus algorithm" race, with both attackers and defenders relying on automation at scale.

Fireside Chat

DEEP DIVE SESSIONS

CYBER FRONTIERS

Deepening Public–Private Collaboration for a More Resilient Future

- **Britta Glade,** Senior Vice President for Content & Communities, RSA Conference
- **Alberto Pardo,** Moderator

Public-private partnerships (PPPs) are widely recognized for their potential impact, yet their effectiveness remains limited. Moreover, insurance rates and compliance incentives are increasingly tied to cooperation and shared data frameworks. Saudi Arabia's Haseen platform was presented as a leading example, enabling real-time intelligence sharing across more than 500 providers and demonstrating measurable national progress.

Smaller nations such as Australia, Fiji, Samoa, and New Zealand underscored the need for trust-based partnerships to address supply-chain vulnerabilities and enhance resilience. Knowledge communities such as those convened under the Global Cybersecurity Forum play a pivotal role in translating collaboration into concrete policy outcomes, shaping regulations, and advancing a unified approach to global cyber defense.

Fireside Chat

DEEP DIVE SESSIONS

CYBERSECURITY AT SCALE

Building Resilience for a Hyperconnected World

- **Alain Sanchez,** EMEA CISO, Fortinet
- **Ryan Chilcote,** Moderator

True resilience in an increasingly hyperconnected cyber landscape extends beyond technical recovery to encompass governance, compliance, and transparency. Security by design was presented as essential, shifting organizations from reactive patching to proactive protection built into systems from inception. While interconnected technologies enhance efficiency, they also expand the attack surface, demanding continuous vigilance and a security-first culture across all departments.

Moreover, AI is reshaping both offensive and defensive strategies, with organizations that integrate it responsibly gaining a long-term advantage.

Saudi Arabia's cybersecurity maturity was noted as a model of vision-driven progress grounded in strong frameworks. Persistent vulnerabilities in legacy systems were identified as a global challenge, and the modern CISO role was described as increasingly multidisciplinary, blending technical, legal, and operational expertise with cultural fluency to align cybersecurity with organizational goals.

Panel Discussion

DEEP DIVE SESSIONS

FROM ARMOR TO ALGORITHMS

Protecting the Modern Defense Ecosystem

- **Olivier Waghorn,** Business Development and Strategy Director, BAE Systems
- **Rahul Anand,** Partner, Kearney
- **Usman Choudhary,** General Manager, VIPRE Security Group
- **Alexandra Topalian,** Moderator

Effective resilience depends on outcome-driven policy, ecosystem-wide collaboration, and sustained talent pipelines. Gulf Cooperation Council (GCC) nations are prioritizing the shift from import dependency to localized defense capabilities.

Achieving this requires parallel skill development across hardware, software, and mission operations to support complex, interdependent supply chains, where the weakest link often defines overall security. Governance frameworks should balance the role of major defense contractors with mechanisms to uplift SMEs, academia, and local operators through co-investment and shared standards.

Risk management emerged as the most dependable strategy for protecting critical national infrastructure, with a call for fit-for-purpose frameworks that move beyond compliance to reflect modern threat environments. Such risk assessments should be tied to mitigation roadmaps, budgets, and readiness drills to ensure findings translate into tangible action.

Panel Discussion

DEEP DIVE SESSIONS

THE CYBER RISK EQUATION

Enabling Security and Readiness Through Cyber Risk Assessment

- **Charlie Sammut,** Deputy Director Assessment, NCSC UK
- **Saâd Elkhadiri,** Director General, Directorate of Information Systems Security (DGSSI), Morocco
- **Elias Aad,** Moderator

Cyber risk management is increasingly recognized as the foundation of effective cybersecurity, serving as the true control plane that aligns protection priorities, investment levels, and operational readiness. As adversaries exploit cyber means for both strategic and economic advantage, risk frameworks should evolve beyond compliance-driven checklists to focus on real threats and measurable outcomes.

Many organizations still rely on audits rather than integrated, threat-led assessments, creating blind spots across IT, OT, cloud, and third-party environments that weaken assurance and distort the overall risk picture. Fragmented reporting and inconsistent scoring further reduce the reliability of board-level risk visibility, while limited simulation of real-world impacts hinders preparedness under pressure. Embedding a unified, risk-led operating model into governance and strategy enables continuous evaluation, informed decision-making, and sustained resilience against evolving cyber threats.

Panel Discussion

DEEP DIVE SESSIONS

THE NEXT FRONTIER OF CYBER RISK

Integrating Technology, Policy and Resilience

- **Frank Van Caenegem,** VP for Cybersecurity and CISO - EMEA, Schneider Electric
- **Prof. Norman Sadeh,** Professor in the School of Computer Science, Carnegie Mellon University
- **Matteo Coppola,** Moderator

Cybersecurity strategies are shifting from compliance-driven checklists toward continuous, risk-based assessment models that are integrated with business operations. Innovation and emerging technologies such as AI are reshaping this landscape, simultaneously creating new opportunities and exposing organizations to expanded threat surfaces that demand agile, adaptive regulation. Regional disparities in regulatory maturity levels underscore uneven global readiness, while small and medium-sized enterprises require a stronger collective voice in shaping regulatory frameworks to ensure inclusivity and practical implementation.

Despite advances in technology, human error continues to be the leading cause of cybersecurity incidents, highlighting the importance of targeted training programs and AI-enabled support systems designed to enhance workforce awareness and resilience.

Briefing

KEARNEY

SPOTLIGHT SESSIONS

THE FUTURE OF CYBER DIPLOMACY – KEY FORCES OF CHANGE AND STRATEGIC OUTLOOK

- **Rudolph Lohmeyer,** Senior Partner, Kearney

Cyber diplomacy is undergoing a fundamental transformation as geopolitical fragmentation, technological acceleration, and misinformation erode trust among nations. Traditional multilateral forums such as the UN, WTO, and ICANN are increasingly gridlocked, giving rise to smaller 'minilateral' coalitions of like-minded states and corporations that can set de facto standards more rapidly. Non-state actors, including technology companies, AI developers, and hacker collectives, now hold significant influence, often possessing greater technical and intelligence capabilities than many governments.

The rapid advancement of technologies such as AI, quantum computing, and autonomous systems has expanded both the threat environment and the diplomatic toolkit, with AI already being used for negotiation modeling and predictive analysis. Cybersecurity and economic policy have become inseparable, as debates over data localization, cross-border governance, and digital sovereignty shift from soft diplomacy to strategic bargaining. Emerging mid-sized nations like Estonia, Singapore, and the UAE are leveraging agility and innovation to shape global norms despite limited military capacity.

The concept of trusted digital alliances is gaining traction, where governments and private actors cooperate to establish voluntary but globally recognized standards for responsible behavior in Cyberspace.

Fireside Chat

DEEP DIVE SESSIONS

THE EVOLVING DYNAMICS OF OT CYBERSECURITY

- **Dr. Saad Alaboodi,** Chief Executive Officer, Saudi Information Technology Company (SITE)
- **Robert M. Lee,** Chief Executive Officer, Dragos

The Operational Technology (OT) cybersecurity landscape is rapidly evolving amid the growing convergence of IT, OT, and IoT systems. The OT market is projected to reach USD 364 billion by 2030, with investments promising up to 400% ROI through improved efficiency and reduced downtime. Manufacturing and oil and gas sectors remain the most exposed, with the majority of OT disruptions traced back to IT and cloud vulnerabilities.

Because OT incidents can endanger physical safety, organizations are shifting from prevention to enhanced visibility, detection, and root cause analysis. Regulators are emphasizing proactive detection and analytical capabilities, signaling a new compliance mindset. While AI can optimize performance, speakers cautioned against over-automation that displaces human oversight.

Skilled operators and continuous talent development were identified as critical to resilience, alongside strong local partnerships. Achieving secure OT infrastructure ultimately requires standardization across fragmented protocols and sustained investment in local engineering expertise.

Panel Discussion

DEEP DIVE SESSIONS

WOMEN IN CYBER BREAKFAST

- **H.E. Kolinda Grabar-Kitarović,** President of Croatia (2015-2020)
- **H.E. Macky Sall,** President of Senegal (2012-2024)
- **H.E. Dr. Hanan Al Ahmadi,** Assistant Speaker of the Shura Council, Kingdom of Saudi Arabia
- **Sarah Hendriks,** Deputy Executive Director, UN Women
- **Jim O'Connor,** Chairman and CEO, USTTI
- **Rebecca McLaughlin-Eastham,** Moderator

Day two of the Annual Meeting began with a "Women in Cyber Breakfast," which focused on women's participation in cybersecurity globally. In a panel discussion moderated by Rebecca McLaughlin-Eastham, speakers provided insights from their experiences to highlight the importance of advancing more women in cyber.

Among the attendees were future women leaders from around 20 countries. They were part of the third cohort of the GCF-USTTI 'Empowering Women to Leadership in Cyber' training and mentorship program, under the Women in Cybersecurity (WEC) global initiative by H.R.H. the Crown Prince.

Speakers highlighted WEC's contributions to advancing action on bridging the global talent gap as an imperative for strengthening the safety and resilience of Cyberspace. They noted the urgency of these efforts in addressing a worldwide shortage of 2.8m cybersecurity professionals whilst women are significantly underrepresented at only 24%. Through global partnerships on research, training, and mentorship, the WEC initiative works to foster a more diverse, inclusive workforce and advance more women to leadership.

Among the key themes of the session was how these collaborative efforts to bridge the gender talent gap can advance national resilience and long-term growth for the cybersecurity sector.

Fireside Chat

DEEP DIVE SESSIONS

QUANTUM SAFE

Accelerating the Enterprise Roadmap for Resilience in the Quantum Era

- **Michael Osborne,** CTO for Quantum Safe, IBM
- **Laura Buckwell,** Moderator

The advent of quantum computing holds profound implications for cybersecurity, and today's cryptographic systems are expected to be vulnerable between 2030 and 2035. There is strong emphasis on the urgency of transitioning to quantum-safe algorithms, as intercepted data can be stored now and decrypted later, a risk that threatens governments, militaries, and industries requiring long-term confidentiality.

While cryptography underpins digital trust, it is often overlooked, and sectors such as healthcare, automotive, and manufacturing lag financial services in readiness. The high cost of migration can be mitigated by aligning cryptographic upgrades with organizational lifecycles, minimizing disruption.

Participants stressed the need to elevate awareness among boards and C-suites, ensuring that security decisions extend beyond technical teams. As hyperscalers (organizations that provide cloud computing services on a massive scale) strengthen infrastructure, organizations should also secure backups and third-party tools.

Coordinated global action, building on European legislative momentum, will be essential to harmonize standards, safeguard supply chains, and prepare critical systems and consumers for the quantum era.

Fireside Chat

DEEP DIVE SESSIONS

GOVERNING CYBERSPACE

Understanding the Applicability of International Law

- **Andraz Kastelic,** Security and Technology Programme, United Nations Institute for Disarmament Research (UNIDIR)
- **Mauricio Zuazua,** Moderator

Debates on cyber governance increasingly center on how to interpret and enforce existing international legal frameworks rather than drafting new treaties. While experts have agreed since 2013 that international law applies to Cyberspace, consensus remains elusive on whether additional instruments are needed to address evolving threats. Core principles such as sovereignty, non-intervention, and state responsibility are interpreted inconsistently across regions, complicating coordination and enforcement. The intangible and cross-border nature of cyber incidents challenges traditional definitions of 'use of force,' particularly when attribution to specific actors or states is difficult.

Regional bodies, including the African Union and the EU, are shaping their own interpretations of international law, contributing to fragmented governance models. Ongoing UN initiatives through the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) continue to foster dialogue, though implementation remains uneven. For smaller states, international law continues to serve as both a deterrent and a protective mechanism in an interconnected digital order.

Fireside Chat

DEEP DIVE SESSIONS

FROM CLOUD TO EDGE

Building a Borderless Security Future

- **Haider Pasha,** Chief Security Officer, EMEA, Palo Alto Networks
- **Nisha Pillai,** Moderator

Cybersecurity has evolved from location-based defenses to identity-centered, borderless security models. Who a user is now matters more than where they are. Zero Trust should be viewed not as a product but as a continuous framework built on verification and least privilege access. Implementation demands strong governance across five layers (identity, device, access, transaction, and user experience) ensuring consistent enforcement.

AI has a growing role both as a defensive accelerator, reducing detection times from days to minutes, and as an enabler of more sophisticated attacks. AI systems themselves should be secured, as unregulated adoption, including generative AI use by employees, introduces new risks. Citing recent outages in a UK airport, the session reinforced the importance of supply chain resilience and ongoing board-level engagement to embed Zero Trust as an organizational culture rather than a one-time technology investment.

Fireside Chat

THE WORLD BANK

DEEP DIVE SESSIONS

CYBERSECURITY ECONOMICS FOR EMERGING MARKETS

- **Dr. Estefania Vergara Cobos,** Economist, World Bank
- **Jan Grasshoff,** Moderator

Cyber incidents increasingly pose significant economic risks for emerging markets, often surpassing the financial impact of natural disasters, especially in lower-income regions such as the Caribbean and Latin America. While the gap between developed and developing economies is narrowing, emerging markets remain more exposed to cyber threats due to weaker institutional frameworks and underdeveloped incident reporting mechanisms.

Information and communication technology (ICT) growth is most sustainable in countries that embed cybersecurity within legal and policy structures, supported by clear data protection laws that incentivize investment and mitigate systemic risk. Persistent challenges include low market transparency, limited vendor accountability, and chronic underreporting of breaches. Enhancing resilience requires both technical and non-technical stakeholders such as business leaders, educators, and regulators to improve cyber literacy and adopt standardized definitions for threats, incidents, and vulnerabilities. Consistent data collection and public awareness are essential to drive accountability and long-term economic stability.

Panel Discussion

unicef for every child | Child Helpline International

DEEP DIVE SESSIONS

CYBERSAFE FUTURES

The Evolving Role of Child Helplines to Protect Children in Cyberspace

- **Helen Mason,** Executive Director, Child Helpline International
- **Michael Marwa,** Director, The Tanzanian National Child Helpline
- **Dr. Afrooz Kaviani Johnson,** Moderator

The importance of unified child helplines is growing as essential infrastructure for safeguarding children from rising online risks. Speakers emphasized that accessible and trusted helplines not only provide immediate support but also generate real-time data that inform national policy and government response. In Tanzania, for instance, helplines manage over 10,000 daily contacts, with 15% relating to cyberbullying, underscoring the urgency of protection as two-thirds of adolescents now have an online presence. Despite this, only one in three children experiencing abuse report it, hindered by barriers to trust and accessibility.

Establishing a single, unified hotline was identified as vital to ensure consistent awareness and coordination across regions and telecom providers. Governments are increasingly using helpline data to shape policy, while collaboration among NGOs, telecoms, and technology platforms was recognized as key to building safer digital ecosystems that empower both children and parents.

Panel Discussion

DEEP DIVE SESSIONS

POWER UP

Empowering Cyber Women Leaders

- **Judith Ann Sarjeant,** Senior Manager - Cloud Security, CIBC Caribbean
- **Vesna Gabrić Kesina,** Senior Legal Advisor, Croatian Regulatory Authority for Network Industries (HAKOM)
- **Yemurai Rabvukwa,** WAF and DDOS Analyst, Cyber Careers Content Creator
- **Frida Inchoga,** Senior Manager, Digital Commerce and Industrial Policy, Tony Blair Institute for Global Change
- **Jim O'Connor,** Moderator

Amongst global efforts to advance women's participation and leadership in cybersecurity, training, mentorship, and visibility are key enablers of change. Global initiatives such as Women Empowerment in Cybersecurity (WEC), implemented by GCF, were highlighted for creating transformative opportunities through skill-building and community support. Despite this progress, persistent barriers remain, such as low STEM-to-cyber transition rates, with only 27% of Croatian women in STEM entering cyber careers, and deep-rooted cultural and confidence challenges in regions like Kenya.

The absence of visible role models and lingering imposter syndrome continue to deter qualified women from applying for roles. Speakers underscored the need for knowledge sharing, intentional mentorship, and targeted training to close representation gaps, particularly at mid- and senior-leadership levels. Cross-sector collaboration among government, media, and civil society is vital to normalizing women's presence in cybersecurity, where these programs empower pathways to both re-entry and leadership in the cyber workforce.

Panel Discussion

DEEP DIVE SESSIONS

SECURING PROSPERITY

Building Trustworthy AI Innovations

- **Srinivas Tummalapenta,** CTO, Security Services, IBM
- **Anand Kashyap,** CEO, Fortanix
- **Rob van Dale,** Moderator

AI is simultaneously driving innovation and heightening cybersecurity risks by expanding the scale, speed, and sophistication of threats. Attackers and defenders now leverage similar AI capabilities, reducing barriers to entry and accelerating attack velocity. Deepfakes, AI-generated phishing, and insider threats have emerged as critical challenges, making trust and authenticity central to digital resilience.

Building trustworthy AI requires identifying and protecting critical assets, applying secure-by-design principles, and maintaining human oversight to balance automation with accountability. Security should function as an enabler of innovation, embedded into product development rather than added retroactively. Ensuring shared responsibility across the supply chain through aligned vendor standards and consistent monitoring is vital to maintaining system integrity. Trustworthy AI depends on fairness, transparency, and explainability, supported by continuous validation, external verification, and sustained investment in AI security expertise and model testing.

Panel Discussion

SPOTLIGHT SESSIONS

THE QUANTUM LEAP – NAVIGATING THE FUTURE OF COMPUTING

- **Dr. Hesham Altaleb,** Vice- President of Research, Development & Innovation, SITE
- **Faisal Hamady,** Managing Director & Partner, BCG
- **Jan Grashoff,** Moderator

Quantum computing is projected to generate up to USD 850 billion in economic value across sectors such as pharmaceuticals, materials science, logistics, and finance, but it also introduces profound cybersecurity risks. Participants highlighted that while the technology promises to solve previously intractable problems through advanced simulation, optimization, and machine learning, it could simultaneously render current encryption standards obsolete once large-scale quantum systems become operational.

Early adopters are already gaining competitive advantages through pilot projects and research collaborations, but the global race for dominance in quantum hardware and algorithms remains highly concentrated among a few nations and corporations, amplifying inequality and dependency risks. A critical concern is that a sufficiently powerful quantum computer could compromise existing encryption protocols securing most of the world's communications and financial systems. To mitigate this, Post Quantum Cryptography was emphasized as the most immediate safeguard, with the U.S. NIST standardization process cited as the global benchmark for quantum-resistant algorithms.

The discussion also underscored the need for governments and enterprises to begin quantum readiness planning now, balancing investment in innovation with the urgency of defensive measures. Beyond risk mitigation, participants viewed quantum technology as a catalyst for national innovation, capable of redefining competitiveness and accelerating progress in science, industry, and security.

Panel Discussion

DEEP DIVE SESSIONS

THE CONVERGENCE EFFECT

The Future of Cyber Threats in an Age of Emerging Tech

- **George Patsis,** CEO, OBRELA
- **Rashed Alharbi,** VP, Cybersecurity Products, SITE
- **Prof. Nicolas Christin,** Faculty Member, CyLab Professor, Carnegie Mellon University
- **Nisha Pillai,** Moderator

The convergence of technology, data, and connectivity is reshaping the cyber threat landscape, creating both opportunities and systemic risks. As Cyberspace becomes a new domain of economic and strategic value, governance and policy frameworks lag. Organizations now operate within fragmented visibility caused by siloed tools and overlapping systems, underscoring the need for unified cyber ecosystems. While AI enhances real-time monitoring and accelerates threat detection, it also amplifies attack automation and scalability. Moreover, legacy weaknesses, unchecked data sharing, and late-stage security integration drive vulnerabilities and costs. Resilience depends on embedding security at the design stage, adopting Zero Trust principles, and simplifying overly complex architectures that undermine response effectiveness. Cybersecurity should therefore be treated not as a static product but as a dynamic, continuous process of adaptation, learning, and coordinated evolution across the global ecosystem.

Fireside Chat

DEEP DIVE SESSIONS

REBALANCING CYBERSECURITY AT HYPER SCALE

Cybersecurity Standardization, the Hidden Growing Force

- **Arnaud Taddei,** Chair, Study Group 17, Telecommunication Standardization Sector, ITU
- **Lukas de Sonnaville,** Moderator

The accelerating cost and complexity of global cybercrime, which has increased from USD 6 trillion to USD 10 trillion within four years, underscores the urgent need for cohesive international standards. The International Telecommunication Union (ITU) Study Group 17 is leading efforts to advance cybersecurity standardization, recognizing that fragmented national approaches are no longer sufficient to manage interconnectivity and shared vulnerabilities. Its work emphasizes multistakeholder collaboration among governments, the private sector, and academia to establish frameworks that can evolve alongside emerging threats.

A unified global model for cybersecurity protection remains a long-term goal, mirroring the consensus achieved in the 1980s on data protection standards. Through ongoing coordination, the ITU continues to serve as the primary platform for nations to strengthen collective defenses, harmonize technical standards, and foster a safer and more resilient digital ecosystem.

Fireside Chat

DEEP DIVE SESSIONS

THE FUTURE OF OT CYBERSECURITY

Building Resilience for the Industries and Infrastructures

- **Abdullah Aljallal,** Senior Commercial Director, Cyberani
- **Radu Balanescu,** Moderator

There are distinct risk dynamics between IT and OT environments, while IT focuses on protecting data availability, OT systems safeguard human lives and critical infrastructure. OT environments are inherently fragile and highly sensitive to downtime, demanding careful risk assessment, continuity planning, and proactive collaboration between IT and OT teams.

AI and machine learning enable adaptive defense, capable of learning normal system behavior and identifying anomalies in real time. However, resilience also depends on regular tabletop exercises, integrated monitoring, and embedding security into OT design from the outset rather than through retrofitting. Regulatory approaches should prioritize measurable outcomes over procedural compliance, while manufacturers and operators should adopt flexible, adaptive frameworks instead of rigid IT models. Ultimately, a cohesive, visibility-driven approach across IT and OT domains was presented as essential to achieving holistic, sustainable security

Panel Discussion

DEEP DIVE SESSIONS

THE FUTURE FORMULA

Women Shaping Tomorrow's Tech Frontier

- **Silvana Koch-Mehrin,** Founder and President, Women Political Leaders (WPL)
- **Carmen March,** President and CEO, United Cybersecurity Alliance and Global Council for Responsible AI
- **Salma Al-Rashid,** Moderator

Women currently make up only 24% of the global cybersecurity workforce, underscoring the persistent gender imbalance across the industry. Moreover, slow curriculum updates often taking up to six years leave education systems lagging industry needs, producing graduates unprepared for rapidly evolving cyber roles.

Bridging this readiness gap requires practical, hands-on training and applied workshops that equip women with the relevant skills and confidence to enter and advance in the field. Accelerators, mentorship programs, and tuition-free certifications were identified as effective pathways for career growth, helping women build networks and secure opportunities through internships and recruitment partnerships.

Despite progress, data suggests that at the current rate, full gender parity could take over a century to achieve. Therefore, leadership commitment remains critical to driving systemic change, challenging misconceptions about women's capability or ambition, and ensuring that inclusive education and career pathways become a sustained priority.

Briefing

DEEP DIVE SESSIONS

CLICKS, AND LINKS, AND URLS — OH MY!

How Organized Crime Exploits the Web

- **Ottavia Galuzzi,** Associate Expert, United Nations Interregional Crime and Justice Research Institute (UNICRI)
- **Odhran McCarthy,** Liaison Officer, United Nations Interregional Crime and Justice Research Institute (UNICRI)
- **Janey Young, Consultant,** United Nations Interregional Crime and Justice Research Institute (UNICRI)

The session marked the launch of the report "Clicks & Links & Tricks, oh My!," which examines how domains, URLs, and web traffic systems, which were designed to sustain the Internet in confidence, are being exploited to sustain serious and organized crime.

Fireside Chat

DEEP DIVE SESSIONS

FROM DATA TO ACTION

Launching the Child Protection in Cyberspace Index

- **Dr. Yuhyun Park,** Founder and CEO, DQ Institute
- **Nisha Pillai,** Moderator

The Child Protection in Cyberspace (CPC) Index has been launched, in alignment with the strategic goals of the global initiative initiated by His Royal Highness Prince Mohammed bin Salman bin Abdulaziz Al Saud, building on sustained efforts since 2018 to advance online child safety. The Index serves as a unified checklist rather than a ranking, helping nations evaluate and strengthen their cyber protection systems.

Findings revealed that 76% of children aged 8–18 faced at least one cyber risk in 2023–2025, up from 72% during the COVID-19 pandemic — and largely unchanged for nearly a decade.

Children's exposure to cyber threats is driven by increased screen time, AI acceleration, and post-pandemic digital reliance, with children from low-income households remaining the most vulnerable, underscoring the urgency of coordinated intervention.

Multi-stakeholder collaboration among governments, companies, educators, and families is vital to reducing online risks by 15% within five years. Examples such as Australia's dedicated child safety agency and age-verification measures on social media illustrated actionable policy progress.

Briefing

SIMULATIONS

ENTERPRISE COMPASS – CYBER RESILIENCE AND PREPAREDNESS SIMULATION FOR BUSINESS LEADERS

- **Prof. Dr. Marco Gercke,** Director, Cybercrime Research Institute

The Enterprise Compass simulation placed senior executives in a realistic, high-pressure scenario involving a major system outage caused by a ransomware campaign, testing leadership in a climate of uncertainty. The exercise demonstrated that clarity, calmness, and decisive communication often determine crisis outcomes more than technical tools. It revealed that while most crisis management frameworks are technically sound, they remain operationally fragile when leadership teams are not directly engaged in rehearsals.

Participants emphasized that true resilience requires an enterprise-wide culture of preparedness extending beyond IT or compliance functions to include legal, communications, and business units. No two crises are identical, and organizations should tailor their strategies to their specific risk appetites, regulatory contexts, and customer expectations. Maintaining offline playbooks and manual fallback systems were identified as critical to ensuring continuity when digital coordination tools fail. Effective communication with boards, regulators, and stakeholders should balance transparency with control, providing clear information without amplifying panic or reputational damage.

The session concluded with a call to institutionalize post-incident learning through documented reviews, updated playbooks, and anonymized knowledge-sharing to strengthen collective resilience across industries.

Panel Discussion

DEEP DIVE SESSIONS

THE CYBER EFFECT

Understanding Technology's Impact on Human Behavior

- **Nirali Bhatia,** Cyber Psychologist & Psychotherapist, Founder Director, Nirali Bhatia Cyber Wellness Foundation
- **Sonali Patankar,** Founder & CEO, Responsible Netism
- **Alexandra Topalian,** Moderator

Online environments are increasingly shaping human behavior and social interaction, often encouraging actions and ideologies that individuals might avoid in offline settings, such as trolling or toxic engagement. Children are particularly vulnerable, facing psychological and emotional risks tied to validation-seeking, exposure to sexual content, and the normalization of violence from an early age.

Strengthening digital wellbeing requires preventive education that helps children identify red flags, complemented by psychological and legal support for victims. Communities should set clear boundaries around screen time and promote digital hygiene within safe, nonjudgmental spaces. Collaboration with technology companies remains essential, but safety-by-design measures are needed to prevent harm before it occurs. Parents, schools, and regulators play a critical role, supported by laws such as the UK's Online Safety Act.

Ensuring AI remains a human-aided tool, increasing awareness of algorithmic bias, and fostering digital empathy are all central to building long-term cyber resilience and emotional safety online.

Briefing

DEEP DIVE SESSIONS

ADVANCING RESPONSIBLE STATE BEHAVIOR IN CYBERSPACE

- **Virginia Browning,** Programme Management Officer, UN Office for Disarmament Affairs

Discussions on responsible state behavior in Cyberspace continue to center on developing voluntary, normative frameworks rather than binding international treaties. While there is broad agreement on the need for clear principles, progress remains limited to non-binding commitments, and no formal mechanisms currently exist to monitor or assess state adherence to these norms.

Efforts are underway to design a system for tracking compliance, though its future implementation depends on achieving consensus among member states. Supply chain security has been recognized as a shared concern, yet concrete collaborative measures or coordinated policies have not been established. The dialogue reflects a transitional phase in global cyber governance shifting from conceptual agreement toward the need for practical accountability structures and measurable adherence frameworks.

COMMUNITY MEETINGS

CCE MEETINGS

Riyadh
Centre for Cyber
Economics

EXECUTIVE COMMITTEE MEETING

The Centre for Cyber Economics (CCE) aims to establish a trusted, data-driven benchmark for understanding the economic impact of cybersecurity, filling a long-standing evidence gap for policymakers and industry leaders. Its first publication will serve as the foundation for standardized measurement across studies, integrating insights from economics, cyber risk, and national resilience. Drawing on established analogues such as disaster loss modeling, the Centre will apply similar methodologies to quantify the ripple effects of cyber incidents on critical infrastructure, comparing outcomes to those from natural disasters to better gauge scale and consequences.

Existing datasets from organizations like the World Bank and Mastercard will support the creation of a continuously updated, publicly accessible database. CCE also plans to form partnerships that define what to collect, how to analyze it, and how to translate findings into practical frameworks that improve cross-sector comparability.

Attribution remains a complex issue, as nation-state and non-state tactics increasingly overlap, requiring refined models to distinguish intent and systemic impact. Ultimately, assessing the economic cost of cyber incidents demands robust metrics that account for both direct losses and secondary effects, supported by international cooperation and consistent data validation to ensure credibility and long-term sustainability.

CCE MEETINGS

Riyadh
Centre for Cyber
Economics

CYBERSECURITY WORKFORCE DEVELOPMENT

The global cybersecurity workforce shortage exceeds 2.8 million professionals, exposing a systemic shortfall in specialized technical skills such as OT security, cloud architecture, and quantitative analysis. Persistent mismatches between education and industry needs highlight the urgency of modernizing curricula and integrating continuous, industry-aligned training into professional development.

The World Economic Forum's Strategic Cyber Talent Framework built on attracting, building, collaborating, and retaining talent offers a scalable foundation for structured workforce growth. GCC economies demonstrate strength in policy and governance but face deficits in hands-on technical and analytical expertise, requiring targeted reskilling programs. Retention challenges among mid-career professionals reinforce the importance of well-being, inclusivity, and recognition as drivers of long-term engagement.

Closing the talent gap will depend on public-private partnerships that align training outcomes with national digital strategies, ensuring skills development is measurable, sustainable, and directly relevant to evolving market demands.

CCE MEETINGS

Riyadh Centre for Cyber Economics

QUANTIFYING THE ECONOMIC IMPACT OF CYBER INCIDENTS

Cyber incidents are now recognized as economic shocks that ripple far beyond IT departments, disrupting productivity, investor confidence, and even GDP in digitally dependent economies. Many organizations still lack the tools to measure true financial exposure, as risk assessments often focus on vulnerabilities rather than business outcomes. The absence of standardized quantification models leads to inconsistent reporting and underestimation of both company-level and macroeconomic impacts.

Effective frameworks should consider both the probability and consequence of an attack, including downtime, regulatory penalties, reputational loss, and insurance implications. Communication gaps between executives and boards remain a major barrier, as cybersecurity success is difficult to quantify when measured by incidents that do not occur. Translating resilience into financial concepts such as avoided losses and operational continuity is key to sustaining investment and funding.

Cyber insurance markets are emerging as both stabilizers and data sources for quantifying aggregate risk, though inconsistent claim classification continues to distort pricing. Small and medium enterprises remain especially vulnerable, facing higher losses per incident and limited access to affordable insurance or analytics expertise. Standardized models and transparent reporting could bridge these gaps, making cyber risk management a measurable component of economic resilience.




CCE MEETINGS

Riyadh Centre for Cyber Economics

THE MACROECONOMIC IMPACT OF CYBERSECURITY

Cybersecurity is increasingly recognized as a macroeconomic issue that directly influences growth, investment, and national competitiveness. Economists estimate that cyber incidents collectively reduce global GDP by around 1.5% annually through lost productivity, supply chain disruptions, and declining consumer confidence.

The discussion highlighted the 'invisible nature' of cyber losses, as most incidents remain underreported, distorting economic data and complicating policy responses. The interconnected nature of global networks means that a single failure, such as a shared software vulnerability or cloud outage, can trigger systemic shocks across multiple sectors, mirroring the contagion effects of traditional financial crises. Participants emphasized that restoring trust after such shocks requires coordinated fiscal and policy interventions at both national and international levels. AI-driven analytics were identified as a tool for improving macro-level understanding by aggregating incident data from across industries and markets.

The healthcare, energy, and critical infrastructure sectors were cited as facing the highest economic burden, given their dual exposure to operational disruption and human impact. The insurance industry was recognized as an underutilized source of actuarial data that could help quantify national cyber exposure, enabling policymakers to better measure and manage the economic cost of digital risk.






CCE MEETINGS

WORLD ECONOMIC FORUM | Riyadh Centre for Cyber Economics

MEASURING CYBER RESILIENCE - FROM INSIGHT TO ACTION

Cyber resilience is now viewed as both an economic and strategic necessity rather than a purely technical goal. As disruptions to cyber operations increasingly affect GDP, productivity, and public trust, leaders agreed that resilience should focus on recovery speed and adaptability, not just prevention. Participants noted that most organizations still measure cybersecurity through compliance metrics, which overlook operational continuity and real-world readiness.

A proposed Cyber Resilience Index would integrate indicators such as preparedness, detection capability, recovery time, and dependency on third parties, creating a standardized benchmark across industries and countries. Red teaming and proactive testing were recognized as practical tools for gathering data beyond theoretical models, helping organizations evaluate their ability to absorb and recover from shocks.

Government participants emphasized the value of mandatory incident reporting, especially for critical infrastructure, to build national datasets and improve benchmarking. Balance between regulation and innovation is needed, while compliance is necessary to ensure accountability, excessive rigidity can slow adaptation and stifle innovation in managing evolving cyber threats.

OTC CoE MEETING

CENTER OF EXCELLENCE OPERATIONAL TECHNOLOGY CYBERSECURITY

OTC COE MEMBERS MEETING

Cybersecurity in the energy sector is becoming a global priority as the convergence of IT, OT, and AI creates complex and high-stakes vulnerabilities. Accounting for roughly 11% of all incidents worldwide, and with ransomware responsible for nearly 40% of energy-related breaches, the sector's resilience now depends on unified standards and proactive collaboration.

The Operational Technology Cybersecurity Centre of Excellence (OTC CoE), established in 2024 and set for independent operation by 2027, aims to harmonize global frameworks, advance applied research, and drive capability development across regions. The introduction of the Cyber HAZOP reframes cyber risk as an operational hazard, integrating safety and security through 'design for breach' principles and Zero Trust architectures.

Participants stressed that the greatest workforce gap lies not in engineering talent but in leadership-level literacy, calling for cross-disciplinary education and sector-wide alignment to embed cybersecurity into operational culture, regulation, and business continuity strategies.

IMPACT NETWORK MEETING

IMPACT NETWORK – PROTECTION OF CRITICAL INFRASTRUCTURE

The protection of critical infrastructure is increasingly viewed as both a national security and humanitarian priority, as attacks on hospitals, utilities, and transportation systems now carry severe social and economic consequences. The Digital Emblem Project by the International Committee of the Red Cross (ICRC) and supported by the ITU and Microsoft, was presented as a cyber equivalent of the Red Cross symbol, marking humanitarian digital assets as protected under international law. The emblem aims to signal that certain digital systems, such as those supporting emergency communications or civil protection, should never be targeted in conflict or peacetime.

Microsoft reaffirmed its support for the effort, citing the rising frequency of attacks on medical and humanitarian services, while the ITU emphasized its role in codifying standards to ensure interoperability across jurisdictions. Private-sector partners, including Broadcom, stressed the need for shared situational awareness and coordinated intelligence as foundational to defending these systems, particularly as the boundary between military and civilian cyber operations continues to blur.

A proposed next step is the creation of machine-readable 'do-not-target' lists, enabling AI systems to automatically identify and respect protected digital assets. This initiative represents a significant step toward embedding humanitarian principles within the rules of digital conflict and global cyber governance.

KNOWLEDGE COMMUNITY MEEETING

Led by:

RIYADH AIR
طيران الرياض

SECURING THE FUTURE SKIES

The Securing the Future Skies Knowledge Community was formally launched to advance global collaboration on aviation cybersecurity, bringing together stakeholders from industry, government, and academia.

The community will follow a four-phase roadmap through 2026 focused on governance setup, research development, peer review, and publication. Initial research themes include safety security convergence in aviation risk management, AI in predictive threat detection and response, quantum readiness for post quantum resilience, and securing connected aircraft within IoT enabled aviation ecosystems. Participants also proposed additional priorities such as supply chain security, decentralized identity management, data privacy, and resilience planning to ensure rapid recovery after cyber incidents.

Discussions emphasized integrating overlapping topics into a unified framework that connects aviation safety, cybersecurity, and IoT connectivity under one strategy. The partnership with Riyadh Air was recognized as instrumental in positioning the GCC as a leading regional hub for aviation cybersecurity research and implementation.

Members agreed on the need for pragmatic, evidence based projects that strengthen both operational safety and cyber resilience while maintaining wide stakeholder engagement to ensure impactful and measurable outcomes in the community's first publication cycle.

KNOWLEDGE COMMUNITY MEEETING

Led by:

FUTURE OF CYBERSECURITY

The Cyber Horizon 2025 report, developed by the Future of Cybersecurity Knowledge Community, was presented as a global foresight study outlining the major forces shaping cybersecurity strategy through 2030. Drawing on input from more than 800 experts across 60 countries, the report identified five systemic trends: AI-driven disinformation eroding public trust, concentration of technological power among a few global providers, proliferation of synthetic identities, emergence of autonomous attacks, and growing interdependence risks from connected systems. Together, these trends mark cybersecurity's evolution from a technical challenge to a strategic and societal issue requiring anticipatory governance.

The findings revealed that more than half of known risks are expected to mature within the next three years, underscoring the urgency of regulatory modernization and cross sector collaboration. Discussions emphasized the importance of cooperation on AI regulation, post quantum readiness, and digital sovereignty, along with human capital development and inclusion to close global skills gaps. The report also positioned trust, autonomy, and foresight as the next pillars of cyber resilience, offering a long-term roadmap for policymakers and industry leaders.

The overarching conclusion was clear: securing the future of Cyberspace will depend on leadership, coordination, and evidence-based action that links policy, technology, and social impact.

KNOWLEDGE COMMUNITY MEEETING

Led by: stc

SAFEGUARDING THE FUTURE NETWORKS AND EMERGING TECHNOLOGIES

The Knowledge Community has grown into a global platform advancing telecom and emerging technology resilience, connecting over 30 organizations. In 2025 it produced two flagship reports that set out a blueprint for strengthening ICT infrastructure and addressing the cybersecurity challenges of AI-driven telecom networks.

The first report, A Global Blueprint for Trusted ICT Infrastructure, projected billions in potential roaming fraud losses by 2028 and highlighted gaps in signaling security, workforce skills, and risks from 5G and edge technologies.

The second report, Intelligent Defense, explored the role of AI in telecom security, endorsing AI-powered security operations centers as best practice for threat anticipation and response. Participants stressed that responsible AI should include transparency, accountability, and human oversight to prevent misuse.

Both reports reinforced that human judgment and collaboration remain central to building resilient networks, linking innovation with governance and ensuring that technological progress serves public trust and safety.

HOSTED EVENTS

TRACK 1.5 EU-GCC CYBER DIALOGUE

The EU GCC Cyber Dialogue opened with a shared call to strengthen cooperation against increasingly sophisticated cyber threats shaped by geopolitical tensions and rapid technological change. The discussion noted that attack patterns are shifting toward smaller enterprises, which are increasingly used as entry points into larger networks, emphasizing the need for tailored protection strategies. References to state backed operations reinforced the urgency of enhancing deterrence mechanisms and attribution capabilities.

Experts highlighted that cyber threats carry both technical and social dimensions, combining ransomware, DDoS, and deepfake campaigns with manipulation and disinformation targeting vulnerable groups. European participants distinguished between noisy and stealth attacks, underscoring the importance of detecting low signature activity that often evades conventional monitoring. The supply chain ransomware nexus was cited as a systemic risk, with examples from the transport and automotive sectors showing how vendor compromises can trigger economic disruptions and financial intervention.

The session also identified human factors, such as insider risk and low awareness, as persistent vulnerabilities that amplify exposure in public sector environments. GCC representatives called for clearer cryptocurrency regulation, sovereign R&D investment, and oversight on spyware use to reduce foreign dependency. The dialogue that joint intelligence sharing, harmonized policies, and mutual recognition of cybersecurity standards are essential to achieving operational alignment between the EU and GCC regions.

Regulatory efforts for Critical National Infrastructure (CNI) remain uneven across the EU and GCC, with enforcement and compliance emerging as shared challenges. EU frameworks tend to prioritize governance and reporting obligations, while GCC models, such as those applied in Qatar, favor more flexible, outcome-oriented approaches. Despite policy progress, compliance remains a weak point as many systems lack real-time monitoring, automation, and cross-border reporting mechanisms. Moreover, workforce shortages extend beyond cybersecurity professionals to general IT functions, where secure-by-design training is still limited.

Overregulation was identified as a growing concern, with practical, risk-based models proving more effective in driving innovation and measurable resilience. Strengthening multilateral cooperation, harmonized reporting standards, and integrated workforce development are recognized as critical steps toward achieving a more coherent and adaptive regional cybersecurity ecosystem.

The second EU-GCC Cyber Dialogue continued discussions from the previous session, focusing on building joint resilience strategies and advancing policy alignment. The conversation addressed shared challenges such as ransomware, supply chain vulnerabilities, and the misuse of AI, emphasizing the need for coordinated responses and stronger institutional cooperation. ENISA's trusted providers initiative was presented as a model for improving transparency and accountability in cybersecurity supply chains, while the EU Cyber Resilience Act was highlighted as a key framework for enhancing vulnerability monitoring and disclosure. GCC representatives linked cyber resilience to economic security and diplomatic stability, describing it as a cornerstone of national reputation and continuity.

Both regions acknowledged their overreliance on foreign vendors and underscored the importance of diversifying partnerships through harmonized standards and regulatory collaboration. The dialogue expanded to include AI and quantum governance, with participants stressing the need for transparency, bias control, and human oversight in AI systems, as well as joint pilots to test post quantum cryptography readiness.

The closing dialogue underscored that cyber capacity building is not only a technical investment but also a cornerstone of national resilience and cyber sovereignty. With the global cybersecurity workforce gap now exceeding 2.8 million professionals, participants agreed that quality, specialization, and leadership development matter more than volume.

Collaboration across governments, private sector entities, and academia was reaffirmed as essential to sustainable progress. Saudi Arabia's Global Initiative for Capacity Building in Cyberspace, launched in partnership with the United Nations and other global stakeholders, was cited as a scalable model for cross-border skills development and knowledge transfer. The EU highlighted its €120 million investment in global capacity programs since 2010, spanning cybersecurity, cybercrime prevention, and data governance. Examples such as Bahrain's integration of cybersecurity and AI education showcased practical national implementation.

The dialogue closed with a shared commitment to deepen EU-GCC cooperation on education, retention, and digital transformation through the GCF and future multilateral initiatives.

CXO MEETINGS

ARAB CXO

Regional cybersecurity CxOs emphasized that collaboration and intelligence sharing are fundamental to building collective resilience across the Arab world. A unified regional threat intelligence platform was identified as essential to enable secure communication, coordinated responses, and trust between public and private entities. The discussion highlighted the growing role of startups in driving innovation and urged the creation of open databases, incubators, and standardized testing frameworks to accelerate product development and adoption.

Establishing a shared directory of cybersecurity providers and customers would enhance visibility and strengthen partnerships, while educational frameworks and training programs should evolve to close talent gaps and promote regional expertise. Participants agreed that transparency and governance are vital to overcoming hesitancy around information exchange, and that joint university–industry initiatives can anchor regional R&D capacity, positioning Arab nations as active contributors to global cybersecurity innovation rather than passive technology adopters.

WEF MEETINGS

CLOSING THE GAP – APPROACHES TOWARDS CYBER EQUITY

Cyber inequity is widening the gap between nations and sectors with strong cybersecurity infrastructure and those lacking even basic defensive or policy capabilities. This divide often mirrors broader economic inequalities, separating developed and emerging economies, large corporations and small businesses, and urban and rural communities.

Only a small fraction of organizations (about 13%) feel confident in their current cybersecurity skills, while incidents continue to rise sharply. Small and mid-sized enterprises face the highest per-incident losses but remain underrepresented in cybersecurity investment, making them particularly vulnerable within supply chains. The education sector also shows persistent underinvestment in digital safety, leaving youth and academia exposed. Vulnerable groups such as older adults and less-educated populations are more frequently targeted by misinformation and online exploitation.

Gender inclusion emerged as a recurring theme, recognized not only as a fairness issue but as a strategic factor for resilience, given that women represent just one-quarter of the global cybersecurity workforce. Public-private partnerships can play a decisive role in closing capability gaps by combining technology innovation, policy frameworks, and academic research. Building cognitive diversity and bringing more women and nontraditional entrants into the field enhances problem-solving, strengthens resilience, and promotes more equitable digital security outcomes.

03

SHAPING THE GLOBAL CONVERSATION

KEY TAKEAWAYS

In line with this year's Annual Meeting theme, "Scaling Cohesive Advancement in Cyberspace," two days of in-depth discussions brought forward a set of strategic imperatives for increased momentum in collectively addressing cybersecurity challenges and opportunities. In addition to the insights generated by each session, summarized in this book, the Annual Meeting 2025 identified four cross-cutting imperatives for global collaboration in Cyberspace that are critical to shaping a secure and prosperous future for all.

As an action-oriented platform, empowered by its community and partners, GCF will continue to elevate the scale and impact of its targeted global initiatives, knowledge creation, multistakeholder platforms, specialized centers and collaborative projects to address these imperatives and drive sustained global progress.

IMPERATIVE #1

FORGING A GLOBAL COOPERATIVE, AND TRUSTED CYBERSPACE

Uniting nations, institutions, and industries behind shared standards, and enforceable norms keeping pace with technological innovation to preserve stability and global trust.

As Cyberspace becomes increasingly interconnected and strategically contested, the lack of harmonized governance and consistent enforcement continues to heighten global vulnerability. The GCF Annual Meeting 2025 emphasized that effective cyber diplomacy, rooted in transparency, accountability, and mutual trust, is essential to maintaining an open, secure, and inclusive cyber environment.

Throughout the discussions, participants identified fragmented rules and the uneven application of standards as key obstacles to resilience. Experts from government, industry, and academia cautioned that without a shared regulatory foundation, cooperation to address risks can give way to unilateral action and competing cyber spheres.

Sessions such as **Against the Odds: Gaining Consensus Amid Complexity** and **Converging Crisis: The Future of Cyberspace in Complex Global Dynamics** underscored that practical, multi-stakeholder diplomacy remains indispensable for achieving coherence in global cyber governance and restoring confidence across borders.

This focus extended into the legal domain in **Cyber Law: Regulating the Next Tech Revolution**, where panelists examined how national frameworks are adapting to emerging technologies. Examples of regional alignment and modernization of cybersecurity laws illustrated that agile, principle-based regulation, supported by cross-border coordination, can strengthen consistency and enforceability. In **The Future of Cyber Diplomacy: Key Forces of Change and Strategic Outlook,** participants considered how diplomatic frameworks should evolve to reflect technological realities and geopolitical shifts.

The outcome was clear: a well-governed Cyberspace is now fundamental to international stability. Advancing this goal requires stronger diplomatic engagement, alignment of standards, and a shared understanding of responsibility across the cyber ecosystem. GCF will continue to champion this agenda, translating the insights from the 2025 Annual Meeting into practical pathways for cohesive and enduring global cooperation.

IMPERATIVE #2

ELEVATING GLOBAL CYBER CAPACITY AND WORKFORCE RESILIENCE

Advancing education, innovation, and inclusion to cultivate the human capital essential for global cyber resilience.

The scaling of cybersecurity capability worldwide continues to be constrained by the limited availability of talent. Closing the global cybersecurity workforce gap, now exceeding 2.8 million professionals, is essential to enabling every nation to contribute meaningfully to collective resilience and economic growth. The 2025 Annual Meeting reaffirmed that capacity building is not solely a technical exercise but a strategic investment in people, institutions, and inclusion.

Participants across sessions emphasized that the talent shortage undermines sectoral growth, deepens inequality, and widens the divide between developed and developing nations. Discussions such as **Strength in Reinforcements: Building Capacity for the Global South** and **From Gaps to Gains: Scaling Global Cyber Capability Development** revealed how underinvestment, legacy infrastructure, and fragmented governance continue to leave developing regions vulnerable. Panelists stressed that equitable access to training, mentorship, and resources should be supported by predictable funding and regional delivery mechanisms to convert ambition into resilience.

Inclusion emerged as a defining factor of sustainable progress. **Shaping Resilience: Investing in Women as a Global Economic Imperative** and **The Talent Imperative: Unlocking the Power of Women in Cyber** underscored that diverse and inclusive workforces are essential to national resilience, innovation, and long-term prosperity.

Women now represent 24% of the global cybersecurity workforce, up from 10% a decade ago, reflecting meaningful progress yet also highlighting the need for continued investment in targeted support, mentorship, and advancement opportunities. Broader economic studies suggest that closing the global gender gap could add up to USD 28 trillion to annual GDP, a reminder that advancing women's participation in cybersecurity is not only a matter of equity but also a driver of global growth and shared prosperity.

A milestone at the GCF Annual Meeting 2025 was the launch of the Global Initiative for Capacity Building in Cyberspace, la cooperation between the Saudi Information Technology Company (SITE) and GCF, and in partnership with the United Nations and its specialized agencies. This initiative will mobilize global expertise to accelerate capacity development at scale, addressing areas of greatest need and strengthening collective resilience.

GCF will build on this momentum by advancing research, publications, and programmatic initiatives that translate this year's discussions on capacity building and workforce development into tangible and measurable outcomes. Following the insights from the 2024 Cybersecurity Workforce Report, GCF will deepen its efforts to foster inclusion in the cybersecurity sector through strategic thought leadership, targeted training, and the development of diverse talent pipelines.

IMPERATIVE #3

UNPACKING CYBERSECURITY'S GLOBAL ECONOMIC VALUE

Demonstrating how cybersecurity drives innovation, safeguards value creation, and underpins long-term prosperity in the digital economy.

Cybersecurity has too often been framed as a cost center rather than a source of economic strength. Reframing it as a driver of value creation is essential to sustaining global prosperity. The GCF Annual Meeting 2025 emphasized that cybersecurity not only protects national and institutional interests but also generates tangible economic returns by reinforcing productivity, investment confidence, and innovation. It is now understood as a cornerstone of economic stability and long-term growth.

Sessions such as **The Economic Dimension of Cyberspace** and Cybersecurity as an **Economic Imperative: Driving Growth in the Global Economy** illustrated how investment in cyber resilience directly correlates with national competitiveness. Participants highlighted that only 4% of global ICT spending is allocated to cybersecurity, while annual losses from cyber incidents are projected to surpass USD 10 trillion. Strengthening national preparedness for cyber incidents (from the bottom 25% to the top 25%) can increase GDP per capita by up to 1.5%, underscoring cybersecurity's role as a measurable driver of growth.

Sectoral discussions reinforced this economic linkage. **Powering Tomorrow: The Economic Imperative for Securing the Global Energy Supply Chain** and **Reinforcing the Links: Securing Global Energy Supply Chains** revealed that one in ten cyberattacks targets the energy sector, while attacks on operational technology continue to rise.

These incidents demonstrate the cost of underinvestment in protection and the economic value of proactive resilience. **Funding the Future of Cyber** and **Securing Investment: Why Cybersecurity is a Key Imperative for FDI** further showed that investor confidence increasingly hinges on the maturity of national cybersecurity frameworks.

In collaboration with the World Economic Forum, GCF co-hosted community meetings that advanced the global conversation on cyber economics. These sessions brought together cross-sector experts to examine cybersecurity's macroeconomic impact, its role in workforce development, and the quantification of economic losses.

Looking ahead, GCF will continue to deepen understanding of cybersecurity's economic dimension and drive global collaboration through the Centre for Cyber Economics. By developing robust analytical tools and expanding data collection across public and private sectors, this effort will provide a comprehensive map of cybersecurity's value creation and its central role in shaping resilient, competitive economies.

IMPERATIVE #4

SCALING GLOBAL PREPAREDNESS TO A NEW ERA OF CYBER THREATS

Strengthening foresight, coordination, and agility to ensure collective preparedness keeps pace with the accelerating scale, speed, and sophistication of global cyber threats.

The acceleration of artificial intelligence, quantum computing, and the connectivity of supply chains is reshaping cybersecurity challenges in both scale and complexity. No single nation or organization can address these risks in isolation. The 2025 Annual Meeting reaffirmed that future cyber resilience depends on collaborative action, interoperability, and shared situational awareness across borders and sectors.

Discussions throughout the event underscored the growing uncertainty and systemic vulnerability created by a continuously evolving threat landscape. Sessions such as **AI for Security and Security for AI: Ensuring Resilience and Building Trust** and **The Q-Cyber Frontier: Harnessing Quantum Innovation for Cyber Resilience** examined how emerging technologies are redefining both attack and defense paradigms.

Participants highlighted the tension between fostering innovation and maintaining security, noting that quantum computing could render current encryption methods obsolete by 2030. The urgency of adopting post-quantum cryptographic standards was recognized as a key component of global readiness.

The imperative for coordinated defense was further emphasized in sessions such as **Defending the Grid: Uniting Forces to Protect Critical Infrastructure** and **The Cyber Frontier: Harnessing Emerging Tech for Global Security.** These discussions demonstrated how interconnectivity across critical sectors creates cascading vulnerabilities that demand joint action.

More than 420 million cyberattacks were recorded against critical infrastructure within a single year, while operational technology systems have faced a surge in targeted incidents, highlighting the scale of exposure. **Next-Gen Cyber Resilience: Turning Tech Disruption into Security Innovation** reinforced that future-proof resilience depends on cross-sector collaboration, underpinned by regulatory frameworks such as the EU Cyber Resilience Act, which embeds security by design across digital products and services.

The outcomes of these discussions will guide GCF's continued work in strengthening global preparedness for the next generation of cyber risks. Advancing cohesive action, real-time information sharing, and coordinated protection of critical infrastructure are now essential priorities. The path forward lies in building collective foresight and adaptive defense strategies that ensure technological innovation and security evolve together.

REACHING A WIDER AUDIENCE GLOBALLY

GCF established several strategic media partnerships, engaged extensively with local, regional, international, and trade publications, and executed a dynamic social media campaign before, during, and following the GCF Annual Meeting 2025 – ultimately amplifying insights and the conversation on key priorities in Cyberspace to a wider global audience. These conversations are imperative given the borderless nature of Cyberspace, with the resounding message at this year's event being that no individual, nation, or organization can address the issues we face alone.

MEDIA COVERAGE AND OUTREACH - KEY FIGURES

LIVE STUDIO

134
Media interviews

81+
News platforms reached

MOMENTS OF GENIUS

3.9M
Impressions

25.5K
Hours of watch time

EARNED COVERAGE

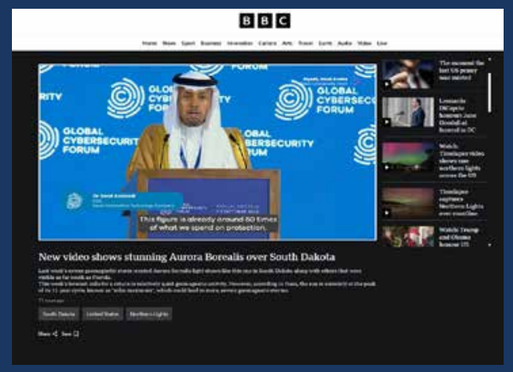
100+
News platforms reached

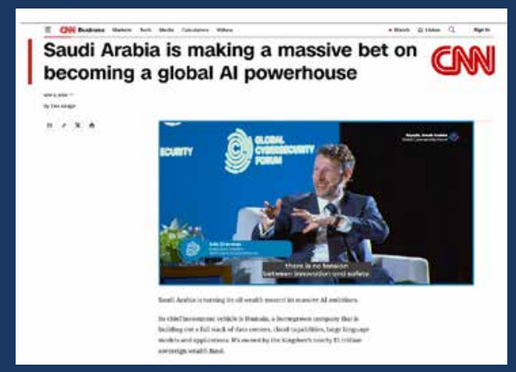
450M
Total reach

MEDIA PARTNERS

5
Global Partners Delivered

40+
Pieces of coverage delivered by partners





MEDIA OUTREACH & IMPACTS

LIVE STUDIO

The GCF Live Studio is an innovative platform enabling real-time connections and interviews with global news networks directly from the Annual Meeting. In 2025, the Live Studio expanded to three on-ground locations, all running simultaneously. This strategic expansion nearly doubled overall coverage and channels reached worldwide.

LIVE STUDIO KEY FIGURES

134 Interviews and coverage facilitated from the Live Studio

81 Individual channels reached across Africa, Asia, Europe and North America

MOMENTS OF GENIUS

GCF's 'Moments of Genius' campaign captured impactful 30-60 second soundbites from a selection of global decision-makers and experts participating in the Annual Meeting 2025, each showcasing thought leadership on issues across the cyber landscape. The 16 episodes were distributed along with GCF branding to leading news websites across the world, bringing GCF and the insights shared during the Annual Meeting to a global audience.

MoG KEY FIGURES

16 Moments of Genius episodes distributed

3.9M Total impressions

25.5K Total hours of footage watched

91% Viewability

MEDIA OUTLETS

GCF MEDIA PARTNERS

CGTN

GCF partnered with China Global Television Network (CGTN) to deliver live editorial, broadcast, online and social coverage from a branded booth at the Annual Meeting. Headquartered in Beijing, CGTN TV channels are available in more than 160 countries and regions worldwide.

cna

GCF partnered with CNA to deliver editorial, broadcast, online and social coverage of the Annual Meeting.

A Singapore-based global news brand with a diverse slate of news, current affairs, and documentaries, CNA is viewed in 29 territories across Asia with its satellite footprint stretching across Asia, the Middle East and Australia.

euronews. africanews.

GCF partnered with Euronews and Africanews, who delivered editorial, broadcast, online and social coverage from a branded booth on-site.

Headquartered in Lyon, France, Euronews broadcasts news and programming to a worldwide audience in 17 languages, and its independent sister channel Africanews is a 24/7 multiplatform, multilingual news service network broadcasting from Congo.

上海广播电视台 SMG SHANGHAI MEDIA GROUP

GCF partnered with Shanghai Media Group (SMG), one of China's largest and most diverse provincial media and cultural conglomerates. An SMG team moderated sessions and delivered live on-ground editorial, broadcast, online and social coverage, including an 11-minute feature documentary that included GCF Live Studio interviews.

العربية
alarabiya

GCF partnered with leading 24-hour digital news platform, Al Arabiya, to provide multi-platform editorial coverage to a global audience and strengthen visibility among a Tier 1 regional business news audience.

As part of the extensive coverage during the Annual Meeting, Al Arabiya aired special thematic bulletins focused on cybersecurity, education, and child protection, featuring short soundbites and insights from GCF experts.

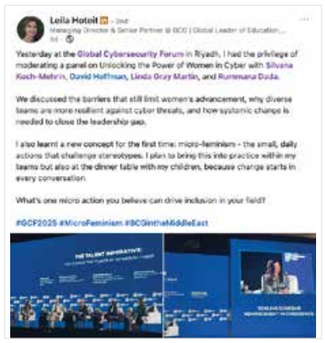
24KZ

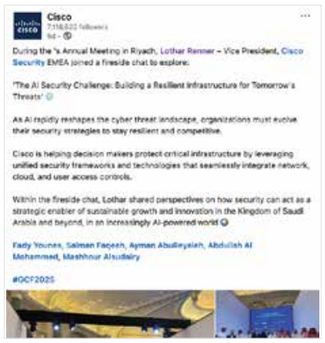
GCF partnered with 24KZm to deliver editorial, broadcast, online and social coverage led by a dedicated presenter on-ground at the Annual Meeting. The 24-hour news channel broadcasts worldwide from Astana, Kazakhstan, in both Kazakh and Russian, providing news updates, commentary and analysis.

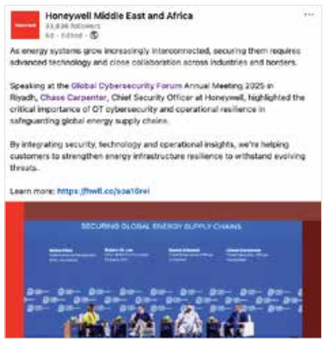
GCF COMMUNITY ENGAGEMENT

The GCF community of experts and decision makers from government, the private sector, international organizations, and academia played an active role in shaping the wider conversation beyond the Annual Meeting stage, generating content that highlighted key moments and brought diverse perspectives into focus across digital platforms.

COMMUNITY-GENERATED CONTENT







GCF PODCAST

The GCF Rethinking Cyber podcast begins its fourth season with a lineup of speakers from the GCF Annual Meeting 2025, offering a compelling look at Cyberspace's impact on our societies, economies, and nations.

Launched in 2022, Rethinking Cyber has brought together experts, policymakers, and innovators across three successful seasons, facilitating thoughtful, accessible conversations on the opportunities and challenges shaping Cyberspace.

The new season promises exclusive insights from global decision-makers as they explore the issues shaping a fast-evolving cyber landscape.

Catch all our episodes on **Spotify & Apple Podcasts**

Listen on Spotify

Listen on

GUESTS FOR SEASON 4

H.E. Kolinda Grabar-Kitarović
President of Croatia (2015 – 2020) on Building a Cyber-Resilient Future

H.E. José Manuel Barroso
President of the European Commission (2004 – 2014) on Navigating Geopolitics with Cyber Diplomacy

Jürgen Stock
Secretary General of INTERPOL (2014 - 2024) on Reimagining Law Enforcement in Cyberspace

Sheema Sen-Gupta
Director of Child Protection & Migration, UNICEF on Protecting Children in Cyberspace

Robert Harrigan
Former Director, GCHQ on the Next Big Leap in Cyber Defense

QUOTES FROM OUR COMMUNITY

"GCF 2025 once again demonstrated the power of global leadership to reframe what is perceived as possible and actionable in defending the digital infrastructure that underpins the health, safety and economic vitality of every nation on earth. I learned much and was greatly inspired by the assembled thought leaders, subject matter experts and international leaders from both the public and private sectors. GCF is a must attend for my 2026 planning."

HON. CHRIS INGLIS
US National Cyber Director (2021-2023)

"Cybersecurity is a global issue, as cybercrime knows no borders. I commend Saudi Arabia for having taken the initiative to establish the Global Cybersecurity Forum. This is a major challenge that can only be addressed through close cooperation between states and the major technology companies."

H.E. MACKY SALL
President of Senegal (2012-2024)

"The Global Cybersecurity Forum convened an amazing range of experts, practitioners and interested parties from all over the world. This unique blend of global experience and deep dives into practical issues made GCF the most memorable and useful cybersecurity event I have attended."

ROBERT HANNIGAN
Director, GCHQ, United Kingdom (2014-2017)

"Taking part in GCF provides a unique international opportunity to share and promote expertise and proposals together to improve global cybersecurity as a crucial pillar of digital transformation."

GENERAL (RTD) JEAN-PAUL PALOMÉROS
Supreme Allied Commander Transformation, NATO (2012-2015)

AN EVENING OF CULTURAL HERITAGE

October 1st, 2025 Al Murabba Historic Palace

Delegates and speakers concluded the first day of the Annual Meeting with a gathering at the iconic Al Murabba Historic Palace.

The curated program included a captivating museum tour and an artistic heritage performance inspired by Saudi Arabia's traditions and culture. Attendees were able to reflect on the day's sessions and build lasting connections with peers across the GCF community.

04

CONCLUSION

CONCLUSION

This book summarizes the key outcomes of the GCF Annual Meeting 2025, capturing insights and next steps emerging from the dialogue and collaboration that took place over the two-day event.

Global leaders, decision-makers and high-level experts from government, the private sector, academia, and international organizations came together at the Annual Meeting in Riyadh to strengthen international collaboration on shared global priorities in Cyberspace.

Under the theme "Scaling Cohesive Advancement in Cyberspace," this year's Annual Meeting marked a deepened phase of collaboration for the GCF community, recognizing that a resilient Cyberspace requires elevating the scope, capacity and impact of collective efforts to strengthen cybersecurity globally. A diversity of perspectives highlighted new pathways to mobilize stronger multistakeholder collaboration that responds to evolving cyber threats – as well as to overcome geopolitical competition and unlock growth opportunities for the global economy.

Discussions demonstrated the need for evidence-based policymaking, inclusive capacity building, and multistakeholder cooperation to unlock the full economic value of cybersecurity and build a safe and empowering Cyberspace. Indeed, at the outset of the event, the Global Initiative for Capacity Building in Cyberspace – a collaboration between the Kingdom of Saudi Arabia and the UN – was announced with the aim of accelerating cybersecurity capacity development at scale in areas of greatest need.

In addition to insightful dialogue across sub-themes spanning geopolitical, socioeconomic, technical, and human dimensions of Cyberspace, the focus of the event, in its fifth edition, was on scaling progress being made in key areas of cohesive advancement. This included furthering the goals of the two global initiatives, Child Protection in Cyberspace (CPC) and Women Empowerment in Cybersecurity (WEC), instated by His Royal Highness Prince Mohammed bin Salman bin Abdulaziz Al-Saud, Crown Prince and Prime Minister of Saudi Arabia. With the support of key partners, meaningful progress is being made toward creating a safer Cyberspace for children and providing women with access to training and mentorship to expand their representation and leadership in the cybersecurity workforce, addressing the 2.8m shortage of cybersecurity professional worldwide.

Advancements were also made across GCF's year-round portfolio of activities, with GCF's Knowledge Communities meeting to further their ongoing work in critical sectors and the launch of the Securing the Future Skies Knowledge Community led by Riyadh Air. The event also brought to the fore the targeted efforts of GCF's specialized centers, the Operational Technology Cybersecurity Center of Excellence (OTC CoE) and the Centre for Cyber Economics (CCE) – a collaboration between GCF and the World Economic Forum – which convened its members to advance understanding of cybersecurity's economic impact and value.

Through these ongoing efforts with local and international partners, GCF is working to achieve meaningful progress toward its strategic goals:

- Catalyzing social impact
- Enabling economic prosperity and security
- Pushing the boundaries of knowledge
- Advancing collaboration and collective action

GCF also extends sincere thanks and appreciation to its founding and strategic partners, whose steadfast support and shared vision make its work possible, and to its esteemed event partners whose engagement enriched the Annual Meeting.

GCF looks forward to strengthening these collaborations and championing actions that proactively address the fast-evolving risks and opportunities on the horizon – ensuring an inclusive, resilient, and secure Cyberspace for all.


GLOBAL
CYBERSECURITY
FORUM